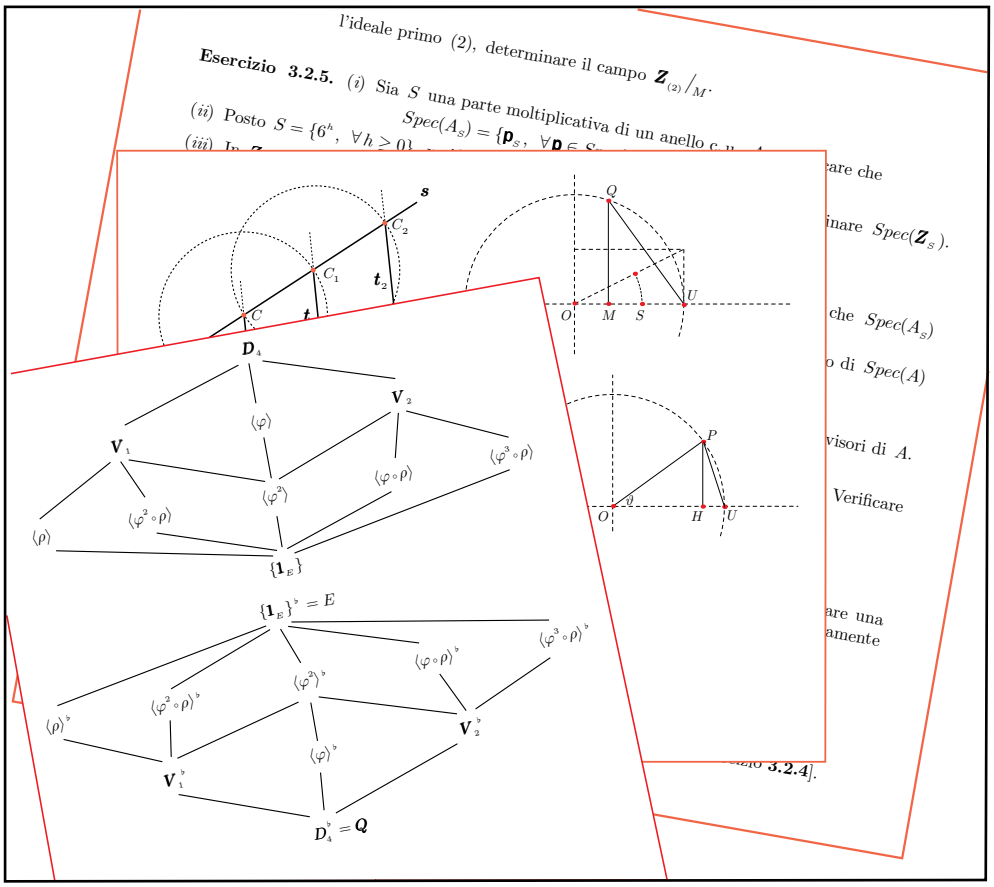
Università degli Studi di Roma "La Sapienza"
Dipartimento di Matematica "G.Castelnuovo"
A.A. 2006-2007

GIULIO CAMPANELLA

APPUNTI DI ALGEBRA 2

con oltre 150 esercizi svolti



Prefazione

Questi appunti contengono le lezioni del Modulo di Algebra 2, da me tenuto presso il Dipartimento "G.Castelnuovo" dell'Università "La Sapienza" di Roma negli A.A. 2005-06 e 2006-07.

Il corso di Algebra 2 propone agli studenti della laurea Triennale in Matematica quegli argomenti di algebra elementare che usualmente non trovano spazio nel corso di Algebra 1, ma che sono necessari per fornire un'adeguata conoscenza di base della materia. Ma non si tratta soltanto di un corso che "colma delle lacune". Nelle mie intenzioni - e speranze - questo corso dovrebbe chiarire allo studente i legami tra l'algebra classica, rivolta alla determinazione algebrica delle radici di un'equazione polinomiale, e l'algebra astratta, o moderna, rivolta allo studio delle strutture algebriche. Questi collegamenti sono spiegati dalla Teoria di Galois e l'intero corso è dunque finalizzato ad introdurre i primi elementi di tale teoria (cfr. Cap. **5***).*

Nel primo capitolo vengono studiati gruppi ed anelli quozienti ed illustrato il teorema fondamentale di omomorfismo e le relative conseguenze (teoremi di isomorfismo). Il secondo e terzo capitolo propongono lo studio di alcuni argomenti di teoria dei gruppi (soprattutto i teoremi di Sylow) e di teoria degli anelli (ideali massimali e primi, domini a fattorizzazione unica, a ideali principali, euclidei). Il quarto capitolo è dedicato allo studio delle estensioni di campi e relative applicazioni (costruzioni con riga e compasso). Il quinto ed ultimo capitolo, come già detto, si occupa di introdurre i primi elementi della teoria di Galois: campi di spezzamento, estensioni normali e separabili, risolubilità di gruppi, gruppo di Galois di un'estensione e corrispondenza di Galois tra sottogruppi del gruppo di Galois e campi intermedi dell'estensione.

Per tutte le definizioni, i risultati e le notazioni impiegate senza adeguati riferimenti, rinvio ai miei appunti del corso di Algebra 1 (cfr. [AA] e [AA2]).

Giugno 2007

Giulio Campanella

Indice

Capitolo 1

Quozienti di gruppi e di anelli. Teoremi di isomorfismo

Capitolo 2

Elementi di teoria dei gruppi

Capitolo 3

Elementi di teoria degli anelli

Capitolo 4

Elementi di teoria dei campi

Capitolo 5

Un'introduzione alla teoria di Galois

Appendici del Cap. 5

Capitolo 1

QUOZIENTI DI GRUPPI E DI ANELLI
TEOREMI DI ISOMORFISMO

1. Sottogruppi normali e gruppi quoziente

Assegnato un gruppo $(G,\cdot)$ ed un suo sottogruppo H, per ogni $a\in G$ gli insiemi

$$Ha=\{ha,\ \forall\, h\in H\}\quad\text{e}\quad aH=\{ah,\ \forall\, h\in H\}$$

sono detti rispettivamente *classe laterale destra* e *classe laterale sinistra di a modulo H*. Risulta:

$$Ha=Hb\iff ab^{-1}\in H;\quad aH=bH\iff a^{-1}b\in H.$$

È noto dal corso di **Alg. 1** (cfr. [AA]) che le classi laterali destre a due a due distinte formano una partizione di G, che denoteremo $\mathcal{L}_d(H)$. Analogamente, le classi laterali sinistre formano la partizione $\mathcal{L}_s(H)$. La relazione di equivalenza su G associata a $\mathcal{L}_d(H)$ è così definita:

$$a\rho_d b\overset{def.}{\iff} Ha=Hb\iff ab^{-1}\in H,\ \ \forall\, a,b\in G.$$

Analogamente, la relazione di equivalenza su G associata a $\mathcal{L}_s(H)$ è:

$$a\rho_s b\overset{def.}{\iff} aH=bH\iff a^{-1}b\in H,\ \ \forall\, a,b\in G.$$

Se G è abeliano, le due relazioni coincidono. Ma, in generale, $\rho_d\neq\rho_s$. Ad esempio, considerato il gruppo $\boldsymbol{S}_3$ delle permutazioni su tre elementi e scelto in esso il sottogruppo $H=\langle\,(1\,2)\,\rangle$, risulta: $(123)\,\rho_d\,(13)$, mentre $(123)\,\not\rho_s\,(13)$. Ci chiediamo quando le due relazioni coincidano.

Lemma 1.1. *Sia H un sottogruppo di G. Risulta:*

$$\rho_d=\rho_s\iff Ha=aH,\ \ \forall\, a\in G.$$

Dim. ($\Longleftarrow$) è evidente. Infatti $a\rho_s b\iff aH=bH\iff Ha=Hb\iff a\rho_d b$.

($\Longrightarrow$). Si verifica subito, in base alle precedenti definizioni, che $\forall\, h\in H,\ \forall\, a\in G$:

$$ah\,\rho_s\,a\quad\text{e}\quad a\,\rho_d\,ha.$$

Pertanto:

$ah\,\rho_s\,a\implies ah\,\rho_d\,a\implies (ah)a^{-1}\in H\implies aha^{-1}=h_1,\ \exists\, h_1\in H\implies ah=h_1a\in Ha;$

$a\,\rho_d\,ha\implies a\,\rho_s\,ha\implies a^{-1}(ha)\in H\implies a^{-1}ha=h_2,\ \exists\, h_2\in H\implies ha=ah_2\in aH.$

Dalle due catene di implicazioni segue che $aH\subseteq Ha$ e $Ha\subseteq aH$.

Definizione 1.1. *H è detto sottogruppo normale di G se $Ha=aH,\ \forall\, a\in G$ (ovvero $\rho_d=\rho_s$). Per indicare che H è un sottogruppo normale di G si scriverà $H\trianglelefteq G$.*

È naturale chiedersi se l'insieme quoziente $G\big/_{\rho_d}$ (identificabile con $\mathcal{L}_d(H)$) sia dotato di struttura algebrica rispetto alla seguente "operazione":

$(*)\qquad Ha\cdot Hb=Hab,\ \ \forall\, Ha,\,Hb\in G\big/_{\rho_d}.$

Non è però detto che $(*)$ sia un'operazione ben definita, cioè indipendente dalla scelta dei rappresentanti delle classi laterali. Vale infatti il seguente risultato.

Proposizione 1.1. *$(*)$ è ben definita $\iff H\trianglelefteq G$.*

Dim. ($\Longleftarrow$). Sia $H\trianglelefteq G$. Bisogna verificare che

$$\begin{cases} Ha=Ha_1\\ Hb=Hb_1\end{cases}\implies Hab=Ha_1b_1,\ \text{cioè}\ \ ab(a_1b_1)^{-1}\in H.$$

Per ipotesi, $aa_1^{-1}, bb_1^{-1} \in H$. Poniamo $h_1 = aa_1^{-1}$, $h_2 = bb_1^{-1}$. Si ha: $ab(a_1b_1)^{-1} = ab\,b_1^{-1}a_1^{-1} = ah_2\,a_1^{-1}$. Ora $ah_2 \in aH = Ha$ (essendo $H \trianglelefteq G$) e dunque $ah_2 = h_3\,a$, $\exists\, h_3 \in H$. Pertanto $ab(a_1b_1)^{-1} = ah_2\,a_1^{-1} = h_3\,a\,a_1^{-1} = h_3h_1 \in H$.

($\Longrightarrow$). È sufficiente verificare che $aH \subseteq Ha$, $\forall\, a \in G$ [cfr. Esercizio **1.1.1**]. Quindi bisogna verificare che $ah \in Ha$, $\forall\, h \in H$. Assumiamo che ($*$) sia ben definita. Essendo $Hh = H1$, allora

$$Hah = Ha \cdot Hh = Ha \cdot H1 = Ha1 = Ha$$

e dunque $aha^{-1} \in H$, cioè $ah \in Ha$.

Proposizione 1.2. *Se $H \trianglelefteq G$, $G/_{\rho_d}$ è un gruppo, rispetto all'operazione ($*$) sopra definita. Tale gruppo viene usualmente denotato $G/_H$ ed è chiamato gruppo quoziente di G modulo H. Se G è abeliano, ogni sottogruppo H è normale in G ed il gruppo quoziente $G/_H$ è abeliano.*

Dim. È un semplice esercizio.

Osservazione 1.1. (*i*) Se $H \trianglelefteq G$, allora $\rho_s = \rho_d$ e quindi $G/_{\rho_s} = G/_H$. Gli elementi del gruppo quoziente possono venire indicati anche come laterali sinistri.

(*ii*) Sia $(G, +)$ un gruppo (espresso con notazione additiva). Se H è un sottogruppo di G e $a \in G$, il laterale destro e sinistro di a modulo H si denotano rispettivamente nella forma $H + a$ e $a + H$. Le due relazioni d'equivalenza ρ_d, ρ_s si scrivono nella forma

$$a\rho_d b \iff a - b \in H, \quad a\rho_s b \iff -a + b \in H, \quad \forall\, a, b \in G.$$

Se $(G, +)$ è abeliano, ogni suo sottogruppo H è ovviamente normale e quindi definisce il gruppo quoziente $G/_H$ (anch'esso abeliano), con la seguente operazione:

$$(H + a) + (H + b) = H + (a + b), \quad \forall\, H + a,\, H + b \in G/_H.$$

(*iii*) Se $H \trianglelefteq G$, l'applicazione

$$\pi : G \to G/_H \text{ tale che } \pi(a) = Ha, \quad \forall\, a \in G,$$

è un omomorfismo suriettivo di gruppi, detto *proiezione canonica di G su $G/_H$*.

(*iv*) Sia $H \leq G$. Si verifica immediatamente che esiste sempre una biiezione tra $\mathcal{L}_d(H)$ e $\mathcal{L}_s(H)$ [data da $Ha \to a^{-1}H$, $\forall\, a \in G$]. Dunque $|G/_{\rho_d}| = |G/_{\rho_s}|$. Tale cardinalità è detta *indice di H in G* e si denota $(G : H)$.

È ben noto che $|G| = |H| \cdot (G : H)$ [infatti, essendo $|Ha| = |H|$, $\forall\, a \in G$, risulta:

$$|G| = \sum_{Ha \in \mathcal{L}_d(H)} |Ha| = \sum_{Ha \in \mathcal{L}_d(H)} |H| = |H| \cdot (G : H)\,].$$

Ne segue che, se G è un gruppo finito e $H \leq G$, si ha: $|H| \,\big|\, |G|$ (*Teorema di Lagrange*). Se poi $H \lhd G$, allora $\left|G/_H\right| = |G|/_{|H|}$ [essendo $\left|G/_H\right| = (G : H)$].

(*v*) Assumiamo che $(G : H) = 2$ [cioè che un sottogruppo H di G determini in G due soli laterali destri (o sinistri)]. Si verifica subito che $H \lhd G$ e quindi che $G/_H \cong \boldsymbol{C}_2$, gruppo ciclico di ordine 2 (cfr. [AA] Osserv. **3**, pag. 170).

Definizione 1.2. *Due sottogruppi H_1, H_2 di G sono detti coniugati (o in relazione di coniugio) se esiste $a \in G$ tale che $H_2 = aH_1\,a^{-1}$. Si scrive in tal caso $H_1 \sim H_2$.*

Nota. Si osservi che, se H è un sottogruppo di G, ogni sottoinsieme aHa^{-1} è un sottogruppo di G. Lo si può provare per verifica diretta oppure osservando che aHa^{-1} è l'immagine di H rispetto all'automorfismo interno γ_a di G (cfr. [AA], pag. 139).

La relazione di coniugio è una relazione di equivalenza nell'insieme dei sottogruppi di G [verificare]. Inoltre si osserva subito che

$H \trianglelefteq G \iff H = a\,H\,a^{-1},\ \forall\, a \in G \iff H$ ammette come sottogruppo coniugato solo se stesso. Poiché due sottogruppi coniugati hanno lo stesso ordine, se H è l'unico sottogruppo di un dato ordine in G, allora $H \trianglelefteq G$. Il viceversa è invece falso [ad esempio nel gruppo di Klein esistono tre sottogruppi (ovviamente normali) di ordine 2].

* * * * * * * * * * * * * * * * * * *

Esercizio 1.1.1. Verificare che le seguenti sette condizioni sono equivalenti:

(*i*) $H \trianglelefteq G$; (*ii*) $aH \subseteq Ha,\ \forall\, a \in G$; (*iii*) $Ha \subseteq aH,\ \forall\, a \in G$;

(*iv*) $aHa^{-1} = H,\ \forall\, a \in G$; (*v*) $aHa^{-1} \subseteq H,\ \forall\, a \in G$; (*vi*) $aHa^{-1} \supseteq H,\ \forall\, a \in G$.

(*vii*) $\forall\, x, y \in G,\ xy \in H \implies yx \in H$.

Esercizio 1.1.2. Sia $\mathbf{Q}$ il gruppo (delle unità) dei quarternioni (cfr. [AA] pag. 174). Verificare che il gruppo quoziente $\mathbf{Q}\big/_{\langle\, -\mathbf{1}\,\rangle}$ è isomorfo ad un gruppo di Klein.

Esercizio 1.1.3. Verificare che $\boldsymbol{S}_n\big/_{\boldsymbol{A}_n} \cong \boldsymbol{C}_2$, con $\boldsymbol{A}_n$ gruppo alterno di $\boldsymbol{S}_n$ e $\boldsymbol{C}_2$ gruppo ciclico di ordine 2.

Esercizio 1.1.4. Sia $n \geq 3$ e sia $H_i = \boldsymbol{S}(\{1, 2, .., \not{i}, .., n\})$ (con $1 \leq i \leq n$). Verificare che H_i è un sottogruppo non normale di $\boldsymbol{S}_n$. Verificare che gli H_i sono a due a due coniugati.

Esercizio 1.1.5. Verificare che, $\forall\, n \geq 2,\ \boldsymbol{SO}_n(\boldsymbol{R}) \trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$ [con

$\boldsymbol{SO}_n(\boldsymbol{R}) = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \,:\, A^{-1} = A^t \ \text{ e } \ det(A) = 1\}$ (*gruppo ortogonale speciale*).

Esercizio 1.1.6. Determinare una catena di gruppi $H < K < G$ tali che

$$H \triangleleft K, \quad K \triangleleft G, \quad \text{ma } H \not\triangleleft G.$$

2. Ideali ed anelli quoziente

Sia $(A,+,\cdot)$ un anello e sia B un suo sottoanello. Ricordiamo che un sottoinsieme non vuoto B di A è un sottoanello di A se sono verificate le due condizioni: $B-B\subseteq B$ e $B\cdot B\subseteq B$.

Poiché $(A,+)$ è un gruppo abeliano e $(B,+)$ ne è un sottogruppo (normale), $(A/_B,+)$ è un gruppo abeliano, rispetto alla seguente operazione di somma:

$$(a_1+B)+(a_2+B)=(a_1+a_2)+B,\ \ \forall\, a_1+B,\ a_2+B\in A/_B.$$

Vogliamo vedere se o in quali ipotesi $A/_B$ è dotato di struttura di anello, rispetto alla seguente "naturale" operazione di moltiplicazione:

$$(*)\qquad (a_1+B)\cdot(a_2+B)=a_1a_2+B,\ \ \forall\, a_1+B,\ a_2+B\in A/_B.$$

Si noti che in generale $(*)$ non è ben definita. Ad esempio, posto $A=\boldsymbol{Q}$, $B=\boldsymbol{Z}$, risulta:

$$\tfrac{4}{3}+\boldsymbol{Z}=\tfrac{1}{3}+\boldsymbol{Z},\ \tfrac{1}{2}+\boldsymbol{Z}=-\tfrac{1}{2}+\boldsymbol{Z},\ \text{ ma }\ (\tfrac{4}{3}+\boldsymbol{Z})(\tfrac{1}{2}+\boldsymbol{Z})\neq(\tfrac{1}{3}+\boldsymbol{Z})(-\tfrac{1}{2}+\boldsymbol{Z})$$

[in quanto $\frac{4}{3}\cdot\frac{1}{2}-\frac{1}{3}(-\frac{1}{2})\notin\boldsymbol{Z}$].

Proposizione 2.1. *$(*)$ è ben definita $\iff$ il sottoanello B verifica le due seguenti condizioni*

$$AB\subseteq B\ \ e\ \ BA\subseteq B.$$

Dim. $(\Longrightarrow)$. Sia $(*)$ ben definita. Scelti arbitrariamente $a\in A$ e $b\in B$, si tratta di verificare che $ab,\, ba\in B$ Infatti, essendo $b+B=0+B$, si ha:

$$ab+B=(a+B)(b+B)=(a+B)(0+B)=a0+B=0+B,$$

cioè $ab+B=0+B$ e quindi $ab\in B$. In modo analogo si verifica che anche $ba\in B$.

$(\Longleftarrow)$. Sia $a_1+B=a'_1+B$ e $a_2+B=a'_2+B$. Bisogna verifcare che $a_1a_2+B=a'_1a'_2+B$, cioè che $a_1a_2-a'_1a'_2\in B$. Per ipotesi, $a_1-a'_1\in B$, $a_2-a'_2\in B$. Allora

$$a_1a_2-a'_1a'_2=a_1a_2-a_1a'_2+a_1a'_2-a'_1a'_2=a_1(a_2-a'_2)+(a_1-a'_1)a'_2\in AB+BA\subseteq B+B\subseteq B.$$

Definizione 2.1. *Un sottoanello B di A verificante le due condizioni $BA\subseteq B$ e $AB\subseteq B$ è detto ideale (o ideale bilatero) di A. Ovviamente, se A è un anello commutativo, le due condizioni si riducono ad una sola.*

Denoteremo gli ideali con la lettera I (o con lettere successive J, ...) [ma sono anche in uso altre notazioni, come $\mathfrak{A}$, $\underline{a}$, ecc.] Riassumendo, un sottoinsieme non vuoto I di un anello A è un ideale di A se valgono le condizioni: $I-I\subseteq I$, $IA\subseteq I$, $AI\subseteq I$.

Osservazione 2.1. (i) A e $\{0\}$ sono ideali di A. Sono detti *ideali banali* di A.

(ii) Sia A un anello unitario (con unità $1=1_A$). Un ideale unitario I di A coincide con l'intero anello A. Infatti, essendo $1\in I$, risulta: $A=1A\subseteq IA\subseteq I\subseteq A$ e dunque $I=A$.

(iii) Sia A un anello commutativo. Per ogni $a\in A$, l'insieme

$$aA=\{ax,\ \forall\, x\in A\}$$

è un ideale di A [verificare], detto *ideale principale generato da a*. È denotato anche (a).

Proposizione 2.2. *Sia A un anello ed I un suo ideale. La terna $(A/_I,+,\cdot)$ è un anello, detto anello quoziente di A modulo I. Se A è commutativo e/o unitario, anche $A/_I$ lo è. Infine, gli anelli quozienti $A/_{\{0\}}$ e $A/_A$ coincidono rispettivamente con A e con $\mathbf{0}$ (anello nullo).*

Dim. È un semplice esercizio.

Osservazione 2.2. Si osserva subito che l'applicazione

$$\pi: A\to A/_I\ \text{ tale che }\ \pi(a)=a+I,\ \ \forall\, a\in A,$$

è un omomorfismo suriettivo di anelli, detto *proiezione canonica di* A *su* $A/_I$.

Si noti che la moltiplicazione di $A/_I$ sopra definita è l'unica possibile moltiplicazione di $A/_I$ che renda π un omomorfismo. Se infatti denotiamo con $*$ una qualsiasi moltiplicazione su $A/_I$, dalla condizione $\pi(a) * \pi(b) = \pi(ab)$ segue che $(a+I) * (b+I) = ab + I = (a+I)(b+I)$. Quindi $*$ coincide con la moltiplicazione di $A/_I$ sopra definita.

Osservazione 2.3. (*Ideali e quozienti di* $\boldsymbol{Z}$). Verifichiamo che ogni ideale I di $\boldsymbol{Z}$ è principale, cioè del tipo $n\boldsymbol{Z}$, per un opportuno $n \in \boldsymbol{N}$.

Se infatti $I = \{0\}$, allora $I = 0\boldsymbol{Z}$. Sia quindi $I \neq \{0\}$; in tal caso $I \cap \boldsymbol{N}^{\cdot} \neq \emptyset$ [se infatti $m \in I$ e $m < 0$, $-m \in I \cap \boldsymbol{N}^{\cdot}$]. In base al principio del minimo, $I \cap \boldsymbol{N}^{\cdot}$ ammette il minimo e sia $n > 0$ tale minimo. Ovviamente $n\boldsymbol{Z} \subseteq I$. Viceversa, $\forall\, x \in I$, se $x = nq + r$, $0 \leq r < n$, allora $r = x - nq \in I - I\boldsymbol{Z} \subseteq I$. Dunque $r \in I$. Se fosse $r > 0$, n non sarebbe più il minimo di $I \cap \boldsymbol{N}^{\cdot}$. Dunque $r = 0$ e pertanto $x = nq \in n\boldsymbol{Z}$. Abbiamo dimostrato che $I = n\boldsymbol{Z}$, cioè che I è principale. Osserviamo infine che $-n\boldsymbol{Z} = n\boldsymbol{Z}$, $\forall\, n \in \boldsymbol{N}$.

Si noti che, $\forall\, n \geq 2$, $\boldsymbol{Z}/_{n\boldsymbol{Z}}$ coincide con l'anello delle classi resto $\boldsymbol{Z}_n = \boldsymbol{Z}/_{\equiv_n}$ [cfr. [AA] pag. 75]. Infatti è ben noto che, $\forall\, a \in \boldsymbol{Z}$, la classe di congruenza di a modulo n è $[a] = a + n\boldsymbol{Z}$. Inoltre $\boldsymbol{Z}/_{0\boldsymbol{Z}} \cong \boldsymbol{Z}$ e $\boldsymbol{Z}/_{1\boldsymbol{Z}} \cong \boldsymbol{0}$ (anello nullo).

Nota. Assegnato un anello A ed un suo ideale I, scriveremo talvolta, con abuso di linguaggio (ma motivati da quanto avviene in $\boldsymbol{Z}$), $x \equiv y\ (mod\ I)$ in luogo di $x - y \in I$ [ovvero di $x + I = y + I$ (in $A/_I$)].

Osservazione 2.4. Si verifica facilmente che l'intersezione di ideali di un anello A è un ideale [e lo stesso è vero, come noto, per i sottogruppi di un gruppo].

Sia A un anello commutativo unitario e sia S un sottoinsieme non vuoto di A. Denotiamo con (S) (o $\langle S \rangle$) l'insieme di tutte le combinazioni lineari (finite) di elementi di S, a coefficienti in A, cioè

$$(S) = \Big\{ \sum_{i=1}^{n} a_i s_i,\ \ \forall\, n \geq 1,\ \ \forall\, a_i \in A,\ \ \forall\, s_i \in S \Big\}.$$

Si verifica facilmente che (S) è un ideale di A contenente S, detto *ideale generato da* S [si noti che, $\forall\, s \in S$, $s = 1 \cdot s \in (S)$]. Verifichiamo ora che (S) è l'intersezione di tutti gli ideali contenenti S (cioè è il più piccolo ideale contenente S):

$$(S) = \bigcap \{ I \mid I \text{ ideale di } A,\ I \supseteq S \}.$$

($\supseteq$). Essendo (S) un ideale e $(S) \supseteq S$, allora $(S) \supseteq \bigcap \{ I \mid ... \}$.

($\subseteq$). Per ogni $\sum a_i s_i \in (S)$ e per ogni ideale $I \supseteq S$, risulta $\sum a_i s_i \in I$. Dunque $(S) \subseteq I$ e pertanto $(S) \subseteq \bigcap \{ I \mid ... \}$.

Osservazione 2.5. Un altro modo per ottenere ideali di un anello è dato dal seguente risultato.

Sia $f : A \to B$ *un omomorfismo di anelli e sia* J *un ideale di* B. *Allora* $f^{-1}(J)$ *è un ideale di* A. *Se poi* f *è suriettivo e* I *è un ideale di* A, *allora* $f(I)$ *è un ideale di* B.

Dimostriamo la prima affermazione. Se $a_1, a_2 \in f^{-1}(J)$, allora $f(a_1), f(a_2) \in J$ e dunque $f(a_1 - a_2) = f(a_1) - f(a_2) \in J$. Quindi $a_1 - a_2 \in f^{-1}(J)$. Abbiamo provato che $f^{-1}(J) - f^{-1}(J) \subseteq f^{-1}(J)$.

Sia ora $a \in f^{-1}(J)$ e $x \in A$. Allora $f(a) \in J$ e $f(x) \in B$. Quindi $f(ax) = f(a)f(x) \in JB \subseteq J$ e pertanto $ax \in f^{-1}(J)$. In modo analogo si verifica che $xa \in f^{-1}(J)$. Abbiamo così provato che $A\, f^{-1}(J) \subseteq f^{-1}(J)$ e $f^{-1}(J)\, A \subseteq f^{-1}(J)$.

Asumiamo ora $f : A \to B$ suriettivo ed I ideale di A. Se $f(x), f(y) \in f(I)$ (con $x, y \in I$), allora $f(x) - f(y) = f(x - y) \in f(I)$. Se poi $b = f(a) \in B$, allora $f(x)b = f(xa) \in f(I)$ e, analogamente, $bf(x) = f(ax) \in f(I)$.

* * * * * * * * * * * * * * * * * * *

Esercizio 1.2.1. Verificare che, per ogni campo K, l'anello $K[X]$ possiede soltanto ideali principali

e risulta $K[X]/_{(P)} = K[X]/_{\equiv_P}$, $\forall\, P \in K[X]$.

Esercizio 1.2.2. Verificare che un campo possiede soltanto i due ideali banali. Viceversa, verificare che ogni anello commutativo unitario che ha solo gli ideali banali è un campo.

Esercizio 1.2.3. Siano I, J ideali di un anello A. Verificare che l'insieme

$$I + J = \{x + y,\ \forall\, x \in I,\ \forall\, y \in J\}$$

è un ideale di A, detto *ideale somma di I e J*. Verificare che si tratta del più piccolo ideale contenente $I \cup J$, cioè $(I \cup J)$ [se A è commutativo e unitario].

Esercizio 1.2.4. Siano I, J ideali di un anello A.

(*i*) Verificare che l'insieme

$$IJ = \Big\{ \sum_{i=1}^{n} x_i\, y_i,\ \forall\, n \geq 1,\ \forall\, x_i \in I,\ \forall\, y_i \in J \Big\}$$

è un ideale di A, detto *ideale prodotto di I e J*.

(*ii*) Verificare che $IJ \subseteq I \cap J$.

(*iii*) Sia A commutativo unitario e sia $I + J = A$. Verificare che in tal caso risulta: $IJ = I \cap J$.

(*iv*) Determinare due ideali I, $J \subseteq \boldsymbol{Z}$ tali che $IJ \subset I \cap J$.

Esercizio 1.2.5. Sia I il sottoinsieme di $\boldsymbol{Z}[X]$ formato dai polinomi a termine noto pari. Verificare che I è un ideale non principale di $\boldsymbol{Z}[X]$.

Esercizio 1.2.6. Sia $\mathcal{F}$ l'insieme delle funzioni continue da $\boldsymbol{R}$ a $\boldsymbol{R}$.

(*i*) Verificare che $(\mathcal{F}, +, \cdot)$ è un anello commutativo unitario rispetto alle due seguenti operazioni:

$$(f + g)(x) = f(x) + g(x),\quad (fg)(x) = f(x) \cdot g(x),\ \forall\, f, g \in \mathcal{F},\ \forall\, x \in \boldsymbol{R}.$$

(*ii*) Si ponga: $\mathcal{I}_0 = \{f \in \mathcal{F} \mid f(0) = 0\}$, $\mathcal{I}_1 = \{f \in \mathcal{F} \mid f(1) = 0\}$, $\mathcal{I} = \mathcal{I}_0 \cap \mathcal{I}_1$. Verificare che $\mathcal{I}$ è un ideale di $\mathcal{F}$ e che l'anello $\mathcal{F}/_{\mathcal{I}}$ è non integro (cfr. [AA], Def. **8**, pag. 22).

3. Teorema fondamentale di omomorfismo

Cominciamo dal ben noto *teorema fondamentale di omomorfismo* (abbreviato nel seguito *TFO*) per i gruppi.

Sia $f : G \to G'$ un omomorfismo di gruppi, entrambi espressi, per comodità, in notazione moltiplicativa. Dal corso di **Alg. 1** è noto che l'insieme

$$Ker f = \{x \in G \mid f(x) = 1'\} = f^{-1}(1')$$

è un sottogruppo di G, detto *nucleo* (o *kernel*) *di* f.

Si verifica con facilità che $Ker f \trianglelefteq G$ [si verifichi che $x\,(Ker f)\,x^{-1} \subseteq Ker\, f,\ \forall\, x \in G$]. Dunque $G/_{Ker\, f}$ è un gruppo [il *gruppo quoziente di* G *mod* $Ker f$] e l'applicazione

$$\pi : G \to G/_{Ker\, f} \text{ tale che } \pi(x) = x\, Ker f,\ \ \forall\, x \in G,$$

è un omomorfismo suriettivo di gruppi [la *proiezione canonica di* G *su* $G/_{Ker\, f}$].

È altresì noto che $Im f$ è un sottogruppo di G'. Infine è evidente che l'applicazione canonica d'inclusione $i : Im f \hookrightarrow G'$ è un omomorfismo iniettivo di gruppi. Vale il seguente teorema.

Teorema 3.1. *[TFO (per i gruppi)]. Sia* $f : G \to G'$ *un omomorfismo di gruppi.* f *induce un unico isomorfismo (di gruppi):*

$$F : G/_{Ker\, f} \to Im f,\ \text{ tale che } \ f = i \circ F \circ \pi.$$

Ne segue subito che $F(x\, Ker f) = f(x),\ \forall\, x \in G$

Nota. Si osservi che F che rende commutativo il seguente diagramma:

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/_{Ker\, f} & \xrightarrow{\ F\ } & Im f \end{array}$$

Dim. Sia ρ_s la relazione sinistra (o destra) associata a $Ker f$. Si ha:

$$a \rho_s b \iff a^{-1}b \in Ker f \iff f(a^{-1}b) = 1' \iff f(a) = f(b) \iff a \rho_f b,$$

dove ρ_f è la relazione associata all'applicazione f (cfr. [AA], Def. **5**, pag. 13). Dunque $\rho_s = \rho_f$ e perciò $[a]_{\rho_f} = a Ker f,\ \forall\, a \in G$.

Dal teorema di decomposizione delle applicazioni (cfr [AA], Prop. **3**, pag. 14), esiste un'unica biiezione $F : G/_{\rho_f} \to Im f$ tale che $f = i \circ F \circ \pi$. Resta quindi solo da verificare che F è un omomorfismo. Infatti, $\forall\, a\, Ker f,\ b\, Ker f \in G/_{Ker\, f}$:

$$F(a\, Ker f \cdot b\, Ker f) = F(ab\, Ker f) = f(ab) = f(a)f(b) = F(a\, Ker f)F(b\, Ker f).$$

Passiamo ora al *TFO* per gli anelli. Sia $f : A \to A'$ un omomorfismo di anelli. Si verifica subito che $Im f$ è un sottoanello di A'. Inoltre l'inclusione canonica $i : Im f \hookrightarrow A'$ è un omomorfismo iniettivo di anelli. Vale il seguente lemma.

Lemma 3.1. *L'insieme* $Ker f = \{a \in A \mid f(a) = 0'\}$ *è un ideale di* A*, detto nucleo di* f.

Dim. Poiché $Ker f = f^{-1}(0')$, basta usare l'Osserv. **2.5**, ovvero eseguire le seguenti semplici verifiche:

$$\forall\, a, b \in Ker f,\ a - b \in Ker f; \qquad \forall\, a \in Ker f,\ \forall\, x \in A,\ ax, xa \in Ker f.$$

Da questo lemma e dalla Prop. **2.2** segue che $A/_{Ker f}$ è un anello. Da Osserv. **2.2** $\pi : A \to A/_{Ker f}$

è un omomorfismo suriettivo di anelli (la *proiezione canonica*).

Teorema 3.2. *[TFO (per gli anelli)]. Sia* $f : A \to A'$ *un omomorfismo di anelli.* f *induce un unico isomorfismo (di anelli):*

$$F : A/_{Ker\, f} \to Im f, \text{ tale che } f = i \circ F \circ \pi.$$

Ne segue subito che $F(a + Ker f) = f(a), \ \forall\, a \in A.$

Dim. $f : (A, +) \to (A', +)$ è un omomorfismo di gruppi additivi, il cui nucleo coincide con l'ideale $Ker\, f$. Dal *TFO* per i gruppi, applicato all'omomorfismo f, esiste un unico isomorfismo di gruppi additivi $F : A/_{Ker\, f} \to Im f$, tale che $f = i \circ F \circ \pi$, ovvero

$$F(a + Ker f) = f(a), \ \forall\, a \in A$$

Per concludere resta solo da verificare che F è un omomorfismo anche rispetto al prodotto. Infatti, $\forall\, a + Ker f,\ b + Ker f \in A/_{Ker\, f}$:

$$F\big((a + Ker f)\cdot(b + Ker f)\big) = F(ab + Ker f) = f(ab) = f(a)f(b) = F(a + Ker f)\, F(b + Ker f).$$

Corollario 3.1. *Sia* A *un anello commutativo unitario. Risulta,* $\forall\, a \in A$*:*

$$A \cong A[X]/_{(X-a)}.$$

Dim. Fissato arbitrariamente $a \in A$, sia

$$\varphi = \varphi_a : A[X] \to A \text{ tale che } \varphi(P) = P(a), \ \forall\, P \in A[X].$$

Si verifica facilmente che φ è un omomorfismo di anelli [infatti $\varphi(P+Q) = \varphi(P) + \varphi(Q)$ e $\varphi(PQ) = \varphi(P)\varphi(Q), \ \forall\, P, Q \in A[X]$]. Inoltre φ è suriettivo [infatti $\varphi(x) = x, \ \forall\, x \in A$]. Resta da verificare che $Ker\varphi = (X - a)$ (e poi applicare il *TFO*).

Certamente $X - a \in Ker\varphi$. Viceversa, sia $P \in Ker\varphi$. Essendo $X - a$ monico, è possibile eseguire la divisione con resto di P per $X - a$ e si ottiene

$$P = (X - a)\, Q + r, \text{ con } Q \in A[X],\ r \in A.$$

Poiché $P(a) = 0$, allora $r = 0$ e dunque $P \in (X - a)$.

Corollario 3.2. *Sia* A *un anello commutativo unitario e siano* I, J *due ideali di* A *tali che* $I + J = A$ *(cfr. Esercizio* **1.2.3***). Indicato con* IJ *l'ideale prodotto di* I *per* J *(cfr. Esercizio* **1.2.4***), risulta:*

$$A/_{IJ} \cong A/_I \times A/_J.$$

Dim. Sia

$$\varphi : A \to A/_I \times A/_J \text{ tale che } \varphi(x) = (x + I,\, x + J), \ \forall\, x \in A.$$

φ è certamente un omomorfismo di anelli [verificare]. Si ha:

$$Ker\varphi = \{x \in A \mid x \in I \cap J\} = I \cap J.$$

Dall'Esercizio **1.2.4**(*iii*), $I \cap J = IJ$ (ideale prodotto). Per concludere la dimostrazione basta verificare che φ è suriettiva (e poi applicare il *TFO*).

Sia $(a + I,\, b + J) \in A/_I \times A/_J$. Bisogna determinare $x \in A$ tale che

$$\varphi(x) = (a + I,\, b + J), \text{ cioè } x + I = a + I \text{ e } x + J = b + J.$$

In altri termini, si tratta di dimostrare che il sistema

$$\begin{cases} X \equiv a \ (mod\ I) \\ X \equiv b \ (mod\ J) \end{cases}$$

ammette soluzione in A.

Per ipotesi, $1 = u + v$, con $u \in I$, $v \in J$. Si ponga $x = av + bu$. Allora:

$$x + I = av + bu + I = av + I = a(1 - u) + I = a + I,$$
$$x + J = av + bu + J = bu + J = b(1 - v) + J = b + J.$$

Dunque $x \equiv a \ (mod\ I)$ e $x \equiv b \ (mod\ J)$, cioè x è un elemento cercato.

Nota. Ponendo $A = \boldsymbol{Z}$, $I = n\boldsymbol{Z}$, $J = m\boldsymbol{Z}$, con n, m coprimi, si ha subito: $\boldsymbol{Z}_{nm} \cong \boldsymbol{Z}_n \times \boldsymbol{Z}_m$. Si tratta, come noto, del *Teorema Cinese del Resto* (cfr. [AA] Teor. **3** pag. 87), di cui il Coroll. **3.2.** è quindi una generalizzazione.

* * * * * * * * * * * * * * * * * * *

Esercizio 1.3.1. Verificare che $\boldsymbol{GL}_n(\boldsymbol{R})\big/_{\boldsymbol{SL}_n(\boldsymbol{R})} \cong (\boldsymbol{R}^{\cdot}, \cdot)$ [dove $\boldsymbol{SL}_n(\boldsymbol{R})$ è il gruppo delle matrici quadrate di ordine n, a valori in $\boldsymbol{R}$ e a determinante $= 1$].

Esercizio 1.3.2. Sia $\boldsymbol{\mathcal{H}} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) \in \boldsymbol{Q}^{\cdot}\}$.
(*i*) Verificare che $\boldsymbol{\mathcal{H}} \trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$.
(*ii*) Verificare che $\boldsymbol{GL}_n(\boldsymbol{R})\big/_{\boldsymbol{\mathcal{H}}} \cong \boldsymbol{R}^{\cdot}\big/_{\boldsymbol{Q}^{\cdot}}$.

Esercizio 1.3.3. In $\boldsymbol{GL}_n(\boldsymbol{R})$ si consideri il sottoinsieme $\boldsymbol{\mathcal{K}} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) > 0\}$.
(*i*) Verificare che $\boldsymbol{\mathcal{K}}$ è un sottogruppo normale di $\boldsymbol{GL}_n(\boldsymbol{R})$.
(*ii*) Determinare il gruppo $\boldsymbol{GL}_n(\boldsymbol{R})\big/_{\boldsymbol{\mathcal{K}}}$.

Esercizio 1.3.4. Dimostrare che $(\boldsymbol{R}, +)\big/_{(\boldsymbol{Z},+)}$ è isomorfo al sottogruppo moltiplicativo dei complessi di norma 1.

Esercizio 1.3.5. (*i*) Esprimere il gruppo $\boldsymbol{SO}_2(\boldsymbol{R})$ come quoziente di $(\boldsymbol{R}, +)$.
(*ii*) Sia $C_2 = \langle -I_2 \rangle$. Verificare che $C_2 \trianglelefteq \boldsymbol{SO}_2(\boldsymbol{R})$ ed esprimere $\boldsymbol{SO}_2(\boldsymbol{R})\big/_{C_2}$ come quoziente di $(\boldsymbol{R}, +)$.

Esercizio 1.3.6. Sia A un anello commutativo. Verificare che gli anelli $A[X, Y]\big/_{(Y)}$ e $A[X]$ sono isomorfi.

Esercizio 1.3.7. Verificare che $\boldsymbol{Z}[X, Y]\big/_{(XY)}$ è isomorfo ad un sottoanello B di $\boldsymbol{Z}[X] \times \boldsymbol{Z}[Y]$. Individuare B come immagine di un opportuno omomorfismo.

Esercizio 1.3.8. Fissato un intero non nullo b, si denoti con $(\boldsymbol{Z})_b$ il sottoinsieme di $\boldsymbol{Q}$ così definito:

$$(\boldsymbol{Z})_b := \left\{ \tfrac{a}{b^k},\ \forall\, a \in \boldsymbol{Z},\ \forall\, k \in \boldsymbol{N} \right\}.$$

(*i*) Verificare che $(\boldsymbol{Z})_b$ è un anello contenente $\boldsymbol{Z}$.
(*ii*) Dimostrare che $(\boldsymbol{Z})_b \cong \boldsymbol{Z}[X]\big/_{(bX-1)}$.

Esercizio 1.3.9. Siano A, B due anelli e sia $A \times B$ il loro prodotto diretto. Sia I un ideale di A. Verificare che $I \times B$ è un ideale di $A \times B$ e calcolare il quoziente $A \times B\big/_{I \times B}$.

Esercizio 1.3.10. Sia $f : A \to B$ un omomorfismo di anelli. Sia J un ideale di B e sia $I = f^{-1}(J)$.
(*i*) Verificare che I è nucleo di un omomorfismo.
(*ii*) Dimostrare che $A\big/_I$ è isomorfo ad un sottoanello di $B\big/_J$
(*iii*) Cosa avviene se f è suriettivo ?.

4. Teoremi di isomorfismo per i gruppi

Dal *TFO* per i gruppi (talora chiamato anche *primo teorema di isomorfismo*) discendono importanti corollari: il *secondo* ed il *terzo teorema di isomorfismo* ed il *teorema di corrispondenza*. Analoghi risultati discendono dal *TFO* per gli anelli e di essi ci occuperemo nel prossimo paragrafo.

Premettiamo alcuni richiami, necessari per illustrare il secondo teorema di isomorfismo.

Definizione 4.1. *Sia $(G,\cdot)$ un gruppo e siano H, K due suoi sottogruppi. Si chiama prodotto di H per K l'insieme*

$$HK = \{hk,\ \forall\, h \in H,\ \forall\, k \in K\}.$$

È ben noto il seguente fatto (cfr. [AA], Prop. **4**, pag. 143):

$$HK \text{ è un sottogruppo di } G \iff HK = KH$$

[dove l'uguaglianza $HK = KH$ va intesa "in senso globale", cioè come uguaglianza di insiemi, e non "elemento per elemento"].

È evidente quindi che, se G è abeliano, HK è sempre un sottogruppo di G. Se inoltre uno dei due sottogruppi è normale, la condizione $HK = KH$ è sempre verificata [discende subito applicando la definizione di normalità] e dunque HK è un sottogruppo di G. Si noti ancora che, se HK è un sottogruppo di G, allora $HK = \langle H \cup K\rangle$, cioè HK è il più piccolo sottogruppo contenente H e K. Infine, va rilevato che, in un gruppo additivo $(G,+)$ il "prodotto" di due sottogruppi H, K coincide con la loro somma e si denota $H + K$.

Teorema 4.1. *(Secondo teorema di isomorfismo). Sia H un sottogruppo normale di $(G,\cdot)$. Per ogni sottogruppo K di G, risulta:*

$$HK/_H \cong K/_{H\cap K}\ .$$

Dim. Per quanto sopra osservato, HK è un sottogruppo di G. Ovviamente $H \leq HK$ e dunque, essendo $H \trianglelefteq G$, anche $H \trianglelefteq HK$. È quindi definito il gruppo quoziente $HK/_H$. Si ponga:

$$\varphi : K \to HK/_H \text{ tale che } \varphi(c) = cH,\ \forall\, c \in K$$

[si noti che $c = 1\cdot c \in HK$]. Risulta:

- φ è un omomorfismo [verificare];
- φ è suriettiva [infatti, $\forall\, hkH \in HK/_H$, si ha: $hkH = k_1h_1H = k_1H = \varphi(k_1)$];
- $Ker\varphi = \{c \in K \mid cH = H\} = \{c \in K \mid c \in H\} = H \cap K$.

Dal *TFO*, applicato a φ, segue che $K/_{H\cap K} \cong HK/_H$.

Teorema 4.2. *(Terzo teorema di isomorfismo). Siano H, K due sottogruppi normali di $(G,\cdot)$, con $H \leq K$. Risulta:*

$$G/_K \cong G/_H\big/_{K/H}\ .$$

Dim. Poiché $H \trianglelefteq G$ e $H \leq K$, allora ovviamente $H \trianglelefteq K$. Dunque sono definiti i tre gruppi quoziente $G/_H$, $G/_K$ e $K/_H$. Si ponga:

$$\varphi : G/_H \to G/_K \text{ tale che } \varphi(aH) = aK,\ \forall\, aH \in G/_H\ .$$

Risulta:

- φ è ben definita [infatti: $aH = a_1H \implies a_1^{-1}a \in H \implies a_1^{-1}a \in K \implies aK = a_1K$];
- φ è suriettiva [infatti $aK = \varphi(aH)$];
- φ è un omomorfismo [infatti $\varphi(aH\cdot bH) = \varphi(abH) = abK = aK\cdot bK = \varphi(aH)\cdot\varphi(bH)$];
- $Ker\varphi = \{aH \mid aK = K\} = \{aH \mid a \in K\} = K/_H$.

Applicando a φ il *TFO* si conclude.

Sia $H \trianglelefteq G$. Il seguente risultato stabilisce una corrispondenza biunivoca tra i sottogruppi di $G/_H$ ed i sottogruppi di G contenenti H. Tale biiezione si estende ai sottogruppi normali.

Teorema 4.3. *(Teorema di corrispondenza). Sia H un sottogruppo normale di $(G,\cdot)$. Denotiamo con $\mathbf{\Sigma} = \mathbf{\Sigma}_H$ l'insieme dei sottogruppi di G contenenti H e con $\mathbf{\Sigma}' = \mathbf{\Sigma}(G/_H)$ l'insieme dei sottogruppi di $G/_H$. La proiezione canonica $\pi : G \to G/_H$ induce una biiezione tra $\mathbf{\Sigma}$ e $\mathbf{\Sigma}'$, così definita:*

$$T \to \pi(T) = T/_H, \quad \forall\, T \in \mathbf{\Sigma}.$$

Inoltre, $\forall\, T \in \mathbf{\Sigma}$, risulta:

$$T \trianglelefteq G \iff T/_H \trianglelefteq G/_H .$$

Dim. Poiché $H \trianglelefteq G$ e $H \leq T$, allora $H \trianglelefteq T$. Dunque $T/_H = \pi(T)$ è un gruppo ed ovviamente è un sottogruppo di $G/_H$, cioè $T/_H \in \mathbf{\Sigma}'$. Quindi resta definita l'applicazione

$$\tilde{\pi} : \mathbf{\Sigma} \to \mathbf{\Sigma}' \text{ tale che } \tilde{\pi}(T) = \pi(T) = T/_H, \quad \forall\, T \in \mathbf{\Sigma}.$$

Verifichiamo che $\tilde{\pi}$ è suriettiva. Sia $\mathcal{L} \in \mathbf{\Sigma}'$. Si osserva subito che $\pi^{-1}(\mathcal{L})$ è un sottogruppo di G [se infatti $x, y \in \pi^{-1}(\mathcal{L})$, allora $xH, yH \in \mathcal{L}$ e dunque $xy^{-1}H \in \mathcal{L}$, cioè $xy^{-1} \in \pi^{-1}(\mathcal{L})$]. Inoltre $H \leq \pi^{-1}(\mathcal{L})$ [infatti $\forall\, h \in H$, $\pi(h) = hH = H \in \mathcal{L}$, essendo H elemento neutro di $G/_H$. Quindi $h \in \pi^{-1}(\mathcal{L})$]. Dunque $\pi^{-1}(\mathcal{L}) \in \mathbf{\Sigma}$ e (essendo π suriettiva) $\pi\big(\pi^{-1}(\mathcal{L})\big) = \mathcal{L}$, cioè $\mathcal{L} \in Im\,\tilde{\pi}$.

Verifichiamo ora che $\tilde{\pi}$ è iniettiva. Siano $T_1, T_2 \in \mathbf{\Sigma}$ tali che $T_1/_H = T_2/_H$. Dobbiamo verificare che $T_1 = T_2$. Sia $x \in T_1$. Poiché $xH \in T_1/_H = T_2/_H$, allora $xH = yH$, $\exists\, y \in T_2$. Ne segue che $y^{-1}x \in H \leq T_2$. Dunque $x = y\,y^{-1}x \in T_2 \cdot T_2 \subseteq T_2$. Abbiamo così verificato che $T_1 \subseteq T_2$ ed in maniera analoga si verifica che $T_1 \supseteq T_2$.

Resta da verificare che $T \trianglelefteq G \iff T/_H \trianglelefteq G/_H$.

($\Longrightarrow$). Se $T \trianglelefteq G$, dal terzo teorema di isomorfismo segue che $G/_T \cong G/_H\big/_{T/_H}$ e dunque $T/_H \trianglelefteq G/_H$.

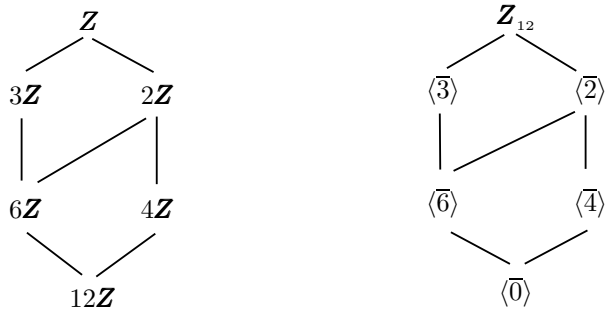
($\Longleftarrow$). Sia $T/_H \trianglelefteq G/_H$ e si consideri la composizione φ delle due seguenti proiezioni canoniche:

$$\varphi : G \to G/_H \to G/_H\big/_{T/_H} .$$

Dunque $\varphi(x) = (xH)\,T/_H$, $\forall\, x \in G$. Se dimostriamo che $Ker\varphi = T$, allora $T \trianglelefteq G$, come richiesto.

Ovviamente $T \subseteq Ker\varphi$ [infatti, $\forall\, t \in T$, $\varphi(t) = (tH)\,T/_H = T/_H$ (essendo $tH \subseteq T$)]. Viceversa, se $x \in Ker\varphi$, allora $xH = tH$, $\exists\, t \in T$. Quindi $t^{-1}x \in H$. Pertanto $x = t\,t^{-1}x \in TH \subseteq T \cdot T \subseteq T$, cioè $x \in T$. Dunque $Ker\varphi \subseteq T$.

Il teorema di corrispondenza ci permette ad esempio di confrontare i sottogruppi di $(\boldsymbol{Z}, +)$ contenenti $12\boldsymbol{Z}$ con i sottogruppi di $(\boldsymbol{Z}_{12}, +)$:



Ci chiediamo ora cosa avvenga per i sottogruppi $K \leq G$ non contenenti H, se ad essi applichiamo la proiezione canonica π di G su $G/_H$. Ovviamente $\pi(K)$ è un sottogruppo di $G/_H$, in quanto

immagine di un sottogruppo rispetto ad un omomorfismo. Proveremo che $\pi(K)$ coincide con $KH/_H$.

Proposizione 4.1. *Sia $H \trianglelefteq G$ e sia $\pi : G \to G/_H$ la proiezione canonica. Per ogni sottogruppo K di G risulta:*

$$\pi^{-1}(\pi(K)) = KH \quad \textit{(sottogruppo di } G\textit{)}.$$

Ne segue che $\pi(K) = KH/_H$.

Dim. Poiché $H \trianglelefteq G$, allora $KH = HK$ e dunque KH è un sottogruppo di G. Verifichiamo che $\pi^{-1}(\pi(K)) = KH$.

($\subseteq$). Sia $x \in \pi^{-1}(\pi(K))$, cioè $\pi(x) \in \pi(K)$. Allora $xH = tH, \exists\, t \in K$. Dunque $t^{-1}x \in H$ e pertanto $x = t(t^{-1}x) \in KH$.

($\supseteq$). Se $kh \in KH$, allora $khH = kH \in \pi(K)$ e quindi $kh \in \pi^{-1}(\pi(K))$.

Poiché KH è un sottogruppo di G e contiene H, allora $\pi(KH) = KH/_H$. Inoltre è noto (cfr. [AA], Prop. **1**, pag. 6) che $\pi\big(\pi^{-1}(\pi(K))\big) = \pi(K)$. Si conclude che $\pi(K) = \pi(KH) = KH/_H$.

Ad esempio, considerata ancora la proiezione $\pi : \boldsymbol{Z} \to \boldsymbol{Z}_{12}$, i sottogruppi $7\boldsymbol{Z}$, $8\boldsymbol{Z}$, $9\boldsymbol{Z}$ di $(\boldsymbol{Z}, +)$ si proiettano tramite π rispettivamente sui sottogruppi $\langle\overline{1}\rangle = \boldsymbol{Z}_{12}$, $\langle\overline{4}\rangle$, $\langle\overline{3}\rangle$. Infatti [osservato che in ogni struttura additiva il prodotto di due sottogruppi è la loro somma] si verifica subito che $7\boldsymbol{Z} + 12\boldsymbol{Z} = \boldsymbol{Z}$, $8\boldsymbol{Z} + 12\boldsymbol{Z} = 4\boldsymbol{Z}$ e $9\boldsymbol{Z} + 12\boldsymbol{Z} = 3\boldsymbol{Z}$.

* * * * * * * * * * * * * * * * * * *

Esercizio 1.4.1. Siano $n, m \in \boldsymbol{Z}$ e siano $d = MCD(n, m)$, $h = mcm(n, m)$. Applicando il secondo teorema di isomorfismo, dimostrare che $d\boldsymbol{Z}/_{n\boldsymbol{Z}} \cong m\boldsymbol{Z}/_{h\boldsymbol{Z}}$.

Esercizio 1.4.2. Siano $H_1 \trianglelefteq H_2 \leq G$ e $K \leq G$. Verificare che $H_1 \cap K \trianglelefteq H_2 \cap K$.

Esercizio 1.4.3. Utilizzando il terzo teorema di isomorfismo, determinare un isomorfismo tra il gruppo additivo $(\boldsymbol{Z}_{12}, +)$ ed un opportuno quoziente di $(\boldsymbol{Z}_{60}, +)$. Esplicitare un siffatto isomorfismo.

Esercizio 1.4.4. In $G = \boldsymbol{GL}_n(\boldsymbol{R})$ si considerino il sottogruppo normale $H = \boldsymbol{SL}_n(\boldsymbol{R})$ ed il sottogruppo $K = \boldsymbol{O}_n(\boldsymbol{R})$. Si calcoli HK e si verifichi se è normale in G.

Esercizio 1.4.5. Nel gruppo diedrale $\boldsymbol{D}_8 = \langle \varphi, \rho \mid \varphi^8 = \rho^2 = 1,\ \rho\circ\varphi = \varphi^7\circ\rho \rangle$ si consideri il sottogruppo $H = \langle\varphi^2\rangle$.

(*i*) Verificare che $H \lhd \boldsymbol{D}_8$.

(*ii*) Determinare i sottogruppi di $\boldsymbol{D}_8$ contenenti H.

(*iii*) Quanti sono i gruppi diedrali del quadrato contenuti in $\boldsymbol{D}_8$?

5. Teoremi di isomorfismo per gli anelli

Procediamo in stretta analogia con il paragrafo precedente, dimostrando per gli anelli due teoremi di isomorfismo ed il teorema di corrispondenza. Come per i gruppi, il *TFO* per gli anelli è talvolta detto *primo teorema di isomorfismo*.

Veniamo al secondo teorema di isomorfismo per gli anelli. Osserviamo che il prodotto HK di due sottogruppi di G, con H normale, corrisponde, passando da un gruppo G ad un anello A, alla somma $I+B$, con I ideale e B sottoanello di A. Il fatto che $H \trianglelefteq HK$ corrisponde, per gli anelli, al seguente risultato.

Lemma 5.1. *Sia I un ideale di un anello A e sia B un sottoanello di A. Risulta: $I+B$ è un anello e I ne è un ideale.*

Dim. Si tratta di verificare che

$$(a)\ \ (I+B)-(I+B)\subseteq I+B; \qquad (b)\ \ (I+B)\,(I+B)\subseteq I+B;$$
$$(c)\ \ I\,(I+B)\subseteq I; \qquad (d)\ \ (I+B)\,I\subseteq I.$$

Verifichiamo soltanto la condizione (b), lasciando le altre tre per esercizio. Presi comunque x_1+b_1, $x_2+b_2\in I+B$. Si ha:

$$(x_1+b_1)(x_2+b_2)=x_1x_2+x_1b_2+b_1x_2+b_1b_2.$$

I primi tre addendi sono in I [ad esempio, $x_1b_2\in IB\subseteq IA\subseteq I$], mentre il quarto addendo è in B. Dunque $(x_1+b_1)(x_2+b_2)\in I+B$.

Teorema 5.1. *(Secondo teorema di isomorfismo). Sia I un ideale di A. Per ogni sottoanello B di A, risulta:*

$$(I+B)\big/_I \cong B\big/_{I\cap B}\ .$$

Dim. Si consideri l'applicazione

$$\varphi: B\to (I+B)\big/_I \ \text{ tale che } \ \varphi(b)=b+I,\ \ \forall\, b\in B$$

[si noti che $b+I=(0+b)+I\in (I+B)\big/_I$]. Si verifica facilmente che φ è un omomorfismo di anelli, che è suriettivo e che

$$Ker\varphi=\{b\in B\mid b+I=I\}=I\cap B\ .$$

Dal *TFO* segue l'isomorfismo di anelli cercato.

Nota. Se I, J sono ideali di A, risulta ovviamente $(I+J)\big/_I \cong J\big/_{I\cap J}$.

Teorema 5.2. *(Terzo teorema di isomorfismo). Siano I, J due ideali di un anello A, con $I\subseteq J$. Risulta:*

$$A\big/_J \cong A\big/_I\big/_{J/I}\ .$$

Dim. Si definisce:

$$\varphi: A\big/_I\to A\big/_J \ \text{ tale che } \ \varphi(a+I)=a+J,\ \ \forall\, a+I\in A\big/_I\ .$$

φ è un ben definito omomorfismo suriettivo di gruppi additivi, con nucleo $Ker\varphi=J\big/_I$ [dal terzo teorema di isomorfismo per i gruppi]. Resta solo da verificare che φ è un omomorfismo anche rispetto al prodotto. Infatti, $\forall\, a+I,\ b+I\in A\big/_I$:

$$\varphi((a+I)(b+I))=\varphi(ab+I)=ab+J=(a+J)(b+J)=\varphi(a+I)\,\varphi(b+I)\,.$$

Teorema 5.3. *(Teorema di corrispondenza). Sia I un ideale di un anello A. Denotiamo con $\boldsymbol{\mathcal{I}}=\boldsymbol{\mathcal{I}}_I$ l'insieme degli ideali di A contenenti I e con $\boldsymbol{\mathcal{I}}'=\boldsymbol{\mathcal{I}}(A\big/_I)$ l'insieme degli ideali di $A\big/_I$. La proiezione canonica $\pi: A\to A\big/_I$ induce una biiezione tra $\boldsymbol{\mathcal{I}}$ e $\boldsymbol{\mathcal{I}}'$, così definita:*

$$J\to J\big/_I,\ \ \forall\, J\in\boldsymbol{\mathcal{I}}.$$

Nota. Si può facilmente dimostrare [con dimostrazione analoga, lasciata per esercizio] che sussiste un'analoga biiezione tra l'insieme $\mathbf{\Sigma} = \mathbf{\Sigma}_I$ dei sottoanelli di A contenenti I e l'insieme $\mathbf{\Sigma}' = \mathbf{\Sigma}(A/_I)$ dei sottoanelli di $A/_I$.

Dim. Si osservi che, $\forall\, J \in \boldsymbol{\mathcal{I}},\ \pi(J) = J/_I \in \boldsymbol{\mathcal{I}}'$ [infatti $J/_I - J/_I \subseteq J/_I,\ J/_I \cdot A/_I \subseteq J/_I$ e $A/_I \cdot J/_I \subseteq J/_I$]. Dunque resta definita l'applicazione

$$\tilde{\pi} : \boldsymbol{\mathcal{I}} \to \boldsymbol{\mathcal{I}}' \text{ tale che } \tilde{\pi}(J) = J/_I,\ \forall\, J \in \boldsymbol{\mathcal{I}}.$$

L'applicazione $\tilde{\pi}$ è iniettiva: ciò segue dal fatto che $\tilde{\pi}$ è iniettiva già a livello di sottogruppi additivi, come provato in Teor. **4.3**. Dimostriamo che $\tilde{\pi}$ è suriettiva. Sia $\mathcal{H} \in \boldsymbol{\mathcal{I}}'$: se verifichiamo che $\pi^{-1}(\mathcal{H}) \in \boldsymbol{\mathcal{I}}$, allora $\tilde{\pi}(\pi^{-1}(\mathcal{H})) = \pi(\pi^{-1}(\mathcal{H})) = \mathcal{H}$ e quindi $\tilde{\pi}$ è suriettiva [si noti che l'ultima uguaglianza è di natura puramente insiemistica].

Che $\pi^{-1}(\mathcal{H})$ sia un ideale di A segue subito dall'Osserv. **2.5**. Inoltre $\pi^{-1}(\mathcal{H}) \supseteq I$: se infatti $x \in I$, allora $x + I = I \in \mathcal{H}$ e dunque $x \in \pi^{-1}(\mathcal{H})$. Ciò conclude la dimostrazione.

Osservazione 5.1. Per ogni ideale J di A, in base all'Osserv. **2.5**, $\pi(J)$ è un ideale di $A/_I$. Verificheremo che (in analogia a Prop. **4.1**) risulta:

$$\pi(J) = (I + J)/_I.$$

Infatti, come già provato a livello di gruppi additivi, $\pi^{-1}(\pi(J)) = I + J$ e quindi $\pi(J) = \pi\big(\pi^{-1}(\pi(J))\big) = \pi(I + J) = (I + J)/_I$.

Concludiamo il capitolo con alcune semplici considerazioni a proposito dei quozienti di spazi vettoriali.

Osservazione 5.2. Sia V un K-spazio vettoriale e W un suo sottospazio. $V/_W$ è ovviamente un gruppo abeliano additivo. Senza ulteriori ipotesi su W è ben definita la seguente moltiplicazione per uno scalare:

$$V/_W \times K \to V/_W \text{ tale che } (v + W, c) \to cv + W,\ \forall\, v + W \in V/_W,\ \forall\, c \in K.$$

[si osservi che: $v + W = v_1 + W \implies cv + W = cv_1 + W$, in quanto $cv - vv_1 = c(v - v_1) \in W$].

Si verifica facilmente che $V/_W$ è un K-spazio vettoriale, detto *spazio vettoriale quoziente di V modulo W*.

Per gli spazi vettoriali vale il *TFO*: *ogni omomorfismo di K-spazi vettoriali $T : V \to V'$ induce un unico isomorfismo di spazi vettoriali*

$$\overline{T} : V/_{KerT} \to Im\,T \text{ tale che } \overline{T}(v + KerT) = T(v),\ \forall\, v + KerT \in V/_{KerT}.$$

Valgono i seguenti teoremi:

Secondo teorema di isomorfismo. Siano W_1, W_2 sottospazi vettoriali di V. Risulta:

$$W_1 + W_2/_{W_1} \cong W_2/_{W_1 \cap W_2}.$$

Terzo teorema di isomorfismo. Siano W_1, W_2 sottospazi vettoriali di V, con $W_1 \subseteq W_2$. Risulta:

$$V/_{W_2} \cong V/_{W_1}/_{W_2/W_1}.$$

Teorema di corrispondenza. Sia W un sottospazio vettoriale di V. I sottospazi vettoriali di V contenenti W sono in corrispondenza biunivoca con i sottospazi vettoriali di $V/_W$.

* * * * * * * * * * * * * * * * * * *

Esercizio 1.5.1. In $A = K[X, Y]$ si considerino il sottoanello $B = K[Y]$ e l'ideale $I = (XY)$ (ideale generato dal polinomio $XY \in A$). Determinare l'anello $(I + B)/_I$.

Esercizio 1.5.2. Sia $\mathcal{A} = \mathfrak{M}_n(\boldsymbol{Z})$ l'anello delle matrici di interi, quadrate e di ordine n. In $\mathcal{A}$ si considerino i sottoinsiemi

$\mathcal{I} = \{\text{matrici di } A \text{ ad elementi pari}\}, \qquad \mathcal{R} = \{A \in \mathcal{A} \mid \text{la prima riga di } A \text{ è nulla}\}.$

(*i*) Verificare che $\mathcal{I}$ è un ideale di $\mathcal{A}$ e che $\mathcal{R}$ è un sottoanello ma non un ideale di $\mathcal{A}$.

(*ii*) Dimostrare che $\mathcal{A}/_{\mathcal{I}} \cong \mathfrak{M}_n(\boldsymbol{Z}_2)$.

(*iii*) Verificare che $\mathcal{I} \cap \mathcal{R}$ è un ideale di $\mathcal{R}$ e determinare l'anello $\mathcal{R}/_{\mathcal{I}\cap\mathcal{R}}$.

Esercizio 1.5.3. Determinare l'anello $\boldsymbol{Z}[X]/_{(X,2)}$ [dove $(X, 2)$ è l'ideale di $\boldsymbol{Z}[X]$ generato dagli elementi X, 2].

Esercizio 1.5.4. Assegnato un campo K, determinare gli eventuali ideali propri dell'anello $A = K[X]/_{(X^3)}$. Di ciascuno calcolare il quoziente rispetto ad A.

Esercizio 1.5.5. Sia d un intero positivo tale che $X^2 - d \in \boldsymbol{Z}[X]$ sia irriducibile. Verificare che

$$\boldsymbol{Z}[\sqrt{d}]/_{(2d)} \cong \boldsymbol{Z}[\sqrt{-d}]/_{(2d)},$$

dove, come noto dal corso di **Alg. 1**, $\boldsymbol{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ \forall\, a, b \in \boldsymbol{Z}\}$ è isomorfo a $\boldsymbol{Z}[X]/_{(X^2-d)}$ (cfr. anche Cap. **3**, Osserv. **2.1**(*iv*)).

Esercizio 1.5.6. Utilizzando il terzo teorema di isomorfismo, verificare che $\boldsymbol{Z}[i]/_{(1+3i)} \cong \boldsymbol{Z}_{10}$. Esplicitare un siffatto isomorfismo.

Esercizio 1.5.7. Dimostrare che $\boldsymbol{Z}[i]/_{(2)}$ è un anello non integro con quattro elementi. Indicarne gli zero-divisori (non banali).

Esercizio 1.5.8. Dimostrare che $\boldsymbol{Z}_6[X]/_{(\overline{2}X-\overline{1})} \cong \boldsymbol{Z}_3$.

Esercizio 1.5.9. (*i*) Sia $z = a + ib$ un elemento non nullo e non invertibile di $\boldsymbol{Z}[i]$ e sia $n = \mathcal{N}(z)$. Esprimere $\boldsymbol{Z}[i]/_{(z)}$ come quoziente di $\boldsymbol{Z}_n[X]$.

(*ii*) Verificare che $\boldsymbol{Z}[i]/_{(3+4i)} \cong \boldsymbol{Z}_{25}$.

Esercizio 1.5.10. Esplicitare un isomorfismo tra gli anelli $\boldsymbol{Z}_6[X]/_{\overline{2}\boldsymbol{Z}_6[X]}$ e $\boldsymbol{Z}_2[X]$. Dedurne che $\boldsymbol{Z}_6[X]/_{(\overline{3}X+\overline{1})} \cong \boldsymbol{Z}_2$.

Esercizio 1.5.11. (*i*) Dimostrare che $\boldsymbol{Z}[\sqrt{-2}]/_{(3-\sqrt{-2})}$ è un campo e indicarne la cardinalità.

(*ii*) Dimostrare che per ogni $a \in \boldsymbol{N}$, a pari, $a \geq 4$, l'anello $\boldsymbol{Z}[\sqrt{2}]/_{(a-\sqrt{2})}$ non è integro.

Capitolo 2

ELEMENTI DI TEORIA DEI GRUPPI

1. Il teorema di Cayley

Ricordiamo una definizione: se X è un insieme non vuoto, l'insieme $\boldsymbol{S}(X)$ delle biiezioni di X in sé è dotato di struttura di gruppo rispetto al prodotto operatorio $\circ$. $(\boldsymbol{S}(X), \circ)$ è detto *gruppo delle permutazioni di* X. In particolare, se $|X| = n$, $\boldsymbol{S}(X)$ è denotato $\boldsymbol{S}_n$ ed è chiamato *gruppo simmetrico* (o gruppo delle permutazioni) *su* n *elementi*.

Vale il seguente teorema, di importanza essenzialmente teorica.

Teorema 1.1. *(Cayley). A meno di isomorfismi, ogni gruppo* $(G, \cdot)$ *è sottogruppo di un gruppo di permutazioni.*

Dim. Basta dimostrare che esiste un omomorfismo iniettivo da G a $(\boldsymbol{S}(G), \circ)$. Per ogni $g \in G$ definiamo l'applicazione

$$T_g : G \to G \text{ tale che } T_g(x) = gx, \ \forall\, x \in G,$$

[si tratta della moltiplicazione a sinistra per g]. Si verifica facilmente che T_g è biiettiva [ha per inversa $T_{g^{-1}}$]. Dunque $T_g \in \boldsymbol{S}(G)$ e pertanto resta definita l'applicazione

$$T : G \to \boldsymbol{S}(G) \text{ tale che } T(g) = T_g, \ \forall\, g \in G.$$

Basta allora verificare che

(i) $T(g_1 g_2) = T(g_1) \circ T(g_2), \ \forall\, g_1, g_2 \in G$;

(ii) $T(g_1) = T(g_2) \implies g_1 = g_2$.

[Le verifiche sono un semplice esercizio]. Dunque T è un omomorfismo iniettivo e la tesi è dimostrata.

Ad esempio il teorema di Cayley afferma che ogni gruppo G di ordine 10 è identificabile ad un sottogruppo di $\boldsymbol{S}_{10}$ (che ha cardinalità 10!). Decisamente il teorema fornisce una "rappresentazione" di G all'interno di un gruppo troppo più grande. Si pone quindi il problema di determinare un più piccolo insieme X tale che G si identifichi ad un sottogruppo di $\boldsymbol{S}(X)$. Vale il seguente risultato, che costituisce una *forma generalizzata* del teorema di Cayley.

Teorema 1.2. *(Cayley generalizzato). Sia* $(G, \cdot)$ *un gruppo e sia* H *un suo sottogruppo. Denotiamo con* $\mathcal{L} = \mathcal{L}_s(H)$ *l'insieme dei suoi laterali sinistri. Esiste un omomorfismo*

$$T : (G, \cdot) \to (\boldsymbol{S}(\mathcal{L}), \circ)$$

il cui nucleo $KerT$ *è contenuto in* H *e verifica la seguente proprietà:*

$KerT$ *è il più grande sottogruppo normale di* G *contenuto in* H.

Prima di dimostrare tale teorema, osserviamo che l'omomorfismo T non risponde del tutto al problema di rappresentare G dentro al gruppo di permutazioni $\boldsymbol{S}(\mathcal{L})$. Ciò avviene infatti $\iff$ T è iniettivo $\iff$ $KerT = \{1\}$ $\iff$ l'unico sottogruppo di H normale in G è $\{1\}$.

Dim. (*Teor.* **1.2**). Per ogni $g \in G$, si ponga:

$$T_g : \mathcal{L} \to \mathcal{L} \text{ tale che } T_g(xH) = gxH, \ \forall\, xH \in \mathcal{L}.$$

Osserviamo che T_g è ben definita e biiettiva. Infatti:

- $T_g(xH) = T_g(yH) \iff gxH = gyH \iff y^{-1}g^{-1}gx \in H \iff y^{-1}x \in H \iff xH = yH$.
- $\forall\, yH \in \mathcal{L}, \ yH = T_g(g^{-1}yH)$.

Ne segue che resta definita l'applicazione:

$$T : G \to \boldsymbol{S}(\mathcal{L}) \text{ tale che } T(g) = T_g, \ \forall\, g \in G.$$

T è un omomorfismo di gruppi, cioè risulta $T(g_1g_2) = T(g_1) \circ T(g_2), \ \forall\, g_1, g_2 \in G$. Infatti

$$T_{g_1g_2}(xH) = g_1g_2xH = g_1(g_2xH) = T_{g_1}(T_{g_2}(xH)) = (T(g_1) \circ T(g_2))(xH).$$

Calcoliamo $KerT$. Risulta:

$$KerT = \{g \in G \mid T_g = \mathbf{1}_{\mathcal{L}}\} = \{g \in G \mid gxH = xH, \ \forall\, x \in G\} = \{g \in G \mid x^{-1}gx \in H, \ \forall\, x \in G\}.$$

Si ha:

- $KerT \leq H$ [infatti, $\forall\, g \in KerT$, $x^{-1}gx \in H$. Posto $x = 1$, $g \in H$].
- $KerT$ è normale in G [infatti è un nucleo].
- se $N \trianglelefteq G$ e $N \leq H$, verifichiamo che $N \subseteq KerT$. Infatti si ha, $\forall\, x \in G$, $\forall\, n \in N$: $x^{-1}nx \in x^{-1}Nx = N \subseteq H$. Ne segue che $x^{-1}nx \in H$, $\forall\, x \in G$, e quindi $n \in KerT$.

Abbiamo così dimostrato che $KerT$ è il più grande sottogruppo in H, normale in G.

Osservazione 1.1. Sia G un gruppo *semplice*, cioè, per definizione, un *gruppo privo di sottogruppi normali (non banali)*. Scelto arbitrariamente un sottogruppo H di G, con $H \neq G$, l'omomorfismo

$$T : G \to \boldsymbol{S}(\mathcal{L}_s(H))$$

(sopra definito) è iniettivo [infatti $KerT$ è un sottogruppo normale di G, contenuto in H; essendo G semplice e $H \neq G$, allora $KerT = \{1\}$]. Dunque G si immerge nel gruppo di permutazioni $\boldsymbol{S}(\mathcal{L})$, con $|\mathcal{L}| = |\mathcal{L}_s(H)| = (G : H)$ [*indice* di H in G, cfr. Cap. **1** Osserv. **1.1**]. Intuitivamente, più H è grande in G, più $(G : H)$ è piccolo e quindi più l'immersione T è conveniente.

Osservazione 1.2. Sia G un gruppo finito, sia H un sottogruppo proprio di G e si ponga $\mathcal{L} = \mathcal{L}_s(H)$. Posto $i = (G : H)$, allora $|\mathcal{L}| = i$ e dunque $|\boldsymbol{S}(\mathcal{L})| = i!$.

Se $T : G \to \boldsymbol{S}(\mathcal{L})$ è iniettiva, allora $|G| = |ImT|$ e dunque, dal teorema di Lagrange, $|G| \,\big|\, i!$. Se quindi, viceversa, è possibile scegliere in G un sottogruppo proprio H tale che $|G| \nmid i!$, allora T non può essere iniettiva e ciò implica che esista in H un sottogruppo non banale, normale in G. Perciò G non è semplice. Questa idea può venire utilizzata quindi per provare che un gruppo non è semplice! Cerchiamo di chiarire il tutto con un esempio.

Sia $|G| = 42$. Supponiamo che G possegga un sottogruppo H di ordine 7 [ciò che del resto è sempre vero, come vedremo, in base al *teorema di Cauchy*, cfr. Teor. **4.1**]. Risulta: $(G : H) = 6$ e $42 \nmid 6!$. Ne segue che H possiede un sottogruppo [cioè $KerT$] normale in G e non banale. Dunque G non è semplice. Poiché inoltre H non ha sottogruppi propri (in quanto ha ordine primo), possiamo concludere che $H = KerT$ e dunque $H \lhd G$.

Abbiamo dimostrato che, se $|G| = 42$, G non è semplice e ogni suo sottogruppo di ordine 7 è normale. Si noti che il *teorema di Sylow* (cfr. il successivo Teor. **4.2**) ci dirà che di sottogruppi di ordine 7 ne esiste uno soltanto.

Nota. Ovviamente tutti i guppi finiti di ordine p primo sono semplici [non hanno sottogruppi propri]. Il più piccolo gruppo semplice non abeliano è il gruppo alterno $\boldsymbol{A}_5$ (di ordine 60) e ne proveremo la semplicità nel Cap. **5**. Va detto che i gruppi semplici giocano un ruolo essenziale nella classificazione dei gruppi finiti.

* * * * * * * * * * * * * * * * * * *

Esercizio 2.1.1. Assumendo nota la struttura dei sottogruppi del gruppo alterno $\boldsymbol{A}_4$ [cfr. [AA] pag. 175], determinare un sottogruppo H di $\boldsymbol{A}_4$, di ordine massimo per cui l'omomorfismo del teorema di Cayley generalizzato sia iniettivo.

Esercizio 2.1.2. Sia G un gruppo di ordine 20. Tenuto conto che G possiede un sottogruppo H di ordine 5 [in base al teorema di Cauchy, cfr. § 4], dimostrare che G non è semplice.

Esercizio 2.1.3. Dimostrare che se G è un gruppo abeliano finito, il teorema di Cayley ed il teorema di Cayley generalizzato forniscono la stessa rappresentazione di G [come sottogruppo di un gruppo simmetrico].

2. Prodotto diretto di gruppi

Ci limitiamo a considerare il prodotto diretto di due gruppi, ma quanto diremo si estende in modo naturale al caso di n gruppi, $n \geq 3$.

Definizione 2.1. *Siano G, G' due gruppi [che, per semplicità scriveremo in notazione moltiplicativa, anche se ciò è inessenziale]. Si chiama prodotto diretto (esterno) di G per G' il gruppo $(G\times G', \cdot)$, con operazione $\cdot$ così definita:*

$$(a,a')\cdot(b,b') = (ab, a'b'), \quad \forall\,(a,a'),\,(b,b') \in G\times G'.$$

[Si tratta di un gruppo, con elemento neutro $(1,1')$ ed inverso $(a,a')^{-1} = (a^{-1}, a'^{-1})$].

Osservazione 2.1. Se G, G' sono abeliani, allora $(G\times G'), \cdot)$, è abeliano. Vale anche il viceversa.

Osservazione 2.2. In $G\times G'$, sono contenuti i due sottogruppi $G\times\{1'\}$ e $\{1\}\times G'$.
Si verifica subito che si tratta di sottogruppi di $G\times G'$ e che si tratta di sottogruppi normali [ad esempio, per verificare che $G\times\{1'\} \trianglelefteq G\times G'$, osserviamo che

$$(a,a')\big(G\times\{1'\}\big)(a,a')^{-1} \subseteq (a\,G\,a^{-1})\times(a'\,\{1'\}\,a'^{-1}) = (a\,G\,a^{-1})\times\{1'\} \subseteq G\times\{1'\}].$$

Inoltre il loro prodotto (che è un sottogruppo) coincide con $G\times G'$ [infatti $(a,a') = (a,1')\cdot(1,a')$, $\forall\,(a,a') \in G\times G'$] e la loro intersezione è il sottogruppo banale $\{1\}\times\{1'\}$.

Viceversa, se un gruppo G possiede due sottogruppi verificanti tali proprietà, allora G è prodotto diretto di due gruppi, come ora vedremo. Questo risultato ci permetterà di riconoscere quando un gruppo è prodotto diretto di due gruppi.

Teorema 2.1. *Sia G un gruppo e siano H, K due sottogruppi di G tali che:*

(i) H, K sono normali in G; (ii) $HK = G$; (iii) $H\cap K = \{1\}$.

Allora $G \cong H\times K$.

Dim. Si pone: $\varphi : H\times K \to G$, tale che $\varphi\big((h,k)\big) = hk$, $\forall\,h\in H$, $\forall\,k\in K$.
Si tratta di verificare che φ è un isomorfismo, cioè:

$$(a)\ \varphi \text{ è iniettiva;} \quad (b)\ \varphi \text{ è suriettiva;} \quad (c)\ \varphi \text{ è un omomorfismo.}$$

(a) Sia $hk = h_1k_1$. Allora $h_1^{-1}h = k_1k^{-1}$. Tale elemento appartiene a $H\cap K$ e quindi $h_1^{-1}h = 1 = k_1k^{-1}$. Ne segue che $h = h_1$, $k = k_1$.

(b) Sia $x\in G$. Da (ii) $x = hk$, per opportuni $h\in H$, $k\in K$. Pertanto $\varphi\big((h,k)\big) = hk = x$.

(c) Bisogna verificare che

$$\varphi\big((h,k)\cdot(h_1,k_1)\big) = \varphi\big((h,k)\big)\varphi\big((h_1,k_1)\big),$$

cioè che $\varphi\big((hh_1,kk_1)\big) = (hk)(h_1k_1)$, ovvero che $hh_1kk_1 = hkh_1k_1$.
Allo scopo è sufficiente verificare che $h_1k = kh_1$. Dunque la tesi è verificata se dimostriamo che i due sottogruppi H, K permutano "elemento per elemento", ovvero che $hk = kh$, $\forall\,h\in H$, $\forall\,k\in K$. Si ponga $x = hkh^{-1}k^{-1}$ [è detto *commutatore di h, k*]. Si tratta di verificare che $x = 1$ [da cui subito $hk = kh$]. Si ha:

$$x = \begin{cases} h(kh^{-1}k^{-1}) \in HH = H & [\text{in quanto } H\trianglelefteq G \implies kh^{-1}k^{-1}\in H],\\ (hkh^{-1})k^{-1} \in KK = K & [\text{in quanto } K\trianglelefteq G \implies hkh^{-1}\in K]. \end{cases}$$

Ne segue che $x\in H\cap K = \{1\}$, cioè $x = 1$.

Proposizione 2.1. *Siano $g\in G$ e $g'\in G'$ elementi di periodo finito nei rispettivi gruppi. Risulta:*

$$\circ\big((g,g')\big) = mcm\big(\circ(g),\circ(g')\big).$$

Se invece almeno uno dei due elementi ha periodo infinito, anche (g,g') ha periodo infinito, e viceversa.

Dim. Si ponga: $\circ(g) := r$, $\circ(g') := s$, $mcm(r,s) := h$. Dalla definizione di mcm, $h = r\,n = s\,m$, per opportuni $n, m \in \boldsymbol{N}$. Dunque

$$(g,g')^h = (g^h, {g'}^h) = \big((g^r)^n, ({g'}^s)^m\big) = (1,1').$$

Ne segue che $\circ\big((g,g')\big) \,\big|\, h$. Si ponga ora $t := \circ\big((g,g')\big)$. Allora $(g^t, {g'}^t) = (1,1')$ e dunque $r \,\big|\, t$, $s \,\big|\, t$. Pertanto $h = mcm(r,s) \,\big|\, t$. Abbiamo così provato che $h \,\big|\, t$ e $t \,\big|\, h$. Dunque $h = t$.

Dimostriamo ora l'ultima affermazione. Se ad esempio $\circ(g) = \infty$, allora $g^n \neq 1$, $\forall\, n > 0$. Pertanto $\circ\big((g,g')\big) = \infty$. Viceversa, sia $\circ\big((g,g')\big) = \infty$; se $\circ(g)$, $\circ(g')$ fossero finiti, procedendo come sopra si otterrebbe $\circ\big((g,g')\big) < \infty$.

Corollario 2.1. *Siano G, G' due gruppi ciclici finiti di ordini coprimi. Anche $G\times G'$ è ciclico, ed ha ordine $|G|\cdot|G'|$.*

Dim. Siano $G = \langle\, a \mid a^r = 1\,\rangle$, $G' = \langle\, b \mid b^s = 1\,\rangle$, con $MCD(r,s) = 1$. In base alla Prop. **2.1**, $\circ((a,b)) = mcm(r,s) = rs$. Poiché $|G\times G'| = rs$, $G\times G'$ è ciclico e (a,b) ne è un generatore.

Proposizione 2.2. *Sia p un numero primo e sia G un gruppo (abeliano) di ordine p^2. [Si noti che nel successivo Cor.* **3.2** *verrà provato che ogni gruppo di ordine p^2 è abeliano]. Risulta: G è un gruppo ciclico oppure G è prodotto diretto di due suoi sottogruppi ciclici di ordine p.*

Dim. Se G ha un elemento di periodo p^2, G è ciclico. Altrimenti ogni $x \in G$, $x \neq 1$, ha periodo p. Si scelgano $x, y \in G$, $x, y \neq 1$, con $y \notin \langle\, x\,\rangle$. Basta verificare che i due sottogruppi $\langle\, x\,\rangle$, $\langle\, y\,\rangle$ verificano le tre condizioni (i), (ii), (iii) del Teor. **2.1**.

(i) I sottogruppi $\langle\, x\,\rangle$, $\langle\, y\,\rangle$ sono ovviamente normali in G [infatti G è abeliano].

(ii) Il prodotto $\langle\, x\,\rangle\langle\, y\,\rangle$ è un sottogruppo di G e contiene propriamente $\langle\, x\,\rangle$ [infatti $y \in \langle\, x\,\rangle\langle\, y\,\rangle$ e $y \notin \langle\, x\,\rangle$]. Dunque $|\langle\, x\,\rangle\langle\, y\,\rangle| > p$ e pertanto $|\langle\, x\,\rangle\langle\, y\,\rangle| = p^2$, cioè $\langle\, x\,\rangle\langle\, y\,\rangle = G$.

(iii) $\langle\, x\,\rangle \cap \langle\, y\,\rangle \subset \langle\, y\,\rangle$ [infatti $y \in \langle\, y\,\rangle$ e $y \notin \langle\, x\,\rangle \cap \langle\, y\,\rangle$]. Dunque $|\langle\, x\,\rangle \cap \langle\, y\,\rangle| < p$ e pertanto $|\langle\, x\,\rangle \cap \langle\, y\,\rangle| = 1$, cioè $\langle\, x\,\rangle \cap \langle\, y\,\rangle = \{1\}$.

* * * * * * * * * * * * * * * * * * *

Esercizio 2.2.1. Considerati i seguenti gruppi:

$$\boldsymbol{C}_6, \quad \boldsymbol{S}_3, \quad \boldsymbol{A}_4, \quad \boldsymbol{S}_4, \quad \boldsymbol{D}_4, \quad \boldsymbol{D}_5,$$

quale/i di essi è isomorfo al prodotto diretto di due suoi sottogruppi propri ?

Esercizio 2.2.2. Determinare in $\boldsymbol{S}_5$ un sottogruppo non abeliano di ordine 12, prodotto diretto di due suoi sottogruppi propri.

Esercizio 2.2.3. Verificare che il gruppo $\boldsymbol{Z}\times\boldsymbol{Z}$ non è ciclico.

Esercizio 2.2.4. (i) Verificare che, per ogni n naturale dispari, $\boldsymbol{O}_n(\boldsymbol{R}) \cong \boldsymbol{SO}_n(\boldsymbol{R}) \times \boldsymbol{C}_2$.

(ii) Verificare che invece $\boldsymbol{O}_2(\boldsymbol{R}) \ncong \boldsymbol{SO}_2(\boldsymbol{R}) \times \boldsymbol{C}_2$.

[*Suggerimento.* Il gruppo $\boldsymbol{O}_2(\boldsymbol{R})$ possiede un'infinità continua di elementi di periodo 2].

Esercizio 2.2.5. (i) Sia G un gruppo finito verificante la seguente proprietà:

per ogni d divisore positivo di $|G|$, G ha al più un solo sottogruppo di ordine d.

Verificare che G è un gruppo ciclico.

(ii) Se K è un campo finito, verificare che il gruppo moltiplicativo $(K^{\cdot}, \cdot)$ è ciclico. [*Suggerimento*: se $H \leq K^{\cdot}$ e $|H| = m$, applicare il teorema di Ruffini al polinomio $X^m - 1 \in K[X]$ e dedurne che G non ha altri sottogruppi di ordine m.]

3. Azione di un gruppo su un insieme

Definizione 3.1. *Sia S un insieme non vuoto e sia $(G,\cdot)$ un gruppo. Si chiama azione di G su S ogni applicazione $\omega : G\times S \to S$, tale che*

(i) $\omega(1,s) = s, \ \forall\, s \in S;$

(ii) $\omega\big(g_1,\omega(g_2,s)\big) = \omega(g_1g_2,s), \ \forall\, s\in S, \ \forall\, g_1,\, g_2 \in G.$

Se ω è un'azione di G su S, si dice che G opera su S tramite ω e che S è un G-insieme.

Per semplificare le notazioni si scrive (quando ciò non crei equivoci) $g\cdot s$ (o addirittura gs) in luogo di $\omega(g,s)$. In tal caso (i) e (ii) diventano:

$$(i)\ \ 1\cdot s = s, \ \forall\, s\in S; \qquad (ii)\ \ g_1\cdot(g_2\cdot s) = g_1g_2\cdot s, \ \forall\, s\in S, \ \forall\, g_1,\, g_2 \in G.$$

Osservazione 3.1. Sia ω un'azione di G su S. Per ogni $g\in G$, si definisce:

$$g_{\_} = \omega(g,\,-) : S \to S \ \text{ tale che } \ \omega(g,\,-)(s) = \omega(g,s), \ \forall\, s\in S$$

[ovvero $g_{\_}(s) = g\cdot s, \ \forall\, s\in S$]. Ovviamente $g_{\_}$ è una biiezione di S in sé, cioè $g_{\_}\in \boldsymbol{S}(S)$. Posto

$$\varphi_\omega : G \to \boldsymbol{S}(S) \ \text{ tale che } \ \varphi_\omega(g) = g_{\_}, \ \forall\, g\in G,$$

si verifica subito che φ_ω è un omomorfismo di gruppi [infatti $(g_1g_2)_{\_} = (g_{1\_})\circ(g_{2\_}), \ \forall\, g_1,g_2\in G$]. Il nucleo $Ker\varphi_\omega$ è detto *nucleo dell'azione* ω e l'azione ω è detta *fedele* se $Ker\varphi_\omega = \{1\}$.

Si verifica facilmente che, viceversa, ogni omomorfismo di gruppi $\varphi : G\to \boldsymbol{S}(S)$ definisce l'azione

$$\omega_\varphi : G\times S \to S \ \text{ tale che } \ \omega_\varphi(g,s) = \varphi(g)(s), \ \forall\, g\in G, \ \forall\, s\in S.$$

Si verifica inoltre che $\omega_{\varphi_\omega} = \omega$ e $\varphi_{\omega_\varphi} = \varphi$. Pertanto le azioni di G su S corrispondono biunivocamente agli omomorfismi da G a $\boldsymbol{S}(S)$.

Definizione 3.2. *Si chiama relazione associata all'azione ω di G su S la seguente relazione $\sim$ (o $\sim_\omega$) su S:*

$$s\sim t \iff t = g\cdot s, \ \exists\, g\in G.$$

Si verifica subito che $\sim$ è una relazione di equivalenza su S. La classe di equivalenza di ogni elemento $s\in S$ è detta orbita di s rispetto ad ω ed è denotata $\boldsymbol{O}(s)$. Dunque:

$$\boldsymbol{O}(s) = [s]_\sim = \{g\cdot s, \ \forall\, g\in G\}.$$

Le orbite (a due a due distinte) di S rispetto ad ω formano una partizione di S. Infine, un'azione ω di G su S è detta transitiva se forma un'unica orbita, cioè se, $\forall\, s,t\in S$, risulta: $t = g\cdot s, \ \exists\, g\in G$.

Definizione 3.3. *Sia ω un'azione di G su S e sia $s\in S$. Si chiama stabilizzatore di s rispetto ad ω l'insieme*

$$\boldsymbol{St}_s = \{g\in G \mid g\cdot s = s\}.$$

Si verifica subito che $\boldsymbol{St}_s$ è un sottogruppo di G [infatti, $\forall\, g,h\in \boldsymbol{St}_s$: $gh^{-1}\cdot s = g\cdot(h^{-1}\cdot s) = g\cdot(h^{-1}\cdot(h\cdot s)) = g\cdot(1\cdot s) = g\cdot s = s$ e quindi $gh^{-1}\in \boldsymbol{St}_s$]. Inoltre $\bigcap\limits_{s\in S} \boldsymbol{St}_s = Ker\varphi_\omega$ [infatti $g\in Ker\varphi_\omega \iff g\cdot s = s, \ \forall\, s\in S$].

Esempio 3.1. $S = G$; $\omega : G\times G\to G$ tale che

$$\omega(g,s) = gs, \ \forall\, g\in G, \ \forall\, s\in G$$

(*azione di moltiplicazione (a sinistra) in G*). Risulta, $\forall\, s\in G$:

$$\boldsymbol{O}(s) = G \ \text{ (l'azione è transitiva)}; \qquad \boldsymbol{St}_s = \{1\}; \qquad Ker\varphi_\omega = \{1\} \ \text{ (l'azione è fedele).}$$

Nota. Il fatto che tale azione sia fedele è il cuore della dimostrazione del teorema di Cayley [infatti φ_ω coincide con l'omomorfismo T della dimostrazione del Teor. **1.1**].

Esempio 3.2. $S = G$; $\omega : G\times G\to G$ tale che

$$\omega(g,s) = gsg^{-1},\ \forall\, g \in G,\ \forall\, s \in G$$

(*azione di coniugio in* G). Per non confondere tale azione con la precedente, scriviamo $\omega(g,s) = g*s$ (e dunque $g*s = gsg^{-1},\ \forall\, g \in G$). Si osserva subito che la relazione di equivalenza associata a tale azione altro non è che la relazione di coniugio su G [cfr. [AA], Cap. **4.3**, Def. **4**]. Risulta, $\forall\, s \in G$:

$\boldsymbol{O}(s) = \{g * s,\ \forall\, g \in G\} = \{gsg^{-1},\ \forall\, g \in G\} = [s]_{\sim}$ (classe di coniugio di s);

$\boldsymbol{St}_s = \{g \in G \mid g * s = s\} = \{g \in G \mid gs = sg\} =: \boldsymbol{C}(s)$ (detto *centralizzante di* s);

$Ker\varphi_* = \bigcap_{s \in G} \boldsymbol{C}(s) = \{g \in G \mid gs = sg,\ \forall\, s \in G\} =: \boldsymbol{Z}(G)$ (detto *centro di* G).

Ovviamente il centro $\boldsymbol{Z}(G)$ è un sottogruppo normale di G e si ha: $\boldsymbol{Z}(G) = G \iff G$ è abeliano.

Esempio 3.3. Sia $\omega : G \times S \to S$ un'azione e sia $H \leq G$. L'applicazione di restrizione

$$\omega' = \omega_{|_{H \times S}} : H \times S \to S \text{ tale che } \omega'(h,s) = \omega(h,s),\ \forall\, h \in H,\ \forall\, s \in S$$

è ovviamente un'azione di H su S (*azione ristretta al sottogruppo* H *di* G). Risulta, $\forall\, s \in S$:

$$\boldsymbol{O}'(s) = \{h \cdot s,\ \forall\, h \in H\} \subseteq \boldsymbol{O}(s);\quad \boldsymbol{St'}_s = \{h \in H \mid h \cdot s = s\} = H \cap \boldsymbol{St}_s;\quad Ker\varphi_{\omega'} = H \cap Ker\varphi_\omega.$$

Ad esempio, indicata con ω' la restrizione ad H della moltiplicazione a sinistra in G, allora

$\boldsymbol{O}'(s) = Hs$ (laterale destro di $s\ mod\ H$), $\boldsymbol{St'}_s = \{1\}$, $Ker\varphi_{\omega'} = \{1\}$ (l'azione è fedele).

Esempio 3.4. Sia $\omega : G \times S \to S$ un'azione e sia $s \in S$. Si verifica subito che l'applicazione di restrizione $\omega_s = \omega_{|_{G \times \boldsymbol{O}(s)}}$ è un'azione di G su $\boldsymbol{O}(s)$ (*azione ristretta ad un'orbita*) [infatti, $\forall\, g \in G,\ \forall\, t = g_1 \cdot s \in \boldsymbol{O}(s)$ si ha: $\omega_s(g,t) = g \cdot (g_1 \cdot s) = gg_1 \cdot s \in \boldsymbol{O}(s)$]. Ovviamente ω_s è un'azione transitiva ed i suoi stabilizzatori coincidono con quelli di ω. Inoltre il suo nucleo contiene $Ker\varphi_\omega$ (essendo intersezione dei soli stabilizzatori degli elementi dell'orbita).

Esempio 3.5. $S = X$ insieme non vuoto; $G = (\boldsymbol{S}(X), \circ)$; $\omega : \boldsymbol{S}(X) \times X \to X$ tale che

$$\omega(f,x) = f(x),\ \forall\, f \in \boldsymbol{S}(X),\ \forall\, x \in X$$

(*azione delle permutazioni di un insieme*). Risulta, $\forall\, x \in X$:

$\boldsymbol{O}(x) = X$ [infatti, $\forall\, x, y \in X$, esiste una biiezione che scambia x con y e fissa $X - \{x,y\}$];

$\boldsymbol{St}_x = \{f \in \boldsymbol{S}(X) \mid f(x) = x\}$ (biiezioni che fissano x).

L'azione ω è fedele. Infatti l'omomorfismo $\varphi_\omega : \boldsymbol{S}(X) \to \boldsymbol{S}(X)$ coincide con l'identità di $\boldsymbol{S}(X)$.

Se ad esempio $X = \{1, 2, \dots, n\}$, allora $\boldsymbol{S}(X) = \boldsymbol{S}_n$ (gruppo simmetrico su n elementi). In tal caso, $\forall\, x \in X$, $\boldsymbol{St}_x \cong \boldsymbol{S}_{n-1}$ (se $n \geq 2$).

Esempio 3.6. $S = \boldsymbol{R}^n$; $G = \boldsymbol{GL}_n(\boldsymbol{R})$; $\omega : \boldsymbol{GL}_n(\boldsymbol{R}) \times \boldsymbol{R}^n \to \boldsymbol{R}^n$ tale che

$$\omega(A, \underline{x}) = A\,\underline{x},\ \forall\, A \in \boldsymbol{GL}_n(\boldsymbol{R}),\ \forall\, \underline{x} \in \boldsymbol{R}^n$$

(*azione di moltiplicazione (righe per colonne) di una matrice per un vettore*). Risulta, $\forall\, \underline{x} \in \boldsymbol{R}^n$:

$\boldsymbol{O}(\underline{x}) = \boldsymbol{R}^n - \{\underline{0}\}$, se $\underline{x} \neq \underline{0}$; $\boldsymbol{O}(\underline{0}) = \{\underline{0}\}$.

[Siano infatti $\underline{x}, \underline{y} \in \boldsymbol{R}^n - \{\underline{0}\}$. Si scelga un operatore lineare invertibile $T : \boldsymbol{R}^n \to \boldsymbol{R}^n$ tale che $T(\underline{x}) = \underline{y}$ e sia $A \in \boldsymbol{GL}_n(\boldsymbol{R})$ la relativa matrice (rispetto alla base canonica). Allora $A\,\underline{x} = \underline{y}$ e quindi $\underline{y} \in \boldsymbol{O}(\underline{x})$].

$\boldsymbol{St}_{\underline{x}} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid A\,\underline{x} = \underline{x}\}$ (sottogruppo di $\boldsymbol{GL}_n(\boldsymbol{R})$).

L'azione ω è fedele. Infatti $A \in Ker\varphi_\omega \iff A\,\underline{x} = \underline{x},\ \forall\, \underline{x} \in \boldsymbol{R}^n \iff A = I_n$ (matrice unità).

Esempio 3.7. $S = \boldsymbol{E}^2$ (piano euclideo); $G = \boldsymbol{Isom}(\boldsymbol{E}^2)$ (isometrie del piano euclideo); $\omega : \boldsymbol{Isom}(\boldsymbol{E}^2) \times \boldsymbol{E}^2 \to \boldsymbol{E}^2$ tale che

$$\omega(f,P) = f(P),\ \forall\, f \in \boldsymbol{Isom}(\boldsymbol{E}^2),\ \forall\, P \in \boldsymbol{E}^2$$

(*azione delle isometrie piane sui punti del piano euclideo*). Si tratta di un caso particolare dell'azione di Esempio **3.5**. Risulta, $\forall\, P \in \boldsymbol{E}^2$:

$\boldsymbol{O}(P) = \boldsymbol{E}^2$ [infatti, $\forall\, Q \in \boldsymbol{E}^2$, $Q = t_{\overrightarrow{PQ}}(P)$, con $t_{\overrightarrow{PQ}}$ traslazione di vettore $\overrightarrow{PQ}$]. L'azione è quindi transitiva.

$\boldsymbol{St}_P = \{f \in \boldsymbol{Isom}(\boldsymbol{E}^2) \mid f(P) = P\}$. Si tratta delle isometrie che fissano P: sono le rotazioni di centro P e le riflessioni intorno ad una retta per P.
L'azione è fedele [se $f(P) = P,\ \forall P \in \boldsymbol{E}^2$, allora $f = \mathbf{1}_{\boldsymbol{E}^2}$].

Si noti che un'isometria trasforma rette in rette e poligoni n-lateri in poligoni n-lateri (congruenti). Dunque, denotati rispettivamente con $\mathfrak{R}$ e $\mathfrak{P}_n$ gli insiemi delle rette e dei poligoni n-lateri di $\boldsymbol{E}^2$, sono definite le seguenti azioni "indotte" da ω:

$\omega' : \boldsymbol{Isom}(\boldsymbol{E}^2) \times \mathfrak{R} \to \mathfrak{R}$ tale che $\omega'(f, \boldsymbol{r}) = f(\boldsymbol{r}),\ \forall \boldsymbol{r} \in \mathfrak{R}$;

$\omega'' : \boldsymbol{Isom}(\boldsymbol{E}^2) \times \mathfrak{P}_n \to \mathfrak{P}_n$ tale che $\omega'(f, \boldsymbol{P}_n) = f(\boldsymbol{P}_n),\ \forall \boldsymbol{P}_n \in \mathfrak{P}_n$.

Si noti che ω' è transitiva (come ω), mentre ω'' ha per orbite le famiglie di poligoni a due a due congruenti. Infine, è noto da **Alg. 1** che, se $\boldsymbol{R}$ è un rettangolo non quadrato, lo stabilizzatore di $\boldsymbol{R}$ (rispetto a ω'') è $\boldsymbol{V}$ (gruppo di Klein), mentre lo stabilizzatore di un poligono regolare $\boldsymbol{P}_n$ è $\boldsymbol{D}_n$ (gruppo diedrale).

Analizziamo ora le relazioni tra orbite e stabilizzatori.

Teorema 3.1. *Sia ω un'azione di G su S e sia $x \in S$. Risulta:*

$$|\boldsymbol{O}(x)| = (G : \boldsymbol{St}_x),$$

cioè "la cardinalità dell'orbita è l'indice dello stabilizzatore". In particolare, se G è un gruppo finito:

$$|\boldsymbol{O}(x)| \cdot |\boldsymbol{St}_x| = |G|.$$

Dim. Poiché $(G : \boldsymbol{St}_x) = |\mathcal{L}|$, dove $\mathcal{L} = \mathcal{L}_s(\boldsymbol{St}_x)$ denota l'insieme dei laterali sinistri di G modulo $\boldsymbol{St}_x$, basta costruire una biiezione $F : \boldsymbol{O}(x) \to \mathcal{L}$. Si pone:

$$F : \boldsymbol{O}(x) \to \mathcal{L} \text{ tale che } F(g \cdot x) = g\,\boldsymbol{St}_x,\ \forall g \cdot x \in \boldsymbol{O}(x).$$

Bisogna verificare:

(*i*) F è ben definita. Sia $g \cdot x = g_1 \cdot x \in \boldsymbol{O}(x)$. Allora $g_1^{-1} g \cdot x = x$, cioè $g_1^{-1} g \in \boldsymbol{St}_x$. Ne segue che $g_1^{-1} g\,\boldsymbol{St}_x = \boldsymbol{St}_x$ e quindi $g\,\boldsymbol{St}_x = g_1\,\boldsymbol{St}_x$.

(*ii*) F è iniettiva. Sia $F(g \cdot x) = F(g_1 \cdot x)$, cioè $g\,\boldsymbol{St}_x = g_1\,\boldsymbol{St}_x$. Procedendo a ritroso, rispetto al punto (*i*) , si ottiene $g \cdot x = g_1 \cdot x$.

(*iii*) F è suriettiva. Per ogni $h\,\boldsymbol{St}_x \in \mathcal{L}$, si ha: $h \cdot x \in \boldsymbol{O}(x)$ e $F(h \cdot x) = h\,\boldsymbol{St}_x$.

L'ultima affermazione segue dal teorema di Lagrange.

Corollario 3.1. *Sia $*$ l'azione di coniugio su un gruppo G. Risulta:*
(i) $\big|[x]_\sim\big| = \big(G : \boldsymbol{C}(x)\big),\ \forall x \in G.$
(ii) Se G è finito vale la seguente formula, detta equazione delle classi in G:

$$|G| = \sum_{x\ \ldots} \tfrac{|G|}{|\boldsymbol{C}(x)|},$$

dove la somma è estesa ad un solo rappresentante x in ogni classe di coniugio.

Dim. (*i*) In Esempio **3.2** è già stato osservato che $\boldsymbol{O}(x) = [x]_\sim$ e che $\boldsymbol{St}_x = \boldsymbol{C}(x),\ \forall x \in G$.

(*ii*) Le orbite formano una partizione di G. Quindi, scegliendo un unico elemento x in ciascuna orbita (o classe di coniugio), si ottiene:

$$|G| = \sum_{x\ \ldots} |\boldsymbol{O}(x)|.$$

Poiché $\boldsymbol{St}_x = \boldsymbol{C}(x)$ e G è finito, $|\boldsymbol{O}(x)| = \frac{|G|}{|\boldsymbol{St}_x|} = \frac{|G|}{|\boldsymbol{C}(x)|}$ e quindi vale la formula cercata.

Nota. Si verifica facilmente che:

$$x \in \boldsymbol{Z}(G) \iff \boldsymbol{C}(x) = G \iff [x]_\sim = \{x\} \iff \boldsymbol{O}(x) = \{x\}$$

Pertanto l'equazione delle classi si può riformulare in questo modo più preciso:

$$|G| = |\boldsymbol{Z}(G)| + \sum_{x\ \dots} \tfrac{|G|}{|\boldsymbol{C}(x)|},$$

dove la somma è estesa ad un solo rappresentante x in ogni classe di coniugio di cardinalità ≥ 2.

Corollario 3.2. *Sia G un p-gruppo (cioè un gruppo di ordine p^n, con p primo e $n \geq 1$). Risulta:*

$$\boldsymbol{Z}(G) \neq \{1\}.$$

In particolare, se $|G| = p^2$, G è abeliano (cioè $\boldsymbol{Z}(G) = G$).

Dim. Se per assurdo $|\boldsymbol{Z}(G)| = 1$, l'equazione delle classi (nell'ultima formulazione) si scriverebbe:

$$p^n = 1 + \sum_{x\ \dots} \tfrac{|G|}{|\boldsymbol{C}(x)|}.$$

Siano $x_1, \dots, x_t$ rappresentanti delle classi di coniugio di cardinalità ≥ 2. Poiché $|C(x_i)| < |G|$, risulta $\frac{|G|}{|\boldsymbol{C}(x_i)|} = p^{h_i}$, con $1 \leq h_i < n$. Dunque $p^n = 1 + \sum_{i=1}^{t} p^{h_i} = 1 + ps$, $\exists\, s \in \boldsymbol{N}$. Allora $p^n - ps = 1$, da cui $p \,\big|\, 1$: assurdo.

Sia ora $|G| = p^2$. Poiché $|\boldsymbol{Z}(G)| \neq 1$, allora $|\boldsymbol{Z}(G)| = p$ oppure $|\boldsymbol{Z}(G)| = p^2$ (e quindi $\boldsymbol{Z}(G) = G$). Per assurdo assumiamo che $|\boldsymbol{Z}(G)| = p$. Scegliamo $a \in G - \boldsymbol{Z}(G)$ e consideriamone il centralizzante $\boldsymbol{C}(a)$. Ovviamente $\boldsymbol{Z}(G) \leq \boldsymbol{C}(a)$. Inoltre $a \in \boldsymbol{C}(a)$ e $a \notin \boldsymbol{Z}(G)$. Dunque $\boldsymbol{Z}(G) < \boldsymbol{C}(a)$ e pertanto $|\boldsymbol{C}(a)| = p^2$, cioè $\boldsymbol{C}(a) = G$. Ma allora $a \in \boldsymbol{Z}(G)$: assurdo.

Concludiamo con una formula per contare il numero delle orbite, nel caso in cui sia il gruppo che l'insieme siano finiti. Introduciamo la seguente notazione: se $\omega : G \times S \to S$ è un'azione, per ogni $g \in G$ poniamo $\mathbf{S}_g := \{s \in S \mid g \cdot s = s\}$ [potremmo chiamarlo *stabilizzatore di* g, ma ovviamente non ha in genere alcuna struttura algebrica (essendo un sottoinsieme di S)].

Teorema 3.2. *(Formula di Burnside) Sia $\omega : G \times S \to S$ un'azione di G su S, con S, G finiti. Sia n il numero delle orbite di S rispetto a ω. Risulta:*

$$n = \tfrac{1}{|G|} \sum_{g \in G} |\mathbf{S}_g\,|.$$

Dim. Sia $A := \{(g, s) \in G \times S \mid g \cdot s = s\}$. Fissato $s_0 \in S$, si ha:

$$\big|\boldsymbol{St}_{s_0}\big| = \big|\{g \in G \mid g \cdot s_0 = s_0\}\big| = \big|\{(g, s_0) \in A\}\big|.$$

Analogamente, fissato $g_0 \in G$, si ha:

$$\big|\mathbf{S}_{g_0}\big| = \big|\{s \in S \mid g_0 \cdot s = s\}\big| = \big|\{(g_0, s) \in A\}\big|.$$

Allora

$$|A| = \sum_{g_0 \in G} \big|\mathbf{S}_{g_0}\big| = \sum_{s_0 \in S} \big|\boldsymbol{St}_{s_0}\big|.$$

Dal Teor. **3.1**, $|\boldsymbol{St}_s\,| = \frac{|G|}{|\boldsymbol{O}(s)|}$, $\forall\, s \in S$, e quindi

$$\sum_{g \in G} |\mathbf{S}_g\,| = \sum_{s \in S} \tfrac{|G|}{|\boldsymbol{O}(s)|}, \text{ cioè } \sum_{s \in S} \tfrac{1}{|\boldsymbol{O}(s)|} = \tfrac{1}{|G|} \sum_{g \in G} |\mathbf{S}_g\,|.$$

Si osservi che ovviamente, $\forall\, s \in S$, $\sum_{t \in \boldsymbol{O}(s)} \frac{1}{|\boldsymbol{O}(t)|} = \sum_{t \in \boldsymbol{O}(s)} \frac{1}{|\boldsymbol{O}(s)|} = 1$. Pertanto, fissati $s_1, \dots, s_n \in S$, uno per ciascuna delle n orbite, risulta:

$$\sum_{s \in S} \tfrac{1}{|\boldsymbol{O}(s)|} = \sum_{i=1}^{n} \big(\sum_{t \in \boldsymbol{O}(s_i)} \tfrac{1}{|\boldsymbol{O}(t)|} \big) = \sum_{i=1}^{n} 1 = n \ \text{ (numero delle orbite).}$$

Ne segue la formula cercata.

* * * * * * * * * * * * * * * * * *

Esercizio 2.3.1. (*i*) Sia $*$ l'azione di coniugio su un gruppo G. Quando tale azione è fedele?

(*ii*) Sia ω l'azione di coniugio su G, ristretta ad un sottogruppo H. Quando tale azione è fedele?

Esercizio 2.3.2. Sia ω un'azione di G su S.

(*i*) Verificare che ω induce un'azione $\tilde{\omega}$ sull'insieme delle parti $\mathfrak{P}(S)$, così definita: $\forall\, T \in \mathfrak{P}(S)$,

$$\tilde{\omega}(g,T) = g{\cdot}T := \{g{\cdot}t,\ \forall\, t \in T\},\ \text{se}\ T \neq \emptyset; \qquad \tilde{\omega}(g,\emptyset) = \emptyset.$$

(*ii*) Sia $|S| \geq n$ e sia $\mathbf{\Sigma}_n$ l'insieme dei sottoinsiemi di S di cardinalità n. Verificare che ω induce un'azione di G su $\mathbf{\Sigma}_n$.

Esercizio 2.3.3. Sia $*$ l'azione di coniugio su un gruppo G e sia H un sottogruppo di G.

(*i*) Determinare l'orbita $\tilde{\boldsymbol{O}}(H)$ rispetto all'azione $\tilde{*}$ indotta su $\mathfrak{P}(G)$ da $*$ (cfr. esercizio precedente).

(*ii*) Denotato con $\tilde{\boldsymbol{S}}t_{_H}$ lo stabilizzatore di tale azione indotta, verificare che

$$\tilde{\boldsymbol{S}}t_{_H} = \{g \in G \mid gH = Hg\}.$$

Tale gruppo è detto *normalizzante di* H *in* G ed è denotato $\mathcal{N}(H)$.

(*iii*) Verificare che $\mathcal{N}(H)$ è il più grande sottogruppo di G in cui H è normale.

Esercizio 2.3.4. Sia H un sottogruppo di G e sia $\mathcal{L} = \mathcal{L}_s(H)$ l'insieme delle sue classi laterali sinistre. È definita l'applicazione

$$\omega : G{\times}\mathcal{L} \to \mathcal{L}\ \text{ tale che }\ \omega(g, aH) = ga\,H,\ \forall\, g \in G,\ \forall\, aH \in \mathcal{L}.$$

(*i*) Verificare che ω è un'azione su $\mathcal{L}$.

(*ii*) Verificare che ω è transitiva.

(*iii*) ω è fedele?

Esercizio 2.3.5. Sia ω l'azione di moltiplicazione (righe per colonne) delle matrici ortogonali $\boldsymbol{O}_n(\boldsymbol{R})$ su $\boldsymbol{R}^n$. Determinare le orbite di tale azione e dire se l'azione è fedele.

Esercizio 2.3.6. Verificare che gli stabilizzatori di elementi di una stessa orbita sono sottogruppi coniugati.

Esercizio 2.3.7. (*i*) Calcolare il numero delle orbite rispetto all'azione di coniugio in $\boldsymbol{D}_6$. Determinare ciascuna orbita.

(*ii*) Verificare la formula di Burnside (per il coniugio) e l'equazione delle classi per $\boldsymbol{A}_4$.

Esercizio 2.3.8. Verificare l'equazione delle classi e la formula di Burnside per il gruppo $\boldsymbol{S}_4$.

Esercizio 2.3.9. Sia ω un'azione di un gruppo G su un anello unitario A.

(*i*) Verificare che ω si estende in modo naturale ad un'azione $\overline{\omega}$ su $A[X]$.

(*ii*) Verificare che $\overline{\omega}$ non è mai transitiva, ma anzi ha sempre infinite orbite.

(*iii*) Verificare che $\boldsymbol{St}_{_X}$ (rispetto a $\overline{\omega}$) coincide con $\boldsymbol{St}_{1_{_A}}$.

Esercizio 2.3.10. Sia G un gruppo non abeliano di ordine p^3, con p primo. Verificare che il suo centro $\boldsymbol{Z}(G)$ ha ordine p.

Esercizio 2.3.11. Sia $H \leq G$. Definiamo *centralizzante di* H *in* G l'insieme

$$\mathcal{C}(H) = \{x \in G \mid xh = hx,\ \forall\, h \in H\}.$$

(*i*) Verificare che $\mathcal{C}(H)$ è un sottogruppo di G e che $\mathcal{C}(H) \leq \mathcal{N}(H)$.

(*ii*) Verificare che $\mathcal{C}(H) \trianglelefteq \mathcal{N}(H)$. *Suggerimento*: costruire un opportuno omomorfismo da $\mathcal{N}(H)$ ad $\boldsymbol{Aut}(H)$, di cui $\mathcal{C}(H)$ sia il nucleo.

4. Esistenza di sottogruppi

In questo paragrafo enunciamo e dimostriamo due classici teoremi di esistenza di sottogruppi di un gruppo finito: il *teorema di Cauchy* ed il *teorema di Sylow*. Come vedremo, le dimostrazioni fanno uso del concetto di azione, presentato nel paragrafo precedente.

Teorema 4.1. *(Cauchy) Sia G un gruppo finito di ordine n e sia p un primo tale che $p \mid n$. Allora G possiede un elemento di periodo p (e quindi un sottogruppo ciclico di ordine p).*

Dim. Si tratta di determinare un elemento $x \in G$ tale che $x \neq 1$ e $x^p = 1$. Si definisce l'insieme

$$X = \{(x_1, \dots, x_p) \in G^p \mid \prod_{i=1}^{p} x_i = 1\}.$$

Verifichiamo che $|X| = n^{p-1}$. A tal fine basta determinare una biiezione tra X e G^{p-1}. Si ponga:

$$\alpha : G^{p-1} \to X \text{ tale che } (x_1, \dots, x_{p-1}) \to (x_1, \dots, x_{p-1}, z), \text{ con } z := (\prod_{i=1}^{p-1} x_i)^{-1}.$$

Tale applicazione, come ora verificheremo, ha per inversa

$$\beta : X \to G^{p-1} \text{ tale che } (x_1, \dots, x_p) \to (x_1, \dots, x_{p-1}).$$

Infatti, che risulti $\beta \circ \alpha = \mathbf{1}_{G^{p-1}}$ è ovvio. Viceversa, per provare che $\alpha \circ \beta = \mathbf{1}_X$, si osservi che, $\forall \underline{x} = (x_1, \dots, x_p) \in X$, $(\alpha \circ \beta)(\underline{x}) = (x_1, \dots, x_{p-1}, z)$, con $\prod_{i=1}^{p-1} x_i \cdot z = 1 = \prod_{i=1}^{p-1} x_i \cdot x_p$. Ne segue che $z = x_p$ e quindi $(\alpha \circ \beta)(\underline{x}) = \underline{x}$.

Facciamo ora agire su X il gruppo $(\boldsymbol{Z}_p, +)$, ponendo:

$$\omega : \boldsymbol{Z}_p \times X \to X \text{ tale che } \omega(\overline{t}, \underline{x}) = (x_{t+1}, \dots, x_p, x_1, \dots, x_t),$$

$\forall \underline{x} = (x_1, \dots, x_p) \in X$ e $\forall \overline{t} \in \boldsymbol{Z}_p$, con rappresentante $t \in [0, p-1]$. In pratica, $\omega(\overline{t}, \underline{x})$ trasla le componenti di $\underline{x}$ di t posti verso sinistra. Si noti che, essendo $(x_1 \dots x_t)(x_{t+1} \dots x_p) = 1$, anche $(x_{t+1} \dots x_p)(x_1 \dots x_t) = 1$, cioè $\omega(\overline{t}, \underline{x}) \in X$. Risulta subito:

$$\omega(\overline{0}, \underline{x}) = \underline{x}, \quad \omega(\overline{s}, \omega(\overline{t}, \underline{x})) = \omega(\overline{s+t}, \underline{x}), \ \forall \underline{x} \in X, \ \forall \overline{s}, \overline{t} \in \boldsymbol{Z}_p,$$

e quindi ω è effettivamente un'azione (che chiameremo *azione di traslazione sinistra su* X).

Per ogni $\underline{x} \in X$, $p = |\boldsymbol{Z}_p| = |\boldsymbol{O}(\underline{x})| \cdot |\boldsymbol{St}_{\underline{x}}|$ e dunque $|\boldsymbol{O}(\underline{x})| \mid p$. Si hanno due possibilità:

$$|\boldsymbol{O}(\underline{x})| = 1 \text{ oppure } |\boldsymbol{O}(\underline{x})| = p.$$

Ad esempio, per l'elemento $\underline{\mathbf{1}} = (1, 1, \dots, 1) \in X$ risulta subito che $\boldsymbol{O}(\underline{\mathbf{1}}) = \{\underline{\mathbf{1}}\}$, cioè $|\boldsymbol{O}(\underline{\mathbf{1}})| = 1$.

Affermiamo che $\exists \underline{x} \in X$, $\underline{x} \neq \underline{\mathbf{1}}$, tale che $|\boldsymbol{O}(\underline{x})| = 1$. Altrimenti, se per assurdo fosse $|\boldsymbol{O}(\underline{x})| = p$, $\forall \underline{x} \in X$, $\underline{x} \neq \underline{\mathbf{1}}$, si avrebbe:

$$|X| = \sum |\boldsymbol{O}(\underline{x})| = 1 + ph, \ \exists h \in \boldsymbol{N}.$$

Ma $p \mid n$ e quindi $p \mid n^{p-1} = |X|$. Pertanto $p \mid 1 + ph$, cioè $p \mid 1$: assurdo.

Sia dunque $\underline{x} \in X$, $\underline{x} \neq \underline{\mathbf{1}}$, con $|\boldsymbol{O}(\underline{x})| = 1$, cioè $\boldsymbol{O}(\underline{x}) = \{\underline{x}\}$. Ne segue che $\omega(\overline{1}, \underline{x}) = \underline{x}$, cioè

$$(x_2, x_3, \dots x_p, x_1) = (x_1, x_2, x_3, \dots x_p).$$

Ma allora $x_2 = x_1$, $x_3 = x_2, \dots, x_p = x_{p-1}$, $x_1 = x_p$ e pertanto $x_1 = x_2 = \dots = x_p$. Posto quindi $x = x_1 (= x_2 = \dots = x_p)$, abbiamo determinato un elemento $x \in G$, $x \neq 1$, tale che $x^p = 1$, come richiesto.

Come conseguenza del teorema di Cauchy dimostriamo il seguente risultato sui p-gruppi.

Corollario 4.1. *Se G è un p-gruppo di ordine p^n, G ammette una catena di $n+1$ sottogruppi*

$$H_0 = \{1\} < H_1 < \dots < H_n = G,$$

tali che: $H_i \lhd H_{i+1}$ e $\left|H_{i+1}/_{H_i}\right| = p$, $\forall i = 0, \dots, n-1$.

In particolare quindi $|H_i| = p^i$ e G ammette un sottogruppo normale di indice p (cioè H_{n-1}).

Dim. Per induzione su n. Se $n = 1$, la tesi è ovvia, con catena $\{1\} < G\ (\cong C_p)$.

Sia $n > 1$ ed assumiamo vero l'asserto per ogni p-gruppo di ordine p^{n-1}. In base a Coroll. **3.2**, G ha centro $\boldsymbol{Z}(G)$ non banale. Poiché $\boldsymbol{Z}(G)$ è un p-gruppo, in base al Teorema di Cauchy $\boldsymbol{Z}(G)$ contiene un sottogruppo H_1 di ordine p. Poiché $H_1 < \boldsymbol{Z}(G)$, allora $aH_1 = H_1 a,\ \forall a \in G$, e quindi $H_1 \triangleleft G$. Allora G/H_1 è un p-gruppo di ordine p^{n-1} e ad esso si applica l'ipotesi induttiva. Esiste quindi una catena di n suoi sottogruppi:

$$\{\overline{1}\} = H_1/H_1 < H_2/H_1 < \ ... \ < H_{n-1}/H_1 < H_n/H_1 = G/H_1,$$

dove $H_i/H_1 \triangleleft H_{i+1}/H_1$ e $\left| \dfrac{H_{i+1}/H_1}{H_i/H_1} \right| = p,\ \forall\ i = 1, ..., n-1.$

In base al teorema di corrispondenza [applicato alla proiezione canonica $H_{i+1} \to H_{i+1}/H_1$], segue che $H_i \triangleleft H_{i+1}$ e quindi, dal terzo teorema di isomorfismo [applicato ai sottogruppi H_1, H_i di H_{i+1}], $\left|H_{i+1}/H_i\right| = p$. Allora $\{1\} < H_1 < \ ... \ < H_{n-1} < H_n = G$ è la catena di sottogruppi cercata.

L'ultima affermazione è ovvia.

Per enunciare il teorema di Sylow occorre la definizione di *p-sottogruppo di Sylow.*

Definizione 4.1. *Sia G un gruppo finito di ordine $p^r m$, con p primo, $r \geq 1$ e p, m coprimi. Ogni (eventuale) sottogruppo di G di ordine p^r è detto p-sottogruppo di Sylow di G, o, più brevemente, p-Sylow di G.*

Teorema 4.2. *(Sylow) Sia G un gruppo finito di ordine $p^r m$, con p primo, $r \geq 1$ e p, m coprimi.*

(1) G contiene un p-Sylow.

(2) - Ogni p-gruppo di G è contenuto in almeno un p-Sylow.

- Due p-Sylow di G sono coniugati.

(3) Il numero s dei p-Sylow di G verifica le due seguenti condizioni:

$$s \mid m; \qquad s \equiv 1\ (mod\ p).$$

Tradizionalmente (*1*), (*2*), (*3*) vengono chiamati rispettivamente *primo, secondo* e *terzo teorema di Sylow.* Cominciamo col dimostrare il primo teorema di Sylow.

Dim. *(Primo teorema di Sylow).* Sia

$$X = \{\text{sottoinsiemi di } G \text{ di cardinalità } p^r\}.$$

Da **Alg. 1** è ben noto che $|X| = \binom{p^r m}{p^r}$. Affermiamo che risulta:

(∗) $\qquad p \nmid \binom{p^r m}{p^r}$

[e lo proveremo alla fine di questa dimostrazione]. Definiamo la seguente azione di G su X:

$$G \times X \to X \ \text{ tale che } \ (g, U) \to g \cdot U,\ \ \forall g \in G,\ \forall U \in X,$$

con $g \cdot U = \{gt,\ \forall t \in U\}$. Si tratta dell'azione indotta su X dalla moltiplicazione (a sinistra) di G (cfr. Esercizio **2.3.2**(*ii*)); si noti che $|g \cdot U| = |U| = p^r$ e quindi $g \cdot U \in X$, come richiesto. Basterà dimostrare che esiste un sottoinsieme $U \in X$ tale che $|\boldsymbol{St}_U| = p^r$: pertanto $\boldsymbol{St}_U$ è un p-Sylow (e la dimostrazione è conclusa).

Verifichiamo subito che, $\forall U \in X$, risulta $|\boldsymbol{St}_U| \leq p^r$. Infatti, scelto un elemento $x \in U$, si ha che $\boldsymbol{St}_U\, x \subseteq U$ [essendo, $\forall g \in \boldsymbol{St}_U,\ gx \in g \cdot U = U$]. Dunque $|\boldsymbol{St}_U| = |\boldsymbol{St}_U\, x| \leq |U| = p^r$.

Possiamo poi affermare che esiste almeno un sottoinsieme $U \in X$ tale che $p \nmid |\boldsymbol{O}(U)|$ [altrimenti $p \mid \sum |\boldsymbol{O}(U)| = |X| = \binom{p^r m}{p^r}$, mentre da (∗) sappiamo che $p \nmid \binom{p^r m}{p^r}$]. Scegliamo un siffatto U.

Poiché $|\boldsymbol{O}(U)| \cdot |\boldsymbol{St}_U| = p^r m$ (cfr. Teor. **3.1**) e poiché $MCD(p^r, |\boldsymbol{O}(U)|) = 1$, dal lemma di Euclide segue che $p^r \mid |\boldsymbol{St}_U|$. Ma allora $p^r \leq |\boldsymbol{St}_U| \leq p^r$ e dunque $|\boldsymbol{St}_U| = p^r$, come richiesto.

Resta da dimostrare $(*)$. A tale scopo è sufficiente verificare che $\binom{p^r m}{p^r} \equiv m \ (mod\ p)$. [Ne segue subito infatti che, essendo $m \not\equiv 0 \ (mod\ p)$, allora anche $\binom{p^r m}{p^r} \not\equiv 0 \ (mod\ p)$, cioè $p \not| \binom{p^r m}{p^r}$].

Osserviamo che in $\boldsymbol{Z}_p[X]$ risulta: $(1+X)^{p^r} = 1+X^{p^r}$. Ne segue che $(1+X)^{p^r m} = (1+X^{p^r})^m$. Sviluppando tali potenze di binomio si ottiene, in $\boldsymbol{Z}_p[X]$:

$$\sum_{h=0}^{p^r m} \binom{p^r m}{h} X^h = \sum_{k=0}^{m} \binom{m}{k} (X^{p^r})^k .$$

In particolare, confrontando gli addendi di grado p^r, si ottiene $\binom{p^r m}{p^r} X^{p^r} = \binom{m}{1} X^{p^r}$ e quindi $\binom{p^r m}{p^r} \equiv m \ (mod\ p)$, come richiesto.

Osservazione 4.1. Verifichiamo che il teorema di Cauchy è ottenibile come semplice corollario del primo teorema di Sylow.

Sia p un primo tale che $p \,|\, |G|$: si tratta di verificare che esiste $y \in G$ con $\circ(y) = p$. Se $|G| = p^r m$, con $r \geq 1$ e $MCD(p, m) = 1$, per il primo teorema di Sylow, esiste un p-Sylow H (di ordine p^r). Per ogni $x \in H$, $x \neq 1$, risulta: $1 = x^{|H|} = x^{p^r}$. Dunque $\circ(x) \,|\, p^r$, cioè $\circ(x) = p^s$, con $1 \leq s \leq r$. Considerato in H l'elemento $y := x^{p^{s-1}}$, risulta: $y \neq 1$ [in quanto $1 \leq p^{s-1} < \circ(x)$] e $y^p = 1$ [in quanto $(x^{p^{s-1}})^p = x^{p^s} = 1$]. Dunque $\circ(y) = p$, come richiesto.

Dim. *(Secondo teorema di Sylow).* (a) Dimostriamo la prima affermazione: se H è un p-gruppo in G, con $|H| = p^h$ $(1 \leq h \leq r)$, bisogna determinare un p-Sylow T contenente H.

Denotiamo con Y l'insieme dei p-Sylow di G [Y è non vuoto in base al primo teorema di Sylow]. Osserviamo subito che G agisce su Y per coniugio, cioè che

$$\omega : G \times Y \to Y, \ \text{tale che} \ \omega(g, S) = g * S = gSg^{-1}, \ \forall\, g \in G, \ \forall\, S \in Y,$$

è un'azione di G su Y [infatti gSg^{-1} è un gruppo dello stesso ordine di S e dunque è un p-Silow]. Per ogni $S \in Y$, si ha:

- $\boldsymbol{O}(S) = \{gSg^{-1}, \ \forall\, g \in G\}$ [è l'insieme dei coniugati di S];
- $\boldsymbol{St}_S = \{g \in G \mid gS = Sg\} = \mathcal{N}(S)$ [è il normalizzante di S in G, cfr. Esercizio **2.3.3**].

Poiché $S \trianglelefteq \mathcal{N}(S)$, esiste il gruppo quoziente $\mathcal{N}(S)/_S$ e ovviamente risulta: $|\mathcal{N}(S)/_S| = \frac{|\mathcal{N}(S)|}{|S|}$. Verifichiamo che $|\boldsymbol{O}(S)| \cdot |\mathcal{N}(S)/_S| = m$ [e pertanto $|\boldsymbol{O}(S)|$ e $|\mathcal{N}(S)/_S|$ sono divisori di m]. Infatti, dal Teor. **3.1**, $|\boldsymbol{O}(S)| \cdot |\mathcal{N}(S)| = |G|$. Dividendo per $|S|$, $|\boldsymbol{O}(S)| \cdot \frac{|\mathcal{N}(S)|}{|S|} = \frac{|G|}{|S|} = \frac{p^r m}{p^r} = m$ e quindi $|\boldsymbol{O}(S)| \cdot |\mathcal{N}(S)/_S| = m$.

Fissiamo arbitrariamente un p-Silow S e consideriamone l'orbita $\boldsymbol{O}(S) \subseteq Y$. L'azione ω sopra definita può essere ristretta a $H \times \boldsymbol{O}(S)$ (cfr. Esempi **3.3** e **3.4**). È quindi definita l'azione

$$\omega' : H \times \boldsymbol{O}(S) \to \boldsymbol{O}(S), \ \text{tale che} \ \omega'(h, T) = h * T, \ \ \forall\, h \in H, \ \forall\, T \in \boldsymbol{O}(S)$$

[si rilevi che, $\forall\, h \in H, \ \forall\, T = g * S \in \boldsymbol{O}(S)$: $h * T = hTh^{-1} = hgSg^{-1}h^{-1} = hg * S \in \boldsymbol{O}(S)$].

Per ogni $T \in \boldsymbol{O}(S)$, denotiamo con $\boldsymbol{O}'(T)$ l'orbita di tale azione. Dunque $|\boldsymbol{O}(S)| = \sum_{T \in ..} |\boldsymbol{O}'(T)|$ [dove la somma è estesa ad un solo rappresentante di ogni orbita di ω'] .

Poiché $|H| = |\boldsymbol{O}'(T)| \cdot |\boldsymbol{St}'_T|$, allora $|\boldsymbol{O}'(T)| \,|\, p^h$, cioè $|\boldsymbol{O}'(T)| = p^{h_T}$, con $0 \leq h_T \leq h$. Possiamo affermare che almeno un'orbita $\boldsymbol{O}'(T)$ è formata da un solo elemento [cioè il p-Silow T]. Infatti, in caso contrario, essendo ogni $h_T > 0$, risulterebbe: $|\boldsymbol{O}(S)| = \sum_{T \in ..} p^{h_T} = p\ell$ (per un opportuno $\ell \in \boldsymbol{N}$). Dunque $p \,|\, |\boldsymbol{O}(S)|$ e, come sopra osservato, $|\boldsymbol{O}(S)| \,|\, m$. Allora $p \,|\, m$: assurdo.

Scelto un siffatto p-Silow T, verificheremo che $H \cap T = H$, da cui seguirà che $H \subseteq T$ e la dimostrazione sarà conclusa. Essendo $\boldsymbol{O}'(T) = \{T\}$, $h * T = T$, $\forall\, h \in H$, cioè $H \subseteq \boldsymbol{St}_T = \mathcal{N}(T)$. Ovviamente $T \trianglelefteq \mathcal{N}(T)$ e quindi è definito nel gruppo quoziente $\mathcal{N}(T)/_T$ il sottogruppo $HT/_T$. L'ordine di tale sottogruppo è un divisore dell'ordine di $\mathcal{N}(T)/_T$ e quindi, per quanto sopra osservato, è un divisore di m. Ma, in base al secondo teorema di isomorfismo,

$$HT/_T \cong H/_{H \cap T}$$

e l'ordine di $H/_{H\cap T}$ è un divisore di $|H|$, cioè un divisore di p^h. Poiché m, p^h sono coprimi, allora $|H/_{H\cap T}| = 1$, cioè $H \cap T = H$, come richiesto.

(b) Dimostriamo ora che due p-Sylow sono coniugati [cioè che l'azione ω è transitiva]. Siano S, T due p-Sylow: va verificato che $T \in \boldsymbol{O}(S)$. Osservato che T è un p-gruppo e scelto $S \in Y$, consideriamo l'azione $\omega' = \omega_{|_{T\times \boldsymbol{O}(S)}}$. Dalla dimostrazione di (a), esiste $T_1 \in \boldsymbol{O}(S)$ tale che $T \subseteq T_1$. Ma, per ragioni di cardinalità, $T = T_1$ e dunque $T \in \boldsymbol{O}(S)$, come richiesto.

Osservazione 4.2. (i) Dal secondo teorema di Sylow segue subito che se un p-Sylow S di G è normale in G, allora è l'unico p-Sylow di G. Se infatti S' è un altro p-Sylow di G, allora $S' = gSg^{-1}$, $\exists\, g \in G$. Ma, essendo S normale in G, $gSg^{-1} = S$ e quindi $S' = S$.

Vale ovviamente anche il viceversa [infatti ogni sottogruppo unico del proprio ordine è normale].

(ii) Sempre dalla precedente dimostrazione evidenziamo il fatto che il numero dei p-Sylow di G è l'indice del normalizzante $\mathcal{N}(S)$ di un qualsiasi p-Sylow S. Infatti:

$$|Y| = |\boldsymbol{O}(S)| = (G : \mathcal{N}(S)).$$

Dim. *(Terzo teorema di Sylow).* Nella dimostrazione del secondo teorema di Sylow abbiamo provato che, fissato un p-Sylow S, $|\boldsymbol{O}(S)| \,\big|\, m$. Inoltre abbiamo provato che l'azione ω è transitiva. Pertanto:

$$s := |Y| = |\boldsymbol{O}(S)| \,\big|\, m.$$

Resta da verificare che $s \equiv 1\ (mod\ p)$. Denotiamo con $\omega' : S \times Y \to Y$ l'azione ω ristretta al sottogruppo S. Si tratta della stessa azione ω' considerata nella dimostrazione della parte (a) del secondo teorema di Sylow [con $H = S$]. Ovviamente, $\forall\, T \in Y$, $|\boldsymbol{O}'(T)| \,\big|\, |S| = p^r$ e dunque $|\boldsymbol{O}'(T)| = p^{h_T}$, con $0 \le h_T \le r$. Se dimostriamo che un unico p-Sylow $T \in Y$ ha orbita $\boldsymbol{O}'(T)$ di cardinalità 1, allora:

$$s = |Y| = \sum_{T\in..} |\boldsymbol{O}'(T)| = \sum_{T\in..} p^{h_T} = 1 + p(...) \ \text{ e quindi } \ s \equiv 1\ (mod\ p).$$

Nella dimostrazione della parte (a) del secondo teorema di Sylow abbiamo provato che esiste almeno un p-Sylow T tale che $\boldsymbol{O}'(T) = \{T\}$. Siano ora $T, T' \in Y$, tali che $\boldsymbol{O}'(T) = \{T\}$ e $\boldsymbol{O}'(T') = \{T'\}$. Per ogni $x \in S$, $x{*}T = T$ e $x{*}T' = T'$, da cui $xT = Tx$, $xT' = T'x$ e quindi $x \in \mathcal{N}(T)$, $x \in \mathcal{N}(T')$. Pertanto $S \le \mathcal{N}(T)$, $S \le \mathcal{N}(T')$.

Da $S \le \mathcal{N}(T) \le G$ segue che $|\mathcal{N}(T)| = p^r v$, con $v \,\big|\, m$. Pertanto S è un p-Sylow anche di $\mathcal{N}(T)$. Poiché però anche T è un p-Sylow di $\mathcal{N}(T)$ ed è normale in $\mathcal{N}(T)$, allora [cfr. Osserv. **4.2**(i)] T è l'unico p-Sylow di $\mathcal{N}(T)$ e quindi $T = S$. Le stesse considerazioni svolte per $\mathcal{N}(T')$ portano a provare che $T' = S$. Allora $T = T'$, come richiesto.

Corollario 4.2. *A meno di isomorfismi, esiste un unico gruppo di ordine* 15.

Dim. Sia $|G| = 15$. Poiché $15 = 3{\cdot}5$, G ammette un 3-Sylow ed un 5-Sylow, di ordini rispettivamente 3 e 5. Sia poi r il numero dei 3-Sylow ed s il numero dei 5-Sylow in G. Dal terzo teorema di Sylow si ha:

$$r \,\big|\, 5,\ r \equiv 1\ (mod\ 3); \qquad s \,\big|\, 3,\ s \equiv 1\ (mod\ 5).$$

Ne segue subito che $r = s = 1$.

Sia quindi H l'unico 3-Sylow e K l'unico 5-Sylow di G. Entrambi sono normali, in quanto unici del rispettivo ordine. Risulta inoltre che $H \cap K = \{1\}$ [in quanto $|H \cap K|$ divide sia 3 che 5] e $HK = G$ [in quanto $HK \supset K$]. Dal Teor. **2.1** $G \cong H \times K$ e dal Coroll. **2.1**, G è ciclico di ordine 15. Abbiamo così provato che esiste, a meno di isomorfismi, un solo gruppo di ordine 15: il gruppo ciclico $\boldsymbol{C}_{15}$ [o $\boldsymbol{Z}_{15}$].

Corollario 4.3. *Ogni gruppo G di ordine* 30 *possiede un unico* 3*-Sylow ed un unico* 5*-Sylow.*

Dim. Utilizziamo il terzo teorema di Sylow. Si ha, posto $s :=$ numero dei 3-Sylow e $t :=$ numero dei 5-Sylow:

$$s \,\big|\, 10 \ \text{ e } \ s \equiv 1\ (mod\ 3); \quad t \,\big|\, 6 \ \text{ e } \ t \equiv 1\ (mod\ 5).$$

Ne segue: $s = 1$ oppure $s = 10$, $t = 1$ oppure $t = 6$.

Dimostriamo che $t = 1$. Per assurdo, sia $t = 6$. Dunque G possiede sei sottogruppi ciclici di ordine 5 e quindi 24 elementi di periodo 5. Se fosse $s = 10$, G avrebbe anche 20 elementi di periodo 3 [i generatori dei dieci sottogruppi ciclici di ordine 3] e quindi almeno $20 + 24 > 30$ elementi: assurdo. Assumiamo allora $s = 1$. In tal caso G possiede un solo sottogruppo ciclico di ordine 3, che denotiamo H (ed è normale in G). Scelto un 5-Sylow K, HK è un sottogruppo di G di ordine 15 [infatti, da $HK/_H \cong K/_{H\cap K} = K/_{\{1\}}$, segue che $|HK| = |H|\cdot|K| = 15$]. Dal Coroll. **4.2** segue che HK è ciclico. Allora G possiede $\varphi(15) = 8$ elementi di periodo 15 e quindi almeno $24 + 8 > 30$ elementi: assurdo.

Dimostriamo ora che anche $s = 1$. Per assurdo sia $s = 10$ e siano $K_1, \dots, K_{10}$ i 3-Sylow di G. Sia H l'unico 5-Sylow di G (normale in G). Come sopra, dall'isomorfismo $HK_1/_H \cong K_1/_{H\cap K_1}$ segue che HK_1, ha ordine 15 (e dunque è ciclico). Ne segue che G contiene: venti elementi di periodo 3, quattro elementi di periodo 5 e $\varphi(15) = 8$ elementi di periodo 15. In tutto si tratta di $20 + 4 + 8 > 30$ elementi: assurdo.

Abbiamo quindi provato che $s = t = 1$.

Nota. In base al terzo teorema di Sylow, il numero r dei 2-Sylow di un gruppo G di ordine 30 è uno dei seguenti quattro: $r = 1, 3, 5, 15$. Esistono effettivamente gruppi di ordine 30 corrispondenti a siffatti valori di r. Sono (rispettivamente): $\boldsymbol{C}_{30}$, $\boldsymbol{C}_5\times\boldsymbol{S}_3$, $\boldsymbol{C}_3\times\boldsymbol{D}_5$ e $\boldsymbol{D}_{15}$.

Corollario 4.4. *A meno di isomorfismi, esistono due soli gruppi di ordine* 21*:*

$$\boldsymbol{C}_{21}\ (\cong \boldsymbol{C}_3\times\boldsymbol{C}_7)\ \text{ e }\ \langle x, y \,|\, x^7 = y^3 = 1,\ yx = x^2y\rangle.$$

Dim. Sia $|G| = 21$. Dal teorema di Sylow, G contiene un unico 7-Sylow $K = \langle x \,|\, x^7 = 1\rangle$ ed almeno un 3-Sylow $H = \langle y \,|\, y^3 = 1\rangle$. Conseguentemente G contiene i seguenti 21 elementi:

$$1,\ x,\ x^2,\ x^3,\ x^4,\ x^5,\ x^6,\ y,\ xy,\ x^2y,\ x^3y,\ x^4y,\ x^5y,\ x^6y,\ y^2,\ xy^2,\ x^2y^2,\ x^3y^2,\ x^4y^2,\ x^5y^2,\ x^6y^2.$$

Tali elementi sono a due a due distinti [si verifichi che se $x^h y^i = x^k y^j$ (con $0 \le h, k \le 6$, $0 \le i, j \le 2$), allora $h = k$ e $i = j$] e dunque costituiscono esattamente il gruppo G.

Ora esaminiamo in G il prodotto yx, che coincide con uno di tali elementi. Poiché $K \lhd G$, si ha:

$$yxy^{-1} \in yKy^{-1} = K \ \text{ e quindi } \ yxy^{-1} = x^k,\ \text{ con } \ 0 \le k \le 6.$$

Ne segue:

$$x^{k^2} = (x^k)^k = (yxy^{-1})(yxy^{-1}) \dots (yxy^{-1}) = yx^k y^{-1} \quad \text{e}$$
$$x^{k^3} = (x^{k^2})^k = (yx^k y^{-1})(yx^k y^{-1}) \dots (yx^k y^{-1}) = yx^{k^2} y^{-1}.$$

Poiché $y^3 = 1$, si ha:

$$x = y^3 x\, y^{-3} = y^2(yxy^{-1})y^{-2} = y^2x^k y^{-2} = y(yx^k y^{-1})y^{-1} = y\, x^{k^2} y^{-1} = x^{k^3}.$$

Da $x = x^{k^3}$ segue che $k^3 \equiv 1\ (mod\ 7)$ e dunque, risolvendo tale congruenza, $k = 1, 2, 4$. Pertanto

$$yxy^{-1} = \begin{cases} x \\ x^2 \\ x^4 \end{cases} \quad \text{e quindi} \quad yx = \begin{cases} xy \\ x^2y \\ x^4y. \end{cases}$$

Se $yx = xy$, G è abeliano. Quindi $H \lhd G$ e, poiché ovviamente $H \cap K = \{1\}$ e $HK \supset H$, allora $G = HK \cong H\times K \cong \boldsymbol{C}_3\times\boldsymbol{C}_7 \cong \boldsymbol{C}_{21}$.

Se invece $yx = x^2y$, allora $G = \langle x, y \,|\, x^7 = y^3 = 1,\ yx = x^2y\rangle$.

Sia infine $yx = x^4y$. In tal caso possiamo subito provare che $y^2x = x^2y^2$. Infatti risulta:

$$y^2x = yx^4y = yx\,x^3y = x^4yx^3y = x^4x^4yx^2y = x\,yx\,xy = x^5yxy = x^9y^2 = x^2y^2.$$

Poiché y^2 è l'altro generatore di H, posto $z = y^2$, si ottiene che $G = \langle x, z \,|\, x^7 = z^3 = 1,\ zx = x^2z\rangle$. Tale gruppo è ovviamente isomorfo a quello considerato nel caso precedente.

Concludendo, i gruppi di ordine 21 sono soltanto due: $\boldsymbol{C}_{21}$ e G.

Nota. Si può subito osservare che G ha sette 3-Sylow [infatti si verifica che ha 14 elementi di periodo 3].

Osservazione 4.3. Concludiamo l'argomento citando un'altra semplice applicazione del teorema di Sylow, per la cui dimostrazione rinviamo ad esempio ad [Artin], Ch. **6**, § **5**.

A meno di isomorfismi, esistono cinque gruppi di ordine 12 *e cioè:*

$\boldsymbol{C}_{12}$ $(\cong \boldsymbol{C}_3 \times \boldsymbol{C}_4)$, $\boldsymbol{V} \times \boldsymbol{C}_3$ $(\cong \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_3)$, $\boldsymbol{A}_4$, $\boldsymbol{D}_6$, $\langle x, y \mid x^4 = y^3 = 1,\ xy = y^2x \rangle$.

* * * * * * * * * * * * * * * * * *

Esercizio 2.4.1. Quanti sono, a meno di isomorfismi, i gruppi di ordine 33 ?

Esercizio 2.4.2. Sia G un gruppo di ordine 20.

(*i*) Dimostrare che G ha un unico sottogruppo normale di ordine 5.

(*ii*) Quanti e quali sottogruppi di ordine 4 può ammettere ?

Esercizio 2.4.3. Determinare tutti i sottogruppi di ordine 8 di $\boldsymbol{S}_4$.

Esercizio 2.4.4. È assegnato il gruppo $G = \langle x, y \mid x^4 = y^3 = 1,\ xy = y^2x \rangle$.

(*i*) Scriverne i dodici elementi e di ciascuno indicare il periodo.

(*ii*) Dall'esame dei periodi degli elementi di G dedurre che G ha soltanto sottogruppi ciclici e determinarne il reticolo.

Esercizio 2.4.5. È assegnato il gruppo "diciclico" $\mathbf{Q}_4 = \langle x, y \mid x^4 = 1;\ y^2 = x^2 = (xy)^2 \rangle$.

(*i*) Verificare che $|\mathbf{Q}_4| = 8$ e individuarne gli elementi.

(*ii*) Dimostrare che $\mathbf{Q}_4 \cong \mathbf{Q}$ (gruppo delle unità dei quaternioni).

Esercizio 2.4.6. Tenuto conto della classificazione dei gruppi di ordine 12 (cfr. Osserv. **4.3**), dimostrare che $\boldsymbol{S}_3 \times \boldsymbol{C}_2 \cong \boldsymbol{D}_6$ ed esplicitare un isomorfismo tra i due gruppi.

Esercizio 2.4.7. Verificare che un gruppo G di ordine 30 non è semplice e contiene un sottogruppo di indice 2.

Esercizio 2.4.8. Perché un gruppo G di ordine 12 non può avere contemporaneamente tre 2-Sylow e quattro 3-Sylow ?

Esercizio 2.4.9. Assegnato il gruppo G, prodotto diretto di $\boldsymbol{S}_3$ per se stesso, determinare i sottogruppi di Sylow di G. [Si ponga $\boldsymbol{S}_3 = \langle x,\ y \,\big|\, x^2 = y^3 = 1,\ yx = xy^2 \rangle$].

Esercizio 2.4.10. (*i*) Se $|G| = p\,q$, con p, q primi, verificare che G non è semplice.

(*ii*) Se $|G| = pq$, con $p < q$ e $q \not\equiv 1 \ (mod\, p)$, verificare che G è ciclico.

Esercizio 2.4.11. Sia S un p-Sylow di un gruppo (finito) G. Verificare che $\mathcal{N}(\mathcal{N}(S)) = \mathcal{N}(S)$.

Esercizio 2.4.12. Sia p un primo e G un gruppo finito. Verificare che

$$G \text{ è } p\text{-gruppo} \iff \forall\, x \in G,\ \circ(x) \text{ è una potenza di } p.$$

5. Gruppi abeliani finiti

Proveremo in questo conclusivo paragrafo un risultato che ci permetterà di determinare tutti i gruppi abeliani finiti, rappresentandoli, a meno di isomorfismo, come prodotto diretto di un numero finito di gruppi ciclici.

Cominciamo con l'estendere la definizione di prodotto diretto (e le relative proprietà) dal caso di due fattori al caso di n fattori.

Definizione 5.1. *Assegnati i gruppi $G_1, G_2, \dots, G_n$, si chiama prodotto diretto di $G_1, G_2, \dots, G_n$ il prodotto cartesiano $G_1 \times G_2 \times \dots \times G_n$ dotato della seguente operazione:*

$$(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

Si verificano immediatamente gli assiomi di gruppo.

Vale un analogo del Teor. **2.1**, relativo ai gruppi che sono prodotto diretto di un numero finito di loro sottogruppi.

Teorema 5.1. *Siano $H_1, H_2, \dots, H_n$ sottogruppi di un gruppo G, tali che:*

(i) $H_1, H_2, \dots, H_n$ sono normali in G;

(ii) il sottogruppo prodotto $H_1 H_2 \dots H_n$ coincide con G;

(iii) $H_i \cap \big(\prod_{j \neq i} H_j\big) = \{1\}, \quad \forall\, i = 1, 2, \dots n.$

Allora $G \cong H_1 \times H_2 \times \dots \times H_n$.

Dim. Si ponga: $\varphi : H_1 \times H_2 \times \dots \times H_n \to G$ tale che

$$\varphi\big((h_1, h_2, \dots, h_n)\big) = h_1 h_2 \dots h_n, \quad \forall\, (h_1, h_2, \dots, h_n) \in H_1 \times H_2 \times \dots \times H_n.$$

Si tratta di verificare che φ è un'applicazione iniettiva e suriettiva ed è un omomorfismo.

Si ponga, $\forall\, i = 1, 2, \dots n$, $T_i := \prod_{j \neq i} H_j$. Si osserva subito:

(a) $T_i \trianglelefteq G$. Infatti, $\forall\, x \in G$, si ha (in base a (i)):

$$xT_i = x(H_1 \dots \not{H}_i \dots H_n) = (H_1 x) H_2 \dots \not{H}_i \dots H_n = H_1 (x H_2) \dots \not{H}_i \dots H_n = H_1 H_2 (x H_3) \dots \not{H}_i \dots H_n =$$
$$= \dots = H_1 \dots \not{H}_i \dots (x H_n) = H_1 \dots \not{H}_i \dots (H_n x) = T_i x.$$

(b) $H_i T_i = G$. Infatti i gruppi H_i (essendo normali in G) permutano tra loro. Dunque $H_i T_i = H_i H_1 \dots \not{H}_i \dots H_n = H_1 \dots H_i \dots H_n = G$.

(c) $H_i \cap T_i = \{1\}$. [È l'ipotesi (iii)].

Dal Teor. **2.1** segue che, $\forall\, i = 1, 2, \dots n$, le applicazioni

$$\varphi_i : H_i \times T_i \to G, \text{ tale che } \varphi_i(h_i, h_1 h_2 \dots \not{h}_i \dots h_n) = h_i\, h_1 h_2 \dots \not{h}_i \dots h_n,$$

sono isomorfismi di gruppi. [In particolare $\varphi_1(h_1, h_2 \dots h_n) = h_1 h_2 \dots h_n = \varphi(h_1, h_2, \dots, h_n)$].

(*1*) Proviamo che φ è suriettiva. Infatti, per ogni $x \in G$, se $x = \varphi_1(h_1, h_2 \dots h_n)$, allora $x = \varphi(h_1, h_2, \dots, h_n)$.

(*2*) Proviamo che φ è iniettiva. Sia

$$\varphi(h_1, h_2, \dots, h_n) = \varphi(k_1, k_2, \dots, k_n).$$

Si tratta di verificare che $h_i = k_i$, $\forall\, i = 1, 2, \dots n$. Poiché φ_1 è un isomorfismo e $\varphi_1(h_1, h_2 \dots h_n) = \varphi_1(k_1, k_2 \dots k_n)$, allora $h_1 = k_1$, $h_2 \dots h_n = k_2 \dots k_n$. Poiché $h_2 \dots h_n = \varphi_2(h_2, 1 \cdot h_3 \dots h_n) = k_2 \dots k_n = \varphi_2(k_2, 1 \cdot k_3 \dots k_n)$ e φ_2 è un isomorfismo, allora $h_2 = k_2$, $h_3 \dots h_n = k_3 \dots k_n$.

Procedendo in modo analogo, $\varphi_3(h_3, 1 \cdot 1 \cdot h_4 \dots h_n) = \varphi_3(k_3, 1 \cdot 1 \cdot k_4 \dots k_n)$ e quindi $h_3 = k_3$, $h_4 \dots h_n = k_4 \dots k_n$. Dopo un numero finito di passi si perviene alla conclusione: $h_i = k_i$, $\forall\, i = 1, 2, \dots n$.

(*3*) Proviamo infine che φ è un omomorfismo e cioè che

$$\varphi\big((h_1, h_2, \dots, h_n)\cdot(k_1, k_2, \dots, k_n)\big) = \varphi\big((h_1, h_2, \dots, h_n)\big)\,\varphi\big((k_1, k_2, \dots, k_n)\big),$$

ovvero

$$h_1k_1\,h_2k_2\dots h_nk_n = h_1h_2\dots h_n\,k_1k_2\dots k_n.$$

Rimarchiamo il fatto che i sottogruppi H_i, T_i permutano elemento per elemento [infatti si ha: $H_i, T_i \trianglelefteq G$; $H_i \cap T_i = \{1\}$; basta quindi ripetere l'argomento contenuto nel punto (c) della dimostrazione di Teor. **2.1** e si ottiene l'asserto]. Si ponga:

$$x := h_1h_2\dots h_n\,k_1k_2\dots k_n,\ \ y := h_1k_1\,h_2k_2\dots h_nk_n.$$

Permutando successivamente $k_1\ (\in H_1)$ con $h_n, \dots, h_2\ (\in T_1)$, si ottiene

$$x = h_1k_1h_2\dots h_n\,k_2\dots k_n.$$

Si permuta ora $k_2\ (\in H_2)$ con $h_n, \dots, h_3\ (\in T_2)$ e si ottiene

$$x = h_1k_1\,h_2k_2\,h_3\dots h_n\,k_3\dots k_n.$$

Si procede in modo analogo con $k_3, \dots, k_{n-1}$ e si conclude che $x = y$.

Un'importante conseguenza del precedente teorema e del secondo teorema di Sylow è il seguente risultato sulla struttura dei gruppi abeliani finiti.

Teorema 5.2. *Sia G un gruppo abeliano finito, non un p-gruppo. Siano $H_1, \dots, H_s$ i suoi sottogruppi di Sylow. Risulta: $G \cong H_1\times H_2\times \dots \times H_s$.*

Dim. Essendo G abeliano, segue dal secondo teorema di Sylow che G possiede un unico p-Sylow, per ogni divisore primo p di $|G|$. Se $|G| = p_1^{r_1}\dots p_s^{r_s}$, con $p_1, \dots, p_s$ primi distinti, denotiamo con $H_1, \dots, H_s$ i sottogruppi di Sylow di G [con $|H_i| = p_i^{r_i}$]. In base al Teor. **5.1**, basterà provare che:

(i) $H_1\dots H_s = G$;

(ii) $H_i \cap \big(\prod_{j\neq i} H_j\big) = \{1\}, \quad \forall\, i = 1, 2, \dots s.$

Dimostriamo (i). Ovviamente $H_1\dots H_s \leq G$. Viceversa, sia $x \in G$. Allora $\circ(x)\,\big|\,|G|$ e quindi $\circ(x) = p_1^{t_1}\dots p_s^{t_s}$, con $0 \leq t_i \leq r_i$. Per ogni $i = 1, \dots, s$, si ponga $q_i := \frac{\circ(x)}{p_i^{t_i}}$. Poiché $MCD(q_1, \dots, q_s) = 1$, esiste un'identità di Bézout:

$$1 = c_1q_1 + \dots + c_sq_s, \ \text{ con } c_1, \dots, c_s \in \boldsymbol{Z}.$$

Ne segue: $x = x^1 = x^{c_1q_1}\dots x^{c_sq_s}$ e basta quindi verificare che $x^{c_iq_i} \in H_i$, per ogni $i = 1, \dots, s$.

Infatti $(x^{q_i})^{p_i^{t_i}} = x^{\circ(x)} = 1$ e dunque $\circ(x^{q_i})\,\big|\,p_i^{t_i}$. Poiché $\circ(x^{c_iq_i})\,\big|\,\circ(x^{q_i})$, allora $\circ(x^{c_iq_i}) = p_i^{\ell_i}$, con $0 \leq \ell_i \leq t_i \leq r_i$. Pertanto $\langle x^{c_iq_i}\rangle$ è un p_i-gruppo e quindi è sottogruppo dell'unico p_i-Sylow H_i. Ciò dimostra che $x^{c_iq_i} \in H_i$, come richiesto.

Dimostriamo ora (ii). Sia $x \in H_i \cap \big(\prod_{j\neq i} H_j\big)$. Da $x \in H_i$ segue che $\circ(x) = p_i^{\ell_i}$, con $0 \leq \ell_i \leq r_i$. Da $x \in \big(\prod_{j\neq i} H_j\big)$ segue che $x = y_1y_2\dots \not{y}_i \dots y_s$, con $y_j \in H_j$. Posto $m_i := p_1^{r_1}\dots p_s^{r_s}\big/_{p_i^{r_i}}$, si ha (essendo $y_i^{p_i^{r_i}} = 1$):

$$x^{m_i} = y_1^{m_i}\dots y_s^{m_i} = 1\cdot\dots\cdot 1 = 1$$

e quindi $p_i^{\ell_i}\,\big|\,m_i$. Si conclude che $\ell_i = 0$, cioè $x = 1$.

Se ora dimostriamo che ogni p-gruppo abeliano è prodotto diretto di gruppi ciclici, possiamo, in virtù del Teor. **5.2**, concludere che ogni gruppo abeliano finito è prodotto diretto di gruppi ciclici. In effetti proveremo tale risultato - per via induttiva - senza far ricorso all'ipotesi che il gruppo abeliano sia un p-gruppo. Ciò rende in qualche modo superfluo il Teor. **5.2** [che resta comunque in sé un risultato significativo ed utile nei calcoli, come subito verificheremo]. Enunciamo il nostro teorema.

Teorema 5.3. *Se G è un gruppo abeliano finito, G è isomorfo ad un prodotto diretto di gruppi ciclici $G_1, \dots, G_t$ $(t \geq 1)$ tali che, posto $|G_i| = e_i$, risulti:*

$$(i)\ \ e_t \,|\, e_{t-1} \,|\, \dots \,|\, e_2 \,|\, e_1; \qquad (ii)\ \ \prod_{i=1}^{t} e_i = |G|.$$

Inoltre i naturali $e_1, \dots, e_t$ *(detti fattori invarianti di* G*) sono univocamente individuati dalle proprietà (i) e (ii).*

Consideriamo ad esempio un gruppo abeliano G di ordine $360\ [= 2^3 \cdot 3^2 \cdot 5]$. In base al Teor. **5.2** $G \cong H \times K \times L$, con $|H| = 8$, $|K| = 9$, $|L| = 5$. Ovviamente $L \cong \boldsymbol{C}_5$ (gruppo ciclico di ordine 5). Relativamente ai gruppi H, K osserviamo quanto segue.

Le possibili liste dei fattori invarianti di H sono le seguenti tre: $\{8\}$, $\{4, 2\}$, $\{2, 2, 2\}$, mentre quelle dei fattori invarianti di K sono le seguenti due: $\{9\}$, $\{3, 3\}$. Conseguentemente H è isomorfo ad uno dei seguenti gruppi:

$$\boldsymbol{C}_8, \quad \boldsymbol{C}_4 \times \boldsymbol{C}_2, \quad \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_2,$$

mentre K è isomorfo ad uno dei seguenti gruppi:

$$\boldsymbol{C}_9, \quad \boldsymbol{C}_3 \times \boldsymbol{C}_3.$$

Si conclude che G è isomorfo (a meno dell'ordine dei fattori) ad uno dei seguenti sei prodotti diretti:

$$\boldsymbol{C}_8 \times \boldsymbol{C}_9 \times \boldsymbol{C}_5\ [\cong \boldsymbol{C}_{360}], \quad \boldsymbol{C}_4 \times \boldsymbol{C}_2 \times \boldsymbol{C}_9 \times \boldsymbol{C}_5, \quad \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_9 \times \boldsymbol{C}_5,$$
$$\boldsymbol{C}_8 \times \boldsymbol{C}_3 \times \boldsymbol{C}_3 \times \boldsymbol{C}_5, \quad \boldsymbol{C}_4 \times \boldsymbol{C}_2 \times \boldsymbol{C}_3 \times \boldsymbol{C}_3 \times \boldsymbol{C}_5, \quad \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_3 \times \boldsymbol{C}_3 \times \boldsymbol{C}_5.$$

Tali gruppi sono manifestamente a due a due non isomorfi [lo si verifica considerandone i periodi degli elementi].

La dimostrazione del Teor. **5.3** necessita di alcuni risultati preliminari: due semplici esercizi (che invitiamo lo studente a risolvere, ma che dimostreremo comunque in conclusione al paragrafo) ed un lemma.

Esercizio 5.1. Sia G un gruppo abeliano e siano $x, y \in G$ elementi di periodo finito.

(*i*) Se x, y hanno periodi coprimi, verificare che $\circ(xy) = \circ(x) \cdot \circ(y)$.

(*ii*) Assumiamo che il gruppo abeliano G sia finito e sia $x \in G$ un elemento di periodo massimo. Verificare che, $\forall\, y \in G,\ \circ(y) \,\big|\, \circ(x)$.

Esercizio 5.2. Sia G un gruppo abeliano e siano H, K due suoi sottogruppi finiti.

(*i*) Verificare che, se $|HK| = |H| \cdot |K|$, allora $HK \cong H \times K$.

(*ii*) Verificare che, se $H \cap K = \{1\}$, allora $HK \cong H \times K$.

Lemma 5.1. *Sia* G *un gruppo abeliano finito e sia* $x \in G$ *un elemento di periodo massimo in* G*. Poniamo:* $h := \circ(x)$ *e* $H := \langle x \rangle$*. Per ogni* $yH \in G/_H$*, se* $\circ(yH) = m$*, esiste* $z \in yH$ *tale che* $\circ(z) = m$*.*

Dim. (Lemma **5.1**). Poniamo $n := \circ(y)$. Si noti che, in base ad Eserc. **5.1**(*ii*), $n \,|\, h$. Per definizione di periodo, $(yH)^m = H$ e quindi $y^m \in H$, cioè $y^m = x^t, \exists\, t \in \boldsymbol{N}$. Ne segue che $\circ(y^m) = \circ(x^t) = \frac{h}{d}$, con $d = MCD(h, t)$. Dimostriamo ora che

$$\circ(y) = m\tfrac{h}{d}.$$

Ricordato che $n = \circ(y)$, si ha:

$$y^{m\frac{h}{d}} = (y^m)^{\frac{h}{d}} = (x^t)^{\frac{h}{d}} = (x^t)^{\circ(x^t)} = 1 \ \text{ e dunque } \ n \,|\, m\tfrac{h}{d}.$$

Viceversa, ricordato che $m = \circ(yH)$, da $(yH)^n = y^n H = 1 \cdot H = H$ segue che $m \,|\, n$. Dunque $n = mq, \exists\, q \in \boldsymbol{N}$. Allora

$$1 = y^n = y^{mq} = (x^t)^q \ \text{ e dunque } \ \tfrac{h}{d} \,|\, q.$$

Ma allora $m\frac{h}{d} \,|\, mq = n$, cioè $m\frac{h}{d} \,|\, n$.

Come inizialmente osservato, $n \,|\, h$. Dunque $m\frac{h}{d} \,|\, h$, da cui subito segue che $m \,|\, d$, ovvero $d = mk, \exists\, k \in \boldsymbol{N}$. Inoltre, siccome $d = MCD(h, t)$, allora $d \,|\, t$, cioè $t = du, \exists\, u \in \boldsymbol{N}$. Segue che

$y^m = x^t = x^{du} = x^{mku}$. Posto ora $z := y\,x^{-ku}$, verifichiamo che z è un elemento cercato. Infatti:

$z \in y\langle x\rangle = yH$;

$\circ(z) \,\big|\, m$. Infatti $z^m = y^m (x^{-ku})^m = x^{mku}\,x^{-kum} = x^0 = 1$;

$m \,\big|\, \circ(z)$. Infatti $(yH)^{\circ(z)} = (zH)^{\circ(z)} = z^{\circ(z)}H = 1\cdot H = H$.

Dim. (Teor. **5.3**). Si procede per induzione su $n = |G|$.

Se $n = 1$, non c'è nulla da dimostrare. Sia quindi $n > 1$ e si scelga in G un elemento g_1 di periodo e_1, massimo in G. Si ponga $G_1 := \langle g_1\rangle$. Il gruppo $G/_{G_1}$ è abeliano, di ordine $\frac{n}{e_1} < n$. Ad esso si applica l'ipotesi induttiva. Dunque

$$G/_{G_1} \cong H_2 \times \ldots \times H_t\,,$$

con H_i ciclico, $H_i = \langle h_i G_1\rangle$, $\circ(h_i G_1) = e_i$, $e_t \,\big|\, e_{t-1} \,\big|\, \ldots \,\big|\, e_3 \,\big|\, e_2$ e $e_2 e_3 \ldots e_t = \frac{n}{e_1}$.

In base al Lemma **5.1**, esistono $g_2, \ldots, g_t \in G$ tali che, $\forall\, i = 2, \ldots, t$,

$$g_i \in h_i G_1 \ \text{ [ovvero } g_i G_1 = h_i G_1\text{]} \ \text{ e } \ \circ(g_i) = e_i\,.$$

Si ponga ora $H := \langle g_2\rangle\langle g_3\rangle \ldots \langle g_t\rangle$. Si tratta di verificare:

$$(a)\ \ H \cong \langle g_2\rangle \times \langle g_3\rangle \times \ \ldots\ \times \langle g_t\rangle; \qquad (b)\ \ G \cong G_1 \times H.$$

Da ciò segue che

$$G \cong \langle g_1\rangle \times \langle g_2\rangle \times \ \ldots\ \times \langle g_t\rangle,$$

cioè G è prodotto diretto di gruppi ciclici. Infine, in base ad Eserc. **5.1**(ii), $\circ(g_2) \,\big|\, \circ(g_1)$, cioè $e_2 \,\big|\, e_1$. Le condizioni (i) e (ii) dell'enunciato sono quindi verificate e restano solo da dimostrare (a) e (b).

Proviamo (a). In base all'Eserc. **5.2**(i) [esteso al caso di più fattori, cfr. *Nota* alla dimostrazione], è sufficiente verificare che

$$|H| = |H_2|\cdot|H_3|\cdot \ldots \cdot |H_t| \ [= e_2 e_3 \ldots e_t].$$

Ovviamente $|H| \le e_2 e_3 \ldots e_t$. Viceversa, si consideri la proiezione canonica $\pi : G \to G/_{G_1}$. Si ha:

$$\pi(H) = G/_{G_1}.$$

Infatti $G/_{G_1} \cong H_2 \times \ldots \times H_t = \langle \overline{g}_2\rangle \times \langle \overline{g}_3\rangle \times \ \ldots\ \times \langle \overline{g}_t\rangle$ e $\overline{g}_i = \pi(g_i) \in \pi(H)$. Ne segue che $|H| \ge |\pi(H)| = |G/_{G_1}| = e_2 e_3 \ldots e_t$.

Proviamo ora (b). Si consideri la restrizione $\pi_{|H} : H \to G/_{G_1}$. Si tratta di un isomorfismo [essendo $|H| = |G/_{G_1}|$]. Dunque $Ker(\pi_{|H}) = \{1\}$. Ma $Ker(\pi_{|H}) = H \cap G_1$ e quindi $H \cap G_1 = \{1\}$. In base all'Eserc. **5.2**(ii), $HG_1 \cong H \times G_1$. D'altra parte, $|H \times G_1| = |H|\cdot|G_1| = |G|$ e quindi $HG_1 = G$. Dunque $G \cong H \times G_1 \cong G_1 \times H$, come richiesto.

Dimostriamo ora l'unicità dei fattori invarianti. Sia

$$G \cong H_1 \times \ldots \times H_t \cong K_1 \times \ldots \times K_s, \ \text{ con } \begin{cases} H_i = \langle x_i\rangle,\ \circ(x_i) = e_i\,,\ \prod_{i=1}^{t} e_i = n,\ e_t \,\big|\, e_{t-1} \,\big|\, \ldots \,\big|\, e_2 \,\big|\, e_1, \\ K_j = \langle y_j\rangle,\ \circ(y_j) = f_j,\ \prod_{j=1}^{s} f_j = n,\ f_s \,\big|\, f_{s-1} \,\big|\, \ldots \,\big|\, f_2 \,\big|\, f_1. \end{cases}$$

Si tratta di verificare che $e_i = f_i$, $\forall\, i = 1, \ldots, t = s$. Poiché x_1, y_1 sono elementi di periodo massimo in G, dall'Eserc. **5.1**(ii) segue che $\circ(x_1) = \circ(y_1)$, cioè $e_1 = f_1$.

Assumiamo, per assurdo, che esista $k \le min(s,t)$ tale che $e_\ell = f_\ell$, per $1 \le \ell < k$ e (ad esempio) $e_k > f_k$. Per semplificare le notazioni, si ponga $f := f_k$. Si consideri in G il sottoinsieme

$$A := \{g^f\,,\ \forall\, g \in G\}.$$

Essendo G abeliano, si verifica subito che A è un sottogruppo di G. Tenuto conto che $G \cong \langle x_1\rangle \times \ldots \times \langle x_t\rangle$, allora

$(*)$ $\quad A \cong \langle x_1^{\,f}\rangle \times \ldots \times \langle x_k^{\,f}\rangle \times \ldots \times \langle x_t^{\,f}\rangle.$

Si noti che i primi k fattori sono sottogruppi non banali, essendo $x_\ell^{\,f} \ne 1$, per $1 \le \ell \le k$. Analogamente, da $G \cong \langle y_1\rangle \times \ldots \times \langle y_s\rangle$, allora

$(**)$ $\quad A \cong \langle y_1^{\,f}\rangle \times \ldots \times \langle y_{k-1}^{\,f}\rangle \times \langle 1\rangle \times \ldots \times \langle 1\rangle$

[in quanto $y_\ell^{\,f} = 1$, per $k \le \ell \le s$].

Da (**),

$$|A| = \prod_{j=1}^{k-1} \frac{\circ(y_j)}{MCD(f, \circ(y_j))} = \prod_{j=1}^{k-1} \frac{f_j}{f} = \frac{1}{f^{k-1}}\, f_1 ... f_{k-1} = \frac{1}{f^{k-1}}\, e_1 ... e_{k-1}\,.$$

Da (*),

$$|A| \ge \prod_{j=1}^{k} \frac{\circ(x_j)}{MCD(f, \circ(x_j))} = \frac{e_1 ... e_{k-1}}{f^{k-1}} \cdot \frac{e_k}{MCD(f, e_k)}.$$

Poiché $e_k > f$, allora $\frac{e_k}{MCD(f,e_k)} > 1$. Confrontando le precedenti espressioni di $|A|$ segue che $|A| \ge |A| \cdot \frac{e_k}{MCD(f,e_k)} > |A|$: assurdo.

Concludiamo il paragrafo con le soluzioni dei due esercizi proposti.

Soluzione Esercizio 5.1. (*i*) Sia $r := \circ(x)$, $s := \circ(y)$, con $MCD(r,s) = 1$. Essendo G abeliano:

$$(xy)^{rs} = x^{rs} y^{rs} = (x^r)^s (y^s)^r = 1 \cdot 1 = 1.$$

Dunque $\circ(xy) \,\big|\, rs$.

Viceversa, posto $h := \circ(xy)$, basta provare che $rs \,\big|\, h$ (da cui $rs = h$, cioè la tesi). Si ha:

$$1 = (xy)^h = x^h y^h, \text{ da cui } y^h = x^{-h} \text{ e quindi } \circ(y^h) = \frac{s}{MCD(s,h)} = \circ(x^{-h}) = \frac{r}{MCD(r,h)}.$$

Pertanto $r \cdot MCD(s,h) = s \cdot MCD(r,h)$. Essendo $MCD(r,s) = 1$, dal lemma di Euclide segue che $r \,\big|\, MCD(r,h)$ e $s \,\big|\, MCD(s,h)$. Quindi $r \,\big|\, h$ e $s \,\big|\, h$. Essendo $MCD(r,s) = 1$, si conclude che $rs \,\big|\, h$, come richiesto.

(*ii*) Per assurdo, esista $y \in G$ tale che $\circ(y) \not| \circ(x)$. Esiste allora un primo p tale che, posto

$$\circ(x) = p^h r,\ \circ(y) = p^k s, \text{ con } h, k \ge 0 \text{ e } MCD(r,p) = MCD(s,p) = 1,$$

si abbia $h < k$. Consideriamo in G l'elemento $x^{p^h} y^s$. Risulta: $\circ(x^{p^h}) = r$ [infatti $(x^{p^h})^r = x^{\circ(x)} = 1$, mentre, $\forall\, r' :\ 0 < r' < r$, $(x^{p^h})^{r'} \ne 1$]. Analogamente: $\circ(y^s) = p^k$ [infatti $(y^s)^{p^k} = y^{\circ(y)} = 1$, mentre, $\forall\, t :\ 0 < t < p^k$, $(y^s)^t \ne 1$]. Poiché $MCD(r, p^k) = 1$, applicando (*i*) si ottiene che

$$\circ(x^{p^h} y^s) = \circ(x^{p^h}) \circ (y^s) = r p^k > r p^h = \circ(x).$$

Ciò contrasta con la massimalità del periodo di x in G.

Soluzione Esercizio 5.2. (*i*) Sia $\varphi : H \times K \to HK$ tale che $\varphi((h,k)) = hk$, $\forall\, (h,k) \in H \times K$. Per definizione di HK, φ è suriettiva. Poiché $|HK| = |H| \cdot |K| < \infty$, φ è anche iniettiva. Per concludere basta provare che φ è un omomorfismo di gruppi. Infatti, $\forall\, (h_1,k_1), (h_2,k_2) \in H \times K$:

$$\varphi\big((h_1,k_1)\cdot(h_2,k_2)\big) = \varphi\big(h_1h_2, k_1k_2\big)\big) = h_1h_2\,k_1k_2 = h_1k_1\,h_2k_2 = \varphi\big((h_1,k_1)\big)\varphi\big(h_2,k_2\big)\big).$$

Nota. La proprietà (*i*) si estende, con ugual dimostrazione, al caso di un numero finito di sottogruppi finiti di G. Precisamente:

Se $H_1, \dots, H_t$ sono sottogruppi finiti di un gruppo abeliano G e se $|H_1 H_2 \dots H_t| = |H_1| \cdot |H_2| \cdot \dots \cdot |H_t|$, allora $H_1 H_2 \dots H_t \cong H_1 \times H_2 \times \dots \times H_t$.

(*ii*) Sia $H \cap K = \{1\}$. Dal secondo teorema di isomorfismo,

$$HK/_H \cong K/_{H \cap K} = K/_{\{1\}} \cong K.$$

Dunque $|HK|/_{|H|} = |K|$, cioè $|HK| = |H| \cdot |K|$. Applicando (*i*) si conclude.

Capitolo 3

ELEMENTI DI TEORIA DEGLI ANELLI

1. Ideali massimali e ideali primi

Assegnato un anello non nullo A, denotiamo con $\mathfrak{I}(A)$ l'insieme di tutti gli ideali propri di A, cioè di tutti gli ideali $\neq A$. Ovviamente $\mathfrak{I}(A)$ è un insieme non vuoto [infatti $\{0\} \in \mathfrak{I}(A)$], ordinato rispetto all'inclusione insiemistica.

Definizione 1.1. *Un ideale $M \in \mathfrak{I}(A)$ è detto massimale in A se M è un elemento massimale di $\mathfrak{I}(A)$ (rispetto all'inclusione), cioè se, $\forall\, I \in \mathfrak{I}(A)$:*

$$M \subseteq I \implies M = I.$$

Ci limiteremo a considerare soltanto anelli unitari e dimostreremo che tali anelli posseggono sempre almeno un ideale massimale: si tratta di un importante risultato, dovuto a W. Krull (1929).

Teorema 1.1. *(Krull) Sia A un anello unitario. Ogni ideale proprio I di A è contenuto in almeno un ideale massimale. In particolare, A ammette sempre ideali massimali.*

Dim. La dimostrazione si basa sul *Lemma di Zorn*:

Sia $(S, \leq)$ un insieme ordinato. Se ogni catena di S ha un maggiorante (in S), S ha almeno un elemento massimale. [Cfr. [AA], Teor. **2**, pag. 18. Ricordiamo che una *catena in S* è una famiglia totalmente ordinata di elementi di S].

Poniamo, per ogni ideale proprio I di A:

$$\mathbf{\Sigma}_I = \{J \in \mathfrak{I}(A) \mid I \subseteq J\}.$$

Ovviamente $\mathbf{\Sigma}_I$ è non vuoto [infatti $I \in \mathbf{\Sigma}_I$] ed è ordinato rispetto all'inclusione. Sia $\{J_\alpha\}_{\alpha \in T}$ una catena in $\mathbf{\Sigma}_I$ e si ponga:

$$B := \bigcup_{\alpha \in T} J_\alpha .$$

Se verifichiamo che $B \in \mathbf{\Sigma}_I$, allora B è un maggiorante della catena e quindi, per il lemma di Zorn, $\mathbf{\Sigma}_I$ possiede elementi massimali. Si tratta di verificare:

- $B - B \subseteq B$ [se $x \in J_\alpha$ e $y \in J_\beta$, allora ad esempio $x, y \in J_\beta$ (se $J_\alpha \subseteq J_\beta$); dunque $x - y \in J_\beta \subseteq B$];
- $BA \subseteq B$ e $AB \subseteq B$ [sia $a \in A$ e sia $x \in B$. Allora $x \in J_\alpha$, $\exists\, \alpha \in T$ e quindi ax, $xa \in J_\alpha \subseteq B$];
- $I \subseteq B$ [$\forall\, \alpha \in T$, $J_\alpha \supseteq I$. Allora $B \supseteq I$];
- $B \neq A$ [altrimenti $1 \in B$ e quindi $\exists\, \alpha \in T \mid 1 \in J_\alpha$: assurdo].

È così provato che $B \in \mathbf{\Sigma}_I$. Si noti che, se M è un elemento massimale in $\mathbf{\Sigma}_I$, lo è anche in $\mathfrak{I}(A)$ [altrimenti $\exists\, J \in \mathfrak{I}(A) \mid M \subset J \subset A$. Ma allora $J \in \mathbf{\Sigma}_I$ e M non sarebbe massimale in $\mathbf{\Sigma}_I$].

Il seguente risultato caratterizza gli ideali massimali di un anello commutativo unitario.

Proposizione 1.1. *Sia A un anello commutativo unitario ed I un suo ideale proprio.*

$$I \text{ è un ideale massimale di } A \iff A/_I \text{ è un campo.}$$

Dim. ($\Longrightarrow$). Poiché $A/_I$ è commutativo e unitario, basta verificare che ogni elemento non nullo di $A/_I$ è invertibile.

Sia $\overline{x} = x + I \in A/_I$, con $\overline{x} \neq \overline{0}$ (cioè $x \notin I$). Poiché $I \subset I + xA \subseteq A$, dalla massimalità di I segue che $I + xA = A$. Dunque $1 = y + xa$, $\exists\, y \in I$, $\exists\, a \in A$. Allora $xa - 1 \in I$, cioè $\overline{x}\,\overline{a} = \overline{1}$ in $A/_I$. Dunque $\overline{x}$ è invertibile (ed ha ha inverso $\overline{a}$).

($\Longleftarrow$). Sia $A/_I$ un campo e sia J un ideale tale che $I \subset J \subseteq A$. Bisogna verificare che $J = A$.

Si scelga $y \in J - I$. Poiché $\overline{y} \neq \overline{0}$ (in $A/_I$), $\overline{y}$ è invertibile: $\exists\, \overline{z} \in A/_I$ tale che $\overline{y}\,\overline{z} = \overline{1}$. Allora $yz - 1 \in I$. Dunque $1 = yz - (yz-1) \in JA + I \subseteq J$, cioè $1 \in J$, ovvero $J = A$.

Nella dimostrazione della proposizione precedente, le ipotesi che A sia commutativo e unitario sono essenziali. Si possono infatti trovare esempi di:

- anello commutativo non unitario A, con ideale massimale M tale che $A/_M$ non è un campo.

- anello non commutativo unitario A, con ideale massimale M tale che $A/_M$ non è integro (e quindi non è un corpo).

Svilupperemo tali esempi in due esercizi (cfr. Esercizio **3.1.1** ed Esercizio **3.1.2**).

Ci limiteremo quindi d'ora in poi, per semplificare la teoria, *a considerare soltanto anelli commutativi unitari* [nel seguito abbreviati *anelli c.u.*].

La Prop. **1.1** permette di individuare facilmente gli ideali massimali di $\boldsymbol{Z}$ e di $K[X]$ (K campo). Infatti dal corso di **Alg. 1** è noto che

(*i*) $\boldsymbol{Z}_n$ è un campo $\iff$ n è un numero primo;

(*ii*) $K[X]/_{\equiv_P}$ è un campo $\iff$ P è un polinomio irriducibile su K.

Ne segue:

(*i*) (n) è massimale $\iff$ n è un numero primo;

(*ii*) (P) è massimale $\iff$ P è un polinomio irriducibile su K.

Osservazione 1.1. Determinare gli ideali massimali di un anello c.u. è un problema non sempre immediato, già con anelli molto semplici. Consideriamo ad esempio l'anello $\boldsymbol{Z}[X]$ e cominciamo col verificare che nessun ideale principale in $\boldsymbol{Z}[X]$ è massimale, cioè che, $\forall\, f \in \boldsymbol{Z}[X]$, $\boldsymbol{Z}[X]/_{(f)}$ non è mai un campo.

L'ideale (0) non è ovviamente massimale. Se $\partial f = 0$, cioè $f = n \in \boldsymbol{Z}^{\cdot}$, risulta $\boldsymbol{Z}[X]/_{(n)} \cong \boldsymbol{Z}_n[X]$, [tramite l'*omomorfismo di riduzione mod n*, cioè l'omomorfismo

$$\boldsymbol{Z}[X] \to \boldsymbol{Z}_n[X] \text{ tale che } \textstyle\sum a_i X^i \to \sum \overline{a}_i X^i,\ \forall \sum a_i X^i \in \boldsymbol{Z}[X]]$$

e ovviamente $\boldsymbol{Z}_n[X]$ non è un campo. Se invece $\partial f \geq 1$, osservato che $\boldsymbol{Z} \hookrightarrow \boldsymbol{Z}[X]/_{(f)}$, allora, assumendo per assurdo $\boldsymbol{Z}[X]/_{(f)}$ campo, si avrebbe che $\boldsymbol{Q} \subseteq \boldsymbol{Z}[X]/_{(f)}$. In particolare quindi $\frac{1}{2} \in \boldsymbol{Z}[X]/_{(f)}$. Allora $\frac{1}{2} = g + (f)$, $\exists\, g \in \boldsymbol{Z}[X]$ e dunque $g - \frac{1}{2} \in (f) \subset \boldsymbol{Z}[X]$: assurdo.

Invece, ad esempio, è massimale in $\boldsymbol{Z}[X]$ l'ideale $(2, X)$ [infatti $\boldsymbol{Z}[X]/_{(2,X)} \cong \boldsymbol{Z}_2$, cfr. Esercizio **1.5.3**]. È anche massimale ad esempio $(5, X^2+3)$, ma non lo è $(7, X^2+3)$ [verificare].

Veniamo ora alla definizione di ideale primo, che riprende il concetto di elemento primo di un anello.

Definizione 1.2. *Sia A un anello c.u. e sia I un ideale proprio di A. I è un ideale primo di A se, contenendo un prodotto, contiene almeno un fattore, cioè*

$$xy \in I \implies x \in I \text{ oppure } y \in I.$$

Un ideale primo viene sovente indicato con $\mathfrak{p}$ (invece che con I).

Osservazione 1.2. Ricordiamo che in un anello A (c.u.) un elemento $a \in A^{\cdot} - \mathcal{U}(A)$ (cioè non nullo e non invertibile) è detto *elemento primo* se

$$a \,|\, xy \implies a \,|\, x \text{ oppure } a \,|\, y$$

[ovvero: $xy \in Aa \implies x \in Aa$ oppure $y \in Aa$]. Come si vede, gli elementi primi generano ideali (principali) primi. Ma vale anche il viceversa: se Aa è un ideale primo non nullo di A, a è un

elemento primo di A [verificare].

Proposizione 1.2. *Sia A un anello c.u. ed I un suo ideale proprio.*

$$I \text{ è un ideale primo di } A \iff A/_I \text{ è un dominio d'integrità.}$$

Dim. ($\Longrightarrow$). Siano $\overline{x}, \overline{y} \in A/_I$ tali che $\overline{x}\,\overline{y} = \overline{0}$. Allora $xy \in I$ e quindi $x \in I$ oppure $y \in I$, cioè $\overline{x} = \overline{0}$ oppure $\overline{y} = \overline{0}$. Pertanto $A/_I$ è integro.

($\Longleftarrow$). Sia $xy \in I$. Allora $\overline{0} = \overline{xy} = \overline{x}\,\overline{y}$. Essendo $A/_I$ integro, allora $\overline{x} = \overline{0}$ oppure $\overline{y} = \overline{0}$, cioè $x \in I$ oppure $y \in I$. Dunque I è primo.

Corollario 1.1. *Ogni ideale massimale di un anello c.u. è primo. Il viceversa è in generale falso.*

Dim. Sia I un ideale massimale in un anello c.u. A. Da Prop. **1.1**, $A/_I$ è un campo e quindi anche un dominio d'integrità. Da Prop. **1.2**, I è primo.

Viceversa, si osserva subito che (0) è un ideale primo ma non massimale di $\boldsymbol{Z}$.

Nota. (0) è un ideale primo di $A \iff A$ è un dominio d'integrità.

Definizione 1.3. *Gli ideali primi di un anello c.u. A formano un sottoinsieme non vuoto di $\mathfrak{I}(A)$, detto spettro (o spetto primo) di A e denotato $Spec(A)$. In $Spec(A)$ è contenuto il sottoinsieme (non vuoto) degli ideali massimali di A, spesso denotato $Max(A)$.*

Si verifica subito che:

- $Spec(\boldsymbol{Z}) = \{(0), (p),\ \forall p \text{ primo}\}$ [$\boldsymbol{Z}$, $\boldsymbol{Z}_p$ sono integri, mentre $\boldsymbol{Z}_n$ non lo è, $\forall n$ non primo];

- $Spec(K[X]) = \{(0), (P),\ \forall P \text{ polinomio irriducibile su } K\}$ [infatti $K[X]/_{(P)}$ non è integro, se P è riducibile su K].

Quanto a $Spec(\boldsymbol{Z}[X])$, la situazione è più complicata. È evidente che:

- $(0), (p) \in Spec(\boldsymbol{Z}[X]),\ \forall p$ numero primo [infatti $\boldsymbol{Z}[X]/_{(p)} \cong \boldsymbol{Z}_p[X]$ dominio];

- $(f) \notin Spec(\boldsymbol{Z}[X]),\ \forall f \in \boldsymbol{Z}[X]$ riducibile [infatti, se $f = gh$, con $g, h \notin \mathcal{U}(\boldsymbol{Z}[X])$, allora $\overline{g}\,\overline{h} = \overline{0}$ in $\boldsymbol{Z}[X]/_{(f)}$, con $\overline{g}, \overline{h} \neq \overline{0}$].

Viceversa, ci chiediamo se, per ogni polinomio irriducibile $f \in \boldsymbol{Z}[X]$, risulti $(f) \in Spec(\boldsymbol{Z}[X])$, ovvero se in $\boldsymbol{Z}[X]$ ogni polinomio irriduibile è anche primo. La risposta è affermativa, ma per far luce sul problema conviene premettere qualche osservazione di carattere generale sui legami tra elementi irriducibili ed elementi primi in un dominio d'integrità.

Osservazione 1.3. Ricordiamo che in ogni anello c.u. A può essere introdotta la nozione di *elemento irriducibile*: un elemento $a \in A^{\cdot} - \mathcal{U}(A)$ è un *elemento irriducibile* se

$$a = xy \implies x \in \mathcal{U}(A) \text{ oppure } y \in \mathcal{U}(A).$$

In altri termini, un elemento è irriducibile $\iff$ ammette soltanto fattorizzazioni banali.

È ben noto che se A è un dominio d'integrità:

$$\textit{elemento primo} \implies \textit{elemento irriducibile.}$$

[sia infatti a un elemento primo e sia $a = xy$. Allora $a \,|\, xy$. Se $a \,|\, x$, risulta $y \in \mathcal{U}(A)$; se $a \nmid x$, allora $a \,|\, y$ e $x \in \mathcal{U}(A)$].

In alcuni domini d'integrità vale anche l'implicazione opposta: *elemento irriducibile* $\implies$ *elemento primo*. Tale fatto, come visto nel corso di **Alg. 1**, è ad esempio verificato se $A = \boldsymbol{Z}$, $K[X]$, $\boldsymbol{Z}[i]$.

Proviamo ora che tale fatto vale più generalmente in ogni dominio d'integrità in cui esiste il MCD e vale l'identità di Bézout [siffatti anelli sono chiamati *domini di Bézout*.]. Infatti in tali anelli vale il *Lemma di Euclide* (abbreviato *EU*), cioè:

se $a \,|\, xy$ *e* $MCD(a, x) = 1$, *allora* $a \,|\, y$.

[Se infatti $1 = ar + xs$ e $xy = at$, allora $y = a(ry + ts)$, cioè $a \,|\, y$]. Sia quindi a irriducibile e $a \,|\, xy$, $a \not| x$. Bisogna verificare che $a \,|\, y$. Si osserva subito che $MCD(a, x) = 1$ [infatti, se $d = MCD(a, x)$, allora $d \,|\, a$ e quindi d è invertibile o associato ad a; in quest'ultimo caso $a \,|\, d$ e quindi $a \,|\, x$, contro l'potesi. Pertanto $d = 1$]. Da EU segue che $a \,|\, y$.

Oltre ai domini di Bézout, esiste però un'altra vasta classe di domini in cui ogni elemento irriducibile è primo: si tratta dei *domini a fattorizzazione unica* (abbr. *UFD*), di cui ci occuperemo nel successivo paragrafo **3** (cfr. Prop. **3.1**).

Torniamo a considerare $\boldsymbol{Z}[X]$. In tale anello non vale l'identità di Bézout [infatti $MCD(2, X) = 1$, ma $1 \notin (2, X)$]. Quindi non se ne può ricavare il lemma di Euclide, da cui concludere che in $\boldsymbol{Z}[X]$ ogni polinomio irriducibile è primo. Ma, come vedremo nel § **3**, $\boldsymbol{Z}[X]$ è un *UFD*: dunque, come sopra affermato, ogni polinomio irriducibile $f \in \boldsymbol{Z}[X]$ è primo, per cui $(f) \in Spec(\boldsymbol{Z}[X])$, come preannunciato. Si noti però che, per quanto provato in Osserv. **1.1**, (f) non è massimale in $\boldsymbol{Z}[X]$.

Nota. Una dimostrazione diretta del fatto che in $\boldsymbol{Z}[X]$ ogni elemento irriducibile è primo (basata sul teorema di Gauss), può essere trovata in [AA], pag. 119.

* * * * * * * * * * * * * * * * * *

Esercizio 3.1.1. Sia $A = 2\boldsymbol{Z}$ (anello non unitario) e sia $M = 4\boldsymbol{Z}$.

(*i*) Verificare che M è un ideale massimale di A.

(*ii*) Verificare che $A/_M$ non è un campo.

Esercizio 3.1.2. (*i*) Verificare che $\mathfrak{M}_2(2\boldsymbol{Z})$ è un ideale massimale dell'anello unitario (non commutativo) $\mathfrak{M}_2(\boldsymbol{Z})$.

(*ii*) Verificare che $\mathfrak{M}_2(\boldsymbol{Z})/_{\mathfrak{M}_2(2\boldsymbol{Z})}$ non è un corpo.

Esercizio 3.1.3. Sia K un campo e sia $P = (a, b) \in K^2$.

(*i*) Verificare che $(X - a, Y - b)$ è un ideale massimale di $K[X, Y]$.

(*ii*) Sia $F \in K[X, Y]$ tale che $F(P) = 0$. Verificare che $(F) \subseteq (X - a, Y - b)$.

Esercizio 3.1.4. Verificare che l'ideale $I = (X^2 + 1, Y)$:

è massimale in $\boldsymbol{R}[X, Y]$, è primo in $\boldsymbol{Z}[X, Y]$, non è primo in $\boldsymbol{C}[X, Y]$.

Calcolarne i rispettivi quozienti.

Esercizio 3.1.5. Per ogni $n \geq 2$, determinare $Spec(\boldsymbol{Z}_n)$.

Esercizio 3.1.6. Sia A un anello c.u. e sia $Spec(A)$ il suo spettro. Per ogni $S \subseteq A$ si definisce:

$$V(S) = \{\mathfrak{p} \in Spec(A) \,|\, \mathfrak{p} \supseteq S\}$$

detto *chiuso di* $Spec(A)$ *definito da* S. Verificare che:

(*i*) $V(A) = \emptyset$ e $V(\emptyset) = Spec(A)$.

(*ii*) $V(S_1) \cup V(S_2) = V(S_1 S_2)$, con $S_1 S_2 := \{s_1 s_2,\ \forall\, s_1 \in S_1,\ \forall\, s_2 \in S_2\}$.

(*iii*) $\bigcap_{i \in I} V(S_i) = V\big(\bigcup_{i \in I} S_i\big)$.

Nota. Poiché le tre proprietà precedenti corrispondono agli assiomi dei chiusi di uno spazio topologico, si è provato che la famiglia $\{V(S),\ \forall\, S \subseteq A\}$ è la famiglia dei chiusi di una topologia su $Spec(A)$, detta *topologia di Zariski di* $Spec(A)$.

Esercizio 3.1.7. Sia $f : A \to B$ un omomorfismo di anelli c. u..

(*i*) Dimostrare che f definisce la seguente applicazione

$$\varphi_f : Spec(B) \to Spec(A) \text{ tale che } \varphi_f(\mathfrak{q}) = f^{-1}(\mathfrak{q}),\ \forall\, \mathfrak{q} \in Spec(B)$$

[la controimmagine $f^{-1}(\mathfrak{q})$ è detta *contrazione* o *fibra di* $\mathfrak{q}$].

(*ii*) Determinare un esempio di omomorfismo f in cui un massimale di B ha contrazione non massimale in A.

(*iii*) Verificare che $\varphi_f : Spec(B) \to Spec(A)$ è una funzione continua, rispetto alle topologie di Zariski di $Spec(A)$, $Spec(B)$ (cfr. l'esercizio precedente).

Esercizio 3.1.8. Sia A un anello c.u. e sia $I \in \mathfrak{I}(A)$ tale che $A - I \subseteq \mathcal{U}(A)$. Verificare che I è l'unico ideale massimale di A. [Un anello c.u. con un unico ideale massimale è detto *anello locale*].

Esercizio 3.1.9. Sia A un anello c.u. e sia I un suo ideale.

(*i*) Verificare che $Spec(A/I) = \{\mathfrak{p}/I,\ \forall\, \mathfrak{p} \in V(I)\}$ [dove $V(I) = \{\mathfrak{p} \in Spec(A) \,|\, \mathfrak{p} \supseteq I\}$].

(*ii*) Posto $I = (X^3, Y) \subset \boldsymbol{Q}[X, Y]$, determinare $Spec(\boldsymbol{Q}[X, Y]/I)$.

Esercizio 3.1.10. (*i*) Sia A un anello c.u.. Verificare che i chiusi della topologia di Zariski di $Spec(A)$ sono tutti e soli della forma $V(I)$, con I ideale di A.

(*ii*) Determinare i chiusi di $Spec(\boldsymbol{Z})$.

Esercizio 3.1.11. Sia A un anello commutativo unitario. È noto da **Alg. 1** che due elementi $a, b \in A$ sono detti *associati* (e si scrive $a \sim b$) se $b = au$, $\exists\, u \in \mathcal{U}(A)$.

(*i*) Verificare che $\sim$ è una relazione di equivalenza su A, che $a \sim b \implies (a) = (b)$ e che, se A è integro, $a \sim b \iff (a) = (b)$.

(*ii*) Verificare che, se $a \sim b$, risulta: a irriducibile [risp. primo] $\implies$ b irriducibile [risp. primo].

Nota. La topologia di Zariski su $Spec(A)$ (introdotta nell'Eserc. **3.1.6**) generalizza la *topologia di Zariski su* K^n, che viene introdotta e studiata nei corsi di Topologia e di Geometria Algebrica. Vogliamo chiarire i legami tra questi due concetti.

Sia K un campo, sia $A = K[X_1, X_2, \dots, X_n]$ e sia I un suo ideale, che supporremo (ciò che non è restrittivo) finitamente generato, con generatori $F_1, \dots, F_t$. Allora

$$V(I) = V(\{F_1, \dots, F_t\}) = \{\mathfrak{p} \in Spec(A) \mid F_1, \dots, F_t \in \mathfrak{p}\}.$$

In $V(I)$ consideriamo il sottoinsieme

$$V_{max}(I) = \{\mathfrak{m} \in Max(A) \mid F_1, \dots, F_t \in \mathfrak{m}\} = V(I) \cap Max(A).$$

Ora definiamo i *chiusi di Zariski in* K^n. Considerato ancora l'ideale $I = (F_1, \dots, F_t) \subseteq A$, poniamo:

$$\Sigma(I) = \{P \in K^n \mid F(P) = 0,\ \forall\, F \in I\} = \{P \in K^n \mid F_i(P) = 0,\ \forall\, i = 1, \dots, t\}.$$

[$\Sigma(I)$ è l'insieme delle soluzioni di un sistema di equazioni polinomiali in n indeterminate, a coefficienti in K]. Si verifica facilmente che tali insiemi, al variare di I in A, verificano gli assiomi dei chiusi di una topologia su K^n, detta *topologia di Zariski su* K^n. Osserviamo inoltre che ogni punto $P = (a_1, a_2, \dots, a_n) \in K^n$ definisce l'ideale massimale $\mathfrak{m}_P = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n) \in Max(A)$. Si può verificare (procedendo come nell'Eserc. **3.1.3**) che $F(P) = 0 \iff F \in \mathfrak{m}_P$.

Nell'ipotesi che sia $K = \boldsymbol{C}$ o, più generalmente, che K sia un campo algebricamente chiuso, risulta, in base ad un famoso teorema di Hilbert, che gli ideali massimali di A sono tutti e soli della forma $\mathfrak{m}_P$, cioè del tipo $(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$. Si conclude allora che, in questa ulteriore ipotesi,

$$\Sigma(I) = \{\mathfrak{m}_P \in Max(A) \mid F_1, \dots, F_t \in \mathfrak{m}_P\} = V_{max}(I).$$

2. Campo dei quozienti e anelli di frazioni

Assegnato un dominio d'integrità A, vogliamo costruirne il *campo dei quozienti*, cioè il più piccolo campo contenente A. Tale costruzione generalizza la ben nota costruzione del campo $\boldsymbol{Q}$ dei razionali, come campo dei quozienti dell'anello $\boldsymbol{Z}$ degli interi.

Lemma 2.1. *Sia A un dominio d'integrità. Sia $\sim$ la seguente relazione su $A\times A^{\cdot}$:*

$$(a,b)\sim(c,d) \iff ad=bc,\ \forall\,(a,b),(c,d)\in A\times A^{\cdot}.$$

Risulta: $\sim$ è una relazione di equivalenza su $A\times A^{\cdot}$. Denotata $\frac{a}{b}$ la classe di equivalenza modulo $\sim$ di (a,b), $\forall\,(a,b)\in A\times A^{\cdot}$, nell'insieme quoziente $A\times A^{\cdot}/_{\sim}$ sono ben definite le due operazioni:

$$\tfrac{a}{b}+\tfrac{c}{d}=\tfrac{ad+bc}{bd},\quad \tfrac{a}{b}\cdot\tfrac{c}{d}=\tfrac{ac}{bd},\ \ \forall\,\tfrac{a}{b},\,\tfrac{c}{d}\in A\times A^{\cdot}/_{\sim}.$$

Dim. $\sim$ è evidentemente riflessiva e simmetrica. Verifichiamo che è transitiva. Se $(a,b)\sim(c,d)$ e $(c,d)\sim(e,f)$, allora $\begin{cases} ad=bc\\ cf=de.\end{cases}$ Ne segue che $\begin{cases} adf=bcf\\ bcf=bde\end{cases}$ e quindi $adf=bde$, cioè $d(af-be)=0$. Essendo $d\neq 0$ e A integro, allora $af=be$, cioè $(a,b)\sim(e,f)$.

Verifichiamo ora che la somma è ben definita. Se $\frac{a}{b}=\frac{a'}{b'}$ e $\frac{c}{d}=\frac{c'}{d'}$, allora $ab'=a'b$ e $cd'=c'd$. Si moltiplichi la prima uguaglianza per dd' e la seconda per bb'; sommando poi membro a membro, si ottiene:

$$ab'\,dd'+cd'\,bb'=a'\,bd\,d'+c'\,db\,b'\,,$$

da cui

$$(ad+bc)b'\,d'\,=(a'\,d'+b'\,c')bd,\ \text{ cioè }\ \tfrac{ad+bc}{bd}=\tfrac{a'\,d'+b'\,c'}{b'\,d'}.$$

In modo analogo si dimostra che anche la moltiplicazione è ben definita.

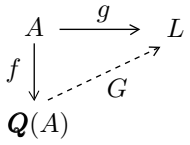
Proposizione 2.1. *$(A\times A^{\cdot}/_{\sim},+,\cdot)$ è un campo, detto campo dei quozienti del dominio A e denotato usualmente $\boldsymbol{Q}(A)$. Risulta, a meno di isomorfismi, che $A\subseteq\boldsymbol{Q}(A)$ e che $\boldsymbol{Q}(A)$ è il più piccolo campo contenente A.*

Dim. Le verifiche che $\boldsymbol{Q}(A)$ è un campo sono un semplice esercizio. Si verifica poi subito che l'applicazione

$$f:A\to\boldsymbol{Q}(A)\ \text{ tale che }\ f(a)=\tfrac{a}{1},\ \ \forall\,a\in A,$$

è un omomorfismo iniettivo di anelli. Tramite f, A si immerge in $\boldsymbol{Q}(A)$.

Sia L un campo tale che $A\subseteq L$, o, più generalmente, sia $g:A\to L$ un omomorfismo iniettivo di anelli. Si tratta di verificare che $\boldsymbol{Q}(A)\subseteq L$, ma più in generale dimostriamo che se $g:A\to L$ è un omomorfismo iniettivo, esiste un omomorfismo iniettivo $G:\boldsymbol{Q}(A)\to L$ tale che $g=G\circ f$, cioè tale che commuti il seguente diagramma di omomorfismi iniettivi



Basta porre:

$$G(\tfrac{a}{b})=\tfrac{g(a)}{g(b)},\ \ \forall\,\tfrac{a}{b}\in\boldsymbol{Q}(A).$$

Tale definizione è ben posta. Infatti $g(b)\neq 0$ se $b\neq 0$ (g è iniettiva); se poi $\frac{a}{b}=\frac{a'}{b'}$, allora $ab'=a'\,b$ e quindi $g(a)g(b')=g(a')g(b)$; essendo $b,\,b'\neq 0$, anche $g(b),\,g(b')\neq 0$ e quindi $\frac{g(a)}{g(b)}=\frac{g(a')}{g(b')}$, cioè $G(\frac{a}{b})=G(\frac{a'}{b'})$.

Lasciamo per esercizio la verifica che G è un omomorfismo iniettivo di anelli e che $g(a)=G(f(a))$, $\forall\,a\in A$. Si conclude che, tramite G, il campo $\boldsymbol{Q}(A)$ si immerge in L. Dunque $\boldsymbol{Q}(A)$ è il più piccolo campo contenente A.

Nota. Per ogni $\frac{a}{b} \in \boldsymbol{Q}(A)$, risulta $\frac{a}{b} = \frac{a}{1}\cdot(\frac{b}{1})^{-1}$. Se identifichiamo ogni $a \in A$ con $\frac{a}{1} = f(a) \in \boldsymbol{Q}(A)$, possiamo concludere che $\boldsymbol{Q}(A)$ è formato dai prodotti $a\cdot b^{-1}$, $\forall\, a, b \in A,\ b \neq 0$.

Osservazione 2.1. Calcoliamo il campo dei quozienti di alcuni domini d'integrità.

(*i*) $\boldsymbol{Q}(\boldsymbol{Z}) = \boldsymbol{Q}$, campo dei razionali.

(*ii*) Per ogni campo K, risulta:

$$\boldsymbol{Q}\big(K[X]\big) = \big\{\tfrac{f}{g},\ \ \forall\, f, g \in K[X],\, g \neq 0\big\}.$$

Tale campo è detto *campo delle funzioni razionali su* K *(nell'indeterminata* X*)* ed è usualmente denotato con $K(X)$. Più in generale risulta:

$$\boldsymbol{Q}\big(K[X_1, X_2, \dots, X_n]\big) = \big\{\tfrac{f}{g},\ \ \forall\, f, g \in K[X_1, X_2, \dots, X_n],\, g \neq 0\big\}.$$

Si tratta del *campo delle funzioni razionali su* K *(nelle indeterminate* $X_1, X_2, \dots, X_n$*)*, denotato $K(X_1, X_2, \dots, X_n)$.

(*iii*) Se A è un dominio, anche $A[X_1, X_2, \dots, X_n]$ lo è e risulta

$$\boldsymbol{Q}\big(A[X_1, X_2, \dots, X_n]\big) = \boldsymbol{Q}(A)(X_1, X_2, \dots, X_n).$$

Per provare tale affermazione è sufficiente verificare che

$$(\bullet) \qquad \boldsymbol{Q}(A)(X_1, X_2, \dots, X_n) \subseteq \boldsymbol{Q}\big(A[X_1, X_2, \dots, X_n]\big).$$

[Se infatti vale $(\bullet)$, $\boldsymbol{Q}(A)(X_1, X_2, \dots, X_n)$ è un campo intermedio tra $A[X_1, X_2, \dots, X_n]$ ed il suo campo dei quozienti; dunque (per minimalità del campo dei quozienti) coincide con esso].

Verifichiamo $(\bullet)$. Sia $\frac{F}{G} \in \boldsymbol{Q}(A)(X_1, X_2, \dots, X_n)$, con $F, G \in \boldsymbol{Q}(A)[X_1, X_2, \dots, X_n]$, $G \neq 0$. Allora, riducendo a comun denominatore i coefficienti dei due polinomi, $F = \frac{1}{a}f$, $G = \frac{1}{b}g$, con $f, g \in A[X_1, X_2, \dots, X_n]$, $g \neq 0$ e $a, b \in A^{\cdot}$. Pertanto $\frac{F}{G} = \frac{bf}{ag} \in \boldsymbol{Q}\big(A[X_1, X_2, \dots, X_n]\big)$.

(*iv*) Per ogni intero d tale che $X^2 - d$ sia un polinomio irriducibile in $\boldsymbol{Z}[X]$, è definito l'anello (detto *anello quadratico (relativo a* d*)*, cfr. [AA] pag. 126):

$$\boldsymbol{Z}[X]\big/_{(X^2-d)} \cong \{a + b\sqrt{d},\ \ \forall\, a, b \in \boldsymbol{Z}\} =: \boldsymbol{Z}[\sqrt{d}].$$

Giustifichiamo l'isomorfismo sopra indicato. Sia $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{C}$ tale che $\varphi(f) = f(\sqrt{d})$, $\forall\, f \in \boldsymbol{Z}[X]$. Ovviamente $X^2 - d \in Ker\varphi$. Viceversa, se $g \in Ker\varphi$ e $g = (X^2 - d)q + (aX + b)$, allora $0 = g(\sqrt{d}) = a\sqrt{d} + b$ e dunque $a = b = 0$, cioè $g \in (X^2 - d)$. Quindi $Ker\varphi = (X^2 - d)$. Inoltre si osserva subito che $Im\varphi = \{a + b\sqrt{d},\ \ \forall\, a, b \in \boldsymbol{Z}\}$ e basta quindi applicare il *TFO*.

L'anello $\boldsymbol{Z}[\sqrt{d}]$ è un dominio (in quanto sottoanello di $\boldsymbol{C}$) e contiene $\boldsymbol{Z}$. Vogliamo verificare che il campo dei quozienti di $\boldsymbol{Z}[\sqrt{d}]$ è il campo

$$\boldsymbol{Q}[X]\big/_{(X^2-d)} \cong \{\tfrac{a}{b} + \tfrac{a'}{b'}\sqrt{d},\ \ \forall\, \tfrac{a}{b}, \tfrac{a'}{b'} \in \boldsymbol{Q}\} =: \boldsymbol{Q}(\sqrt{d}).$$

Poiché $\boldsymbol{Z}[\sqrt{d}] \subseteq \boldsymbol{Q}(\sqrt{d})$, basta verificare, seguendo la stessa idea sviluppata nel punto (*iii*), che $\boldsymbol{Q}(\sqrt{d}) \subseteq \boldsymbol{Q}(\boldsymbol{Z}[\sqrt{d}])$. Infatti, $\forall\, \alpha = \frac{a}{b} + \frac{a'}{b'}\sqrt{d} \in \boldsymbol{Q}(\sqrt{d})$, risulta $\alpha = \frac{ab' + ba'\sqrt{d}}{bb'} \in \boldsymbol{Q}(\boldsymbol{Z}[\sqrt{d}])$.

(*v*) Sia A un dominio e sia B un anello c.u. tale che $A \subseteq B \subseteq \boldsymbol{Q}(A)$. Risulta subito che B è un dominio e $\boldsymbol{Q}(B) = \boldsymbol{Q}(A)$. Infatti, che B sia un dominio segue dal fatto che $B \subseteq \boldsymbol{Q}(A)$. Per la minimalità di $\boldsymbol{Q}(B)$ rispetto a B, segue che $\boldsymbol{Q}(B) \subseteq \boldsymbol{Q}(A)$, mentre, per la minimalità di $\boldsymbol{Q}(A)$ rispetto ad A, segue che $\boldsymbol{Q}(A) \subseteq \boldsymbol{Q}(B)$.

Sia A un dominio d'integrità. Nel passaggio da A a $\boldsymbol{Q}(A)$ tutti gli elementi di $A^{\cdot}$ vengono invertiti (in $\boldsymbol{Q}(A)$). Come ora vedremo, è possibile però, con analoga costruzione, rendere invertibili soltanto una parte di elementi di $A^{\cdot}$ (in un opportuno "sovranello" di A). Tale costruzione potrà poi essere facilmente estesa, con qualche modifica anche al caso di anelli non integri.

Si noti che gli elementi da invertire devono avere una "struttura moltiplicativa" [se infatti due elementi si invertono, anche il loro prodotto si inverte]. Introduciamo pertanto la seguente definizione.

Definizione 2.1. *Sia* A *un anello c. u. e sia* S *un sottoinsieme di* A. S *è detto parte moltiplicativa di* A *(o insieme moltiplicativo di* A*) se verifica le due condizioni:*

$$1 \in S, \qquad S \cdot S \subseteq S.$$

Lemma 2.2. *Sia A un dominio d'integrità ed S una parte moltiplicativa in A, con $0 \notin S$. In $A \times S$ è definita la seguente relazione $\sim$:*

$$(a,s) \sim (b,t) \iff at = bs, \ \forall\, (a,s), (b,t) \in A \times S.$$

Risulta: $\sim$ è una relazione di equivalenza su $A \times S$. Indicata con $\frac{a}{s}$ la classe di equivalenza di (a,s) modulo $\sim$, l'insieme quoziente $A \times S/_{\sim}$ è un anello c. u. rispetto alle due operazioni:

$$\tfrac{a}{s} + \tfrac{b}{t} = \tfrac{at+bs}{st}, \qquad \tfrac{a}{s} \cdot \tfrac{b}{t} = \tfrac{ab}{st}, \ \ \forall\, \tfrac{a}{s}, \tfrac{b}{t} \in A \times S/_{\sim}.$$

Dim. Si procede come nella dimostrazione del Lemma **2.1**, che è un caso particolare di questo lemma, con $S = A^{\cdot}$. Si noti poi che la proprietà transitiva è verificata in quanto $0 \notin S$. Ovviamente risulta $\frac{a}{s} = \frac{at}{st}$, $\forall\, t \in S$; inoltre si osserva subito che gli elementi neutri rispetto alla somma ed al prodotto sono rispettivamente $0 = \frac{0}{s}$, $\forall\, s \in S$, e $1 = \frac{s}{s}$, $\forall\, s \in S$. Infine, ogni elemento $s \in S$ è invertibile in tale anello [infatti $s \cdot \frac{1}{s} = 1$].

Definizione 2.2. *Sia A un dominio d'integrità ed S un parte moltiplicativa di A, con $0 \notin S$. L'anello $(A \times S/_{\sim}, +, \cdot)$ è detto anello delle frazioni di A (rispetto ad S) ed è denotato A_S [o anche $S^{-1}A$].*

Proposizione 2.2. *Sia A un dominio d'integrità ed S una sua parte moltiplicativa, con $0 \notin S$. Risulta:*

$$A \subseteq A_S \subseteq \boldsymbol{Q}(A).$$

Ne segue che A_S è un dominio e $\boldsymbol{Q}(A_S) = \boldsymbol{Q}(A)$.

Dim. Sia

$$f : A \to A_S \ \text{ tale che } \ f(a) = \tfrac{a}{1}, \ \forall\, a \in A.$$

Ovviamente f è un omomorfismo di anelli. Inoltre f è iniettivo [infatti $a \in Ker f \iff \frac{a}{1} = 0 \iff as = 0, \exists\, s \in S \iff a = 0$ (essendo A integro e $s \neq 0$)]. Allora $A \subseteq A_S$ tramite f. Tale omomorfismo prende nome di *omomorfismo canonico (d'inclusione) di A in A_S*.

Poiché $\boldsymbol{Q}(A) = A_{A^{\cdot}}$ e $A^{\cdot}$ è una parte moltiplicativa di A (contenente S), per dimostrare che $A_S \subseteq \boldsymbol{Q}(A)$ basta dimostrare, più in generale, il seguente risultato:

Se S, T sono parti moltiplicative di A, con $S \subseteq T$ e $0 \notin T$, allora l'applicazione

$$F : A_S \to A_T \ \text{ tale che } \ F(\tfrac{a}{s}) = \tfrac{a}{s}, \ \forall\, \tfrac{a}{s} \in A_S,$$

è un omomorfismo iniettivo di anelli (e quindi immerge A_S in A_T).

Dimostriamo tale risultato. F è ben definita [se $\frac{a}{s} = \frac{a'}{s'}$ in A_S, allora $as' = a's$, con $s, s' \in S \subseteq T$. Dunque $\frac{a}{s} = \frac{a'}{s'}$ in A_T]. F è un omomorfismo di anelli (evidente). Infine:

$$\tfrac{a}{s} \in Ker F \iff \tfrac{a}{s} = 0 \text{ in } A_T \iff at = 0, \exists\, t \in T \iff a = 0 \ \text{ (essendo } t \neq 0)$$

e pertanto F è iniettivo.

L'ultima affermazione segue dall'Osserv. **2.1**(v).

Se A è un anello c. u. non integro, la relazione $\sim$ (definita in Lemma **2.2**) può non essere transitiva. Infatti, se $(a,s) \sim (b,t)$ e $(b,t) \sim (c,r)$, allora $(ar - cs)t = 0$. Ma se t è uno 0-divisore di A, non può essere cancellato e quindi non si può concludere che $ar = cs$, cioè che $(a,s) \sim (c,r)$.

Si può però modificare la definizione di $\sim$ in questo modo:

$$(a,s) \sim (b,t) \iff \exists\, u \in S \text{ tale che } \ (at - bs)u = 0.$$

Si può verificare che anche tale nuova relazione $\sim$ è di equivalenza. Che $\sim$ sia riflessiva e simmetrica è ovvio. Verichiamo che è transitiva: sia $(a,s) \sim (b,t)$ e $(b,t) \sim (c,r)$; esistono $u, v \in S$ tali che $atu = bsu$ e $brv = ctv$; moltiplicando la prima uguaglianza per vr, la seconda per su e semplificando, si ottiene $arutv = csutv$, da cui $(a,s) \sim (c,r)$, essendo $utv \in S$.

Si noti in particolare che se A è integro e $0 \notin S$, tale relazione coincide con quella precedentemente definita.

Resta poi inalterata la definizione di anello delle frazioni A_S; ma in generale $A \not\subseteq A_S$, in quanto l'omomorfismo "canonico" $f : A \to A_S$ può non essere iniettivo [infatti $\frac{a}{1} = 0 \iff as = 0, \exists\, s \in S$. Se però s è uno 0-divisore (non nullo) associato ad a, allora $a \neq 0$ e $a \in Kerf$].

Osservazione 2.2. Con la più generale definizione di relazione $\sim$ sopra definita, non è più necessario supporre che $0 \notin S$. In effetti, con tale definizione la proprietà transitiva è sempre verificata. Ma osserviamo subito che, se $0 \in S$, allora $(a, s) \sim (0, 0)$, $\forall\, (a, s) \in A \times S$. Ciò comporta che $A_S = \mathbf{0}$ (anello nullo). Per questo continueremo tacitamente a supporre che $0 \notin S$.

Proposizione 2.3. *Sia A un anello c.u. ed S una sua parte moltiplicativa.*

Gli ideali di A_S sono tutti e soli della forma: $I_S = \{\frac{a}{s},\ \forall\, a \in I,\ \forall\, s \in S\}$, $\forall\, I$ ideale di A. Risulta inoltre: $I_S = A_S \iff S \cap I \neq \emptyset$.

Dim. Sia I un ideale di A. Risulta:

$$I_S - I_S \subseteq I_S \quad \text{e} \quad A_S I_S \subseteq I_S\,.$$

Infatti, $\forall\, \frac{a}{s}, \frac{b}{t} \in I_S$, $\forall\, \frac{x}{t} \in A_S$ si ha: $\frac{a}{s} - \frac{b}{t} = \frac{at-bs}{st} \in I_S$, $\frac{a}{s}\frac{x}{t} = \frac{ax}{st} \in I_S$. Ne segue che I_S è un ideale di A_S.

Viceversa, sia J un ideale di A_S. Considerato l'omomorfismo canonico $f : A \to A_S$, è noto che $f^{-1}(J)$ è un ideale di A (cfr. Osserv. **2.5**, Cap. **1**). Verifichiamo che risulta $f^{-1}(J)_S = J$.

Infatti, $\forall\, \frac{x}{s} \in J$, $\frac{x}{1} = \frac{x}{s}\frac{s}{1} \in J$; quindi $x \in f^{-1}(J)$ e $\frac{x}{s} \in f^{-1}(J)_S$. Viceversa, $\forall\, \frac{x}{s} \in f^{-1}(J)_S$, si ha: $x \in f^{-1}(J) \implies \frac{x}{1} \in J \implies \frac{x}{1}\frac{1}{s} = \frac{x}{s} \in J$.

Veniamo all'ultima affermazione. Se $I_S = A_S$, allora $1 \in I_S$, cioè $\frac{1}{1} = \frac{x}{s}$, con $x \in I$; ne segue che $su = xu$ $(\exists\, u \in S)$ ed ovviamente $su = xu \in I \cap S$. Viceversa, se $s \in I \cap S$, allora $1 = \frac{s}{s} \in I_S$, cioè $I_S = A_S$.

Concludiamo con alcuni semplici esempi di parti moltiplicative in un anello c.u. A.

(*1*) Per ogni ideale primo $\mathfrak{p}$ di A, l'insieme $S = A - \mathfrak{p}$ è una parte moltiplicativa di A [se infatti $a, b \in A - \mathfrak{p}$, anche $ab \in A - \mathfrak{p}$]. Il corrispondente anello di frazioni viene denotato $A_{\mathfrak{p}}$.

(*2*) Per ogni $a \in A^{\cdot}$, l'insieme $S = \{a^k,\ \forall\, k \geq 0\}$ è una parte moltiplicativa di A (verificare). Il corrispondente anello di frazioni viene denotato A_a.

(*3*) Se $\mathcal{Z}(A)$ denota l'insieme degli 0-divisori di A, l'insieme $S = A - \mathcal{Z}(A)$ è una parte moltiplicativa di A [se infatti $a, b \notin \mathcal{Z}(A)$, anche $ab \notin \mathcal{Z}(A)$]. Il corrispondente anello di frazioni è chiamato *anello totale delle frazioni di A*.

(*4*) Per ogni ideale I di A, l'insieme $S = 1+I$ è una parte moltiplicativa di A [se $1+a, 1+b \in 1+I$, allora $(1 + a)(1 + b) = 1 + (a + b + ab) \in 1 + I$].

* * * * * * * * * * * * * * * * * * *

Esercizio 3.2.1. Siano A, B due domini d'integrità e sia $f : A \to B$ un omomorfismo iniettivo.

(*i*) Verificare che f induce un omomorfismo iniettivo $F : \boldsymbol{Q}(A) \to \boldsymbol{Q}(B)$.

(*ii*) Sia S una parte moltiplicativa di A. Verificare che $f(S)$ è una parte moltiplicativa di B e che f induce un omomorfismo iniettivo $F : A_S \to B_{f(S)}$.

Esercizio 3.2.2. Sia A un anello c.u..

(*i*) Verificare che l'insieme $\mathcal{U}(A)$ degli elementi invertibili di A è una parte moltiplicativa di A e determinare l'anello $A_{\mathcal{U}(A)}$.

(*ii*) Sia S una parte moltiplicativa di A. Verificare che $S \cdot \mathcal{U}(A) \subseteq \mathcal{U}(A_S)$.

(*iii*) Sia K un campo, $A = K[X]$ e $S = A - (X)$. Verificare che $S \cdot \mathcal{U}(A) \subset \mathcal{U}(A_S)$.

Esercizio 3.2.3. In $\boldsymbol{Z}_{12}$ sia $S = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\}$.

(*i*) Verificare che S è una parte moltiplicativa di $\boldsymbol{Z}_{12}$ e che l'omomorfismo $f : \boldsymbol{Z}_{12} \to (\boldsymbol{Z}_{12})_S$ non è iniettivo.

(*ii*) Dimostrare che $(\boldsymbol{Z}_{12})_S \cong \boldsymbol{Z}_3$ (campo).

Esercizio 3.2.4. (*i*) Sia A un anello c. u. e sia $\mathfrak{p}$ suo ideale primo. Verificare che $A_{\mathfrak{p}}$ possiede un unico ideale massimale M [usualmente denotato $\mathfrak{p}A_{\mathfrak{p}}$].

(*ii*) Scelto in $\boldsymbol{Z}$ l'ideale primo (2), determinare il campo $\boldsymbol{Z}_{(2)}/_M$.

Esercizio 3.2.5. (*i*) Sia S una parte moltiplicativa di un anello c. u. A. Verificare che

$$Spec(A_S) = \{\mathfrak{p}_S, \ \forall \mathfrak{p} \in Spec(A) \mid \mathfrak{p} \cap S = \emptyset\}.$$

(*ii*) Posto $S = \{6^h, \ \forall h \geq 0\}$, verificare che ogni ideale di $\boldsymbol{Z}_S$ è principale e determinare $Spec(\boldsymbol{Z}_S)$.

(*iii*) In $\boldsymbol{Z}_{16}$ sia $S = \{\overline{2}^h, \ \forall h \geq 0\}$. Determinare $Spec((\boldsymbol{Z}_{16})_S)$.

Esercizio 3.2.6. (*i*) Sia S una parte moltiplicativa di un anello c. u. A. Verificare che $Spec(A_S)$ può essere immerso in $Spec(A)$.

(*ii*) Se $a \in A$ e $S = \{a^h, \ \forall h \geq 0\}$, verificare che $Spec(A_S)$ si identifica ad un aperto di $Spec(A)$ (rispetto alla topologia di Zariski).

Esercizio 3.2.7. (*i*) Sia A un anello c. u. e sia $S_0 = A - \mathcal{Z}(A)$ l'insieme dei non 0-divisori di A. Verificare che S_0 è una parte moltiplicativa di A e che A è un sottoanello di A_{S_0}.

(*ii*) Sia S una parte moltiplicativa di A tale che l'omomorfismo canonico sia iniettivo. Verificare che $S \subseteq S_0$ [per questo motivo A_{S_0} è detto *anello totale delle frazioni di* A].

(*iii*) Calcolare $(\boldsymbol{Z}_{12})_{S_0}$.

Esercizio 3.2.8. In $\boldsymbol{Z}$ siano assegnati i numeri primi distinti $p_1, p_2, \ldots, p_n$. Determinare una parte moltiplicativa S di $\boldsymbol{Z}$ tale che il dominio $\boldsymbol{Z}_S$ ammetta come ideali primi non nulli esattamente $(p_1)_S, (p_2)_S, \ldots, (p_n)_S$.

Esercizio 3.2.9. Sia A un anello c. u. e sia $\mathfrak{p}$ un suo ideale primo. Dimostrare che

$$\boldsymbol{Q}(A/_{\mathfrak{p}}) \cong A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$$

[dove $\mathfrak{p}A_{\mathfrak{p}} = \{\frac{a}{s}, \ \forall a \in \mathfrak{p}, \ \forall s \in A - \mathfrak{p}\}$ è l'unico ideale massimale di $A_{\mathfrak{p}}$, cfr. Esercizio **3.2.4**].

3. Domini d'integrità

In questo paragrafo studieremo proprietà legate alla relazione di divisibilità in un dominio, descrivendo tre importanti famiglie di domini d'integrità, incluse l'una nell'altra. Cominciamo dalla più vasta.

Definizione 3.1. *Sia A un dominio d'integrità. A è detto dominio a fattorizzazione unica (o dominio fattoriale), abbreviato UFD, se*

(i) ogni $a \in A^{\cdot} - \mathcal{U}(A)$ è prodotto di un numero finito di elementi irriducibili di A.

(ii) sia $a \in A^{\cdot} - \mathcal{U}(A)$. Se $a = p_1 \dots p_r = q_1 \dots q_s$ sono due fattorizzazioni di a come prodotto di elementi irriducibili, i fattori dell'una coincidono con quelli dell'altra, a meno dell'ordine e di fattori invertibili.

Proposizione 3.1. *In ogni UFD ogni elemento irriducibile è primo.*

Dim. Sia A un *UFD*. Se $a \in A$ è un elemento irriducibile e $a \,|\, xy$, dobbiamo verificare che $a \,|\, x$ oppure $a \,|\, y$.

Sia $xy = at$, con $t \in A$. Assumiamo x, y non invertibili e non nulli (per evitare casi di ovvia soluzione). Allora $x = p_1 \dots p_r$ e $y = q_1 \dots q_s$ (con $p_1, \dots, p_r, q_1, \dots, q_s$ irriducibili). Essendo quindi

$$p_1 \dots p_r \, q_1 \dots q_s = at$$

ed a irriducibile, dalla condizione (*ii*) della precedente definizione segue che a coincide (a meno di un fattore invertibile) con uno dei p_i o con uno dei q_j. Dunque $a \,|\, x$ oppure $a \,|\, y$.

Proposizione 3.2. *In ogni UFD esistono il massimo comun divisore (abbr. MCD) ed il minimo comune multiplo (abbr. mcm) di due elementi.*

Dim. Sia A un *UFD* e siano $a, b \in A$. Se $a, b \in A^{\cdot} - \mathcal{U}(A)$, i due elementi ammettono fattorizzazioni come prodotto finito di elementi irriducibili (o primi). Assumiamo che

$$a = \prod_{i=1}^{n} {p_i}^{r_i}, \quad b = \prod_{i=1}^{n} {p_i}^{s_i},$$

con $p_1, \dots, p_n$ elementi irriducibili e $r_i, s_i \geq 0$. Poniamo:

$$d := \prod_{i=1}^{n} {p_i}^{d_i}, \text{ con } d_i = min\{r_i, s_i\}; \quad h := \prod_{i=1}^{n} {p_i}^{D_i}, \text{ con } D_i = max\{r_i, s_i\}.$$

Si tratta di provare che i due elementi $d, h \in A$ sopra definiti sono rispettivamente MCD e mcm di a, b, cioè verificano le definizioni di MCD e di mcm, che, per comodità del lettore, qui richiamiamo:

$$d := MCD(a,b) \iff d \,\Big|\, \begin{matrix} a \\ b \end{matrix} \text{ e } \Big[d' \,\Big|\, \begin{matrix} a \\ b \end{matrix} \implies d' \,|\, d \Big]; \quad h := mcm(a,b) \iff \begin{matrix} a \\ b \end{matrix} \,\Big|\, h \text{ e } \Big[\begin{matrix} a \\ b \end{matrix} \,\Big|\, h' \implies h \,|\, h' \Big].$$

La verifica è un semplice esercizio. Si ponga infine:

$$MCD(a,0) := a, \; mcm(a,0) := 0; \quad MCD(a,u) := 1, \; mcm(a,u) := a, \; \forall\, u \in \mathcal{U}(A).$$

Nota. $MCD(a,b)$ e $mcm(a,b)$ sono definiti a meno di un fattore invertibile (perché lo sono i fattori irriducibili di a, b).

Importanti esempi di *UFD* sono $\boldsymbol{Z}$ e $K[X]$, per ogni campo K. Ciò segue, come visto nel corso di **Alg. 1**, dal *teorema fondamentale dell'aritmetica* e da un analogo teorema per $K[X]$. Inoltre si osserva subito che ogni campo K è (banalmente) un *UFD* [infatti $K^{\cdot} - \mathcal{U}(K) = \emptyset$]. Un'altra vasta classe di esempi di *UFD* discende dal seguente teorema.

Teorema 3.1. *Se A è un UFD, $A[X]$ è un UFD.*

Il procedimento di *induzione forte* sul grado, utilizzato in **Alg. 1** per dimostrare che $K[X]$ è un

UFD (quando K è un campo), non può essere utilizzato per dimostrare che $A[X]$ è un *UFD* (quando A è un *UFD*, ma non un campo). Infatti la dimostrazione (per induzione) in $K[X]$ poggia sul fatto che tutti i polinomi di grado 0 sono invertibili e tutti quelli di grado 1 sono irriducibili, consentendo così la base induttiva, al grado 1; viceversa, in $A[X]$ esistono polinomi di grado 1 (e 0) riducibili. Per dimostrare il nostro risultato (Teor. **3.1**) utilizzeremo invece il lemma ed il teorema di Gauss [già studiati in $\boldsymbol{Z}[X]$ e $\boldsymbol{Q}[X]$, cfr. [AA], Cap. **3.3**], che sono facilmente estendibili ad $A[X]$ e a $\boldsymbol{Q}(A)[X]$, come vedremo nell'osservazione che segue.

Osservazione 3.1. Sia A un *UFD*. Poiché in A è definito il *MCD*, in analogia a quanto fatto in $\boldsymbol{Z}[X]$, si definisce il *contenuto* di ogni polinomio $f \in A[X]$:

$$c = c(f) := MCD(a_0, a_1, \dots a_n), \quad \forall\, f = \sum_{i=o}^{n} a_i X^i \in A[X].$$

Si dice poi che f è *primitivo* se $c(f) \in \mathcal{U}(A)$. Si verifica subito che, come avviene in $\boldsymbol{Z}[X]$, ogni polinomio $f \in A[X]$, $\partial f \geq 1$, si fattorizza in modo unico (a meno di fattori invertibili) nella forma

$$f = c\, f_*, \ \text{ con } \ c = c(f) \in A \ \text{ e } \ f_* \ \text{ primitivo.}$$

Si possono dimostrare (come in $\boldsymbol{Z}[X]$), il *lemma* ed il *teorema di Gauss*. Precisamente:

Lemma di Gauss. Per ogni $f, g \in A[X]$:

(i) se f, g sono primitivi, anche fg è primitivo.

(ii) $c(fg) = c(f)\, c(g)$ (a meno di fattori invertibili).

Teorema di Gauss. Se $f \in A[X]$ è irriducibile in $A[X]$, allora f è irriducibile anche in $\boldsymbol{Q}(A)[X]$.

Infine, per ogni $F \in \boldsymbol{Q}(A)[X]$, posto $F = \frac{a}{b}\, f$, con $\frac{a}{b} \in \boldsymbol{Q}(A)$ e $f \in A[X]$ primitivo, risulta:

$$F \text{ è irriducibile in } \boldsymbol{Q}(A)[X] \iff f \text{ è irriducibile in } A[X].$$

Dim. (*Teor.* **3.1**). Vanno dimostrate per $A[X]$ le condizioni (*i*) e (*ii*) di Def. **3.1**.

(*i*) Sia $f \in A[X]^{\cdot} - \mathcal{U}(A[X])$.

Se $\partial f = 0$, allora $f \in A^{\cdot} - \mathcal{U}(A)$ [si osservi che $\mathcal{U}(A) = \mathcal{U}(A[X])$] e dunque, essendo A un *UFD*, f è prodotto di un numero finito di elementi irriducibili in A. Tali elementi sono irriducibili anche in $A[X]$ [infatti, se a è irriducibile in A e $a = gh$ (in $A[X]$), allora $\partial g = \partial h = 0$, cioè $g, h \in A^{\cdot}$; pertanto $g \in \mathcal{U}(A) = \mathcal{U}(A[X])$ oppure $h \in \mathcal{U}(A) = \mathcal{U}(A[X])$].

Sia $\partial f \geq 1$. Denotiamo con K il campo dei quozienti di A. Ovviamente $A[X] \subset K[X]$ e $K[X]$ è un *UFD*. Allora f può essere scritto nella forma:

$$(*) \qquad f = \prod_{i=1}^{m} P_i\,, \ \text{ con } \ P_1, \dots P_m \in K[X], \ \text{ irriducibili in } \ K[X].$$

Si tratta allora di verificare che esistono $p_1, \dots, p_m \in A[X]$ polinomi irriducibili ed esiste $a \in A$, tali che $f = a \prod_{i=1}^{m} p_i$. Fattorizzando poi a (in A), si ottiene una fattorizzazione di f richiesta.

Possiamo porre (cfr. Osserv. **3.1**) $P_i = \frac{a_i}{b_i}\, p_i$, con p_i polinomio primitivo ed irriducibile in $A[X]$. La $(*)$ si riscrive quindi nella forma:

$$f = c\, f_* = \prod_{i=1}^{m} \tfrac{a_i}{b_i} \prod_{i=1}^{m} p_i\,, \ \text{ da cui } \ c\big(\prod_{i=1}^{m} b_i\big) f_* = \big(\prod_{i=1}^{m} a_i\big)\big(\prod_{i=1}^{m} p_i\big).$$

Dal lemma di Gauss, $\prod_{i=1}^{m} p_i$ è primitivo. Pertanto i contenuti dei due polinomi coincidono (a meno di un fattore invertibile), cioè

$$c\,\big(\prod_{i=1}^{m} b_i\big) = u \prod_{i=1}^{m} a_i\,, \ \text{ con } \ u \in \mathcal{U}(A).$$

Semplificando si ottiene: $f_* = \frac{1}{u} \prod_{i=1}^{m} p_i$ e dunque $f = a \prod_{i=1}^{m} p_i$, con $a\,(= u^{-1}c) \in A$, come richiesto.

(*ii*) Supponiamo che $f \in A[X]$, con $\partial f \geq 1$, ammetta le due seguenti fattorizzazioni:

$$a_1 \dots a_t \prod_{i=1}^{m} p_i = f = b_1 \dots b_s \prod_{j=1}^{l} q_j\,,$$

dove gli a_i, b_j sono elementi irriducibili in A ed i polinomi p_i, q_j sono irriducibili e primitivi in $A[X]$. Passando ai contenuti si ottiene (a meno di un fattore invertibile):

$$a_1 \dots a_t = b_1 \dots b_s .$$

Dunque, essendo A un *UFD*, gli a_i coincidono con i b_j (a meno dell'ordine e di fattori invertibili). Semplificando le due fattorizzazioni di f, si ottiene: $\prod_{i=1}^{m} p_i = u \prod_{j=1}^{l} q_j$ (con $u \in \mathcal{U}(A)$). In base al teorema di Gauss, i p_i ed i q_j sono polinomi irriducibili anche in $K[X]$. Dunque (essendo $K[X]$ un *UFD*) tali polinomi coincidono, a meno dell'ordine e di un fattore invertibile [contenuto in K e quindi, essendo primitivi, in A].

Corollario 3.1. *Se A è un UFD, per ogni $n \geq 1$ gli anelli $A[X_1, \dots, X_n]$ sono UFD.*

Dim. Basta osservare che $A[X_1, \dots, X_n] \cong A[X_1][X_2] \dots [X_n]$ ed applicare ripetutamente il Teor. **3.1**

Segnaliamo che se A è un *UFD* ed S è una parte moltiplicativa di A, con $0 \notin S$, si può dimostrare che anche l'anello delle frazioni A_S è un *UFD* (cfr. Esercizio **3.3.2**).

Completiamo il nostro studio sugli *UFD* con un *esempio di dominio d'integrità non UFD*. A tale scopo è necessario ricordare alcune nozioni sugli anelli quadratici $\boldsymbol{Z}[\sqrt{d}\,]$.

Osservazione 3.2. Sia $X^2 - d \in \boldsymbol{Z}[X]$ un polinomio irriducibile (su $\boldsymbol{Z}$). Come già osservato in Osserv. **2.1**(iv), l'anello quadratico $\boldsymbol{Z}[\sqrt{d}\,]$ è un dominio contenuto in $\boldsymbol{C}$ e contenente $\boldsymbol{Z}$, il cui campo dei quozienti è $\boldsymbol{Q}(\sqrt{d}\,)$. Per ogni $z = a + b\sqrt{d} \in \boldsymbol{Z}[\sqrt{d}\,]$ sono definiti:

$$\overline{z} = a - b\sqrt{d} \ \ (\textit{coniugato di } z); \quad \mathcal{N}(z) = z\,\overline{z} = a^2 - db^2 \in \boldsymbol{Z} \ \ (\textit{norma di } z).$$

Si verifica con semplici calcoli che

$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} \ \text{ e } \ \mathcal{N}(z_1\,z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2), \ \ \forall\, z_1,\, z_2 \in \boldsymbol{Z}[\sqrt{d}\,].$$

Se $d < 0$, $\mathcal{N}(z)$ coincide con l'usuale norma in $\boldsymbol{C}$ e risulta $\mathcal{N}(z) \geq 0$. Se invece $d > 0$, $\mathcal{N}(z)$ può anche essere negativa e non va confusa con la norma in $\boldsymbol{C}$. Verifichiamo poi che, in ogni caso,

$$\mathcal{N}(z) = 0 \iff z = 0.$$

L'implicazione ($\Longleftarrow$) è ovvia. Dimostriamo ($\Longrightarrow$). Sia $z \in \boldsymbol{Z}[\sqrt{d}\,]$ tale che $\mathcal{N}(z) = z\,\overline{z} = 0$. Poiché $\boldsymbol{Z}[\sqrt{d}\,]$ è integro, allora $z = 0$ oppure $\overline{z} = 0$, ma in tal caso ovviamente anche $z = 0$. Dunque $z = 0$.

Risulta subito:

$$z \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}\,]) \iff \mathcal{N}(z) = \pm 1.$$

Infatti, se $zw = 1$, allora $1 = \mathcal{N}(z)\mathcal{N}(w)$ e quindi $\mathcal{N}(z) = \pm 1$. Viceversa, se $\mathcal{N}(z) = z\,\overline{z} = \pm 1$, allora $z^{-1} = \pm\overline{z} \in \boldsymbol{Z}[\sqrt{d}\,]$ e dunque $z \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}\,])$.

In particolare, se $d = -1$, $\mathcal{U}(\boldsymbol{Z}[i]) = \{\pm 1, \pm i\}$; se invece $d \leq -2$, $\mathcal{U}(\boldsymbol{Z}[\sqrt{d}\,]) = \{\pm 1\}$ [infatti $a^2 - db^2 = 1 \iff a^2 = 1, b = 0$]. Se invece $d > 0$, la determinazione di $\mathcal{U}(\boldsymbol{Z}[\sqrt{d}\,])$ è più complicata. Ad esempio si verifica subito che $\mathcal{U}(\boldsymbol{Z}[\sqrt{5}\,])$ contiene (oltre a ± 1) anche gli elementi $\pm 2 \pm \sqrt{5}$, $\pm 9 \pm 4\sqrt{5}$ e tutte le rispettive potenze $(\pm 2 \pm \sqrt{5})^k$, $(\pm 9 \pm 4\sqrt{5})^k$, $\forall\, k \geq 0$.

Infine, dalle considerazioni precedenti segue subito che

se $\mathcal{N}(z)$ è primo (anche negativo), z è irriducibile.

Se infatti $z = z_1 z_2$ e $\mathcal{N}(z) = p$ primo (anche negativo), allora $\mathcal{N}(z_1)\mathcal{N}(z_2) = p$. Dunque, ad esempio, $\mathcal{N}(z_1) = \pm 1$ e quindi $z_1 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}\,])$.

Proposizione 3.3. $\boldsymbol{Z}[\sqrt{-5}\,]$ *non è un UFD.*

Dim. Ricordato che in un *UFD* ogni elemento irriducibile è primo, basta verificare che in $\boldsymbol{Z}[\sqrt{-5}\,]$ l'elemento $z = 1 + \sqrt{-5}$ è irriducibile ma non primo.

Verifichiamo che $z = 1 + \sqrt{-5}$ è irriducibile. Sia $z = w_1 w_2$. Allora $6 = \mathcal{N}(z) = \mathcal{N}(w_1)\mathcal{N}(w_2)$. Se dimostriamo che $\mathcal{N}(w_1) \neq 2$ (oppure $\mathcal{N}(w_1) \neq 3$), allora risulta necessariamente $\mathcal{N}(w_1) = 1, 6$ e $\mathcal{N}(w_2) = 6, 1$: dunque $w_1 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{-5}\,])$ oppure $w_2 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{-5}\,])$, cioè la fattorizzazione di z

è banale. Per assurdo, sia $\mathcal{N}(w_1) = 2$ [oppure $= 3$]. Posto $w_1 = a + b\sqrt{-5}$, allora $a^2 + 5b^2 = 2$ [oppure $= 3$]. Ma tale equazioni non ammettono soluzioni in $\boldsymbol{Z}$: assurdo.

Proviamo ora che $z = 1 + \sqrt{-5}$ non è primo. Poiché $z \mid z\,\overline{z} = 6 = 2\cdot 3$, sarà sufficiente verificare che $z \not| 2$ e $z \not| 3$. Per assurdo, $z \mid 2$. Allora $2 = (1 + \sqrt{-5})(a + b\sqrt{-5}) = a - 5b + (a + b)\sqrt{-5}$, con $a, b \in \boldsymbol{Z}$. Quindi

$$\{a - 5b = 2,\ a + b = 0,\ \text{cioè}\ 6a = 2:\ \text{assurdo (in } \boldsymbol{Z}).$$

In modo analogo si verifica che $z \not| 3$.

Nota. Per dimostrare che z non è primo in $\boldsymbol{Z}[\sqrt{-5}]$ si può anche verificare che $\boldsymbol{Z}[\sqrt{-5}]/_{(z)} \cong \boldsymbol{Z}_6$.

Poiché $\boldsymbol{Z}[i]$ è un quoziente di $\boldsymbol{Z}[X]$, il risultato appena dimostrato fornisce un esempio di un *UFD* un cui quoziente, modulo un ideale primo, non è *UFD*. Dunque la proprietà *UFD "non passa al quoziente"*.

Introduciamo ora un'altra famiglia di domini d'integrità. Come subito vedremo, è una sottofamiglia degli *UFD*.

Definizione 3.2. *Sia A un dominio. A è detto dominio a ideali principali, abbreviato PID, se ogni ideale I di A è principale, cioè $I = (a)$, $\exists\, a \in A$.* [*PID* è abbreviazione di *"Principal Ideal Domain"*].

Conosciamo già almeno quattro esempi di *PID*: $\boldsymbol{Z}$, K, $K[X]$ e $\boldsymbol{Z}[i]$. Non sono invece *PID* altri *UFD* già incontrati, come $\boldsymbol{Z}[X]$ e $K[X_1, \dots X_n]$, $\forall\, n \geq 2$. Infatti, ad esempio l'ideale $(X, 2)$ non è principale in $\boldsymbol{Z}[X]$ e $(X_1, \dots, X_n)$ non lo è in $K[X_1, \dots, X_n]$.

Teorema 3.2. *Ogni PID è un UFD.*

Premettiamo alla dimostrazione il seguente lemma.

Lemma 3.1. *Sia A un PID e sia $a \in A^{\cdot} - \mathcal{U}(A)$. Risulta:*

$$a \text{ è un elemento irriducibile in } A \iff (a) \text{ è un ideale massimale di } A.$$

Dim. ($\Longrightarrow$). Sia a irriducibile e sia I un ideale tale che $(a) \subseteq I \subseteq A$. Essendo A un *PID*, $I = (b)$, $\exists\, b \in A$. Allora $a = bc$, $\exists\, c \in A$. Poiché a è irriducibile, allora $b \in \mathcal{U}(A)$ oppure $c \in \mathcal{U}(A)$. Se $b \in \mathcal{U}(A)$, $I = A$. Se $c \in \mathcal{U}(A)$ (con $cd = 1$), allora $b = bcd = ad$, cioè $b \in (a)$; quindi $(b) = (a)$, cioè $I = (a)$. Dunque (a) è massimale.

($\Longleftarrow$). Sia (a) massimale. Allora (a) è primo e dunque a è un elemento primo di A. Quindi a è un elemento irriducibile di A (cfr. Osserv. **1.3**).

Nota. Ogni elemento irriducibile contenuto in un ideale massimale è un generatore di tale ideale.

Dim. (*Teor.* **3.2**). Si tratta di verificare le condizioni (*i*) e (*ii*) di Def. **3.1**.

(*i*) Sia $a \in A^{\cdot} - \mathcal{U}(A)$. Poiché $(a) \subset A$, esiste un ideale massimale (necessariamente principale) (q_1) tale che $(a) \subseteq (q_1)$. In base al Lemma **3.1**, q_1 è irriducibile. Sia $a = a_1 q_1$ [e quindi $(a) \subseteq (a_1)$].

Se $a_1 \in \mathcal{U}(A)$, la fattorizzazione di a è del tipo richiesto e la (*i*) è dimostrata. Sia invece $a_1 \notin \mathcal{U}(A)$. Risulta allora $(a) \subset (a_1) \subset A$ [si noti che se fosse $(a) = (a_1)$, allora $a = a_1 u$, con $u \in \mathcal{U}(A)$ e quindi $u = q_1$: assurdo]. Poiché $(a_1) \subset A$, esiste un ideale massimale (q_2) tale che $(a_1) \subseteq (q_2)$. L'elemento q_2 è irriducibile e $a_1 = a_2 q_2$, da cui $a = a_2 q_1 q_2$. Se $a_2 \in \mathcal{U}(A)$, la richiesta fattorizzazione di a è ottenuta; se invece $a_2 \notin \mathcal{U}(A)$, allora [come sopra] $(a_1) \subset (a_2) \subset A$. Iterando il procedimento, si ottiene una catena di ideali:

$$(a) \subset (a_1) \subset (a_2) \subset (a_3) \subset \dots .$$

Per ottenere la fattorizzazione di a richiesta, basta dimostrare che tale catena, dopo un numero finito di inclusioni proprie, si stabilizza, cioè

$$(*) \qquad (a) \subset \ ... \ \subset (a_{t-1}) \subset (a_t) = (a_{t+1}) = (a_{t+2}) = \ ... \ , \ \exists\, t \in \boldsymbol{N}.$$

Si ponga infatti $I = \bigcup_{i \geq 1} (a_i)$. Si verifica facilmente che I è un ideale. Quindi, per ipotesi, $I = (b)$, $\exists\, b \in A$. Allora $b \in (a_t)$, $\exists\, t \in \boldsymbol{N}$. Pertanto $(b) \subseteq (a_t) \subseteq (a_{t+1}) \subseteq \ ... \ \subseteq (b)$, da cui $(a_t) = (a_{t+1}) = \ ... \ ,$ come richiesto.

Se $(a_t) = (a_{t+1})$, allora $a_t \in \mathcal{U}(A)$ [altrimenti si avrebbe $a_t = a_{t+1} q_{t+1}$, $a_{t+1} = a_t v$ e quindi $v\, q_{t+1} = 1$, con q_{t+1} irriducibile: assurdo]. Dunque $a = a_t\, q_1 ... q_t$ è la fattorizzazione cercata.

(*ii*) Siano

$$a = p_1 ... p_r = q_1 ... q_s \ \ (\text{con } r \leq s)$$

due fattorizzazioni di $a \in A$ come prodotto di elementi irriducibili. In un *PID* ogni elemento iriducibile è primo (cfr. Lemma **3.1**). Allora, poiché $p_1 \,|\, q_1 ... q_s$ e p_1 è primo, p_1 divide un fattore q_i; per semplicità assumiamo che $p_1 \,|\, q_1$. Allora p_1, q_1 sono associati, cioè $q_1 = p_1 u_1$, con $u_1 \in \mathcal{U}(A)$ [infatti sono irriducibili]. Semplificando: $p_2 ... p_r = u_1 q_2 ... q_s$. Procedendo in modo analogo, $p_2 \,|\, q_2$ (ad esempio) e $q_2 = p_2 u_2$, con $u_2 \in \mathcal{U}(A)$, ecc.. Essendo $r \leq s$, $1 = u_1 u_2 ... u_r \ ... \ q_s$. Ne segue che $r = s$ e quindi i fattori delle due fattorizzazioni coincidono a meno dell'ordine (e di fattori invertibili).

Osservazione 3.3. Dal Lemma **3.1** discende subito che in un *PID* ogni ideale primo non nullo è massimale [infatti, se (a) è un ideale primo non nullo, allora $a \in A^{\cdot} - \mathcal{U}(A)$ ed a è un elemento primo; dunque a è irriducibile e quindi (dal Lemma **3.1**) (a) è massimale]. Vale anzi il seguente risultato (che non dimostriamo): *per ogni dominio d'integrità A,*

A è un PID $\iff$ A è un UFD ed ogni suo ideale primo non nullo è massimale.

Come applicazione dei risultati di questo e dei precedenti paragrafi dimostriamo il seguente fatto.

Proposizione 3.4. *Per ogni campo K, l'anello quoziente $K[X,Y]/_{(XY-1)}$ è un PID.*

Dim. Posto $A = K[X,Y]/_{(XY-1)}$, dimostreremo che tale anello è isomorfo ad un anello di frazioni di $K[X]$. Poiché $K[X]$ è un *PID* e la proprietà di essere *PID* passa ovviamente agli anelli di frazioni (cfr. Prop. **2.3**), allora A è un *PID*.

Posto $S = \{X^n, \ \forall\, n \in \boldsymbol{N}\}$, proveremo che

$$K[X,Y]/_{(XY-1)} \cong K[X]_S\,.$$

Allo scopo consideriamo l'applicazione

$$\Phi : K[X,Y] \to K[X]_S \ \text{ tale che } \ \Phi(F) = F(X, \tfrac{1}{X}), \ \ \forall\, F \in K[X,Y].$$

Lasciamo al lettore la verifica che Φ è un omomorfismo suriettivo di anelli. In base al *TFO*, per concludere basta provare che $Ker\Phi = (XY-1)$. L'inclusione $(\supseteq)$ è ovvia. Viceversa, si scelga $F \in Ker\Phi$. Osservato che nell'anello $K(X)[Y]$ è possibile eseguire la divisione con resto, dividiamo F per $XY-1$. Otteniamo:

$$F = (XY-1)\, Q + R, \ \text{ con } \ R,\, Q = \tfrac{H(X,Y)}{G(X)} \in K(X)[Y] \ \text{ e } \ \partial_{_Y} R < 1.$$

Pertanto $R \in K(X)$ e , dal fatto che $0 = F(X, \frac{1}{X}) = 0\, Q + R$, segue che $R = 0$. Quindi in $K[X,Y]$ si ha: $F\, G = (XY-1)\, H$. Dunque $(XY-1) \,|\, FG$.

Il polinomio $XY-1$ è evidentemente irriducibile in $K[X,Y]$ e dunque è primo (in quanto $K[X,Y]$ è un *UFD*). Poiché $XY-1 \not| G$, allora $XY-1 \,|\, F$, cioè $F \in (XY-1)$, come richiesto.

Vogliamo ora descrivere una famiglia ancor più ristretta di domini: quelli in cui è definita una divisione con resto (o euclidea). Tali domini, detti *domini euclidei*, sono, come vedremo, *PID*.

Dal corso di **Alg. 1**, sono noti i seguenti domini euclidei: $\boldsymbol{Z}$, $K[X]$, $\boldsymbol{Z}[i]$. Infatti è noto che:

(*1*) $\forall\, a, b \in \boldsymbol{Z}$, $b \neq 0$, $\exists!\, (q,r) \in \boldsymbol{Z} \times \boldsymbol{Z}$ tale che $a = bq + r$, $0 \leq r < |b|$;

(*2*) $\forall\, f, g \in K[X]$, $g \neq 0$, $\exists!\, (q,r) \in K[X] \times K[X]$ tale che $f = gq + r$, $\partial r < \partial g$ oppure $r = 0$;

(*3*) $\forall\, z,\, w \in \boldsymbol{Z}[i],\, w \neq 0,\ \exists\,(q,r) \in \boldsymbol{Z}[i]\times\boldsymbol{Z}[i]$ tale che $z = wq + r,\ \mathcal{N}(r) < \mathcal{N}(w)$.

Come si vede, in questi tre esempi è comune l'esistenza di una funzione definita su A ed a valori in $\boldsymbol{N}$, che *"valuta il resto inferiore al divisore"*. Si tratta rispettivamente del *valore assoluto* in $\boldsymbol{Z}$, del *grado* in $K[X]$ e della *norma* in $\boldsymbol{Z}[i]$. Denoteremo in generale con v tale funzione. Nei tre casi sopra esposti si può facilmente verificare che $v(ab) \geq v(a),\ \forall\, a, b \in A$. Inoltre si noti che nel caso (*2*) la funzione v [cioè ∂] non è definita in 0 [polinomio nullo], mentre nel caso (*3*) q ed r non sono unici. Con queste premesse arriviamo alla definizione "astratta" di dominio euclideo.

Definizione 3.3. *Sia A un dominio. A è detto dominio euclideo, abbreviato ED, se esiste una funzione $v : A^{\cdot} \to \boldsymbol{N}$ tale che*

(i) $v(ab) \geq v(a),\ \forall\, a, b \in A^{\cdot}$;

(ii) $\forall\, a, b \in A,\, b \neq 0,\ \exists\,(q,r) \in A\times A$ *tale che* $a = bq + r$ e $r = 0$ *oppure* $v(r) < v(b)$.

La funzione v viene talvolta detta valutazione euclidea su A o anche funzione d'innesco dell'algoritmo euclideo su A.

Osservazione 3.4. (*i*) Un dominio euclideo può essere dotato di differenti valutazioni euclidee. Ad esempio si noti che

$$v' : \boldsymbol{Z}^{\cdot} \to \boldsymbol{N} \text{ tale che } v'(a) = a^2,\ \forall\, a \in \boldsymbol{Z}^{\cdot},$$

è un'altra valutazione euclidea su $\boldsymbol{Z}$ [verificare].

(*ii*) Dalla (*i*) di Def. **3.3** segue subito che $v(1) \leq v(a),\ \forall\, a \in A^{\cdot}$. Inoltre si ha, $\forall\, a \in A^{\cdot}$:

$$a \in \mathcal{U}(A) \iff v(a) = v(1).$$

Infatti, se $a \in \mathcal{U}(A)$ e $ab = 1$, allora $v(1) = v(ab) \geq v(a) \geq v(1)$ e quindi $v(a) = v(1)$. Viceversa, sia $1 = aq + r$, con $r = 0$ oppure $v(r) < v(a)$. Poichè $v(a) = v(1) \leq v(r)$, necessariamente $r = 0$ e quindi $a \in \mathcal{U}(A)$.

(*iii*) Ogni campo K è un *ED*. Infatti si osserva subito che, $\forall\, a, b \in K,\, b \neq 0$ risulta $a = bq + 0$, con $q = \frac{a}{b}$. In altri termini in un campo la divisione con resto c'è ed ha sempre resto nullo! Si può porre

$$v : K^{\cdot} \to \boldsymbol{N} \text{ tale che } v(c) = 1,\ \forall\, c \in K^{\cdot}.$$

v è una valutazione euclidea su K. Si verifica facilmente che le valutazioni euclidee su K sono tutte e sole le funzioni costanti (non nulle) da $K^{\cdot}$ ad $\boldsymbol{N}$. [Sia infatti v una valutazione euclidea di K e, per assurdo, $\exists\, a \in K^{\cdot}$ tale che $v(a) > v(1)$. Allora $v(1) < v(a) \leq v(a\, a^{-1}) = v(1)$: assurdo].

(*iv*) In ogni *ED* esiste l'*algoritmo euclideo delle divisioni successive*. Infatti, $\forall\, a, b \in A^{\cdot}$, si ha:

$$\begin{aligned} &a = b\, q_1 + r_1, \text{ con } v(r_1) < v(b),\\ &b = r_1\, q_2 + r_2, \text{ con } v(r_2) < v(r_1),\\ &r_1 = r_2\, q_3 + r_3, \text{ con } v(r_3) < v(r_2),\\ &\ldots\ldots \end{aligned}$$

La successione $\{v(r_i)\}$ è strettamente decrescente in $\boldsymbol{N}$. Pertanto, dopo un numero finito di passi, l'algoritmo termina con un resto nullo, cioè con

$$r_{n-1} = r_n\, q_{n+1} + 0.$$

Proposizione 3.5. *Ogni ED è un PID.*

Dim. Sia A un *ED*, con valutazione euclidea v, e sia I un ideale non nullo di A. Dimostreremo che I è principale, generato da un suo elemento di valutazione minima.

Sia $S := \{v(x),\ \forall\, x \in I^{\cdot}\}$. S è un sottoinsieme non vuoto di $\boldsymbol{N}$ e quindi ha un minimo. Sia tale minimo $s_0 = v(x_0)$ [$x_0 \in I^{\cdot}$]. Evidentemente $(x_0) \subseteq I$. Viceversa, $\forall\, x \in I$, dalla (*ii*) di Def. **3.3** segue che esistono $q, r \in A$ tali che $x = x_0\, q + r$, con $r = 0$ oppure $v(r) < v(x_0)$. Poiché $r = x - x_0\, q \in I$, dalla minimalità di $v(x_0)$ segue che $r = 0$. Pertanto $x = x_0\, q \in (x_0)$.

Osservazione 3.5. Dalla proposizione ora dimostrata e dalla Prop. **3.1** segue in particolare che in ogni *ED* è definito il *MCD* (ed il *mcm*) di due elementi. Per calcolarlo si può utilizzare (come si

fa per $\boldsymbol{Z}$) l'algoritmo euclideo delle divisioni successive, sfruttando il seguente semplice risultato:

Sia A un ED e siano $a, b \in A$, $b \neq 0$. Se $a = bq + r$, con $r = 0$ oppure $v(r) < v(b)$, allora $MCD(a,b) = MCD(b,r)$ (a meno di un fattore invertibile).

Infatti, posto $d := MCD(a,b)$, $d_1 := MCD(b,r)$, risulta:

$$d \,\Big|\, \begin{matrix} a \\ b \end{matrix} \implies d \,|\, a - bq = r \implies d \,\Big|\, \begin{matrix} b \\ r \end{matrix} \implies d \,|\, d_1; \quad d_1 \,\Big|\, \begin{matrix} b \\ r \end{matrix} \implies d_1 \,|\, bq + r = a \implies d_1 \,\Big|\, \begin{matrix} a \\ b \end{matrix} \implies d_1 \,|\, d.$$

Dunque $d = d_1$ (a meno di un fattore invertibile). Ne segue (con le notazioni di Osserv. **3.4**(*iv*)) che

$$MCD(a,b) = MCD(b,r_1) = \ ... \ = MCD(r_{n-1}, r_n) = MCD(r_n, 0) = r_n,$$

cioè $MCD(a,b) = r_n$. Infine, rimontando dall'ultima espressione dell'algoritmo euclideo alla prima, si ottiene un'*identità di Bézout*, del tipo $r_n = ax + by$.

Concludiamo con due domande che dovremmo porci:

- esiste un *PID* non *ED*? - quali esempi di *ED* esistono, diversi da quelli sopra considerati?

Si ottengono risposte a queste domande nell'ambito della *teoria algebrica dei numeri*. Ci limitiamo qui a citare alcuni risultati. Premettiamo un lemma, lasciato per esercizio (cfr. Esercizio **3.3.11**).

Lemma 3.2. *Sia $d \in \boldsymbol{Z}$ tale che $d \equiv 1 \ (mod\ 4)$ e d non quadrato perfetto. Posto $\omega_d := \frac{1+\sqrt{d}}{2}$ e $d - 1 = 4s$ ($s \in \boldsymbol{Z}$), risulta che ω_d è zero del polinomio $f = X^2 - X - s \in \boldsymbol{Z}[X]$, irriducibile in $\boldsymbol{Z}[X]$. Ne segue che*

$$\boldsymbol{Z}[X]\big/_{(f)} \cong \{a + b\,\omega_d, \ \ \forall\, a,\, b \in \boldsymbol{Z}\} := \boldsymbol{Z}[\omega_d]$$

è un dominio d'integrità, contenente $\boldsymbol{Z}[\sqrt{d}]$ ed avente per campo dei quozienti $\boldsymbol{Q}(\sqrt{d})$.

Nota. Il "prototipo" degli $\boldsymbol{Z}[\omega_d]$ è $\boldsymbol{Z}[\omega_5]$. Tale anello è stato utilizzato da Dirichlet e Legendre per dimostrare (nel 1825) l'*Ultimo Teorema di Fermat* per $n = 5$, cioè: *l'equazione $X^5 + Y^5 = Z^5$ non ha soluzioni intere positive.* [Si noti che ω_5 è il *numero d'oro* (cfr. Cap. **4**, Def. **4.3**)].

I primi esempi di *PID* non *ED* sono stati trovati tra i domini $\boldsymbol{Z}[\omega_d]$. Il più semplice (individuato già da Dedekind) è $\boldsymbol{Z}[\omega_{-19}]$. Altri esempi sono i domini $\boldsymbol{Z}[\omega_d]$, con $d = -163, -67, -43, 53, 61, 69, 77, 89$, ecc. ed i domini $\boldsymbol{Z}[\sqrt{d}]$, con $d = 14, 22, 23, 31, 38$, ecc..

Nella prima metà del 1900, con il contributo di vari matematici, sono stati individuati tutti e soli gli interi d per cui $\boldsymbol{Z}[\omega_d]$ è un *ED* (con valutazione euclidea data dal modulo della norma). Si tatta dei domini:

$$\boldsymbol{Z}[\omega_d], \ \text{con} \ \ d = -11, -7, -3, 5, 13, 17, 21, 29, 33, 37, 41, 57, 73.$$

Relativamente agli $\boldsymbol{Z}[\sqrt{d}]$, sono *ED* (sempre rispetto al modulo della norma) i seguenti domini:

$$\boldsymbol{Z}[\sqrt{d}], \ \text{con} \ \ d = -2, -1, 2, 3, 6, 7, 11, 19,$$

mentre non sono *ED* tutti i domini $\boldsymbol{Z}[\sqrt{d}]$, con $d \leq -3$ (cfr. Eserc. **3.3.7**).

Più complicato, con varie questioni tuttora aperte, è il problema della determinazione dei *PID* tra i domini $\boldsymbol{Z}[\sqrt{d}]$ e $\boldsymbol{Z}[\omega_d]$.

Nota. Si osservi che il termine *"ideale"* è nato nello studio di tali anelli, precisamente quando E.Kummer (nel 1844), scelti in A ($= \boldsymbol{Z}[\sqrt{d}]$ o $\boldsymbol{Z}[\omega_d]$) una coppia di elementi z, w privi di MCD, chiamò *"numero ideale"* l'insieme di numeri $zA + wA$ [cioè l'ideale $(z,\, w)$ di A].

* * * * * * * * * * * * * * * * * *

Esercizio 3.3.1. Dimostrare che ogni dominio d'integrità finito è un campo.

Esercizio 3.3.2. Dimostrare che se A è un *UFD* e se S è una parte moltiplicativa di A, con

$0 \notin S$, anche l'anello delle frazioni A_S è un *UFD*.

Esercizio 3.3.3. (*i*) Posto $I = (X^2 + Y^2) \subset \boldsymbol{Z}[X, Y]$, verificare che I è primo.
(*ii*) Determinare un ideale massimale di $\boldsymbol{Z}[X, Y]$ contenente I.
(*iii*) Rispondere alle precedenti domande assumendo $I \subset \boldsymbol{R}[X, Y]$.

Esercizio 3.3.4. (*i*) Verificare che in $\boldsymbol{Z}[\sqrt{2}]$ i due elementi $z = 1 - \sqrt{2}$, $w = 7 + 5\sqrt{2}$ sono invertibili e calcolarne l'inverso.
(*ii*) Verificare che $\mathcal{U}(\boldsymbol{Z}[\sqrt{2}])$ è un gruppo infinito non ciclico.
(*iii*) Verificare che $1 + 2\sqrt{2}$ è un elemento primo di $\boldsymbol{Z}[\sqrt{2}]$.
(*iv*) Verificare che l'elemento 2 non è irriducibile in $\boldsymbol{Z}[\sqrt{2}]$.

Esercizio 3.3.5. In $\boldsymbol{Z}[\sqrt{2}]$ fattorizzare gli interi primi 2, 3, 5, 7 come prodotto di elementi irriducibili di $\boldsymbol{Z}[\sqrt{2}]$.

Esercizio 3.3.6. Sono assegnati in $\boldsymbol{Z}[\sqrt{-5}]$ i due elementi $z_1 = 9$, $z_2 = 3(2 + \sqrt{-5})$.
(*i*) Determinare i divisori comuni di z_1, z_2. (*ii*) Verificare se tali divisori sono elementi primi.
(*iii*) Verificare che non esiste $MCD(z_1, z_2)$.

Esercizio 3.3.7. Sia d un intero ≤ -3. (*i*) Verificare che 2 non è primo in $\boldsymbol{Z}[\sqrt{d}]$.
(*ii*) Verificare che 2 è irriducibile in $\boldsymbol{Z}[\sqrt{d}]$. (*iii*) Confrontare (*i*) e (*ii*) con la Prop. **3.3**.

Esercizio 3.3.8. In $\boldsymbol{Z}[\sqrt{6}]$ fattorizzare $z = 4 + \sqrt{6}$ come prodotto di elementi irriducibili.

Esercizio 3.3.9. Fattorizzare in $\boldsymbol{Z}[\sqrt{-2}]$ i tre elementi 2, 3, $z = 2 + \sqrt{-2}$, come prodotto di fattori iriducibili.

Esercizio 3.3.10. Sia A un dominio e siano $a, b, c \in A$.
(*i*) Verificare che se $(a, b) = (c)$, allora $c = MCD(a, b)$.
(*ii*) Se esiste $MCD(a, b) =: d$, è vero che $(a, b) = (d)$?
Suggerimento. Considerare in $\boldsymbol{Z}[\sqrt{-3}]$ gli elementi 2, $1 + \sqrt{-3}$.

Esercizio 3.3.11. Dimostrare il Lemma **3.2**.

Esercizio 3.3.12. Sia A un *ED* e v una sua valutazione euclidea. Scelti $a, b \in A^{\cdot}$, dimostrare che:
(*i*) $v(ab) = v(a) \iff b \in \mathcal{U}(A)$.
(*ii*) $v(ab) = max\{v(a), v(b)\} \iff a \in \mathcal{U}(A)$ oppure $b \in \mathcal{U}(A)$.

Esercizio 3.3.13. È noto che $\boldsymbol{Z}[\sqrt{2}]$ è un *ED* (rispetto al valore assoluto della norma). Scelti $z = 10 + 3\sqrt{2}$, $w = 1 + 2\sqrt{2} \in \boldsymbol{Z}[\sqrt{2}]$:
(*i*) Calcolare quoziente e resto della divisione euclidea di z per w. [*Suggerimento.* Procedere come visto in $\boldsymbol{Z}[i]$, cfr. [AA] pag. 126].
(*ii*) Con l'algoritmo euclideo delle divisioni successive, verificare che $MCD(z, w) = 1$ e determinare un'identità di Bézout relativa a z, w.

4. Caratteristica di un anello

Sia A un anello commutativo unitario. Denotata con 1_A la sua unità, è definita l'applicazione

$$f : \boldsymbol{Z} \to A \text{ tale che } f(n) = n\,1_A, \ \forall\, n \in \boldsymbol{Z},$$

[con $n\,1_A = 1_A + \ldots + 1_A$ (n volte), se $n > 0$, $0\,1_A = 0_A$, $n\,1_A = -(|n|1_A)$, se $n < 0$]. Si verifica subito che f è un omomorfismo di anelli e che trasforma l'unità 1 di $\boldsymbol{Z}$ in 1_A [o, come si dice, che f è un *omomorfismo unitario*].

$Im\, f = \{n\,1_A, \ \forall\, n \in \boldsymbol{Z}\}$ è un sottoanello di A ed ovviamente è il più piccolo sottoanello unitario di A; viene anche chiamato *sottoanello fondamentale di* A e denotato $\boldsymbol{F}_A$. Il nucleo $Ker f = \{n \in \boldsymbol{Z} : \ n\,1_A = 0_A\}$ è un ideale di $\boldsymbol{Z}$ e quindi è principale; porremo $Ker f = (c)$, con $c \geq 0$.

Definizione 4.1. *Sia A un anello c. u. e sia $f : \boldsymbol{Z} \to A$ l'omomorfismo sopra considerato. Si dice che A ha caratteristica c [e si scrive $car(A) = c$] se $Ker f = (c)$, con $c \geq 0$.*

Dal *TFO*, $\boldsymbol{F}_A \cong \boldsymbol{Z}/_{(c)}$. Ne segue:

$$\boldsymbol{F}_A \cong \boldsymbol{Z}, \text{ se } car(A) = 0; \qquad \boldsymbol{F}_A \cong \boldsymbol{Z}_c, \text{ se } car(A) = c \geq 2.$$

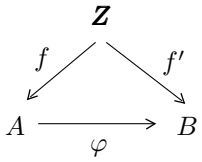
[Si noti che $car(A) = 1 \iff Ker f = \boldsymbol{Z} \iff f = \boldsymbol{0} \iff 1_A = 0_A \iff A = \boldsymbol{0}$ (anello nullo)].

Si verifica immediatamente che $car(\boldsymbol{Z}_n) = n$ e che $car(\boldsymbol{Z}) = 0$. Si noti inoltre che ogni anello c. u. di caratteristica 0 è infinito [in quanto contiene $\boldsymbol{Z}$, a meno di isomorfismi]. Ne segue che ogni anello c. u. finito ha caratteristica > 0. Tale risultato non si inverte: esistono anelli infiniti di caratteristica positiva. Infatti, come subito seguirà dalla Prop. **4.1**(ii), $\boldsymbol{Z}_n[X]$ è un anello infinito, con $car(\boldsymbol{Z}_n[X]) = n$, $\forall\, n \geq 2$.

Proposizione 4.1. *(i) Sia $\varphi : A \to B$ un omomorfismo iniettivo ed unitario di anelli c. u.. Risulta: $car(A) = car(B)$.*

(ii) Per ogni anello c. u. A, risulta: $car(A) = car(A[X])$.

Dim. (i) Si consideri il diagramma:



con $f(n) = n1_A$, $f'(n) = n1_B$, $\forall\, n \in \boldsymbol{Z}$.

Poiché $\varphi(1_A) = 1_B$, risulta allora $\varphi \circ f = f'$ [infatti $(\varphi \circ f)(n) = \varphi(n1_A) = n\varphi(1_A) = n1_B = f'(n)$]. Poiché φ è iniettiva, $Ker(\varphi \circ f) = Ker f$. Ne segue che $Ker f' = Ker f$, cioè $car(B) = car(A)$.

(ii) Basta utilizzare (i) ed osservare che l'inclusione canonica $i : A \hookrightarrow A[X]$ è un omomorfismo iniettivo unitario.

Proposizione 4.2. *Sia A un anello c. u. di caratteristica $c > 0$. Risulta:*

c è il minimo intero positivo tale che $cx = 0$, $\forall\, x \in A$.

Dim. Sia $car(A) = c > 0$. Poiché $Ker f = (c)$, c è il minimo intero positivo in $Ker f$, cioè tale che $c1_A = 0$. Per ogni $x \in A$, risulta: $cx = c(1_A\, x) = (c\,1_A)x = 0\,x = 0$. Sia poi $c' > 0$ tale che $c'\,x = 0$, $\forall\, x \in A$. In particolare $c'\,1_A = 0$ e dunque $c' \geq c$.

Nota. Se $car(A) = 0$, 0 è l'unico intero c tale che $cx = 0$, $\forall\, x \in A$ [infatti da $cx = 0$, $\forall\, x \in A$, segue che $c\,1_A = 0$ e quindi $c \in Ker f = (0)$].

Proposizione 4.3. *Sia A un dominio d'integrità. Se $car(A) \geq 2$, $car(A)$ è un primo p. Ne*

segue che $\boldsymbol{F}_A \cong \boldsymbol{Z}_p$.

Dim. Sia $car(A) = c \geq 2$. Sia $c = c_1 c_2$, con $1 \leq c_1, c_2 \leq c$. Risulta:

$$0_A = c\,1_A = (c_1 c_2)1_A = (c_1\,1_A)(c_2\,1_A).$$

Essendo A integro, uno dei due fattori è nullo, ad esempio $c_1\,1_A = 0$. Ne segue che $c_1 = c$ [e quindi $c_2 = 1$]. Allora la fattorizzazione di c è banale e quindi c è un numero primo.

Se K è un campo, ha caratteristica 0 oppure p (primo). Il sottoanello fondamentale $\boldsymbol{F}_K$ è un dominio (in quanto sottoanello di un campo). Sia $\boldsymbol{Q}(\boldsymbol{F}_K)$ il suo campo dei quozienti. Ovviamente $\boldsymbol{Q}(\boldsymbol{F}_K) \subseteq K$ (a meno di isomorfismi). Dai risultati precedenti:

$$\boldsymbol{F}_K \cong \boldsymbol{Z}, \text{ se } car(K) = 0; \qquad \boldsymbol{F}_K \cong \boldsymbol{Z}_p, \text{ se } car(K) = p \geq 2.$$

Ne segue:

$$\boldsymbol{Q}(\boldsymbol{F}_K) \cong \boldsymbol{Q}, \text{ se } car(K) = 0; \qquad \boldsymbol{Q}(\boldsymbol{F}_K) \cong \boldsymbol{Z}_p, \text{ se } car(K) = p \geq 2.$$

Il campo $\boldsymbol{Q}(\boldsymbol{F}_K)$ è detto *sottocampo fondamentale di* K [o *sottocampo primo di* K] ed è usualmente denotato K_f. Abbiamo dimostrato che ogni campo K contiene (a meno di isomorfismi)

$$\boldsymbol{Q}, \text{ se } car(K) = 0; \ \boldsymbol{Z}_p, \text{ se } car(K) = p \geq 2.$$

Osservazione 4.3. (*i*) Il sottocampo fondamentale K_f è l'intersezione di tutti i sottocampi di K (cioè il più piccolo sottocampo di K).
Se infatti $L \subseteq K$ ed L è un campo, allora $1_K \in L$ e quindi $\boldsymbol{F}_K \subseteq L$. Allora $K_f = \boldsymbol{Q}(\boldsymbol{F}_K) \subseteq L$.

(*ii*) Se H, K sono campi ed esiste un omomorfismo non nullo $\varphi : H \to K$, allora $car(H) = car(K)$.

Basta verificare che φ è unitario ed iniettivo ed applicare la Prop. **4.1**(*i*). Sia infatti $\varphi(1_H) = a$, con $a \neq 0$ (essendo φ non nullo). Allora $a = \varphi(1_H \cdot 1_H) = \varphi(1_H)\varphi(1_H) = a^2$ e quindi $a = 1_K$. Inoltre, poiché $Ker\varphi$ è un ideale di H e $Ker\varphi \neq H$ (essendo φ non nullo), allora $Ker\varphi = \{0\}$, cioè φ è iniettivo.

* * * * * * * * * * * * * * * * * * *

Esercizio 3.4.1. Sia K un campo di caratteristica $p > 0$. Verificare che l'applicazione

$$\varphi : K \to K \text{ tale che } \varphi(a) = a^p, \ \forall\, a \in K,$$

è un omomorfismo iniettivo di anelli. Se K è finito, verificare che φ è un automorfismo di K. Tale automorfismo è detto *automorfismo di Frobenius di* K.

Esercizio 3.4.2. Siano A, B anelli commutativi unitari, entrambi di caratteristica positiva. Determinare la caratteristica del prodotto diretto $A \times B$.

Esercizio 3.4.3. Sia $\varphi : A \to B$ un omomorfismo unitario di anelli commutativi unitari. Verificare che $car(B) \,|\, car(A)$.

Esercizio 3.4.4. Sia A un anello commutativo unitario.
(*i*) Indicato con A_{S_0} l'anello totale delle frazioni di A, verificare che $car(A_{S_0}) = car(A)$.
(*ii*) Determinare un esempio di parte moltiplicativa S di A tale che $car(A_S) \neq car(A)$.

Esercizio 3.4.5. Ogni anello commutativo unitario A contiene, come sottoanello unitario, al più un solo anello $\boldsymbol{Z}_n$, $n \geq 2$.

Capitolo 4

ELEMENTI DI TEORIA DEI CAMPI

1. Estensioni di campi

Siano K, L due campi. L'applicazione *nulla* $\mathbf{0} : K \to L$ [tale che $\mathbf{0}(c) = 0,\ \forall\, c \in K$] è un omomorfismo di anelli, detto *omomorfismo banale*. Ogni altro eventuale omomorfismo $\varphi : K \to L$ è iniettivo [infatti, essendo $Ker\varphi$ un ideale di K e $Ker\varphi \neq K$ (perché $\varphi \neq \mathbf{0}$), allora $Ker\varphi = \{0\}$]. Dunque, a meno di isomorfismi, φ identifica K ad un sottocampo di L [cioè la sua immagine $Im\,\varphi = \varphi(K)$].

Definizione 1.1. *Siano K, L due campi. Se K è un "sottocampo" [cioè un sottoanello che è un campo] di L, diremo che $K \subseteq L$ è un'estensione di campi, ovvero che L è un'estensione di K. [Talora è usato il termine ampliamento come sinonimo di estensione].*

Come osservato sopra, ogni omomorfismo non banale di campi $\varphi : K \to L$ determina l'estensione di campi $\varphi(K) \subseteq L$. Viceversa, un'estensione di campi $K \subseteq L$ definisce l'omomorfismo canonico d'inclusione (non banale) $i : K \hookrightarrow L$. Pertanto è lecito generalizzare la definizione precedente come segue.

Definizione 1.1'. *Si chiama estensione di campi ogni omomorfismo non banale di campi $\varphi : K \to L$.*

Tale generalizzazione si renderà necessaria per alcuni risultati dei prossimi paragrafi. Ma, dove possibile, indicheremo un'estensione di campi nella forma $K \subseteq L$, piuttosto che $\varphi : K \to L$.

Definizione 1.2. *Siano $K \subseteq L$ e $K \subseteq \tilde{L}$ due estensioni di campi, a partire da uno stesso campo K. Un omomorfismo di campi $F : L \to \tilde{L}$ è detto K-omomorfismo se risulta $F(c) = c,\ \forall\, c \in K$ (cioè se F fissa tutti gli elementi di K). In altri termini, F è un K-omomorfismo se è commutativo il seguente diagramma di omomorfismi:*

$$\begin{array}{ccc} L & \xrightarrow{\ F\ } & \tilde{L} \\ \uparrow i & & \uparrow \tilde{\imath} \\ K & \xrightarrow{\ \mathbf{1}_K\ } & K \end{array}$$

ovvero $F \circ i = \tilde{\imath} \circ \mathbf{1}_K$ [infatti $(F \circ i)(c) = F(c)$, $(\tilde{\imath} \circ \mathbf{1}_K)(c) = c,\ \forall\, c \in K$. Scriveremo (impropriamente) tale relazione nella forma $F_{|_K} = \mathbf{1}_K$]. *Ogni K-omomorfismo è ovviamente non banale (e dunque è un'estensione di campi). Infine si chiama K-isomorfismo ogni K-omomorfismo biiettivo.*

Osservazione 1.1. (*i*) Se le due estensioni sono definite dagli omomorfismi non banali $\varphi : K \to L$ e $\tilde{\varphi} : K \to \tilde{L}$, un omomorfismo $F : L \to \tilde{L}$ è detto K-omomorfismo se $F \circ \varphi = \tilde{\varphi}$ [$= \tilde{\varphi} \circ \mathbf{1}_K$].

(*ii*) Se $F : L \to \tilde{L}$ è un omomorfismo non banale di campi, in base all'Osserv. **4.3** del Cap. **3** risulta $car(L) = car(\tilde{L})$ e quindi $L, \tilde{L}$ hanno (a meno di isomorfismi) lo stesso sottocampo fondamentale K_f. Si osserva subito allora che F è un K_f-omomorfismo [infatti, $\forall\, n \in \boldsymbol{Z},\ F(n1) = n\,F(1) = n1$ e quindi $F(c) = c,\ \forall\, c \in K_f$].

(*iii*) La definizione di K-omomorfismo si estende inalterata al caso di due anelli contenenti un campo K.

Definizione 1.3. *Siano $\varphi : K \to L$ e $\tilde{\varphi} : \tilde{K} \to \tilde{L}$ due estensioni di campi. Tali estensioni sono dette isomorfe se esistono due isomorfismi di campi $f : K \to \tilde{K}$, $F : L \to \tilde{L}$, tali che $F \circ \varphi = \tilde{\varphi} \circ f$,*

cioè tali che sia commutativo il seguente diagramma di omomorfismi:

$$\begin{array}{ccc} L & \xrightarrow[\cong]{F} & \tilde{L} \\ \varphi\uparrow & & \uparrow\tilde{\varphi} \\ K & \xrightarrow[\cong]{f} & \tilde{K} \end{array}$$

Nota. Si verifica facilmente che la relazione di *isomorfismo tra estensioni di campi* è una relazione di equivalenza nell'insieme delle estensioni di campi.

Data un'estensione di campi $K \subseteq L$ (ovvero, più generalmente, un omomorfismo non banale $\varphi : K \to L$), L è dotato in modo naturale di struttura di K-spazio vettoriale. Infatti $(L, +)$ è un gruppo abeliano ed è definita la seguente moltiplicazione scalare

$$L \times K \to L \text{ tale che } (\ell, c) \to \ell c \text{ [ovvero } (\ell, c) \to \ell\,\varphi(c)], \quad \forall\, \ell \in L, \ \forall\, c \in K.$$

La verifica degli assiomi di spazio vettoriale è un semplice esercizio.

Definizione 1.4. *Si chiama grado dell'estensione $K \subseteq L$ la dimensione $dim_{K} L$ di L come K-spazio vettoriale. Il grado di $K \subseteq L$ verrà denotato $[L : K]$. Un'estensione $K \subseteq L$ è detta finita se $[L : K] < \infty$.*

Esempi 1.1. (*i*) $[\boldsymbol{C} : \boldsymbol{R}] = 2$. Infatti ad esempio $\{1, i\}$ è una base di $\boldsymbol{C}$ come $\boldsymbol{R}$-spazio vettoriale.

(*ii*) $[K(X) : K] = \infty$. Infatti, $\forall\, n \in \boldsymbol{N}$, gli $n+1$ polinomi $1, X, X^2, \ldots X^n$ (in $K(X)$) sono K-linearmente indipendenti [cioè $\sum_{i=0}^{n} a_i X^i = 0 \implies a_0 = \ldots = a_n = 0$]. Dunque $[K(X) : K] > n$, $\forall\, n \in \boldsymbol{N}$, e quindi $[K(X) : K] = \infty$.

(*iii*) $[L : K] = 1 \iff K = L$ (a meno di isomorfismi). Infatti $[L : K] = 1 \iff \{1\}$ è una base di L su $K \iff K = L$.

(*iv*) Siano $K \subseteq L$ e $\tilde{K} \subseteq \tilde{L}$ due estensioni isomorfe (con isomorfismi $f : K \to \tilde{K}$ e $F : L \to \tilde{L}$). Allora $[L : K] = [\tilde{L} : \tilde{K}]$. Infatti si verifica subito che se $\{\ell_i\}_{i \in I}$ è una base di L su K, allora $\{F(\ell_i)\}_{i \in I}$ è una base di $\tilde{L}$ su $\tilde{K}$.

Proposizione 1.1. *Sia K un campo finito. Allora $|K| = p^n$, con p primo e $n \geq 1$.*

Dim. Essendo K finito, il suo sottocampo fondamentale K_f è isomorfo a $\boldsymbol{Z}_p$ (p primo). Ovviamente $[K : \boldsymbol{Z}_p] < \infty$. Se $[K : \boldsymbol{Z}_p] = n$ e $\{\alpha_1, \ldots, \alpha_n\}$ è una base di K su $\boldsymbol{Z}_p$, ogni elemento di K si scrive in modo unico come combinazione lineare di $\alpha_1, \ldots, \alpha_n$, a coefficienti in $\boldsymbol{Z}_p$. Pertanto $|K| = p^n$.

La seguente proprietà, nota col nome di *moltiplicatività del grado*, permette di calcolare il grado di un'estensione di campi, spezzandola in un'opportuna *catena* di estensioni (cioè una sequenza finita di estensioni consecutive).

Teorema 1.1. *Sia $K \subseteq M \subseteq L$ una catena di estensioni di campi. Risulta:*

$$[L : K] = [L : M] \cdot [M : K].$$

Dim. Sia $\{m_i\}_{i \in I}$ una base di M su K e sia $\{\ell_j\}_{j \in J}$ una base di L su M. Basterà verificare che $\{m_i \ell_j\}_{i \in I,\, j \in J}$ è una base di L su K. Ne segue infatti che

$$[L : K] = |\{m_i \ell_j\}_{i \in I,\, j \in J}| = |I \times J| = |I| \cdot |J| = [M : K] \cdot [L : M].$$

Proviamo che $\{m_i \ell_j\}_{i \in I,\, j \in J}$ è un sistema di generatori di L su K. Risulta, per ogni $\ell \in L$,

$$\ell = \sum_{t=1}^{k} a_t \ell_{j_t}\,, \ \text{con} \ \ a_t \in M.$$

Se $a_t = \sum_{s=1}^{h_t} c_{ts} m_{i_s}$, con $c_{ts} \in K$, allora

$$\ell = \sum_{t=1}^{k} \sum_{s=1}^{h_t} c_{ts} \ell_{j_t} m_{i_s}\,.$$

Proviamo ora che $\{m_i \ell_j\}_{i\in I,\, j\in J}$ è formata da vettori K-linearmente indipendenti. Sia

$$\sum_{t=1}^{k} \sum_{s=1}^{h} c_{ts} \ell_{j_t} m_{i_s} = 0, \ \text{con} \ \ c_{ts} \in K.$$

Allora $0 = \sum_{t=1}^{k} \big(\sum_{s=1}^{h} c_{ts} m_{i_s}\big)\ell_{j_t}$. Essendo $\ell_{j_1}, \dots, \ell_{j_k}$ M-linearmente indipendenti, allora

$$\sum_{s=1}^{h} c_{ts} m_{i_s} = 0, \ \ \forall\, t = 1, \dots, k.$$

Essendo $m_{i_1}, \dots, m_{i_h}$ K-linearmente indipendenti, allora $c_{ts} = 0, \ \forall\, s = 1, \dots, h, \ \forall\, t = 1, \dots, k.$

Un'immediata conseguenza del teorema precedente è il seguente fatto:

se $[L : K] = p$ è primo, non esistono campi intermedi (propri) tra K ed L.

Si noti che la ricerca di campi intermedi di una data estensione è un problema centrale della teoria di Galois (di cui ci occuperemo nel prossimo capitolo). Concludiamo il paragrafo illustrando un modo per ottenere campi intermedi di un'estensione.

Definizione 1.5. *Sia L un campo e sia T un suo sottoinsieme non vuoto. Si chiama sottocampo di L generato da T l'intersezione di tutti i sottocampi di L contenenti T, cioè il minimo sottocampo di L contenente T* [si osservi che l'intersezione di campi è un campo]. *Si denota usualmente $\langle T \rangle$ [oppure (T)].*

Osservazione 1.2. (*i*) Indicato con L_f il sottocampo fondamentale di L, allora $\langle T \rangle = \langle T \cup L_f \rangle$ [infatti ogni sottocampo di L contiene L_f].

(*ii*) Se $\emptyset \neq T_1 \subseteq T_2 \subseteq L$, è evidente che $\langle T_1 \rangle \subseteq \langle T_2 \rangle$.

(*iii*) $\langle T \rangle$ è la *chiusura di $T \cup L_f$ in L*, cioè è l'insieme di tutti gli elementi di L ottenuti a partire da $T \cup L_f$ con una successione finita di operazioni del campo [addizioni, sottrazioni, moltiplicazioni e divisioni]. Dimostriamo tale affermazione. Denotiamo con Σ_T la chiusura di $T \cup L_f$ in L. Si verifica subito che Σ_T è un sottocampo di L e contiene T: dunque $\Sigma_T \supseteq \langle T \rangle$. Viceversa, per ogni sottocampo E di L contenente T, risulta che $E \supseteq T \cup L_f$ e dunque $E \supseteq \Sigma_T$. Pertanto $\langle T \rangle \supseteq \Sigma_T$.

Sia ora $K \subseteq L$ un'estensione di campi e sia T un sottoinsieme non vuoto di L. Il campo $\langle K \cup T \rangle$ (sottocampo di L) viene usualmente denotato $K(T)$. Valgono ovviamente i tre seguenti fatti:

$$K \subseteq K(T) \subseteq L; \quad K(T) = K \iff T \subseteq K; \quad K(T) = K(T - K).$$

Se poi $T = \{\alpha\}$ (con $\alpha \in L$), si scrive $K(\alpha)$ in luogo di $K(\{\alpha\})$; se infine $T = \{\alpha_1, \dots, \alpha_s\}$ ($\subseteq L$), si scrive $K(\alpha_1, \dots, \alpha_s)$ in luogo di $K(\{\alpha_1, \dots, \alpha_s\})$. Si noti che $K(\alpha_1, \dots, \alpha_s)$ (in quanto chiusura di $K \cup \{\alpha_1, \dots, \alpha_s\}$) è formato da tutte e sole le espressioni del tipo $\frac{P(\alpha_1, \dots, \alpha_s)}{Q(\alpha_1, \dots, \alpha_s)}$, $\forall\, P, Q \in K[X_1, \dots, X_s]$, $Q(\alpha_1, \dots, \alpha_s) \neq 0$.

Nota. Con le notazioni ora introdotte, ad esempio $\boldsymbol{Q}(\sqrt{2})$ denota il sottocampo $\langle \boldsymbol{Q} \cup \{\sqrt{2}\} \rangle$ di $\boldsymbol{R}$, mentre in Cap. **3**, Osserv. **2.1** abbiamo denotato con $\boldsymbol{Q}(\sqrt{2})$ il campo $\boldsymbol{Q}[X]/_{(X^2-2)}$. Tale confusione non crea però alcuna contraddizione. Infatti entrambi i campi coincidono con $\{a + b\sqrt{2}, \ \forall\, a, b \in \boldsymbol{Q}\}$.

Definizione 1.6. *Un'estensione $K \subseteq L$ è detta finitamente generata se esistono $\alpha_1, .., \alpha_s \in L$ tali*

che $L = K(\alpha_1, \dots, \alpha_s)$. *È detta semplice se* $L = K(\alpha)$, $\exists\, \alpha \in L$.

Esempi 1.2. (*i*) $\boldsymbol{R} \subset \boldsymbol{C}$ è un'estensione semplice. Infatti $\boldsymbol{C} = \boldsymbol{R}(i)$ $(= \langle \boldsymbol{R} \cup \{i\} \rangle)$.

(*ii*) $K \subset K(X)$ è un'estensione semplice. Infatti si ha:

$$K(X) = \boldsymbol{Q}(K[X]) = \left\{ \tfrac{p(X)}{q(X)},\ \forall\, p(X),\, q(X) \in K[X],\, q(X) \neq 0 \right\} = \langle\, K \cup \{X\} \,\rangle.$$

(*iii*) L'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2}, \sqrt{3})$ è ovviamente finitamente generata. Ma possiamo provare che è anche semplice. Possiamo infatti dimostrare che

$$\boldsymbol{Q}(\sqrt{2}, \sqrt{3}) = \boldsymbol{Q}(\sqrt{2} + \sqrt{3})$$

Più generalmente, dimostreremo che, se r, s sono due interi distinti, $\boldsymbol{Q}(\sqrt{r}, \sqrt{s}) = \boldsymbol{Q}(\sqrt{r} + \sqrt{s})$.

Ovviamente $\sqrt{r} + \sqrt{s} \in \boldsymbol{Q}(\sqrt{r}, \sqrt{s})$ e quindi vale l'inclusione $(\supseteq)$. Viceversa, va verificato che $\sqrt{r}, \sqrt{s} \in \boldsymbol{Q}(\sqrt{r} + \sqrt{s})$. Si ponga $\alpha := \sqrt{r} + \sqrt{s}$. Si ha:

$$\alpha^2 = r + s + 2\sqrt{rs} \ \text{ e dunque } \ \sqrt{rs} = \tfrac{1}{2}(\alpha^2 - r - s) \in \boldsymbol{Q}(\alpha).$$

Ne segue:

$$\alpha\sqrt{rs} = r\sqrt{s} + s\sqrt{r} \in \boldsymbol{Q}(\alpha), \ \text{ da cui anche } \ \alpha\sqrt{rs} - r\,\alpha \in \boldsymbol{Q}(\alpha) \ \text{ e quindi } \ (s-r)\sqrt{r} \in \boldsymbol{Q}(\alpha).$$

Pertanto anche $\sqrt{r} \in \boldsymbol{Q}(\alpha)$. Infine $\sqrt{s} = \alpha - \sqrt{r} \in \boldsymbol{Q}(\alpha)$.

Nota. Che tale estensione finitamente generata sia semplice non è un fatto casuale. Infatti tale estensione, come vedremo, è finita e, in base al *teorema dell'elemento primitivo* (cfr. Teor. **3.1**), ogni estensione finita di $\boldsymbol{Q}$ è semplice.

(*iv*) Un esempio di estensione finitamente generata ma non semplice è $K \subset K(X, Y)$ (campo delle funzioni razionali in due indeterminate su un campo K). Ciò potrebbe essere dimostrato utilizzando il fatto che le due indeterminate X, Y sono *algebricamente indipendenti*, cioè non esiste alcun polinomio non nullo P in due variabili ed a coefficienti in K tale che $P(X, Y) = 0$.

Osservazione 1.3. Ogni estensione finita è anche finitamente generata. Se infatti $K \subseteq L$ è finita e $\{\ell_1, \dots, \ell_n\}$ è una base di L su K, allora $L = K(\ell_1, \dots, \ell_n)$. Il viceversa è ovviamente falso: ad esempio $K \subset K(X)$ è semplice ma non finita.

* * * * * * * * * * * * * * * * * * *

Esercizio 4.1.1. Si consideri in $\boldsymbol{R}$ l'insieme

$$L = \{a + b\sqrt[3]{2} + c\sqrt[3]{4},\ \ \forall\, a, b, c \in \boldsymbol{Q}\}.$$

Verificare che L è un campo ed è un'estensione semplice di $\boldsymbol{Q}$.

Esercizio 4.1.2. Dire se sono isomorfe le seguenti estensioni di campi

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2}), \qquad \boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{3}).$$

Esercizio 4.1.3. Si consideri in $\boldsymbol{R}$ il sottoinsieme $T = \{\sqrt{2^k},\ \forall\, k \in \boldsymbol{Z}\}$. Verificare che

$$\langle\, T \,\rangle = \boldsymbol{Q}(\sqrt{2}).$$

Esercizio 4.1.4. Nel campo $\boldsymbol{C}(X)$ è assegnato il sottoinsieme $T = \{X^4, X^{-6}\}$. Determinare il sottocampo $\langle\, T \,\rangle$.

Esercizio 4.1.5. Dimostrare che l'estensione $\boldsymbol{Q} \subset \boldsymbol{R}$ è non semplice.

[*Suggerimento.* Valutare la cardinalità di un'estensione semplice di $\boldsymbol{Q}$.]

Esercizio 4.1.6. Sia K un campo e si consideri l'estensione $K(X^2) \subset K(X)$. Verificare che $\{1, X\}$ è una base di $K(X)$ su $K(X^2)$.

2. Estensioni semplici

Sia $K \subseteq L$ un'estensione di campi e sia $\alpha \in L$. Vogliamo studiare l'estensione semplice $K \subseteq K(\alpha)$. Si consideri l'applicazione

$$\varphi_\alpha : K[X] \to L \text{ tale che } \varphi_\alpha(p) = p(\alpha), \ \forall\, p \in K[X].$$

È evidente che φ_α è un omomorfismo, che fissa gli elementi di K (cioè un K-omomorfismo). Risulta:

$$Ker\varphi_\alpha = \{p \in K[X] \mid p(\alpha) = 0\}; \quad Im\,\varphi_\alpha = \{\sum_{i=0}^{n} a_i \alpha^i, \ \forall\, n \geq 0, \ \forall\, a_i \in K\}.$$

Poniamo: $I_\alpha := Ker\varphi_\alpha$ (ideale di $K[X]$) e $K[\alpha] := Im\,\varphi_\alpha$ (sottoanello di L e quindi dominio d'integrità). In base al *TFO*, $K[\alpha] \cong K[X]/_{I_\alpha}$. Quindi I_α è un ideale primo e principale.

Definizione 2.1. *Sia $K \subseteq L$ un'estensione di campi e sia $\alpha \in L$. L'elemento α è detto algebrico su K se $I_\alpha \neq \{0\}$, cioè se esiste un polinomio non nullo $p \in K[X]$ tale che $p(\alpha) = 0$. Altrimenti, α è detto trascendente su K. Nel primo caso l'estensione semplice $K \subseteq K(\alpha)$ è detta estensione algebrica semplice; nel secondo caso è detta estensione trascendente semplice.*

Ad esempio, considerata l'estensione $\boldsymbol{Q} \subset \boldsymbol{C}$, gli elementi i, $\sqrt{2}$ sono algebrici su $\boldsymbol{Q}$ e dunque le estensioni $\boldsymbol{Q} \subset \boldsymbol{Q}(i)$, $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2})$ sono algebriche semplici. Invece è noto che ad esempio i numeri reali e e π sono trascendenti su $\boldsymbol{Q}$ [risp. *teorema di Hermite* (1873) e *teorema di Von Lindemann* (1882)] e dunque le estensioni $\boldsymbol{Q} \subset \boldsymbol{Q}(e)$, $\boldsymbol{Q} \subset \boldsymbol{Q}(\pi)$ sono trascendenti semplici.

Cominciamo ad esaminare le estensioni trascendenti semplici.

Proposizione 2.1. *Sia $K \subseteq L$ un'estensione di campi e sia $\alpha \in L$ trascendente su K. Il campo $K(\alpha)$ è K-isomorfo a $K(X)$ (campo delle funzioni razionali su K in una indeterminata X). Dunque tutte le estensioni trascendenti semplici di K sono isomorfe tra loro ed hanno grado infinito.*

Dim. L'omomorfismo $\varphi_\alpha : K[X] \to L$ è iniettivo e quindi stabilisce un K-isomorfismo tra gli anelli $K[X]$ e $Im\,\varphi_\alpha = K[\alpha]$. Tale isomorfismo induce un K-isomorfismo tra i rispettivi campi dei quozienti

$$F_\alpha : \boldsymbol{Q}(K[X]) \to \boldsymbol{Q}(K[\alpha]) \text{ tale che } F_\alpha(\tfrac{f}{g}) = \tfrac{f(\alpha)}{g(\alpha)}, \ \forall\, \tfrac{f}{g} \in \boldsymbol{Q}(K[X]).$$

Poiché $\boldsymbol{Q}(K[X]) = K(X)$ e poiché $\boldsymbol{Q}(K[\alpha]) = K(\alpha)$ [in quanto $\boldsymbol{Q}(K[\alpha])$ è il più piccolo sottocampo di L contenente $K \cup \{\alpha\}$], abbiamo ottenuto il richiesto K-isomorfismo tra $K(X)$ e $K(\alpha)$.

La parte conclusiva dell'enunciato è ovvia [cfr. Esempi **1.1**(*ii*),(*iv*)].

Veniamo ora alle estensioni algebriche semplici.

Proposizione 2.2. *Sia $K \subseteq L$ un'estensione di campi e sia $\alpha \in L$ algebrico su K. Risulta:*

(1) Esiste un unico polinomio monico irriducibile $m_\alpha \in K[X]$ che ammette α come zero. Tale polinomio è detto polinomio minimo di α su K.

(2) $K(\alpha) = K[\alpha] \cong K[X]/_{(m_\alpha)}$.

(3) Se $p = \partial m_\alpha$, risulta $[K(\alpha) : K] = p$ ed una base di $K(\alpha)$ su K è data dalle successive potenze $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$.

Dim. (*1*) Poiché $K[X]/_{I_\alpha} \cong K[\alpha] \subseteq L$ (campo), $K[\alpha]$ è un dominio e quindi I_α è un ideale primo. Inoltre è non nullo. Poiché $K[X]$ è un *PID* [e in un *PID* ogni ideale primo non nullo è massimale (e principale)], I_α è massimale e principale. I suoi generatori sono irriducibili (cfr. Cap. **3**, Lemma **3.1**) e sono definiti a meno di un fattore invertibile. Pertanto uno solo di essi è monico: si tratta del polinomio minimo m_α.

(*2*) Poichè $K[\alpha] \cong K[X]/_{(m_\alpha)}$ è un campo, esso coincide con il proprio campo dei quozienti $\boldsymbol{Q}(K[\alpha]) = \langle K \cup \{\alpha\}\rangle = K(\alpha)$.

(*3*) Poichè m_α è monico e $m_\alpha(\alpha) = 0$, allora α^p è una combinazione lineare (a coefficienti in K) di $1, \alpha, \alpha^2, ..., \alpha^{p-1}$. Ne segue che tutte le successive potenze α^h (con $h \geq p$) sono combinazioni lineari di $1, \alpha, \alpha^2, ..., \alpha^{p-1}$ e pertanto tali elementi sono un sistema di generatori di $K[\alpha]$ su K, cioè di $K(\alpha)$ su K. Per provare che si tratta di una base basta verificare che sono K-linearmente indipendenti. Infatti un'eventuale relazione di dipendenza lineare non banale di $1, \alpha, \alpha^2, ..., \alpha^{p-1}$ determinerebbe un polinomio non nullo in I_α di grado $< p$, che non esiste [in quanto m_α ha grado minimo possibile in I_α, cfr. Cap. **3**, dim. Prop. **3.4**]. Essendo $\{1, \alpha, \alpha^2, ..., \alpha^{p-1}\}$ una base di $K(\alpha)$ su K, segue che $[K(\alpha) : K] = p$.

Osservazione 2.1. Assegnato un polinomio irriducibile e monico $p \in K[X]$, è possibile costruire un'estensione algebrica semplice $K \subset K(x)$ tale che p sia il polinomio minimo di x su K.

Infatti (essendo p irriducibile) $K[X]/_{(p)}$ è un campo. Ponendo $x := X + (p)$ e scegliendo opportuni rappresentanti delle classi *mod* (p), tale campo si identifica col campo

$$\{\sum_{i=0}^{\partial p-1} a_i x^i, \ \ \forall\, a_i \in K;\ p(x) = 0\},$$

che denotiamo $K[x \,|\, p(x) = 0]$ o, più semplicemente, $K[x]$. $K \subset K[x]$ è un'estensione di campi e x è algebrico su K (in quanto $p(x) = 0$). Essendo p monico e irriducibile su K, allora p è il polinomio minimo di x su K. Infine $K[x] = \langle K \cup \{x\}\rangle$, cioè $K[x] = K(x)$. Il problema è così risolto.

Si noti che l'elemento x sopra considerato è puramente formale (o "simbolico"). Esaminiamo ora due esempi apparentemente diversi.

(*a*) Sia $p = X^2 + 1 \in \boldsymbol{Q}[X]$. Tale polinomio è irriducibile su $\boldsymbol{Q}$ e dalle considerazioni appena svolte risulta che

$$\boldsymbol{Q}(x) = \{a + bx, \ \ \forall\, a, b \in \boldsymbol{Q};\ x^2 = -1\}.$$

Si noti che p ammette in $\boldsymbol{C}$ i due zeri $\pm i$, di cui è polinomio minimo su $\boldsymbol{Q}$. Segue dalla Prop. **2.2** che $\boldsymbol{Q}(x)$ può essere identificato al sottocampo $\boldsymbol{Q}(i)$ [o $\boldsymbol{Q}(-i)$] di $\boldsymbol{C}$. In particolare x si identifica a i [o $-i$].

(*b*) Sia $p = X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$. Tale polinomio è irriducibile su $\boldsymbol{Z}_2$ e risulta quindi

$$\boldsymbol{Z}_2(x) = \{a + bx, \ \ \forall\, a, b \in \boldsymbol{Z}_2;\ x^2 = x + \overline{1}\} = \{\overline{0}, \overline{1}, x, x + \overline{1}\}.$$

In questo caso x non si identifica ad alcun elemento già noto di un campo contenente $\boldsymbol{Z}_2$. Viceversa, x ha creato un nuovo campo di cardinalità 4 [cioè $\boldsymbol{Z}_2(x)$].

Ma la differenza tra i due casi è di natura puramente "psicologica" (o meglio non esiste). In fondo anche i è stato in qualche momento "creato" [circa 500 anni fa].

Osservazione 2.2. Sia $K \subseteq L$ un'estensione di campi. Due elementi distinti $\alpha, \beta \in L$, algebrici su K, in genere determinano estensioni algebriche semplici non K-isomorfe. Quando tali estensioni sono isomorfe? Ciò avviene, come ora vedremo, se α, β hanno lo stesso polinomio minimo su K. Ma può avvenire anche in altri casi. Ad esempio, $\alpha = \sqrt{5}$, $\beta = \frac{-1+\sqrt{5}}{2} \in \boldsymbol{R}$ determinano la stessa estensione algebrica semplice di $\boldsymbol{Q}$ [infatti si verifica che $\alpha \in \boldsymbol{Q}(\beta)$ e $\beta \in \boldsymbol{Q}(\alpha)$], ma i due elementi hanno differenti polinomi minimi su $\boldsymbol{Q}$ [rispettivamente $X^2 - 5$ e $X^2 + X - 1$].

Proposizione 2.3. *Sia $K \subseteq L$ un'estensione di campi e siano $\alpha, \beta \in L$ algebrici su K ed aventi lo stesso polinomio minimo su K. Esiste un K-isomorfismo $\varphi : K(\alpha) \to K(\beta)$ tale che $\varphi(\alpha) = \beta$.*

Dim. Sia $m \in K[X]$ il comune polinomio minimo di α e β su K. Sia $p = \partial m$. Allora

$$K(\alpha) = \{\sum_{i=0}^{p-1} a_i \alpha^i, \ \ \forall\, a_i \in K;\ m(\alpha) = 0\}, \quad K(\beta) = \{\sum_{i=0}^{p-1} a_i \beta^i, \ \ \forall\, a_i \in K;\ m(\beta) = 0\}.$$

Si definisce

$$\varphi : K(\alpha) \to K(\beta) \ \text{ tale che } \ \varphi\big(\sum_{i=0}^{p-1} a_i \alpha^i\big) = \sum_{i=0}^{p-1} a_i \beta^i, \ \ \forall \sum_{i=0}^{p-1} a_i \alpha^i \in K(\alpha).$$

φ è certamente biiettiva; inoltre $\varphi_{|_K} = \mathbf{1}_K$ e $\varphi(\alpha) = \beta$. Per concludere che φ è un K-isomorfismo, bisogna verificare che è un omomorfismo di anelli.

Siano $f(\alpha),\, g(\alpha) \in K(\alpha)$, con $f,\, g \in K[X]$ e $\partial f,\, \partial g < p$. Bisogna verificare che

$$\varphi\big(f(\alpha) + g(\alpha)\big) = \varphi\big(f(\alpha)\big) + \varphi\big(g(\alpha)\big), \quad \varphi\big(f(\alpha)\cdot g(\alpha)\big) = \varphi\big(f(\alpha)\big)\cdot\varphi\big(g(\alpha)\big).$$

La prima uguaglianza è ovvia [verificare]. La seconda è un po' più complicata [in quanto $\partial(fg)$ può superare p]. Si divida fg per m e sia r il resto della divisione [$\partial r < p$]. Allora $f(\alpha)\cdot g(\alpha) = r(\alpha)$ e $f(\beta)\cdot g(\beta) = r(\beta)$ [infatti $m(\alpha) = m(\beta) = 0$]. Ne segue:

$$\varphi\big(f(\alpha)\cdot g(\alpha)\big) = \varphi\big(r(\alpha)\big) = r(\beta) = f(\beta)\cdot g(\beta) = \varphi\big(f(\alpha)\big)\cdot\varphi\big(g(\alpha)\big).$$

Il risultato che segue generalizza la proposizione precedente e sarà utilizzato come lemma per dimostrare l'unicità del *campo di spezzamento* (cfr. Cap. **5**, Teor. **2.1**). Osserviamo preliminarmente che ogni isomorfismo di campi $\varphi : K \to \tilde{K}$ induce l'isomorfismo di anelli

$$\varphi' : K[X] \to \tilde{K}[X] \text{ tale che } \varphi'(\textstyle\sum a_i X^i) = \sum \varphi(a_i) X^i, \ \ \forall \sum a_i X^i \in K[X].$$

Proposizione 2.4. *Siano $K \subseteq L$ e $\tilde{K} \subseteq \tilde{L}$ due estensioni di campi. Sia $\varphi : K \to \tilde{K}$ un isomorfismo. Siano $\alpha \in L$ e $\tilde{\alpha} \in \tilde{L}$ elementi algebrici rispettivamente su K e $\tilde{K}$. Siano $m \in K[X]$ e $\tilde{m} \in \tilde{K}[X]$ i rispettivi polinomi minimi. Se $\tilde{m} = \varphi'(m)$, esiste un isomorfismo di campi*

$$\Phi : K(\alpha) \to \tilde{K}(\tilde{\alpha}) \ \textit{tale che} \ \Phi_{|_K} = \varphi \ \text{ e } \ \Phi(\alpha) = \tilde{\alpha}.$$

Dim. Sia

$$F := \pi \circ \varphi' : K[X] \to \tilde{K}[X] \to \tilde{K}[X]\big/_{(\tilde{m})}.$$

Essendo φ' un isomorfismo e π suriettivo, F è un omomorfismo suriettivo di anelli. Inoltre F è non nullo [infatti $F(c) = \varphi(c), \ \forall\, c \in K$]. Infine $(m) \subseteq KerF$ [infatti $F(m) = \varphi'(m) + (\tilde{m}) = \tilde{m} + (\tilde{m}) = 0 + (\tilde{m})$ (zero del campo)]. Poiché m è irriducibile in $K[X]$, allora $KerF = (m)$ (cfr. Cap. **3**, Lemma **3.1**). Dal *TFO* esiste un isomorfismo di campi

$$\overline{F} : K[X]\big/_{(m)} \to \tilde{K}[X]\big/_{(\tilde{m})}, \text{ tale che } \overline{F}(X + (m)) = X + (\tilde{m}) \text{ e } \overline{F}_{|_K} = \varphi.$$

Denotiamo con $f : K(\alpha) \to K[X]\big/_{(m)}$ il K-isomorfismo tale che

$$f\big(\textstyle\sum a_i \alpha^i\big) = \sum a_i X^i + (m), \ \ \forall \sum a_i \alpha^i \in K(\alpha).$$

Analogamente, poniamo

$$\tilde{f} : \tilde{K}(\tilde{\alpha}) \to \tilde{K}[X]\big/_{(\tilde{m})} \text{ tale che } \tilde{f}\big(\textstyle\sum \tilde{a}_i \tilde{\alpha}^i\big) = \sum \tilde{a}_i X^i + (\tilde{m}), \ \ \forall \sum \tilde{a}_i \tilde{\alpha}^i \in \tilde{K}(\tilde{\alpha}).$$

Si consideri allora l'isomorfismo $\Phi = \tilde{f}^{-1} \circ \overline{F} \circ f : K(\alpha) \to \tilde{K}(\tilde{\alpha})$. Tale isomorfismo agisce come segue: per ogni $\sum a_i \alpha^i \in K(\alpha)$,

$$\textstyle\sum a_i \alpha^i \ \to \sum a_i X^i + (m) \to \sum \varphi(a_i) X^i + (\tilde{m}) \to \sum \varphi(a_i) \tilde{\alpha}^i.$$

In particolare, $\Phi(\alpha) = \tilde{\alpha}$ e $\Phi_{|_K} = \varphi$, come richiesto.

Nota. In accordo con la Def. **1.3**, le due estensioni $K \subseteq K(\alpha)$ e $\tilde{K} \subseteq \tilde{K}(\tilde{\alpha})$ sono isomorfe.

Per ogni $n \geq 1$, sia $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} \in \boldsymbol{C}$. Si tratta, come noto, di una radice primitiva n-sima dell'unità. Ci chiediamo quale sia il polinomio minimo di ζ_n su $\boldsymbol{Q}$ e quale sia il grado dell'estensione algebrica semplice $\boldsymbol{Q} \subset \boldsymbol{Q}(\zeta_n)$.

È noto dal corso di **Alg. 1** che tutte e sole le radici primitive n-sime dell'unità sono

$$\zeta_n^{\,k}, \ \text{ con } \ 1 \leq k \leq n \ \text{ e } \ MCD(k, n) = 1.$$

Il loro numero è $\varphi(n)$ [dove φ è la funzione di Eulero]. Denotiamo con $\Phi_n = \Phi_n(X)$ il polinomio

$$\Phi_n(X) = \prod_{1 \leq k \leq n,\ (k,n)=1} (X - \zeta_n^{\,k}).$$

Φ_n è detto *n-simo polinomio ciclotomico*. Si tratta ovviamente di un polinomio monico di grado $\varphi(n)$, a priori in $\boldsymbol{C}[X]$. Invitiamo lo studente a verificare le seguenti proprietà (cfr. ad esempio [AA], pag. 195):

$$(1) \ \ X^n - 1 = \prod_{d|n,\ 1 \leq d \leq n} \Phi_d(X); \qquad (2) \ \ \Phi_n \in \boldsymbol{Z}[X], \ \ \forall\, n \geq 1.$$

La (*1*) consente di determinare ricorsivamente Φ_n, sfruttando il fatto che

$$\Phi_n = (X^n - 1) \Big/ \prod_{d|n,\, 1\le d<n} \Phi_d(X).$$

Ad esempio si verifica subito che, $\forall\, p$ primo:

$$\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$$

e che tale polinomio è irriducibile su $\boldsymbol{Q}$. Analogamente si può verificare (sempre con p primo) che

$$\Phi_{p^2} = X^{p(p-1)} + X^{p(p-2)} + \ldots + X^p + 1$$

e che anche tale polinomio è irriducibile su $\boldsymbol{Q}$ (cfr. Esercizio **4.2.8**). Ma dimostreremo ora, più generalmente, che ogni Φ_n è irriducibile su $\boldsymbol{Q}$. Alla luce di questo fatto si ricavano i due seguenti risultati:

$$\Phi_n \text{ è il polinomio minimo di } \zeta_n \text{ su } \boldsymbol{Q}; \qquad [\boldsymbol{Q}(\zeta_n) : \boldsymbol{Q}] = \varphi(n).$$

Teorema 2.1. *Per ogni $n \ge 1$, il polinomio ciclotomico Φ_n è irriducibile in $\boldsymbol{Q}[X]$.*

Dim. Dal teorema di Gauss è sufficiente dimostrarne l'irriducibilità su $\boldsymbol{Z}$. Sia quindi $\Phi_n = fg$, con $f, g \in \boldsymbol{Z}[X]$, monici e f irriducibile su $\boldsymbol{Z}$. Tenuto conto che $\partial\Phi_n = \varphi(n)$, basta dimostrare che $\partial f = \varphi(n)$ [da cui $g = 1$ e la fattorizzazione è banale].

Poiché $\partial f \ge 1$, dal teorema fondamentale dell'algebra f ha uno zero $\zeta \in \boldsymbol{C}$, che è necessariamente uno zero di Φ_n e dunque una radice primitiva n-sima dell'unità.

Sia p un primo tale che $p \nmid n$. Poiché $\circ(\zeta^p) = n$, anche ζ^p è una radice primitiva n-sima dell'unità. Quindi $\Phi_n(\zeta^p) = 0$ e pertanto $f(\zeta^p) = 0$ oppure $g(\zeta^p) = 0$. Vogliamo provare che assumere che $g(\zeta^p) = 0$ porta ad un assurdo [e quindi necessariamente $f(\zeta^p) = 0$].

Sia $g(\zeta^p) = 0$. Allora ζ è uno zero del polinomio $g(X^p) \in \boldsymbol{Z}[X]$. Quindi i due polinomi f, $g(X^p)$ hanno uno zero in comune. Poiché f è il polinomio minimo di ζ, allora $f \,\big|\, g(X^p)$ in $\boldsymbol{Q}[X]$ e quindi anche in $\boldsymbol{Z}[X]$. Dunque $g(X^p) = fh$, $\exists\, h \in \boldsymbol{Z}[X]$.

Tramite l'omomorfismo di riduzione *mod* p (cioè $\boldsymbol{Z}[X] \to \boldsymbol{Z}_p[X]$) trasferiamo in $\boldsymbol{Z}_p[X]$ la precedente uguaglianza: $\overline{g(X^p)} = \overline{f}\,\overline{h}$. Ora dimostriamo che in $\boldsymbol{Z}_p[X]$:

$$\overline{g(X^p)} = \overline{g}^{\,p}.$$

Osserviamo preliminarmente che in un dominio A di caratteristica p:

$$\Big(\sum_{i=1}^{t} \alpha_i\Big)^p = \sum_{i=1}^{t} \alpha_i^{\,p}, \quad \forall\, \alpha_1, \ldots, \alpha_t \in A$$

[infatti $\Big(\sum_{i=1}^{t} \alpha_i\Big)^p = \Big(\alpha_1 + \sum_{i=2}^{t} \alpha_i\Big)^p = \alpha_1^{\,p} + \Big(\sum_{i=2}^{t} \alpha_i\Big)^p = \ldots = \alpha_1^{\,p} + \ldots + \alpha_t^{\,p}$]. In particolare in $\boldsymbol{Z}_p[X]$, se $\overline{g} = \sum_{i=0}^{t} a_i X^i$, allora $\overline{g}^{\,p} = \sum_{i=0}^{t} a_i^{\,p} X^{ip} = \sum_{i=0}^{t} a_i X^{ip} = \overline{g}(X^p) = \overline{g(X^p)}$ [si ricorda che, in base al Piccolo Teorema di Fermat, $a_i^{\,p} = a_i$ (in $\boldsymbol{Z}_p$)].

Da $\overline{g(X^p)} = \overline{g}^{\,p}$, segue che $\overline{g}^{\,p} = \overline{f}\,\overline{h}$. Essendo $\boldsymbol{Z}_p[X]$ un *UFD*, ogni fattore irriducibile $\overline{f}_i$ di $\overline{f}$ dividendo $\overline{g}^{\,p}$ divide anche $\overline{g}$. Pertanto $\overline{f}, \overline{g}$ hanno un fattore comune [cioè $\overline{f}_i$].

Ricordiamo che $\Phi_n \,\big|\, X^n - 1$. Dunque $X^n - 1 = \Phi_n \cdot G = fg\,G$, con $G \in \boldsymbol{Z}[X]$. Allora, in $\boldsymbol{Z}_p[X]$: $X^n - \overline{1} = \overline{f}\,\overline{g}\,\overline{G}$. Ne segue che $X^n - \overline{1}$ ha un fattore multiplo [cioè $\overline{f}_i$].

Denotiamo con D l'*operatore di derivazione formale* in $A[X]$ (cfr. [AA], Esercizio **3.7**), con A anello c. u.. Se un qualsiasi polinomio $P \in A[X]$ ha un fattore multiplo, cioè $P = U^2V$, allora $DP = 2UV\,DU + U^2DV = U(2V\,DU + U\,DV)$ e dunque P, DP hanno un fattore comune.

Applichiamo tale fatto al polinomio $X^n - \overline{1} \in \boldsymbol{Z}_p[X]$. Essendo $D(X^n - \overline{1}) = \overline{n}X^{n-1} \ne \overline{0}$ (in quanto $\overline{n}$ è invertibile in $\boldsymbol{Z}_p$), $X^n - \overline{1}$ ha in $\boldsymbol{Z}_p[X]$ un fattore X^i, con $1 \le i < n$. Ne segue subito che $X \,\big|\, \overline{1}$: assurdo. Abbiamo così dimostrato che $g(\zeta^p) \ne 0$.

Possiamo quindi affermare che $f(\zeta^p) = 0$. Dunque abbiamo provato che esiste una radice primitiva n-sima dell'unità ζ tale che, per ogni primo p coprimo con n, risulta:

$$f(\zeta) = 0 \implies f(\zeta^p) = 0.$$

Consideriamo i numeri naturali $1, k_2, \ldots, k_{\varphi(n)}$ coprimi con n e minori di n. Per ogni siffatto k, sia $k = p_1 p_2 \ldots p_t$, con $p_1, \ldots, p_t$ primi (con eventuali ripetizioni). Tali primi sono coprimi con n e

dalla precedente dimostrazione otteniamo successivamente:

$$f(\zeta) = 0 \implies f(\zeta^{p_1}) = 0 \implies f(\zeta^{p_1 p_2}) = 0 \implies \ldots \implies f(\zeta^k) = 0.$$

Dunque f ammette come zeri $\zeta, \zeta^{k_2}, \ldots, \zeta^{k_{\varphi(n)}}$. Tali elementi sono distinti (essendo ogni $k_i < n$) e dunque f ammette almeno $\varphi(n)$ zeri e pertanto $\partial f \geq \varphi(n)$, da cui $\partial f = \varphi(n)$, come richiesto.

Nota. Si osservi che i polinomi ciclotomici non sono generalmente irriducibili *mod p*. Ad esempio $\Phi_{12} = X^4 - X^2 + 1$, pensato in $\boldsymbol{Z}_{11}[X]$ si fattorizza nella forma: $\Phi_{12} = (X^2 - \overline{5}X + \overline{1})(X^2 + \overline{5}X + \overline{1})$.

* * * * * * * * * * * * * * * * * * *

Esercizio 4.2.1. Sia $z \in \boldsymbol{C} - \boldsymbol{R}$.

(*i*) Determinare il polinomio minimo di z su $\boldsymbol{R}$ [in funzione della norma e della traccia di z].

(*ii*) Esiste il polinomio minimo di z su $\boldsymbol{Q}$?

Esercizio 4.2.2. Siano p, q due primi distinti. Determinare il grado $[\boldsymbol{Q}(\sqrt{p}, \sqrt{q}) : \boldsymbol{Q}]$ ed una base di $\boldsymbol{Q}(\sqrt{p}, \sqrt{q})$ su $\boldsymbol{Q}$.

Esercizio 4.2.3. Determinare il grado ed una base dell'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2}, \sqrt[3]{2})$.

Esercizio 4.2.4. Determinare il grado ed il polinomio minimo dell'estensione algebrica semplice $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2} + \sqrt{3})$.

Esercizio 4.2.5. Assegnato $\alpha = \sqrt{2 + \sqrt{2}} \in \boldsymbol{R}$,

(*i*) determinare il polinomio minimo di α su $\boldsymbol{Q}$;

(*ii*) esprimere $\frac{1}{\sqrt{2}}$ come combinazione lineare (a coefficienti razionali) delle potenze di α.

(*iii*) determinare il polinomio minimo di α su $\boldsymbol{Q}(\frac{1}{\sqrt{2}})$.

Esercizio 4.2.6. Sia $K := \boldsymbol{Z}_2(x) = \boldsymbol{Z}_2[X]/_{(p)}$, con $p = X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$ (estensione algebrica semplice di $\boldsymbol{Z}_2$). Sia $q = X^2 + xX + \overline{1} \in K[X]$.

(*i*) Verificare che q è irriducibile su K e determinare gli elementi del campo $K[y] := K[X]/_{(q)}$ (con $y := X + (q)$).

(*ii*) Calcolare il grado di $[K[y] : \boldsymbol{Z}_2]$ e studiare l'estensione algebrica semplice $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(y)$, determinando il polinomio minimo di y su $\boldsymbol{Z}_2$.

Esercizio 4.2.7. Sia $K \subset L$ un'estensione finita di campi e sia $f \in K[X]$ un polinomio irriducibile. Verificare che, se f ha uno zero in L, $\partial f \,\big|\, [L : K]$.

Esercizio 4.2.8. Sia p un primo. Calcolare il polinomio ciclotomico $\Phi_{p^2} \in \boldsymbol{Z}[X]$ e verificare che è irriducibile.

[*Suggerimento*: applicare il criterio di Eisenstein a $\Phi_{p^2}(X + 1)$].

Esercizio 4.2.9. Determinare $[\boldsymbol{Q}(\zeta_3, \zeta_4) : \boldsymbol{Q}]$, con $\zeta_3 = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$, $\zeta_4 = \cos\frac{2\pi}{4} + i \sin\frac{2\pi}{4}$.

Esercizio 4.2.10. Sia K_4 [rispett. K_5] l'estensione di $\boldsymbol{Z}_3$ generata dalle radici quarte [rispett. quinte] dell'unità (su $\boldsymbol{Z}_3$). Calcolare $[K_4 : \boldsymbol{Z}_3]$ e $[K_5 : \boldsymbol{Z}_3]$.

Esercizio 4.2.11. Determinare un isomorfismo tra i due campi

$$K_1 = \boldsymbol{Z}_3[X]/_{(X^2+\overline{1})}, \quad K_2 = \boldsymbol{Z}_3[X]/_{(X^2+X+\overline{2})}\,.$$

3. Estensioni algebriche

Definizione 3.1. *Un'estensione di campi $K \subseteq L$ è detta estensione algebrica se ogni $\alpha \in L$ è algebrico su K.*

Proposizione 3.1. *Ogni estensione finita è algebrica. In particolare, ogni estensione algebrica semplice è algebrica.*

Dim. Sia $K \subseteq L$ un'estensione finita di grado n. Per ogni $\alpha \in L$, consideriamo gli $n+1$ elementi $1, \alpha, \alpha^2, \dots, \alpha^n$. Sono $n+1$ elementi di L e dunque sono K-linearmente dipendenti: esistono $a_0, a_1, \dots, a_n \in K$, non tutti nulli, tali che $\sum_{i=0}^{n} a_i \alpha^i = 0$. Allora α è zero di $p = \sum_{i=0}^{n} a_i X^i \in K[X]$ e quindi è algebrico su K.

L'ultima affermazione è ovvia: ogni estensione algebrica semplice è finita (di grado uguale al grado del polinomio minimo).

La proposizione precedente non si inverte: verificheremo che esistono estensioni algebriche infinite. Premettiamo la seguente caratterizzazione delle estensioni finite.

Proposizione 3.2. *Sia $K \subseteq L$ un'estensione di campi. Risulta:*

$$K \subseteq L \text{ è finita} \iff \text{è algebrica e finitamente generata.}$$

Dim. ($\Longrightarrow$). Tale implicazione è già stata dimostrata (cfr. Prop. **3.1** ed Osserv. **1.3**).

($\Longleftarrow$). Sia $K \subseteq L$ algebrica e finitamente generata. Dunque $L = K(\alpha_1, \dots, \alpha_s)$. Costruiamo la seguente catena di estensioni:

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \dots \subseteq K(\alpha_1, \dots, \alpha_{s-1}) \subseteq K(\alpha_1, \dots, \alpha_s) = L.$$

Poniamo: $M_0 = K$ e $M_i = K(\alpha_1, \dots, \alpha_i)$, con $1 \leq i \leq s$. La precedente catena si riscrive nella forma:

$$K = M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots \subseteq M_{s-1} \subseteq M_s = L.$$

Per ogni $i = 1, \dots, s$, l'estensione $M_{i-1} \subseteq M_i$ è algebrica semplice. Infatti $M_i = M_{i-1}(\alpha_i)$ e α_i è algebrico su M_{i-1} [in quanto lo è su K]. Ne segue che $[M_i : M_{i-1}] < \infty$. Applicando ripetutamente il Teor. **1.1** si ottiene che

$$[L : K] = [L : M_{s-1}] \cdot [M_{s-1} : M_{s-2}] \cdot \dots \cdot [M_1 : K] < \infty.$$

Definizione 3.2. *Sia $K \subseteq L$ un'estensione di campi. Si chiama chiusura algebrica di $K \subseteq L$ l'insieme*

$$L_{alg,K} := \{\alpha \in L \mid \alpha \text{ è algebrico su } K\}.$$

Proposizione 3.3. *$L_{alg,K}$ è un campo intermedio tra K ed L. Inoltre l'estensione $K \subseteq L_{alg,K}$ è un'estensione algebrica.*

Dim. Ovviamente $K \subseteq L_{alg,K}$ [infatti ogni $c \in K$ è zero del polinomio $X - c \in K[X]$]. L'ultima affermazione è ovvia e resta soltanto da verificare che $L_{alg,K}$ è un campo, cioè che, $\forall\, \alpha, \beta \in L_{alg,K}$:

$$\alpha - \beta \in L_{alg,K} \quad \text{e} \quad \tfrac{\alpha}{\beta} \in L_{alg,K} \quad (\text{se } \beta \neq 0).$$

Si consideri il sottocampo $K(\alpha, \beta)$ di L. L'estensione $K \subseteq K(\alpha, \beta)$ è finita [infatti è ottenuta tramite la catena di estensioni algebriche semplici $K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta)$]. Dalla Prop. **3.1** segue che $K \subseteq K(\alpha, \beta)$ è algebrica. In particolare $\alpha - \beta$ e $\frac{\alpha}{\beta}$ (se $\beta \neq 0$) appartengono a $K(\alpha, \beta)$ e quindi sono algebrici su K, cioè appartengono a $L_{alg,K}$.

Veniamo ora al preannunciato esempio di estensione algebrica infinita. Considerata l'estensione $\boldsymbol{Q} \subset \boldsymbol{R}$, sia $\boldsymbol{R}_{alg,\boldsymbol{Q}} = \{x \in \boldsymbol{R} \mid x \text{ è algebrico su } \boldsymbol{Q}\}$ la sua chiusura algebrica. L'estensione $\boldsymbol{Q} \subset \boldsymbol{R}_{alg,\boldsymbol{Q}}$

è ovviamente algebrica. Verifichiamo che $[\boldsymbol{R}_{alg,\boldsymbol{Q}} : \boldsymbol{Q}] = \infty$, provando che $[\boldsymbol{R}_{alg,\boldsymbol{Q}} : \boldsymbol{Q}] \geq n$, $\forall\, n \in \boldsymbol{N}$. In $\boldsymbol{Q}[X]$ si consideri il polinomio $f_n = X^n - 2$. Tale polinomio è irriducibile su $\boldsymbol{Q}$ [in base al criterio di Eisenstein] e $\sqrt[n]{2}$ ne è uno zero. Dunque $\sqrt[n]{2} \in \boldsymbol{R}_{alg,\boldsymbol{Q}}$ e f_n è il polinomio minimo di $\sqrt[n]{2}$ su $\boldsymbol{Q}$. Pertanto:

$$[\boldsymbol{R}_{alg,\boldsymbol{Q}} : \boldsymbol{Q}] = [\boldsymbol{R}_{alg,\boldsymbol{Q}} : \boldsymbol{Q}(\sqrt[n]{2})]\cdot[\boldsymbol{Q}(\sqrt[n]{2}) : \boldsymbol{Q}] = [\boldsymbol{R}_{alg,\boldsymbol{Q}} : \boldsymbol{Q}(\sqrt[n]{2})]\cdot n \geq n.$$

Sia $K \subseteq L$ un'estensione algebrica. Per ogni campo intermedio M, le due estensioni $K \subseteq M$ e $M \subseteq L$ sono ovviamente algebriche. Vale anche il viceversa, che ora dimostriamo.

Proposizione 3.4. *Se $K \subseteq M$ e $M \subseteq L$ sono due estensioni algebriche, anche $K \subseteq L$ è una estensione algebrica.*

Dim. Sia $\ell \in L$. Dobbiamo provare che ℓ è algebrico su K. Per ipotesi lo è su M: dunque esiste un polinomio $p = \sum_{i=0}^{n} a_i X^i \in M[X]$ tale che $p(\ell) = 0$.

Consideriamo l'estensione $K \subseteq K(a_0, a_1, \dots, a_n, \ell)$. Vogliamo dimostrare che è finita. La spezziamo nella forma:

$$K \subseteq K(a_0, a_1, \dots, a_n) \subseteq K(a_0, a_1, \dots, a_n)(\ell).$$

La prima estensione è algebrica [perché $K(a_0, a_1, \dots, a_n) \subseteq M$ e $K \subseteq M$ è algebrica]; poiché è anche finitamente generata, da Prop. **3.2** segue che è finita. La seconda estensione è algebrica semplice [infatti ℓ è algebrico su $K(a_0, a_1, \dots, a_n)$ perché è zero del polinomio $p \in K(a_0, a_1, \dots, a_n)[X]$] e dunque è finita. In base alla moltiplicatività del grado, l'estensione $K \subseteq K(a_0, a_1, \dots, a_n, \ell)$ è finita. Dunque è algebrica e quindi ℓ è algebrico su K.

Osservazione 3.1. Sia $K \subseteq L$ un'estensione finita (e dunque algebrica e finitamente generata). Vogliamo rimarcare che, se $L = K(\alpha_1, .., \alpha_s)$, L è formata da tutte e sole le espressioni polinomiali

$$f(\alpha_1, .., \alpha_s), \quad \forall\, f \in K[X_1, .., X_s].$$

Spezziamo infatti $K \subseteq L$ nella catena di estensioni algebriche semplici

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1)(\alpha_2) \subseteq \ \dots\ \subseteq K(\alpha_1)(\alpha_2)\dots(\alpha_s).$$

Risulta:

$K(\alpha_1) = K[\alpha_1]$ è formato da tutte e sole espressioni della forma $g(\alpha_1)$, con $g \in K[X_1]$;

$K(\alpha_1)(\alpha_2) = K(\alpha_1)[\alpha_2]$ è formato da tutte e sole espressioni della forma $\sum_i g_i(\alpha_1)\,{\alpha_2}^i$, cioè da espressioni del tipo $f(\alpha_1, \alpha_2)$, con $f \in K[X_1, X_2]$.

Proseguendo in questo modo si arriva alla conclusione.

Concludiamo il paragrafo con il *teorema dell'elemento primitivo*, che afferma che *"se $car(K) = 0$, ogni estensione finita di K è semplice."*

La dimostrazione di tale teorema poggia sul seguente risultato, che sarà dimostrato in seguito (cfr. Cap. **5**, Teor. **3.1**) [e che naturalmente non è conseguenza del teorema dell'elemento primitivo]:

(∗) *Sia $car(K) = 0$ e sia $f \in K[X]$, $\partial f = n$. Se f è irriducibile su K i suoi n zeri [in un'opportuna estensione di K] sono a due a due distinti.*

Teorema 3.1. *(Teorema dell'elemento primitivo). Sia $car(K) = 0$ e sia $K \subseteq L$ un'estensione finita. Allora $L = K(\xi)$, per un opportuno $\xi \in L$ (detto elemento primitivo dell'estensione).*

Dim. Poiché $K \subseteq L$ è finitamente generata, basta dimostrare che, se $L = K(\alpha, \beta)$ è un'estensione finita di K, allora $L = K(\xi)$, $\exists \xi \in L$. Ne segue che è possibile ridurre di un'unità il numero dei generatori di L; iterando il procedimento si perviene alla conclusione.

Per evitare casi banali, assumiamo che $\alpha, \beta \notin K$ e denotiamo con f, g rispettivamente i polinomi minimi di α, β su K. Sia $\partial f = n$, $\partial g = m$ e siano $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ e $\beta_1 = \beta, \beta_2, \dots, \beta_m$ i rispettivi zeri di f, g, contenuti in un'opportuna estensione M di K. [L'esistenza di una siffatta

estensione è facilmente desumibile dall'Osserv. **2.1**, ma sarà formalmente provata in Cap. **5**, Prop. **2.1**]. In base ad $(*)$, gli elementi $\alpha, \alpha_2, \dots \alpha_n$ sono a due a due distinti, e lo stesso è vero per $\beta, \beta_2, \dots \beta_m$.

Si può scegliere un elemento $c \in K$ tale che

$$\alpha_i + c\beta_j \neq \alpha + c\beta, \quad \forall\, i = 1, \dots, n, \ \forall\, j = 2, \dots, m.$$

Un siffatto elemento esiste perché $|K| = \infty$ e dunque si può scegliere in K un elemento diverso dagli $n(m-1)$ elementi $\frac{\alpha_i - \alpha}{\beta - \beta_j} \in M$. Si ponga ora $\xi := \alpha + c\beta$. Ovviamente $K(\xi) \subseteq K(\alpha, \beta)$. Per ottenere l'inclusione opposta (e quindi la tesi), basta provare che $\beta \in K(\xi)$ [in tal caso infatti anche $\alpha = \xi - c\beta \in K(\xi)$].

Consideriamo il polinomio $h(X) = f(\xi - cX)$. Tale polinomio ha coefficienti in $K(\xi)$ e quindi in M. Risulta:

$$h(\beta) = f(\xi - c\beta) = f(\alpha) = 0, \quad h(\beta_j) = f(\xi - c\beta_j) \neq 0, \ \forall\, j = 2, \dots, m,$$

[perché $\xi - c\beta_j \neq \alpha_i$, $\forall\, i = 1, \dots, n$]. Quindi (in $M[X]$) $X - \beta \,\big|\, h$ mentre $X - \beta_j \not| h$.

Poniamo $D := MCD(h, g)$ in $M[X]$ e $d := MCD(h, g)$ in $K(\xi)[X]$. Ovviamente $d \,\big|\, D$ [in base alla definizione di MCD]. Poiché g in $M[X]$ è prodotto degli m fattori distinti

$$(X - \beta)(X - \beta_2) \dots (X - \beta_m),$$

allora $D = X - \beta$. In $K(\xi)[X]$ i due polinomi h, g non possono essere coprimi [se lo fossero, varrebbe un'identità di Bézout del tipo $1 = gr + hs$, in $K(\xi)[X]$ e quindi anche in $M[X]$, contrariamente al fatto che $D \neq 1$]. Pertanto $d \neq 1$ e siccome $d \,\big|\, D = X - \beta$, allora $d = X - \beta$. Poiché $d = X - \beta \in K(\xi)[X]$, segue che $\beta \in K(\xi)$, come richiesto.

* * * * * * * * * * * * * * * * * * *

Esercizio 4.3.1. Sia K un campo. È assegnata l'estensione di campi

$$K(X^2, XY) \subset K(X, Y).$$

Verificare che tale estensione è algebrica semplice e determinarne il grado.

Esercizio 4.3.2. Sia K un campo. Verificare che l'estensione di campi

$$K(X^2Y, XY^2) \subseteq K(X, Y)$$

è algebrica semplice, di grado 3.

Esercizio 4.3.3. È assegnata l'estensione algebrica semplice $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{1 + \sqrt{3}})$.

(*i*) Determinarne grado, base e polinomio minimo.

(*ii*) Esprimere $\frac{1}{\sqrt{3}\sqrt{1+\sqrt{3}}}$ in tale base.

Esercizio 4.3.4. È assegnata l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.

(*i*) Determinarne il grado.

(*ii*) Determinare tutti i possibili elementi primitivi della forma $\sqrt[3]{2} + c\sqrt[3]{3}$, al variare di $c \in \boldsymbol{Q}$.

Esercizio 4.3.5. Si denoti con $\mathbf{A}$ la chiusura algebrica $\boldsymbol{C}_{alg,\boldsymbol{Q}}$ dell'estensione $\boldsymbol{Q} \subseteq \boldsymbol{C}$. [$\mathbf{A}$ è detto *campo dei numeri algebrici*].

(*i*) Utilizzando il *TFA* (teorema fondamentale dell'algebra) verificare che ogni polinomio non costante $p \in \mathbf{A}[X]$ ammette uno zero in $\mathbf{A}$.

(*ii*) Dimostrare che $\mathbf{A}$ non ha estensioni algebriche proprie.

Esercizio 4.3.6. Siano n, m due naturali relativamente primi. Verificare che

$$[\boldsymbol{Q}(\zeta_n, \zeta_m) : \boldsymbol{Q}] = \varphi(nm).$$

Cosa avviene se n, m non sono coprimi?

4. Costruzioni con riga e compasso

Le estensioni di campi giocano un ruolo risolutivo, come vedremo, nello studio di un importante problema classico della geometria euclidea.

Secondo Platone, *le rette e le circonferenze sono le sole figure geometriche perfette*. Per i geometri della Grecia antica, la geometria euclidea piana è stata quindi lo studio delle figure geometriche ottenute tracciando una sequenza finita di rette o circonferenze, costruite a partire da punti già ottenuti (o assegnati). Gli strumenti usati per tracciare rette e circonferenze sono rispettivamente la *riga* (non graduata) ed il *compasso*. Precisiamo cosa significa operare *con riga e compasso* [nel seguito abbreviato *R&C*] su un assegnato insieme $\boldsymbol{\mathcal{P}}_0$ (con almeno due punti distinti) del piano euclideo $\boldsymbol{E}^2$.

Definizione 4.1. *Un'operazione con la riga su* $\boldsymbol{\mathcal{P}}_0$ *consiste nel tracciare un (arbitrario) segmento della retta* $\boldsymbol{R}(A,B)$ *passante per due punti distinti* $A, B \in \boldsymbol{\mathcal{P}}_0$. *Un'operazione col compasso su* $\boldsymbol{\mathcal{P}}_0$ *consiste nel tracciare un (arbitrario) arco della circonferenza* $\boldsymbol{C}(A,d)$ *di centro un punto* $A \in \boldsymbol{\mathcal{P}}_0$ *e di raggio la distanza* $d = d(B,C) = \overline{BC}$ *di due punti distinti* $B, C \in \boldsymbol{\mathcal{P}}_0$.

Definizione 4.2. *Un punto* $P \in \boldsymbol{E}^2$ *è detto costruibile (con R&C) in un passo a partire da* $\boldsymbol{\mathcal{P}}_0$ *se* P *è intersezione di due rette, oppure di una retta ed una circonferenza, oppure di due circonferenze, ottenute con operazioni con la riga o col compasso su* $\boldsymbol{\mathcal{P}}_0$. *Un punto* $P \in \boldsymbol{E}^2$ *si dice poi costruibile (con R&C) a partire da* $\boldsymbol{\mathcal{P}}_0$ *se esiste una sequenza finita di punti di* $\boldsymbol{E}^2$ $P_1, P_2, \dots, P_n = P$, *tali che:*

- P_1 *è costruibile in un passo a partire da* $\boldsymbol{\mathcal{P}}_0$;
- P_2 *è costruibile in un passo a partire da* $\boldsymbol{\mathcal{P}}_0 \cup \{P_1\}$;

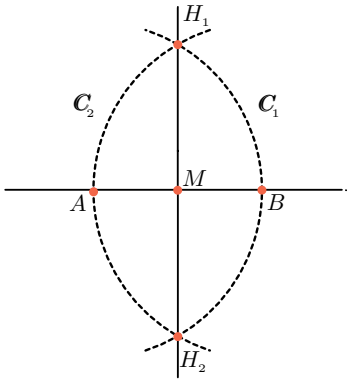
$\vdots$

- $P_n = P$ *è costruibile in un passo a partire da* $\boldsymbol{\mathcal{P}}_0 \cup \{P_1, P_2, \dots, P_{n-1}\}$.

Illustriamo alcune semplici costruzioni geometriche in $\boldsymbol{E}^2$ che si ottengono con operazioni con *R&C*.

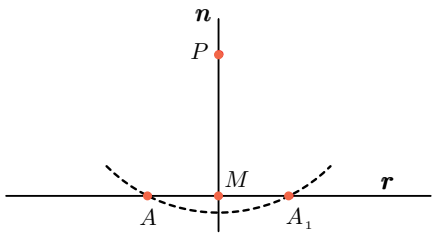
(A) *punto medio* M *di un segmento di estremi* $A, B \in \boldsymbol{\mathcal{P}}_0$.
Si ottiene con questa costruzione:

$\boldsymbol{C}_1 = \boldsymbol{C}(A, d(A,B))$;
$\boldsymbol{C}_2 = \boldsymbol{C}(B, d(A,B))$;
$\boldsymbol{C}_1 \cap \boldsymbol{C}_2 = \{H_1, H_2\}$;
$M = \boldsymbol{R}(H_1, H_2) \cap \boldsymbol{R}(A,B)$.



(B) *retta* $\boldsymbol{n}$ *normale ad un'assegnata retta* $\boldsymbol{r}$ *e passante per un punto* $P \notin \boldsymbol{r}$.
Si ottiene con questa costruzione:

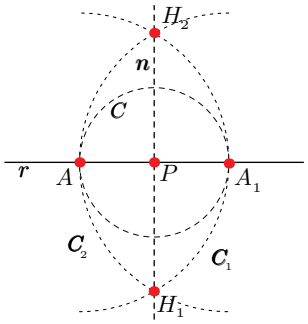
Si fissa $A \in \boldsymbol{r} \cap \boldsymbol{\mathcal{P}}_0$;
$\boldsymbol{C}(P, d(A,P)) \cap \boldsymbol{r} = \{A, A_1\}$;
$M =$ punto medio tra A, A_1 [cfr. (A)];
$\boldsymbol{n} = \boldsymbol{R}(M,P)$.



(C) *retta* $\boldsymbol{n}$ *normale ad un'assegnata retta* $\boldsymbol{r}$ *e passante per un punto* $P \in \boldsymbol{r}$ *assegnato.*

Si ottiene con questa costruzione:

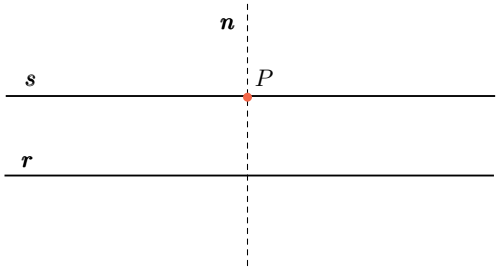
Si fissa $A \in \boldsymbol{r} \cap \boldsymbol{\mathcal{P}}_0,\ A \neq P$;
$\boldsymbol{C} = \boldsymbol{C}(P, d(A,P))$;
$\boldsymbol{C} \cap \boldsymbol{r} = \{A,\ A_1\}$;
$\boldsymbol{C}_1 = \boldsymbol{C}(A, d(A,A_1)),\ \boldsymbol{C}_2 = \boldsymbol{C}(A_1, d(A,A_1))$;
$\boldsymbol{C}_1 \cap \boldsymbol{C}_2 = \{H_1, H_2\}$;
$\boldsymbol{n} = \boldsymbol{R}(H_1,\ H_2)$.



(D) *retta* $\boldsymbol{s}$ *parallela ad un'assegnata retta* $\boldsymbol{r}$ *e passante per un punto* $P \notin \boldsymbol{r}$ *assegnato.*

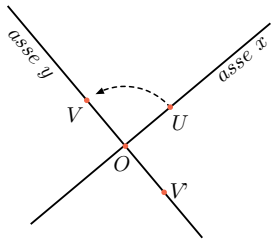
Si ottiene con questa costruzione:

$\boldsymbol{n} =$ retta normale a $\boldsymbol{r}$ per P [cfr. (B)];
$\boldsymbol{s} =$ retta normale a $\boldsymbol{n}$ per P [cfr. (C)].



Fissati in $\boldsymbol{\mathcal{P}}_0$ due punti distinti O, U, resta ad essi associato un unico riferimento cartesiano antiorario $RC = RC(O,U)$, avente O come origine ed U come punto unità dell'*asse* x. Tale RC è costruibile con *R&C*, come segue:

- *asse* $x = \boldsymbol{R}(O,U)$;
- *asse* $y =$ retta per O, normale all'*asse* x [cfr. (C)];
- se *asse* $y \cap \boldsymbol{C}(O, d(O,U)) = \{V, V'\}$ e se V è il primo dei due punti che si incontra, percorrendo in senso antiorario la circonferenza a partire da U, il punto V è scelto come punto unità dell'*asse* y.



D'ora in poi assumeremo che, assegnato $\boldsymbol{\mathcal{P}}_0$ in $\boldsymbol{E}^2$, sia fissato in esso un riferimento cartesiano antiorario $RC = RC(O,U)$. Rispetto ad RC, ogni punto $P \in \boldsymbol{E}^2$ corrisponde biunivocamente ad una coppia $(x,y) \in \boldsymbol{R}^2$, detta *coppia di coordinate cartesiane di* P *(rispetto ad* RC*)*; scriveremo, per semplicità, $P = (x,y)$.

Diremo che una *coppia di numeri reali* (x,y) *è costruibile con R&C a partire da* $\boldsymbol{\mathcal{P}}_0$ se il punto $P = (x,y)$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$. Diremo poi che $a \in \boldsymbol{R}$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$ se il punto $(a,0)$ [ovvero, equivalentemente, il punto $(0,a)$] lo è. Si verifica subito che $(x,y) \in \boldsymbol{R}^2$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0 \iff x, y \in \boldsymbol{R}$ lo sono.

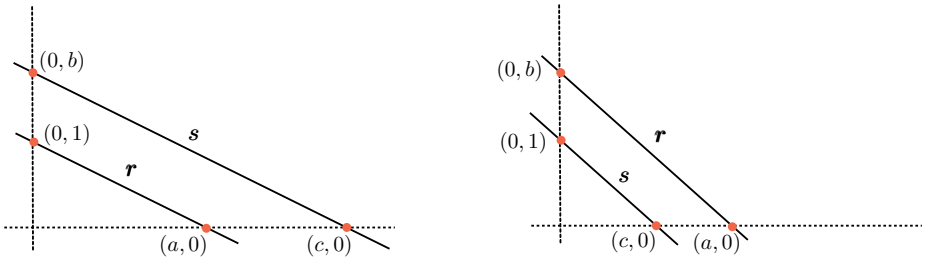
Lemma 4.1. *Siano* $a, b \in \boldsymbol{R}$ *costruibili (con R&C) a partire da* $\boldsymbol{\mathcal{P}}_0$. *Allora anche* $a \pm b$, ab *e* $\frac{a}{b}$ *(se* $b \neq 0$*) lo sono. Ne segue in particolare che tutti i punti di* $\boldsymbol{E}^2$ *a coordinate razionali sono costruibili con R&C a partire da* $\boldsymbol{\mathcal{P}}_0$.

Dim. Essendo a, b costruibili da $\boldsymbol{\mathcal{P}}_0$, i punti $(a,0)$, $(-a,0)$, $(b,0)$ e $(-b,0)$ lo sono (semplice verifica). Assumiamo $a,\ b > 0$. Allora

$$\boldsymbol{C}\big((a,0),b\big) \cap \ asse\ x = \{(a+b,0),\ (a-b,0)\}.$$

Se $a \leq 0$ o/e $b \leq 0$, si procede in modo analogo.

Per costruire ab e $\frac{a}{b}$ si ricorre al *teorema di Talete*. Assumiamo infatti ancora $a,\ b > 0$. Sia $\boldsymbol{r}$ la retta per $(0,1)$ e $(a,0)$ ed $\boldsymbol{s}$ la retta parallela ad $\boldsymbol{r}$, per $(0,b)$ [cfr. la figura seguente a sinistra]. Se $\boldsymbol{s} \cap \ asse\ x = (c,0)$, dal teorema di Talete $\frac{b}{1} = \frac{c}{a}$ e quindi $c = ab$. Pertanto ab è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$.



Infine, sempre nell'ipotesi $a,\ b > 0$, sia $\boldsymbol{r}$ la retta per $(a,0)$, $(0,b)$ e sia $\boldsymbol{s}$ la parallela ad $\boldsymbol{r}$, per $(0,1)$ [cfr. la figura precedente a destra]. Sia $(c,0) = \boldsymbol{s} \cap \ asse\ x$. Dal teorema di Talete $\frac{b}{1} = \frac{a}{c}$ e quindi $c = \frac{a}{b}$. Pertanto anche $\frac{a}{b}$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$.

L'ultima affermazione è evidente: $\forall\, q = \frac{a}{b} \in \boldsymbol{Q}$, gli interi a, b sono somma dell'unità 1 (o del suo opposto -1). Quindi q è costruibile con *R&C* a partire da $\{O,\ U\}$. Ne segue subito che lo stesso è vero per ogni $P = (q_1, q_2) \in \boldsymbol{Q} \times \boldsymbol{Q}$.

Sia $\boldsymbol{\mathcal{P}}_0 \subseteq \boldsymbol{E}^2$. Denotiamo con K_0 il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\boldsymbol{\mathcal{P}}_0$. Ovviamente $\boldsymbol{Q} \subseteq K_0$. Inoltre ogni $x \in K_0$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$. Ciò segue dal lemma precedente, tenendo conto che x è un quoziente di due espressioni polinomiali a coefficienti razionali nelle coordinate di punti di $\boldsymbol{\mathcal{P}}_0$.

Ma ci sono altri punti (oltre a quelli di K_0) costruibili con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$. Per individuarli ci dobbiamo chiedere come si estende K_0 quando costruiamo con *R&C* un punto $P = (x,y) \in \boldsymbol{E}^2$ a partire da $\boldsymbol{\mathcal{P}}_0$. Cominciamo con i punti costruibili in un passo.

Proposizione 4.1. *Sia K_0 il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\boldsymbol{\mathcal{P}}_0 \subseteq \boldsymbol{E}^2$. Sia $P = (x,y) \in \boldsymbol{E}^2$.* [Si noti che il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\boldsymbol{\mathcal{P}}_0 \cup \{P\}$ è $K_0(x,y)$]. *Risulta: se P è costruibile in un passo a partire da $\boldsymbol{\mathcal{P}}_0$, allora* $[K_0(x,y) : K_0] \leq 2$.

Dim. Da elementari considerazioni geometriche segue subito che l'equazione cartesiana di una retta o di una circonferenza costruita con punti di $\boldsymbol{\mathcal{P}}_0$ ha coefficienti in K_0.

Sia ora $P = (x,y)$ un punto costruibile in un passo a partire da $\boldsymbol{\mathcal{P}}_0$. Sono possibili tre casi:

(a) P è intersezione di due rette $aX+bY = c,\ a'X+b'Y = c'$ (con $a,b,c,a',b',c' \in K_0$). Il sistema formato da tali equazioni ha un'unica soluzione (x,y), con $x,\ y \in K_0$. Dunque $[K_0(x,y) : K_0] = 1$.

(b) P è intersezione della retta $aX + bY = c$ con la circonferenza $X^2 + Y^2 + dX + eY = f$ (con $a,b,c,d,e,f \in K_0$). Esplicitando l'equazione della retta rispetto (ad esempio) alla variabile Y e sostituendo tale espressione nell'equazione della circonferenza, si ottiene un'equazione del tipo

$$\alpha X^2 + \beta X + \gamma = 0, \ \text{ per opportuni } \ \alpha,\ \beta,\ \gamma \in K_0,$$

di cui x è soluzione. Si osserva poi subito che $y \in K_0(x)$ [essendo $ax + by = c$]. Si ha quindi:

$$[K_0(x,y) : K_0] = [K_0(x,y) : K_0(x)] \cdot [K_0(x) : K_0] = [K_0(x) : K_0] = 2 \ \text{ oppure } \ 1,$$

a seconda che il polinomio $\alpha X^2 + \beta X + \gamma \in K_0[X]$ sia o meno irriducibile su K_0.

(c) P è intersezione di due circonferenze $\boldsymbol{C}:\ X^2+Y^2+aX+bY = c,\ \boldsymbol{C}':\ X^2+Y^2+a'X+b'Y = c'$ (con $a,b,c,a',b',c' \in K_0$). Sottraendo tra loro le due equazioni si ottiene $(a-a')X+(b-b')Y = c-c'$, che rappresenta (in generale) una retta $\boldsymbol{r}$ tale che $\boldsymbol{C} \cap \boldsymbol{r} = \boldsymbol{C} \cap \boldsymbol{C}'$. Dunque P è intersezione di una

retta ed una circonferenza. Si ritorna così al caso (b).

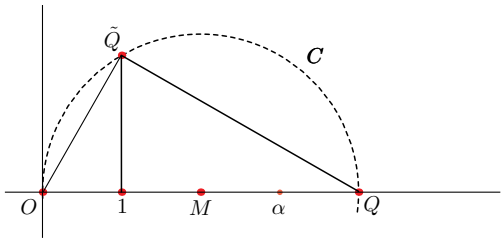
La Prop. **4.1** può essere approssimativamente invertita, nella seguente forma.

Proposizione 4.2. *Sia $x \in \boldsymbol{R}$ tale che $[K_0(x) : K_0] = 2$. Allora $(x, 0)$ è costruibile con R&C a partire da $\boldsymbol{\mathcal{P}}_0$.*

Dim. Se denotiamo con $X^2+aX+b \in K_0[X]$ il polinomio minimo di x su K_0, risulta $x = \frac{-a \pm \sqrt{\Delta}}{2}$, con $\Delta = a^2-4b > 0$. Ovviamente il punto $(\Delta, 0)$ è costruibile con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$. Se proviamo che anche il punto $(\sqrt{\Delta}, 0)$ è costruibile con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$, allora anche $(x, 0)$ lo è. Quindi basterà provare la seguente affermazione:

$(*)$ *Se $\alpha \in K_0$ e $\alpha > 0$, il punto $(\sqrt{\alpha}, 0)$ è costruibile con R&C a partire da $\boldsymbol{\mathcal{P}}_0$.*

Dimostriamo $(*)$. Il punto $Q = (\alpha+1, 0)$ è costruibile con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$. Sia M il punto medio del segmento di estremi O, Q e sia $\boldsymbol{C} = \boldsymbol{C}(M, d(O, M))$. Sia poi $\tilde{Q} = (1, h)$ il punto costruito intersecando $\boldsymbol{C}$ con la semiretta $X = 1,\ Y \geq 0$



Il triangolo $O\tilde{Q}Q$ è rettangolo (nel vertice $\tilde{Q}$). Ad esso applichiamo il *secondo teorema di Euclide*: *"il quadrato costruito sull'altezza relativa all'ipotenusa coincide con il prodotto delle proiezioni dei due cateti sull'ipotenusa"*. Tali proiezioni sono $1, \alpha$. Pertanto $h^2 = 1 \cdot \alpha$ e quindi $h = \sqrt{\alpha}$. Poiché $\tilde{Q} = (1, h)$ è costruibile a partire da $\boldsymbol{\mathcal{P}}_0$, anche $(\sqrt{\alpha}, 0)$ lo è.

Veniamo ora ad una caratterizzazione dei punti in $\boldsymbol{E}^2$ costruibili con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$.

Teorema 4.1. *Sia K_0 il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\boldsymbol{\mathcal{P}}_0 \subseteq \boldsymbol{E}^2$. Sia $P = (x, y) \in \boldsymbol{E}^2$. Risulta: P è costruibile con R&C a partire da $\boldsymbol{\mathcal{P}}_0 \iff$ esistono $\alpha_1, \ldots, \alpha_n \in \boldsymbol{R}$ tali che $x, y \in K_0(\alpha_1, \ldots, \alpha_n)$ e $\alpha_1^2 \in K_0$, $\alpha_2^2 \in K_0(\alpha_1)$, $\ldots$, $\alpha_n^2 \in K_0(\alpha_1, \ldots, \alpha_{n-1})$.*

Dim. $(\Longrightarrow)$. Per definizione, $\exists\, P_1, P_2, \ldots, P_m = P \in \boldsymbol{E}^2$ tali che P_i è costruibile in un passo da $\boldsymbol{\mathcal{P}}_0 \cup \{P_1, \ldots, P_{i-1}\}$, $\forall\, i = 1, \ldots, m$. Sia K_i il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\boldsymbol{\mathcal{P}}_0 \cup \{P_1, \ldots, P_i\}$ [in particolare, $x, y \in K_m$]. Risulta:

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \ \ldots\ \subseteq K_m, \ \text{ con } \ [K_i : K_{i-1}] \leq 2$$

(in base alla Prop. **4.1**). Possiamo limitarci a considerare la sottocatena formata dalle sole estensioni proprie (cioè di grado 2). Cambiando gli indici, otteniamo la catena di estensioni proprie

$$K_0 \subset K_1 \subset \ \ldots\ \subset K_n\ (= K_m).$$

Per ogni $i = 1, \ldots, n$, si scelga $x_i \in K_i - K_{i-1}$ e sia $f_i \in K_{i-1}[X]$ il relativo polinomio minimo (di grado 2). Se denotiamo con Δ_i il discriminante di f_i, risulta $K_i = K_{i-1}(x_i) = K_{i-1}(\sqrt{\Delta_i})$. Posto $\alpha_i := \sqrt{\Delta_i}$, sono verificate le condizioni $\alpha_i^2 \in K_{i-1}\ (1 \leq i \leq n)$ e risulta: $x, y \in K_m = K_{n-1}(\alpha_n) =$ $.... = K_0(\alpha_1, \ldots \alpha_n)$.

$(\Longleftarrow)$. Poniamo $Q_i = (\alpha_i, 0)$, $\forall\, i = 1, \ldots, n$. In base all'affermazione $(*)$ di Prop. **4.2**, essendo $\alpha_i = \pm\sqrt{\alpha_i^2}$, risulta:

Q_1 è costruibile a partire da $\boldsymbol{\mathcal{P}}_0$; Q_2 è costruibile a partire da $\boldsymbol{\mathcal{P}}_0 \cup \{Q_1\}$; $\ldots$;
Q_n è costruibile a partire da $\boldsymbol{\mathcal{P}}_0 \cup \{Q_1, \ldots, Q_{n-1}\}$.

Poiché $x, y \in K_0(\alpha_1, \ldots, \alpha_n)$ e tale campo è il sottocampo generato dalle coordinate dei punti di $\mathcal{P}_0 \cup \{Q_1, \ldots, Q_n\}$, si conclude che $P = (x, y)$ è costruibile con *R&C* in $\mathcal{P}_0 \cup \{Q_1, \ldots, Q_n\}$ e quindi a partire da $\mathcal{P}_0$ [essendo ogni Q_i costruito con *R&C* a partire da $\mathcal{P}_0$].

Corollario 4.1. *Sia K_0 il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\mathcal{P}_0$. Se $P = (x, y)$ è costruibile con R&C a partire da $\mathcal{P}_0$, $[K_0(x, y) : K_0]$ è una potenza di 2. Ne segue subito che anche $[K_0(x) : K_0]$ e $[K_0(y) : K_0]$ sono potenze di 2.*

Dim. In base alla dimostrazione del Teor. **4.1**, posto $K_i = K_{i-1}(\alpha_i)$, risulta:

$$[K_0(\alpha_1, \ldots, \alpha_n) : K_0] = [K_n : K_{n-1}] \cdot \ldots \cdot [K_1 : K_0] = 2^t, \text{ con } 0 \leq t \leq n.$$

Allora

$$2^t = [K_0(\alpha_1, \ldots, \alpha_n) : K_0(x, y)] \cdot [K_0(x, y) : K_0] \text{ e quindi } [K_0(x, y) : K_0] = 2^s, \text{ con } 0 \leq s \leq t.$$

L'ultima affermazione è immediata, in quanto $[K_0(x) : K_0]$ e $[K_0(y) : K_0]$ sono divisori di 2^s.

Dal precedente Coroll. **4.1**, segue che non sono costruibili con *R&C* a partire da $\mathcal{P}_0$ tutti quei punti $(x, y) \in \boldsymbol{E}^2$ tali che $[K_0(x, y) : K_0]$ non è potenza di 2. Da questa semplice osservazione segue la risoluzione di famosi problemi della geometria euclidea classica.

Corollario 4.2. *Con R&C non è possibile duplicare un cubo né rettificare o quadrare un cerchio.*

Dim. Sia $\mathcal{P}_0 = \{O, U\} \subset \boldsymbol{E}^2$ (e quindi $K_0 = \boldsymbol{Q}$). Sia $\boldsymbol{\mathcal{Q}}$ un cubo di lato 1 (e quindi volume 1). *"Duplicare $\boldsymbol{\mathcal{Q}}$ con R&C"* significa costruire con *R&C* un cubo di volume doppio, cioè il cui lato ha misura $\ell \in \boldsymbol{R}$ tale che $\ell^3 = 2$. Poiché ℓ ha polinomio minimo $X^3 - 2 \in \boldsymbol{Q}[X]$, allora $[\boldsymbol{Q}(\ell) : \boldsymbol{Q}] = 3$. In base al Coroll. **4.1**, $(\ell, 0)$ non è costruibile con *R&C* a partire da $\mathcal{P}_0$.

Sia $\boldsymbol{C}$ una circonferenza unitaria (cioè di raggio 1). La sua lunghezza è 2π e la sua area è π. *"Rettificare $\boldsymbol{C}$ con R&C"* significa costruire con *R&C* un punto $(\ell, 0)$ tale che $\ell = 2\pi$, mentre *"quadrare $\boldsymbol{C}$ con R&C"* significa costruire con *R&C* un quadrato di lato ℓ tale che $\ell^2 = \pi$, cioè $\ell = \sqrt{\pi}$. Ma $[\boldsymbol{Q}(2\pi) : \boldsymbol{Q}] = [\boldsymbol{Q}(\sqrt{\pi}) : \boldsymbol{Q}] = \infty$ [perché π è trascendente su $\boldsymbol{Q}$]. Dunque $(\ell, 0)$ non è costruibile con *R&C* a partire da $\mathcal{P}_0$.

Il Coroll. **4.1** non si inverte. Utilizzando argomenti della teoria di Galois è infatti possibile ottenere un'estensione M di grado 4 su $\boldsymbol{Q}$ ed un elemento $x \in M$ non costruibile con *R&C* a partire da $\mathcal{P}_0 = \{O, U\}$.

Sussiste però il seguente inverso parziale (molto più debole) del Coroll. **4.1**. Di esso avremo bisogno per dimostrare il successivo Teor. **4.2**.

Proposizione 4.3. *Sia K_0 il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti di $\mathcal{P}_0$ e sia M un sottocampo di $\boldsymbol{R}$ contenente K_0, tale che $[M : K_0] = 2^r$, con $r \geq 1$. Se esiste una catena di estensioni tutte di grado 2*

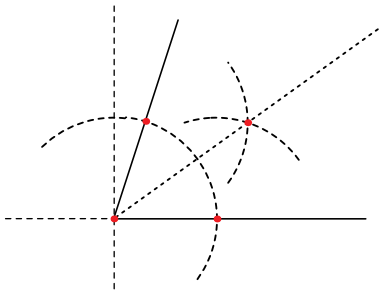
$$K_0 \subset M_1 \subset M_2 \subset \ldots \subset M_{r-1} \subset M_r = M,$$

ogni $x \in M$ è costruibile con R&C a partire da $\mathcal{P}_0$.

Dim. Procediamo per induzione su r. Se $r = 1$, $[M : K_0] = 2$. Per ogni $x \in M - K_0$, $M = K_0(x)$ e l'asserto è quindi conseguenza di Prop. **4.2**. Sia $r \geq 2$. Poiché $[M : M_{r-1}] = 2$, da Prop. **4.2** segue che x è costruibile con *R&C* da $\mathcal{P}_0$ e da un numero finito di punti le cui coordinate generano M_{r-1}. Poiché $[M_{r-1} : K_0] = 2^{r-1}$, per ipotesi induttiva tali punti sono costruibili con *R&C* a partire da $\mathcal{P}_0$. Si conclude che x è costruibile con *R&C* a partire da $\mathcal{P}_0$.

Ci occuperemo ora di *bisezione* e *trisezione di angoli*. Bisecare un angolo è un problema facilmente

risolubile con *R&C*. Basta procedere come suggerito nella figura che segue.



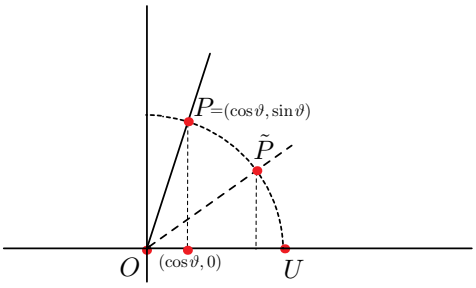
Vogliamo comunque dimostrare che la bisettrice di un angolo è costruibile con *R&C*, come conseguenza dei precedenti risultati.

Corollario 4.3. *La bisezione di un angolo è un problema risolubile con R&C.*

Dim. Sia ϑ la misura in radianti di un angolo di vertice O ed avente come lati il *semiasse* $x > 0$ e la semiretta di origine O, passante per il punto $P = (\cos\vartheta, \sin\vartheta)$. Assumiamo $\boldsymbol{\mathcal{P}}_0 = \{O, U, (\cos\vartheta, 0)\}$ e quindi $K_0 = \boldsymbol{Q}(\cos\vartheta)$. [Si noti che $P = (\cos\vartheta, \sin\vartheta)$ è facilmente costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$: basta intersecare la circonferenza $\boldsymbol{C}(O, 1)$ con la semiretta $\{X = \cos\vartheta,\ Y \geq 0\}$.

Per bisecare l'angolo bisogna costruire con *R&C* il punto $(\cos\frac{\vartheta}{2}, 0)$ [da cui subito si costruisce il punto $\tilde{P} = (\cos\frac{\vartheta}{2}, \sin\frac{\vartheta}{2})$ e la retta $\boldsymbol{R}(O, \tilde{P})$ che biseca l'angolo assegnato].

Poiché $\cos\frac{\vartheta}{2} = \pm\sqrt{\frac{1+\cos\vartheta}{2}}$ e ovviamente $\frac{1+\cos\vartheta}{2} \in K_0$, dall'affermazione $(*)$ di Prop. **4.2** segue subito che $(\cos\frac{\vartheta}{2}, 0)$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$.



Corollario 4.4. *La trisezione di un angolo è un problema non sempre risolubile con R&C.*

Dim. Manteniamo le notazioni della dimostrazione del precedente Coroll. **4.3**. A partire da $\boldsymbol{\mathcal{P}}_0 = \{O, U, (\cos\vartheta, 0)\}$ [e quindi $K_0 = \boldsymbol{Q}(\cos\vartheta)$], per trisecare l'angolo assegnato bisogna costruire con *R&C* il punto $(\cos\frac{\vartheta}{3}, 0)$. Dall'identità trigonometrica $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ segue:

$$\cos\vartheta = 4\cos^3\tfrac{\vartheta}{3} - 3\cos\tfrac{\vartheta}{3}.$$

Dunque $\cos\frac{\vartheta}{3}$ è uno zero del polinomio $f = 4X^3 - 3X - \cos\vartheta \in K_0[X]$.

Se f è irriducibile su K_0, $[K_0(\cos\frac{\vartheta}{3}) : K_0] = 3$ e dunque, in base al Coroll. **4.1**, il punto non è costruibile con *R&C*. Se invece f è riducibile su K_0, allora $[K_0(\cos\frac{\vartheta}{3}) : K_0] \leq 2$ e dunque, in base a Prop. **4.2**, il punto $(\cos\frac{\vartheta}{3}, 0)$ è costruibile con *R&C*.

Esempi 4.1. (*i*) *L'angolo retto è trisecabile con R&C.*
Posto $\vartheta = \frac{\pi}{2}$, $\cos\vartheta = 0$ e quindi $K_0 = \boldsymbol{Q}$. Il polinomio $f = 4X^3 - 3X \in \boldsymbol{Q}[X]$ è ovviamente riducibile e quindi l'angolo retto è trisecabile con *R&C*. Ne segue che $(\cos\frac{\pi}{6}, 0)$ è costruibile con *R&C* [infatti $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$].

(*ii*) *L'angolo di* 60^0 *non è trisecabile con R&C.*

Posto $\vartheta = \frac{\pi}{3}$, $\cos\vartheta = \frac{1}{2}$ e quindi $K_0 = \boldsymbol{Q}(\frac{1}{2}) = \boldsymbol{Q}$. Il polinomio $f = 4X^3 - 3X - \frac{1}{2} \in \boldsymbol{Q}[X]$ è irriducibile su $\boldsymbol{Q}$ [infatti il polinomio $8X^3 - 6X - 1 \in \boldsymbol{Z}[X]$ è irriducibile su $\boldsymbol{Z}$, in quanto, come facilmente si verifica, non ha zeri razionali]. Dunque $\cos\frac{\pi}{9}$ non è costruibile con *R&C*. Ne segue che l'angolo di 60^0 non è trisecabile con *R&C*.

Vogliamo ora studiare la costruibilità con *R&C* dei poligoni regolari, a partire da un insieme $\{O, U\} \subset \boldsymbol{E}^2$. Introduciamo la seguente notazione: per ogni $n \geq 3$, denotiamo con $\boldsymbol{\mathcal{P}}_n$ il *poligono regolare n-latero unitario standard*, cioè il poligono centrato in O, inscritto nella circonferenza unitaria e con un vertice in U. I suoi vertici si identificano, nel piano di Gauss, con le n radici n-sime dell'unità

$$\zeta_n^k = \cos\tfrac{2k\pi}{n} + i\sin\tfrac{2k\pi}{n} \quad (0 \leq k < n).$$

In particolare, ζ_n si identifica con il vertice $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ di $\boldsymbol{\mathcal{P}}_n$. Ovviamente, $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C* $\iff$ tale punto lo è.

Nel lemma che segue abbiamo raccolto alcune semplici considerazioni sulla costruibilità con *R&C* di $\boldsymbol{\mathcal{P}}_n$.

Lemma 4.2. *(a) Se $m \,|\, n$ e $\boldsymbol{\mathcal{P}}_n$ è costruibile con R&C, anche $\boldsymbol{\mathcal{P}}_m$ lo è.*

(b) Se $MCD(n, m) = 1$ e se $\boldsymbol{\mathcal{P}}_n, \boldsymbol{\mathcal{P}}_m$ sono costruibili con R&C, anche $\boldsymbol{\mathcal{P}}_{nm}$ lo è.

(c) Sia $n = p_1^{k_1} \ldots p_s^{k_s}$ (con i p_i primi a due a due distinti e $k_i > 0$). Risulta:

$$\boldsymbol{\mathcal{P}}_n \text{ è costruibile con R\&C} \iff \text{ogni } \boldsymbol{\mathcal{P}}_{p_i^{k_i}} \text{ lo è.}$$

(d) Ogni $\boldsymbol{\mathcal{P}}_{2^k}$ è costruibile con R&C.

Dim. (*a*) Sia $n = md$. Poiché $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C*, in particolare lo è il suo vertice $\zeta_n^d = \zeta_m$. Ne segue che $\boldsymbol{\mathcal{P}}_m$ è costruibile con *R&C*.

(*b*) Sia $1 = an + bm$ (identità di Bézout). Allora $\frac{1}{nm} = \frac{a}{m} + \frac{b}{n}$ e quindi

$$\cos\tfrac{2\pi}{nm} = \cos\big(a\,\tfrac{2\pi}{m} + b\,\tfrac{2\pi}{n}\big).$$

Utilizzando le formule di addizione e sottrazione del coseno, si ottiene che $\cos\frac{2\pi}{nm}$ è un'espressione polinomiale (a coefficienti interi) di

$$x_n = \cos\tfrac{2\pi}{n},\ y_n = \sin\tfrac{2\pi}{n},\ x_m = \cos\tfrac{2\pi}{m},\ y_m = \sin\tfrac{2\pi}{m}.$$

Dunque $\cos\frac{2\pi}{nm} \in \boldsymbol{Q}(x_n, y_n, x_m, y_m)$. Essendo x_n, y_n, x_m, y_m costruibili con *R&C*, anche $\cos\frac{2\pi}{nm}$ è costruibile con *R&C*.

(*c*) discende subito da (*a*) e (*b*).

(*d*) Per ogni intero $k \geq 3$, il poligono $\boldsymbol{\mathcal{P}}_{2^k}$ è ottenuto da $\boldsymbol{\mathcal{P}}_{2^{k-1}}$ bisecando gli angoli al centro (che insistono sui lati) di ampiezza $\vartheta = \frac{2\pi}{2^{k-1}}$. Poiché la bisezione di un angolo è realizzabile con *R&C* e poiché $\boldsymbol{\mathcal{P}}_{2^2}$ è ovviamente costruibile con *R&C*, si ha la tesi (per induzione su $k \geq 2$).

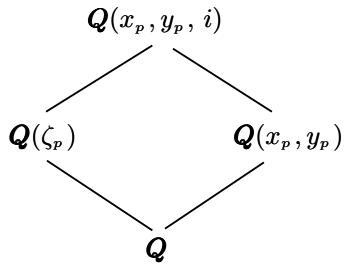
Nota. Si noti che, se $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C*, anche $\boldsymbol{\mathcal{P}}_{2n}$ lo è [basta bisecare l'angolo $\vartheta = \frac{2\pi}{n}$].

La maggior parte dei poligoni regolari $\boldsymbol{\mathcal{P}}_p$, con p primo, non sono però costruibili con *R&C* (a partire da $\{O, U\}$). Vale infatti il seguente risultato, conseguenza del Coroll. **4.1**.

Corollario 4.5. *Sia p un primo ≥ 3. Se $p - 1$ non è una potenza di 2, $\boldsymbol{\mathcal{P}}_p$ non è costruibile con R&C (a partire da $\{O, U\}$).*

Dim. Sia $P = (x_p, y_p)$, con $x_p = \cos\frac{2\pi}{p}$, $y_p = \sin\frac{2\pi}{p}$ [e dunque $\zeta_p = x_p + i\,y_p$]. Per ipotesi, $p - 1 = qh$, con $q, h \in \boldsymbol{N}$ e q primo dispari. Se proviamo che $q \,|\, [\boldsymbol{Q}(x_p, y_p) : \boldsymbol{Q}]$, in base al Coroll. **4.1**, P non è costruibile con *R&C*.

Si ha: $[\boldsymbol{Q}(\zeta_p):\boldsymbol{Q}]=p-1$, in quanto ζ_p ha polinomio minimo $\Phi_p=X^{p-1}+X^{p-2}+...+X+1\in \boldsymbol{Q}[X]$ [cfr. Osserv. **2.3**]. Consideriamo il seguente diagramma di estensioni



Ovviamente $[\boldsymbol{Q}(x_p, y_p, i):\boldsymbol{Q}(x_p, y_p)]=2$ e $[\boldsymbol{Q}(\zeta_p):\boldsymbol{Q}]=p-1$, come sopra osservato. Se poniamo $a:=[\boldsymbol{Q}(x_p, y_p):\boldsymbol{Q}]$ e $b:=[\boldsymbol{Q}(x_p, y_p, i):\boldsymbol{Q}(\zeta_p)]$, allora $2a=b(p-1)=bqh$. Poiché $q\,|\,2a$ e $q\not|\,2$, allora $q\,|\,a$, come richiesto.

Dal Coroll. **4.5**, se $p=7, 11, 13, 19, 23, 29, ...$, $\boldsymbol{\mathcal{P}}_p$ non è costruibile con *R&C*. Lo stesso è vero per $\boldsymbol{\mathcal{P}}_{pk}$, $\forall k\geq 1$ (in base al Lemma **4.2**(a)). Restano fuori dalla lista precedente i primi 3, 5, 17 e, più generalmente, tutti i primi della forma $1+2^{2^k}$, $k\geq 0$.

Che $\boldsymbol{\mathcal{P}}_3$ e $\boldsymbol{\mathcal{P}}_5$ fossero costruibili con *R&C* era già noto ai matematici dell'antica Grecia. Che anche $\boldsymbol{\mathcal{P}}_{17}$ fosse costruibile con *R&C* fu dimostrato (all'età di 19 anni) da Gauss (nel 1796). Lo stesso Gauss ha poi caratterizzato i poligoni $\boldsymbol{\mathcal{P}}_n$ costruibili con *R&C*, dimostrando il seguente teorema.

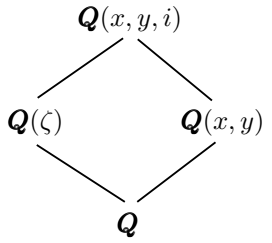
Teorema 4.2. *(Gauss)* $\boldsymbol{\mathcal{P}}_n$ *è costruibile con R&C (a partire da* $\{O,U\}$*)* $\iff$ $n=2^r p_1...p_s$, *con* $r,s\geq 0$ *e* $p_1, ..., p_s$ *primi a due a due distinti, tali che* $p_i=2^{2^{k_i}}+1$.

La dimostrazione di tale teorema necessita di un lemma (che ripresenta gli argomenti della dimostrazione del Coroll. **4.5**).

Lemma 4.3. *Se* p *è un primo* ≥ 3, *il poligono regolare* $\boldsymbol{\mathcal{P}}_{p^2}$ *non è costruibile con R&C.*

Dim. Posto $\zeta=\zeta_{p^2}=x+iy$, con $x=\cos\frac{2\pi}{p^2}$, $y=\sin\frac{2\pi}{p^2}$, basta dimostrare che $[\boldsymbol{Q}(x,y):\boldsymbol{Q}]$ non è una potenza di 2.

È noto che ζ ha polinomio minimo $\Phi_{p^2}=1+X^p+X^{2p}+...+X^{p(p-1)}\in\boldsymbol{Q}[X]$ (cfr. Osserv. **2.3**). Si consideri il diagramma di campi



Si osserva subito che $[\boldsymbol{Q}(\zeta):\boldsymbol{Q}]=p(p-1)$ e $[\boldsymbol{Q}(x,y,i):\boldsymbol{Q}(x,y)]=2$. Posto $a:=[\boldsymbol{Q}(x,y):\boldsymbol{Q}]$ e $b:=[\boldsymbol{Q}(x,y,i):\boldsymbol{Q}(\zeta)]$, allora $2a=bp(p-1)$. Poiché $p\,|\,2a$ e $MCD(p,2)=1$, allora $p\,|\,a$. Pertanto $[\boldsymbol{Q}(x,y):\boldsymbol{Q}]$ non è una potenza di 2.

Possiamo ora dimostrare il teorema di Gauss.

($\Longrightarrow$). Sia $\boldsymbol{\mathcal{P}}_n$ costruibile con *R&C* e sia $n=2^r p_1^{r_1}...p_s^{r_s}$, con $r, s\geq 0$ e (se $s\geq 1$) $p_1, ..., p_s$ primi dispari (due a due distinti) e $r_1, ..., r_s\geq 1$.

Se per assurdo $r_i \geq 2$, allora, in base al Lemma **4.2**(a), $\boldsymbol{\mathcal{P}}_{p_i^2}$ sarebbe costruibile con $R\&C$: ciò è assurdo, in base al Lemma **4.3**. Dunque $n = 2^r p_1 \dots p_s$.

Sia $s \geq 1$. Essendo ogni $\boldsymbol{\mathcal{P}}_{p_i}$ costruibile con $R\&C$, in base al Coroll. **4.5** risulta $p_i - 1 = 2^{s_i}$. Resta soltanto da verificare che $s_i = 2^{k_i}$ $(1 \leq i \leq s)$. Per assurdo, s_i non sia una potenza di 2 ed abbia quindi un fattore dispari $d > 1$. Dunque $s_i = dh$, $\exists\, h \in \boldsymbol{N}$, $h \geq 1$. Si verifica subito che in $\boldsymbol{Z}[X]$ vale l'identità

$$X^d + 1 = (X+1)g, \text{ con } g = \sum_{t=0}^{d-1} (-1)^t X^t = 1 - X + X^2 - X^3 + \dots + X^{d-1}.$$

Calcolando tale identità in 2^h, si ottiene:

$$p_i = 2^{hd} + 1 = (2^h + 1)\, g(2^h).$$

Poiché $1 < 2^h + 1 < 2^{hd} + 1 = p_i]$, si è ottenuta una fattorizzazione non banale del primo p_i: assurdo.

Nota. Abbiamo dimostrato che un naturale della forma $1 + 2^s$, con s non potenza di 2, non può essere primo.

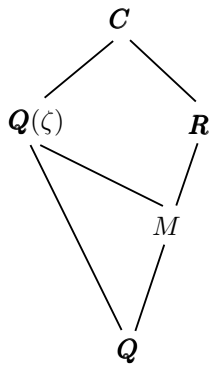
($\Longleftarrow$). La dimostrazione che segue è incompleta in quanto, per poterla concludere, è necessario utilizzare la *corrispondenza di Galois* (che studieremo in Cap. **5**, § **5**).

In base al Lemma **4.2**(c),(d), è sufficiente dimostrare che i poligoni regolari $\boldsymbol{\mathcal{P}}_{p_1}$, ... , $\boldsymbol{\mathcal{P}}_{p_s}$ sono costruibili con $R\&C$. Per ipotesi, $p_i - 1 = 2^r$, con $r = 2^{k_i}$. Poniamo:

$$\zeta := \zeta_{p_i} = x + iy, \text{ con } x = \cos\tfrac{2\pi}{p_i},\ y = \sin\tfrac{2\pi}{p_i}.$$

Per ottenere la tesi va dimostrato che x è costruibile con $R\&C$ (perché allora ovviamente anche y lo è e quindi lo è $\boldsymbol{\mathcal{P}}_{p_i}$.

Osserviamo che $x = \frac{1}{2}(\zeta + \zeta^{-1})$ [infatti $\zeta^{-1} = \overline{\zeta}$ e quindi $\zeta + \zeta^{-1} = 2\,Re(\zeta) = 2x$]. Dunque $x \in \boldsymbol{Q}(\zeta) \cap \boldsymbol{R}$. Posto $M := \boldsymbol{Q}(\zeta) \cap \boldsymbol{R}$, ovviamente $x \in M$ e sussiste il seguente diagramma di estensioni.



Per ipotesi $[\boldsymbol{Q}(\zeta) : \boldsymbol{Q}] = p_i - 1 = 2^r$. Inoltre $\zeta \notin M$ e si verifica subito che ζ è zero del polinomio $f = X^2 - 2xX + 1 \in M[X]$ [infatti risulta: $f = (X - \zeta)(X - \overline{\zeta})$]. Ne segue che $[\boldsymbol{Q}(\zeta) : M] = 2$ e pertanto $[M : \boldsymbol{Q}] = 2^{r-1}$.

[Si noti che $M = \boldsymbol{Q}(x)$. Infatti ovviamente $\boldsymbol{Q}(x) \subseteq M$ e $[Q(\zeta) : \boldsymbol{Q}(x)] = 2$, in quanto $f \in \boldsymbol{Q}(x)[X]$; pertanto $[M : \boldsymbol{Q}(x)] = 1]$.

A questo punto per concludere va provato, tenuto conto della Prop. **4.3**, che esiste una catena di estensioni

$$(*) \qquad \boldsymbol{Q} \subset M_1 \subset M_2 \subset \ \dots\ \subset M_{r-1} = M,$$

tutte di grado 2. Ne segue che $x \in M$ è costruibile con $R\&C$.

Per provare l'esistenza della catena $(*)$ occorrono alcuni risultati relativi alla corrispondenza di Galois, che qui anticipiamo, avvertendo il lettore di leggere i punti successivi dopo aver studiato il Cap. **5**.

(*1*) $\boldsymbol{Q} \subset \boldsymbol{Q}(\zeta)$ è un'estensione finita, normale e separabile.

(*2*) il gruppo di Galois $G = G(\boldsymbol{Q}(\zeta) \,|\, \boldsymbol{Q})$ ha ordine 2^r [segue dal $TFTG(i)$].

(*3*) G è abeliano [segue dall'Esercizio **5.5.2**].

(*4*) l'estensione $\boldsymbol{Q} \subset M$ è normale [segue da (*3*) e dal *TFTG*(*iv*)] ed ovviamente finita e separabile.
(*5*) il gruppo di Galois $G' = G(M \,|\, \boldsymbol{Q})$ ha ordine 2^{r-1} [segue dal *TFTG*(*i*)]. Essendo un 2-gruppo, G' possiede (cfr. Cap. **2**, Coroll. **4.1**) una catena di sottogruppi

$$\{1\} = H_0 < H_1 < \ ... \ < H_{r-1} = G', \ \text{con} \ |H_i| = 2^i .$$

(*6*) La corrispondente catena di campi fissi [cfr. *TFTG*(*ii*)]:

$$M = H_0^{\flat} \supset H_1^{\flat} \supset \ ... \ \supset G'^{\flat} = \boldsymbol{Q}$$

è la richiesta catena di estensioni di grado 2.

Osservazione 4.1. Abbiamo quindi dimostrato che, se $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C*, gli eventuali fattori primi dispari di n sono della forma $1 + 2^{2^k}$. Tali numeri sono detti *numeri di Fermat*. Precisamente: *si chiama k-simo numero di Fermat il numero naturale* $F_k = 1 + 2^{2^k}$, $k \geq 0$.

Fermat osservò (nel 1640) che

$$F_0 = 3, \ F_1 = 5, \ F_2 = 17, \ F_3 = 257 \ \text{e} \ F_4 = 65537$$

sono numeri primi. Congetturò quindi che ogni F_k fosse primo. Ma ciò è falso: nel 1732 Eulero dimostrò che F_5 non è primo [si tratta di un naturale dell'ordine di 10^9]. A tutt'oggi non si conoscono altri numeri di Fermat che siano primi e non si sa se i numeri di Fermat primi siano in numero finito o infinito.

Concludiamo con un semplice corollario del teorema di Gauss.

Corollario 4.6. *Risulta:*

$$\boldsymbol{\mathcal{P}}_n \ \textit{è costruibile con R\&C} \iff \varphi(n) = 2^h, \ \exists\, h \geq 1$$

[dove φ *è la funzione di Eulero, cfr. Osserv.***2.3***].*

Dim. ($\Longrightarrow$). Sia $n = 2^r p_1 ... p_s$, con $r \geq 0$ e $p_1, ... p_s$ primi di Fermat a due a due distinti. Allora

$$\varphi(n) = 2^{r-1}(p_1 - 1) ... (p_s - 1) = 2^{r-1} \ 2^{2^{k_1}} \ ... \ 2^{2^{k_s}} = 2^h, \ \exists\, h \geq 1.$$

($\Longleftarrow$). Sia $n = 2^r p_1^{r_1} ... p_s^{r_s}$. Allora

$$2^h = \varphi(n) = 2^{r-1} \ p_1^{r_1 - 1}(p_1 - 1) ... \ p_s^{r_s - 1}(p_s - 1).$$

Ne segue subito (essendo i p_i dispari) che $r_i = 1$ e che $p_i - 1 = 2^{s_i}$. Infine, che s_i non possa avere un fattore dispari lo abbiamo già osservato nella *Nota* all'interno della dimostrazione del teorema di Gauss.

La parte conclusiva di questo paragrafo è dedicata alla costruzione con *R&C* del pentagono regolare standard $\boldsymbol{\mathcal{P}}_5$. Costruiremo $\boldsymbol{\mathcal{P}}_5$ unendo i vertici "dispari" consecutivi di $\boldsymbol{\mathcal{P}}_{10}$. $\boldsymbol{\mathcal{P}}_{10}$ in effetti è facilmente costruibile con *R&C*, in quanto, come vedremo, gode di questa importante proprietà: *"il lato di un poligono regolare* 10*-latero è la sezione aurea del raggio della propria circonferenza circoscritta"*.

Cominciamo dalla definizione di *sezione aurea*.

Definizione 4.3. *Sia* AB *un segmento del piano euclideo* $\boldsymbol{E}^2$ *e sia* P *un punto di* AB. *Siano* $\ell = \overline{AB}$ $[= d(A, B)]$ *e* $x = \overline{AP}$ $[= d(A, P)]$ *le misure dei due segmenti* AB *e* AP. *Il segmento* AP *è detto sezione aurea di* AB *se*

$$\tfrac{\ell}{x} = \tfrac{x}{\ell - x} \qquad [\textit{ovvero} \ \tfrac{\ell}{x} = \tfrac{\ell + x}{\ell}].$$

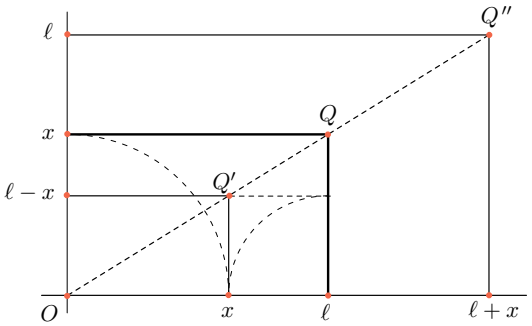
Il numero reale $\frac{\ell}{x}$ *è detto rapporto aureo, o numero d'oro, e verrà denotato con* G *[iniziale di "golden ratio"]. Ovviamente* $\overline{AP} = G^{-1}\overline{AB}$.

Più generalmente, diremo che un arbitrario segmento CD *del piano euclideo* $\boldsymbol{E}^2$ *è sezione aurea*

di un segmento AB *se* $\overline{CD} = G^{-1}\,\overline{AB}$.

Osservazione 4.2. Sia $\mathfrak{R}$ un rettangolo di $\boldsymbol{E}^2$, la cui altezza è sezione aurea della base. Fissiamo in $\boldsymbol{E}^2$ un riferimento cartesiano in modo che $\mathfrak{R}$ abbia un vertice nell'origine O e lati paralleli agli assi. Indicati con ℓ, x rispettivamente la misura della base e dell'altezza, $\mathfrak{R}$ ha un vertice in $Q = (\ell,\, x)$. Consideriamo i rettangoli $\mathfrak{R}'$, $\mathfrak{R}''$ [sempre con vertice in O e lati paralleli agli assi], aventi base ed altezza di misure $x, \ell - x$ e, rispettivamente, $\ell + x, \ell$.

Dalle proporzioni $\frac{\ell}{x} = \frac{x}{\ell - x} = \frac{\ell + x}{\ell}$ segue facilmente che tali rettangoli sono legati ad $\mathfrak{R}$ dalla seguente proprietà: il vertice $Q' = (x, \ell - x)$ di $\mathfrak{R}'$ ed il vertice $Q'' = (\ell + x, \ell)$ di $\mathfrak{R}''$ sono allineati con i vertici Q ed O, come evidenziato nella figura che segue.



Lemma 4.4. *Il rapporto aureo* G *verifica le seguenti proprietà:*

$$G^{-1} = \tfrac{\sqrt{5}-1}{2}; \quad G = G^{-1} + 1 = \tfrac{\sqrt{5}+1}{2}.$$

Dim. Da $\frac{\ell}{x} = \frac{x}{\ell - x}$ segue l'uguaglianza: $x^2 + \ell\, x - \ell^2 = 0$. Dunque x è zero del polinomio $X^2 + \ell X - \ell^2 \in \boldsymbol{R}[X]$. Tale polinomio ha zeri $\frac{-\ell \pm \ell\sqrt{5}}{2}$. Poiché $x > 0$, allora $x = \frac{-\ell + \ell\sqrt{5}}{2}$. Ne segue che

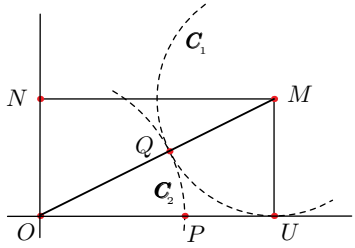
$$G^{-1} = \tfrac{x}{\ell} = \tfrac{\sqrt{5}-1}{2}.$$

Dividendo l'uguaglianza $x^2 + \ell\, x - \ell^2 = 0$ per x^2 si ottiene: $1 + G - G^2 = 0$, cioè $G(G-1) = 1$. Allora $G - 1 = G^{-1}$, cioè $G = G^{-1} + 1$.

Nota. Si può verificare che $G^{-1} \approx 0,618034$ [e dunque $G \approx 1,618034$]. Inoltre, dalla relazione $G^2 - G - 1 = 0$, segue che G ha polinomio minimo $X^2 - X - 1$ su $\boldsymbol{Q}$.

Per costruire con *R&C* la sezione aurea del segmento unitario OU, si procede come segue. Si fissi il rettangolo $\boldsymbol{\mathcal{R}}$ di vertici O, U, $M = (1, \frac{1}{2})$, $N = (0, \frac{1}{2})$, e se ne consideri la diagonale OM.
La sezione aurea OP di OU ottiene con questa costruzione:

$$\begin{aligned}
&\boldsymbol{C}_1 = \boldsymbol{C}(M, \overline{MU}) = \boldsymbol{C}(M, \tfrac{1}{2});\\
&Q = OM \cap \boldsymbol{C}_1;\\
&\boldsymbol{C}_2 = \boldsymbol{C}(O, \overline{OQ});\\
&P = OU \cap \boldsymbol{C}_2.
\end{aligned}$$



Si noti infatti che $\overline{OM} = \sqrt{1 + \frac{1}{4}} = \frac{\sqrt{5}}{2}$. Ne segue che $\overline{OQ} = \overline{OM} - \overline{MQ} = \frac{\sqrt{5}}{2} - \frac{1}{2} = G^{-1}$. Allora $\overline{OP} = \overline{OQ} = G^{-1} = G^{-1}\overline{OU}$. Dunque $\overline{OP} = G^{-1}\,\overline{OU}$.

Se AB è un segmento arbitrario, di lunghezza ℓ, per costruirne la sezione aurea AP si procede in modo analogo: si costruisce un rettangolo $\boldsymbol{\mathcal{R}}$ di vertici (successivi) A, B, M, N, con $\overline{BM} = \frac{\ell}{2}$. La diagonale AM di $\boldsymbol{\mathcal{R}}$ ha lunghezza $\frac{\ell\sqrt{5}}{2}$. Si pone

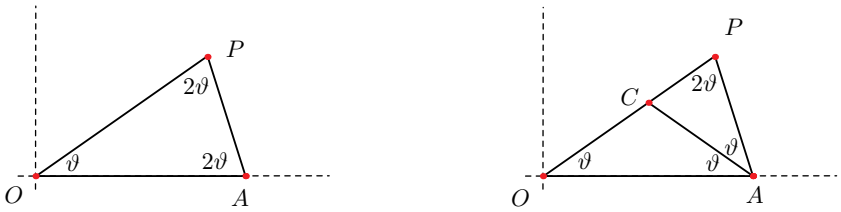
$$Q := AM \cap \boldsymbol{C}(M, \tfrac{\ell}{2}) \quad \text{e} \quad P := AB \cap \boldsymbol{C}(A, \overline{AQ}).$$

Poiché $\overline{AP} = \overline{AQ} = \overline{AM} - \overline{MB} = \ell\, G^{-1} = G^{-1}\,\overline{AB}$, allora AP è sezione aurea del segmento AB.

Lemma 4.5. *Sia $\mathcal{P}$ un poligono regolare 10-latero. Il lato di $\mathcal{P}$ è la sezione aurea del raggio della circonferenza circoscritta a $\mathcal{P}$.*

Dim. Scegliamo un RC tale che $\mathcal{P}$ abbia centro O ed un vertice A sul *semiasse* $x > 0$. Denotiamo con P il vertice di $\mathcal{P}$ successivo (in senso antiorario) ad A.

Sia ϑ la misura in radianti dell'angolo $\hat{O}$ del triangolo POA; risulta: $\vartheta = \frac{2\pi}{10} = \frac{\pi}{5}$. Poiché $\pi = 5\vartheta$ e POA è un triangolo isoscele, gli altri due angoli $\hat{P}$ ed $\hat{A}$ di POA misurano 2ϑ.



Si consideri la bisettrice AC dell'angolo $\hat{A}$ del triangolo POA. Si verifica subito che anche i due triangoli OCA e ACP sono isosceli. Ne segue che $\overline{AP} = \overline{AC} = \overline{OC}$. Ricordiamo ora il *teorema delle bisettrici* (cfr. Esercizio **4.4.8**):

Sia $\boldsymbol{\mathcal{T}}$ un arbitrario triangolo di vertici A, O, P e sia AC la bisettrice di $\boldsymbol{\mathcal{T}}$ relativa al vertice A [e quindi $C \in OP$]. Risulta: $\frac{\overline{AO}}{\overline{AP}} = \frac{\overline{OC}}{\overline{CP}}$.

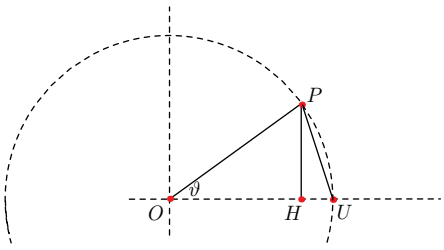
Essendo (nel nostro triangolo isoscele POA) $\overline{AP} = \overline{OC}$, allora

$$\frac{\overline{AO}}{\overline{AP}} = \frac{\overline{AP}}{\overline{CP}} = \frac{\overline{AP}}{\overline{OP}-\overline{OC}} = \frac{\overline{AP}}{\overline{AO}-\overline{AP}}.$$

In base alla Def. **4.3**, AP (lato di $\boldsymbol{\mathcal{P}}$) è sezione aurea di AO (raggio della circonferenza circoscritta).

Lemma 4.6. *Risulta: $\cos\frac{2\pi}{5} = \frac{1}{2}\,G^{-1}$.*

Dim. Si ponga $\vartheta = \frac{2\pi}{10}$ e $P = (\cos\vartheta, \sin\vartheta)$ (vertice di $\boldsymbol{\mathcal{P}}_{10}$). Dal Lemma **4.5**, essendo $\overline{OU} = 1$, $\overline{UP} = G^{-1} = \frac{\sqrt{5}-1}{2}$.



Sia H la proiezione ortogonale di P sull'*asse* x. Applichiamo il teorema di Pitagora al triangolo PHU:

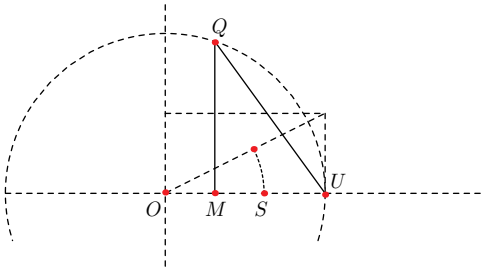
$$(G^{-1})^2 = \sin^2\vartheta + (1-\cos\vartheta)^2 = 2 - 2\cos\vartheta.$$

Ne segue $\cos\vartheta = \frac{1+\sqrt{5}}{4}$ e pertanto

$$\cos\left(\tfrac{2\pi}{5}\right) = \cos 2\vartheta = 2\cos^2\vartheta - 1 = \tfrac{1}{2}\,G^{-1}.$$

Dal Lemma **4.6** segue subito la costruzione con $R\&C$ di $\boldsymbol{\mathcal{P}}_5$. Basta costruire prima la sezione aurea OS del segmento unitario OU e poi calcolare il punto medio M di OS. Poiché $S = (G^{-1}, 0)$, allora $M = (\frac{1}{2}\,G^{-1}, 0) = (\cos(\frac{2\pi}{5}), 0)$. Da M si ricava subito il punto $Q = \big(\cos(\frac{2\pi}{5}), \sin(\frac{2\pi}{5})\big)$,

vertice di $\boldsymbol{\mathcal{P}}_5$



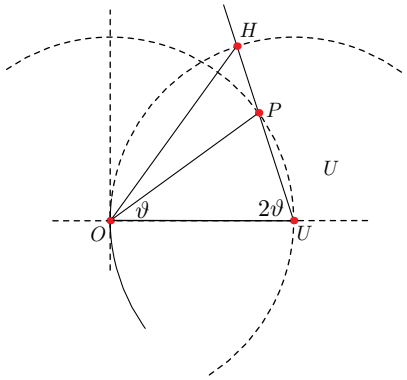
Osservazione 4.3. (*i*) Naturalmente il punto Q poteva essere ottenuto a partire da P (vertice di $\boldsymbol{\mathcal{P}}_{10}$) intersecando la circonferenza unitaria $\boldsymbol{C}(O,1)$ con la circonferenza $\boldsymbol{C}(P,G^{-1})$.

(*ii*) Per ottenere la lunghezza del lato di $\boldsymbol{\mathcal{P}}_5$ basta calcolare la distanza tra U e Q. Tenuto conto che $U=(1,0)$ e $Q=\big(\frac{1}{2}\,G^{-1},\sin(\frac{2\pi}{5})\big)$, si ottiene:

$$\overline{UQ}=\sqrt{(\tfrac{1}{2}\,G^{-1}-1)^2+1-\tfrac{1}{4}\,G^{-2}}\;=\frac{\sqrt{5-\sqrt{5}}}{\sqrt{2}}.$$

(*iii*) Un'altra costruzione del lato di $\boldsymbol{\mathcal{P}}_5$ a partire da quello di $\boldsymbol{\mathcal{P}}_{10}$ si ottiene come segue.

Costruito il segmento UP (lato di $\boldsymbol{\mathcal{P}}_{10}$), lo si prolunga sino ad incontrare in H la circonferenza $\boldsymbol{C}(U,1)$. Poiché l'angolo in U del triangolo OPU ha ampiezza $2\vartheta=\frac{2\pi}{5}$, il segmento OH (che insiste su tale angolo) ha la lunghezza del lato di $\boldsymbol{\mathcal{P}}_5$.



* * * * * * * * * * * * * * * * * * *

Esercizio 4.4.1. Sia $\boldsymbol{\mathcal{P}}_0=\{O,U\}\subset\boldsymbol{E}^2$ e sia $\boldsymbol{Q}_c$ il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti costruibili con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$. Verificare che $\boldsymbol{Q}\subset\boldsymbol{Q}_c$ è un'estensione algebrica infinita, con $\boldsymbol{Q}_c$ contenuto propriamente in $\boldsymbol{R}_{alg,\boldsymbol{Q}}$ (chiusura algebrica di $\boldsymbol{Q}$ in $\boldsymbol{R}$).

Esercizio 4.4.2. Utilizzando $R\&C$ dividere in tre parti uguali un assegnato segmento di $\boldsymbol{E}^2$.

Esercizio 4.4.3. Verificare che l'angolo di 120^0 non è trisecabile con $R\&C$. Dedurne che il poligono regolare 9-latero non può essere costruito con $R\&C$.

Esercizio 4.4.4. Verificare se l'angolo di 45^0 è trisecabile con $R\&C$.

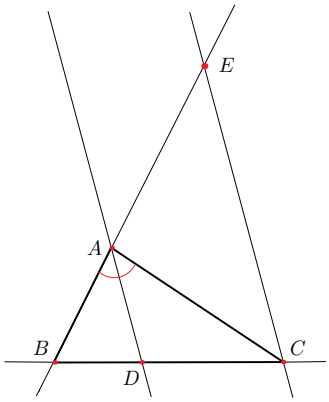
Esercizio 4.4.5. Verificare che l'angolo retto è *pentasecabile* con $R\&C$ e determinare un'espressione algebrica per il coseno dell'angolo di 18^0.

Suggerimento. Utilizzare l'identità trigonometrica $\cos 5\vartheta = 16\cos^5\vartheta - 20\cos^3\vartheta + 5\cos\vartheta$.

Esercizio 4.4.6. Spiegare, senza eseguire costruzioni grafiche, perché, assegnato un angolo di ampiezza ϑ (radianti), è possibile con *R&C* costruire un angolo di ampiezza $n\vartheta$, $\forall\, n \geq 1$.

Esercizio 4.4.7. Determinare tutti i naturali n, con $3 \leq n \leq 100$, per cui il poligono regolare $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C*.

Esercizio 4.4.8. Dimostrare il teorema delle bisettrici, utilizzando il teorema di Talete (come suggerito dalla figura che segue)



Capitolo 5

UN'INTRODUZIONE ALLA TEORIA DI GALOIS

1. Risolubilità per radicali

Dal corso di **Alg. 1** è noto il seguente semplice risultato, attribuito a Ruffini:

Sia $f \in K[X]$ *e sia* $\alpha \in L$ *(estensione di* K*).* α *è uno zero di* $f \iff X - \alpha \,|\, f$ *(in* $L[X]$*).*

Ne segue subito la seguente definizione:

uno zero α *di* f *ha molteplicità* $t \iff (X-\alpha)^t \,|\, f$ *e* $(X-\alpha)^{t+1} \nmid f$.

In particolare, uno zero di f è detto *semplice* se ha molteplicità 1 ed è detto *multiplo* se ha molteplicità ≥ 2. Vale infine (e si dimostra per induzione forte su ∂f) il seguente risultato (per il quale rinviamo ad [AA], Prop. **4** di Cap. **3.2**):

Sia $f \in K[X]$, *con* $\partial f = n \geq 0$. *In ogni estensione* L *di* K, f *ammette al più* n *zeri, contando ciascuno di essi un numero di volte pari alla sua molteplicità.*

Ci poniamo preliminarmente due domande relative ad un polinomio $f \in K[X]$, con $\partial f = n \geq 1$:

(**A**) *Esiste un'estensione finita* L *di* K, *in cui* f *ammette esattamente* n *zeri, contati con la rispettiva molteplicità, cioè in cui* f *si fattorizza "linearmente" (ovvero con fattori tutti di grado* 1*) ?*

Vedremo nel prossimo paragrafo **2** che la risposta a tale domanda è positiva. Saremo in particolare interessati ad ottenere un'estensione "minimale" rispetto a tale proprietà, cioè a verificare l'esistenza (e l'unicità) del cosiddetto *campo di spezzamento di* f *su* K, che nel seguito denoteremo $\Sigma_{f,K}$. Si tratta della più piccola estensione di K contenente tutti gli zeri di f. Se tali zeri sono noti e sono $\alpha_1, \ldots, \alpha_n$, allora $\Sigma_{f,K} = K(\alpha_1, \ldots, \alpha_n)$.

(**B**) *Se* f *è irriducibile, i suoi zeri (contenuti in un'opportuna estensione di* K*) sono tutti semplici [cioè di molteplicità* 1*] ?*

Ci occuperemo di questa questione nel prossimo paragrafo **3**. Diciamo però già sin da ora che la risposta è affermativa se $car(K) = 0$ [e di tale fatto ci siamo già serviti nella dimostrazione del Teor. **4.1** del Cap. **4**]. Se invece $car(K) = p > 0$, esistono polinomi irriducibili con zeri multipli. Questo fatto motiva la definizione di *polinomio separabile*, cioè polinomio i cui fattori irriducibili hanno tutti zeri semplici. In $\boldsymbol{Q}[X]$ tutti i polinomi sono ovviamente separabili.

Veniamo ora al problema centrale dell'Algebra classica: la *risolubilità per radicali* di un polinomio in una indeterminata.

Era già conosciuta dai matematici dell'antica Grecia la ben nota formula per il calcolo degli zeri di un "generico" polinomio di grado 2. Intuitivamente "generico" significa che i coefficienti del polinomio sono di natura "simbolica", ad esempio esprimibili con lettere, e privi di legami algebrici.

Ai matematici italiani del Rinascimento (Cardano, Tartaglia, Ferrari ed altri) si devono analoghe formule per i polinomi di gradi 3 e 4 [cfr. ad esempio [AA], Appendice Cap. **3**]. Tutte queste formule forniscono gli zeri del generico polinomio f (di grado ≤ 4) in funzione dei coefficienti di f e di espressioni radicali da essi ottenute: sono perciò chiamate *formule risolutive per radicali*.

Fino agli inizi del 1800 era ancora in piedi il problema di stabilire se esistessero formule risolutive per radicali di polinomi generici di grado ≥ 5 o se viceversa esistesse qualche polinomio di $\boldsymbol{Q}[X]$ non risolubile per radicali. Una prima risposta (parziale) fu data da Ruffini (nel 1813) ed una risposta completa da Abel (nel 1824). Si tratta del celebre *teorema di Abel-Ruffini*:

Il generico polinomio di grado 5 *non è risolubile per radicali.*

Torneremo in conclusione di questo paragrafo a questo importante risultato [e formalizzeremo la nozione di "polinomio generico"]. Per il momento con le due definizioni che seguono precisiamo la definizione di "polinomio risolubile per radicali".

Definizione 1.1. *Sia* $car(K) = 0$ *e sia* $K \subseteq L$ *un'estensione finita. Tale estensione è detta radicale*

se esistono $\alpha_1, \dots, \alpha_t \in L$ *tali che* $L = K(\alpha_1, \dots, \alpha_t)$ *e, per opportuni* $n_1, \dots, n_t \in \boldsymbol{N}^*$, *risulti:*

$$\alpha_1^{n_1} \in K,\ \alpha_2^{n_2} \in K(\alpha_1),\ \alpha_3^{n_3} \in K(\alpha_1, \alpha_2),\ \dots, \alpha_t^{n_t} \in K(\alpha_1, \dots, \alpha_{t-1}).$$

$\{\alpha_1, \dots, \alpha_t\}$ *è detta sequenza radicale dell'estensione.*

Nota. In caratteristica p positiva, questa definizione andrebbe lievemente modificata, per rendere poi vero, anche in caratteristica p, il successivo Teor. **1.1**. Rinviamo per i dettagli a [Stewart], Ch.**15**.

Dunque un'estensione radicale di K è ottenuta aggiungendo a K una sequenza di radici n-sime (per valori differenti di n) di elementi appartenenti ai campi intermedi che vengono via via generati. Ad esempio il campo $L = \boldsymbol{Q}(\sqrt{2}, \sqrt{\sqrt{2} + \sqrt[3]{2}})$ è un'estensione radicale di $\boldsymbol{Q}$, con sequenza radicale ad esempio $\{\alpha_1 = \sqrt{2}, \alpha_2 = \sqrt[3]{2}, \alpha_3 = \sqrt{\sqrt{2} + \sqrt[3]{2}}\}$. Infatti risulta: $\alpha_1^2 = 2 \in \boldsymbol{Q}$, $\alpha_2^3 = 2 \in \boldsymbol{Q}(\alpha_1)$, $\alpha_3^2 = \alpha_1 + \alpha_2 \in \boldsymbol{Q}(\alpha_1, \alpha_2)$; inoltre si verifica subito che $L = \boldsymbol{Q}(\alpha_1, \alpha_2, \alpha_3)$.

Definizione 1.2. *Sia* $car(K) = 0$ *e sia* $f \in K[X]$. f *è detto risolubile per radicali se* <u>tutti</u> *i suoi zeri sono contenuti in un'estensione radicale* $K \subseteq L$ *[cioè se esiste un'estensione radicale* $K \subseteq L$ *tale che* $K \subseteq \Sigma_{f,K} \subseteq L$*].*

Nel 1832, prima di morire (in un duello, all'età di 20 anni), E. Galois lasciò un manoscritto (pubblicato postumo, nel 1846), in cui caratterizzava i polinomi $f \in K[X]$ (con $car(K) = 0$) risolubili per radicali, in termini di una proprietà [la "risolubilità"] del gruppo dei K-automorfismi di $\Sigma_{f,K}$ [detto "gruppo di Galois" di f]. Precisamente:

Teorema 1.1. *Sia* $car(K) = 0$ *e sia* $f \in K[X]$. *Risulta:*

$$f \text{ è risolubile per radicali} \iff \text{il gruppo di Galois di } f \text{ è risolubile.}$$

Per chiarire questo fondamentale risultato [dal quale si fa risalire la nascita dell'Algebra moderna] occorre innanzitutto dare la definizione di gruppo "risolubile".

Definizione 1.3. *Un gruppo* $(G, \cdot)$ *è detto risolubile se esiste una catena di suoi sottogruppi*

$$\{1\} = G_0 < G_1 < \dots < G_n = G,$$

tali che, $\forall\, i = 1, \dots, n$: *(i)* $G_{i-1} \lhd G_i$; *(ii)* $G_i/_{G_{i-1}}$ *è abeliano.*

Come si vede, la risolubilità di un gruppo è una proprietà inerente la struttura dei suoi sottogruppi. È altresì evidente che ogni gruppo abeliano è risolubile [con catena $\{1\} < G$]. Dei gruppi risolubili ci occuperemo nel paragrafo **4**, mentre dimostreremo il Teor. **1.1** nell'**Appendice 2** al presente capitolo.

Denotiamo con $G(\Sigma_{f,K}|K)$ o, più semplicemente, con $G(f|K)$ il gruppo di Galois di f su K, cioè, come già detto, il gruppo degli automorfismi di $\Sigma_{f,K}$ che fissano K (elemento per elemento). [Che tali automorfismi formino un gruppo lo verificheremo in seguito, nel paragrafo **5**].

Supponiamo che $f = \sum_{t=0}^{m} c_t X^t$ e che $\alpha_1, \dots, \alpha_n$ siano gli zeri a due a due distinti di f [e dunque $\Sigma_{f,K} = K(\alpha_1, \dots, \alpha_n)$]. Preso comunque $\varphi \in G(f|K)$, risulta:

$$f(\varphi(\alpha_i)) = \sum_{t=0}^{m} c_t \varphi(\alpha_i)^t = \varphi\big(\sum_{t=0}^{m} c_t \alpha_i^t\big) = \varphi(f(\alpha_i)) = \varphi(0) = 0.$$

Dunque anche $\varphi(\alpha_i)$ è uno zero di f. Tenuto conto che φ è iniettiva, φ induce quindi una permutazione σ_φ degli zeri $\alpha_1, \dots, \alpha_n$ di f. Abbiamo così costruito un'applicazione

$$G(f|K) \to \boldsymbol{S}_n \text{ tale che } \varphi \to \sigma_\varphi,\ \forall\, \varphi \in G(f|K).$$

Tale applicazione è un omomorfismo di gruppi [cioè $\sigma_{\varphi_1 \circ \varphi_2} = \sigma_{\varphi_1} \circ \sigma_{\varphi_2}$] ed è iniettiva [infatti $\Sigma_{f,K} = K(\alpha_1, \dots, \alpha_n)$ e quindi (cfr. Osserv. **3.1**, Cap. **4**) φ è completamente individuata dal comportamento sugli zeri $\alpha_1, \dots, \alpha_n$ di f, cioè da σ_φ]. Dunque il gruppo di Galois $G(f|K)$ è un sottogruppo di $\boldsymbol{S}_n$.

Nota. Da quanto precede si deduce che il gruppo di Galois $G = G(f|K)$ agisce sull'insieme $S := \{\alpha_1, \dots, \alpha_n\}$ degli zeri (a due a due distinti) di f con la seguente azione:

$$\omega : G \times S \to S \text{ tale che } \omega(\varphi, \alpha_i) = \varphi(\alpha_i), \ \forall\, \varphi \in G, \ \forall\, \alpha_i \in S.$$

Tale azione è fedele [essendo $\varphi \to \sigma_\varphi$ iniettiva].

Si noti che all'epoca di Galois il concetto di gruppo non era ancora noto [la prima definizione di gruppo "astratto" ed i primi risultati sui gruppi risalgono al 1870 circa, ad opera soprattutto di Cayley, Jordan e Kronecker]. Dunque i gruppi sono nati - con Galois - come *gruppi di permutazioni degli zeri di un polinomio*.

Allo scopo di generalizzare il Teor. **1.1** (ad esempio al caso di campi di caratteristica $p > 0$) e di facilitarne la dimostrazione, la definizione di gruppo di Galois è stata successivamente estesa al caso di estensioni qualunque [invece che a solo quelle di tipo $K \subseteq \Sigma_{f,K}$], definendo, per ogni estensione $K \subseteq L$, il gruppo di Galois $G(L|K)$ di tale estensione come il gruppo dei K-automorfismi di L.

Come vedremo nel successivo paragrafo **5**, esiste una naturale corrispondenza tra i sottogruppi di $G(L|K)$ ed i campi intermedi tra K ed L. Nell'ipotesi poi che l'estensione $K \subseteq L$ sia finita, normale e separabile [condizioni di cui tratteremo nei paragrafi **2** e **3** e che sono automaticamente verificate se $L = \Sigma_{f,K}$ e $car(K) = 0$] vale il *teorema fondamentale della teoria di Galois*, che stabilisce - tra l'altro - che la predetta corrispondenza è biunivoca. Ne segue che dalla conoscenza dei sottogruppi di $G(L|K)$ seguono informazioni sui campi intermedi (e viceversa).

Si noti che la conoscenza di tali campi intermedi agevola, nel caso in cui $L = \Sigma_{f,K}$, ad esempio la determinazione algebrica degli zeri di f. Se infatti $K \subseteq M \subseteq L$ ed f si fattorizza in $M[X]$ nella forma $f = gh$, per ottenere gli zeri di f basterà calcolare gli zeri di g ed h in $M[X]$ [ciò che è più semplice, perché tali polinomi hanno grado inferiore al grado di f].

Veniamo ora ad una più precisa formulazione del teorema di Abel-Ruffini. Per "polinomio generico", meglio detto *polinomio generale di grado n su K*, intendiamo il polinomio

$$f_n = X^n - a_1 X^{n-1} + a_2 X^{n-2} - \dots + (-1)^n a_n \in K(a_1, \dots, a_n)[X],$$

dove $a_1, \dots, a_n$ sono elementi trascendenti su K ed *algebricamente indipendenti su K* [nel senso che non esiste alcun polinomio $P \in K[X_1, \dots, X_n]$ tale che $P(a_1, \dots, a_n) = 0$].

Teorema 1.2. *(Abel-Ruffini) Se $car(K) = 0$ e $n \geq 5$, il polinomio generale f_n su K non è risolubile per radicali.*

Tale teorema può essere dimostrato (come conseguenza del Teor. **1.1**), provando due fatti:

(a) $G\big(f_n|K(a_1, \dots, a_n)\big) \cong \boldsymbol{S}_n$;

(b) il gruppo $\boldsymbol{S}_n$ non è risolubile, $\forall\, n \geq 5$.

Dimostreremo il punto (b) [nel paragrafo **4**], ma non il punto (a), per il quale è necessario addentrarsi più profondamente nello studio della teoria dei polinomi simmetrici (cfr. ad esempio [Machì] o [Stewart]).

Il teorema di Abel-Ruffini dimostra che non esiste una formula risolutiva generale per "risolvere per radicali" i polinomi di grado ≥ 5. Ciò non escluderebbe a priori che ogni singolo polinomio di grado ≥ 5, ad esempio in $\boldsymbol{Q}[X]$, possa essere risolubile per radicali. Ma non è così: concluderemo il paragrafo **5** dimostrando che siffatti polinomi esistono. Infatti proveremo che ad esempio il polinomio $f = X^5 - 6X + 3 \in \boldsymbol{Q}[X]$ [che è irriducibile in base al criterio di Eisenstein] è non risolubile per radicali. Il motivo di ciò sta nel fatto che si dimostra facilmente, studiando il grafico della funzione reale $Y = f(X)$ [con le tecniche di Calcolo **1**], che tale polinomio ammette esattamente tre zeri reali distinti (e quindi altri due complessi coniugati) e conseguentemente dimostrando un risultato "ad hoc" (cfr. Prop. **5.5**), che garantisce che in questo caso il gruppo di Galois di f è esattamente $\boldsymbol{S}_5$ (e dunque non è risolubile).

2. Campi di spezzamento ed estensioni normali

Sia K un campo e sia $f \in K[X]$, $\partial f \geq 1$. Poiché $K[X]$ è un *UFD*, f è prodotto (a meno di una costante moltiplicativa) di un numero finito di polinomi monici irriducibili in $K[X]$, cioè f si scrive nella forma

(*) $$f = c\, f_1^{r_1} \ldots f_t^{r_t},$$

con $c \in K^{\cdot}$, $r_i \geq 1$, $t \geq 1$ e $f_1, \ldots, f_t$ polinomi monici e irriducibili in $K[X]$, a due a due distinti. Tale espressione è unica (a meno dell'ordine dei fattori) ed è detta *fattorizzazione irriducibile di* f.

Definizione 2.1. *Sia $f \in K[X]$, $\partial f \geq 1$, con fattorizzazione irriducibile (*). Si dice che f si spezza (linearmente) su K se $\partial f_1 = \partial f_2 = \ldots = \partial f_t = 1$. In tal caso:*

$$f = c(X - \alpha_1)^{r_1} \ldots (X - \alpha_t)^{r_t},$$

dove $\alpha_1, \ldots, \alpha_t \in K$ sono gli zeri (a due a due distinti) di f.

Assegnata un'estensione di campi $K \subseteq L$, allora $K[X] \subseteq L[X]$. Ogni polinomio $f \in K[X]$ può quindi essere interpretato in $L[X]$. Se f non si spezza su K, potrebbe però spezzarsi su L. Anzi, come ora vedremo, esiste certamente un campo contenente K su cui f si spezza. Saremo poi interessati a costruire un'estensione minimale rispetto a tale proprietà. Si tratta del *campo di spezzamento di f su K*, che ora definiamo.

Definizione 2.2. *Sia $f \in K[X]$, $\partial f \geq 1$, e sia $K \subseteq E$ un'estensione di campi. E è detto campo di spezzamento di f su K se*

(i) f si spezza (linearmente) su E;

(ii) sia E' un campo tale che $K \subseteq E' \subseteq E$ ed f si spezza su E'. Allora $E' = E$.

Per indicare che E è un campo di spezzamento di f su K, useremo, come già fatto nel paragrafo precedente, la notazione $E = \Sigma_{f,K}$.

Se gli zeri di $f \in K[X]$ sono $\alpha_1, \ldots, \alpha_t$ (in un'opportuna estensione L di K), il problema di individuare il campo di spezzamento E di f su K si risolve molto semplicemente: infatti $K(\alpha_1, \ldots, \alpha_t)$ verifica le condizioni (i) e (ii) di Def. **2.2** e dunque $E = K(\alpha_1, \ldots, \alpha_t)$. Se invece gli zeri di f non sono noti, il problema è più complicato e si risolve, come ora vedremo, con successive estensioni algebriche semplici.

Proposizione 2.1. *Sia $f \in K[X]$, $\partial f \geq 1$.*

(i) Esiste un'estensione finita $K \subseteq L$ tale che f si spezza su L.

(ii) Esiste un campo di spezzamento E di f su K.

Dim. (i) Si procede per induzione su $n = \partial f$.

Se $\partial f = 1$, basta porre $L = K$.

Sia $n = \partial f > 1$. Se f si spezza su K, si pone ovviamente $L = K$. Altrimenti, f ammette un fattore irriducibile $f_1 \in K[X]$, con $\partial f_1 \geq 2$. Sia

$$K(x_1) = K[X]/_{(f_1)}$$

(estensione algebrica semplice di K). In $K(x_1)[X]$, f si fattorizza nella forma $f = (X - x_1)\, g$, con $g \in K(x_1)[X]$ e $\partial g = n - 1$. Al polinomio g si può applicare l'ipotesi induttiva: esiste un'estensione finita $K(x_1) \subseteq L$ tale che g si spezza su L. Ne segue che f si spezza su L e $K \subseteq L$ è finita.

(ii) In base a (i) esiste un campo $L \supseteq K$ tale che $f = c(X - \alpha_1)^{r_1} \ldots (X - \alpha_t)^{r_t}$ (in $L[X]$). Allora $E = K(\alpha_1, \ldots, \alpha_t)$ è un campo di spezzamento di f su K.

Ci dobbiamo ora chiedere se il campo di spezzamento è unico. Dalla Prop. **2.1**, una volta ottenuto

$K(x_1)$ si può scegliere un eventuale fattore irriducibile g_1 di g, di grado ≥ 2, e costruire il campo $K(x_1)(x_2) = K(x_1)[X]/_{(g_1)}$. Su tale campo f si fattorizza nella forma $f = (X - x_1)(X - x_2)\, h$, con $\partial h = n - 2$. Procedendo in modo analogo si ottiene in un numero finito di passi una fattorizzazione completa di f in $E = K(x_1)(x_2) \dots (x_s) = K(x_1, x_2, \dots, x_s)$, con $s \leq n$. Ma tale procedimento non sembra garantire a priori l'unicità del campo di spezzamento. Non è evidente infatti che, variando l'ordine di scelta dei successivi fattori irriducibili, si pervenga alla fine alla stessa estensione. Inoltre, visto che gli zeri di f possono non essere già noti e vanno in tal caso assunti esistenti solo "formalmente", l'unicità del campo di spezzamento non potrà che essere ottenuta a meno di K-isomorfismi. Vale infatti il seguente teorema.

Teorema 2.1. *Sia $f \in K[X]$. Se E ed E' sono campi di spezzamento di f su K, esiste un K-isomorfismo $\Phi : E \to E'$.*

Quando parleremo de **il** campo di spezzamento di un polinomio, intenderemo quindi che tale campo è stato scelto a meno di K-isomorfismi.

Il Teor. **2.1** verrà dimostrato in una forma più complessa (cfr. il successivo Teor. **2.1'**), che però si presta ad utilizzare un procedimento induttivo, che svilupperemo nel prossimo lemma.

Teorema 2.1'. *Sia $\varphi : K \to K'$ un isomorfismo di campi. Sia $f \in K[X]$, $\partial f \geq 1$, e sia $f' := \varphi'(f) \in K'[X]$ [si ricorda che $\varphi' : K[X] \to K'[X]$ è l'isomorfismo indotto da φ, cfr. Cap. **4**, § **2**]. Siano rispettivamente E ed E' campi di spezzamento di f su K e di f' su K'. Esiste un isomorfismo $\Psi : E \to E'$ tale che $\Psi_{|_K} = \varphi$. Inoltre $[E : K] = [E' : K']$.*

Il Teor. **2.1** segue subito dal Teor. **2.1'** ponendo $K' = K$ e $\varphi = \mathbf{1}_K$. Per dimostrare il Teor. **2.1'** facciamo uso del seguente lemma.

Lemma 2.1. *Sia $\varphi : K \to K'$ un isomorfismo di campi. Sia $f \in K[X]$, $\partial f \geq 1$. Sia E un campo di spezzamento di f su K e sia L' un'estensione di K' tale che $f' = \varphi'(f)$ si spezza su L'. Esiste un omomorfismo $\Psi : E \to L'$ tale che $\Psi_{|_K} = \varphi$.*

Dim. (Lemma **1**) Per induzione su $n = \partial f$.

Se $n = 1$, allora $E = K$. Basta quindi porre $\Psi = i \circ \varphi : K \to K' \hookrightarrow L'$ e Ψ verifica le condizioni richieste.

Sia $n > 1$. Supponiamo che $f = c(X - \alpha_1) \dots (X - \alpha_n) \in E[X]$ (con gli α_i non necessariamente distinti). L'elemento α_1 è algebrico su K e sia $f_1 \in K[X]$ il suo polinomio minimo su K. f_1 è un fattore monico irriducibile di f e quindi anche $f_1' := \varphi'(f_1)$ è un fattore monico irriducibile di $f' \in K'[X]$. Denotiamo con $\beta_1 \in L'$ uno zero di f_1'. Poiché f_1' è il polinomio minimo di β_1 su K', in base a Prop. **2.4** di Cap. **4**, esiste un isomorfismo

$$\Phi : K(\alpha_1) \to K'(\beta_1) \text{ tale che } \Phi(\alpha_1) = \beta_1 \text{ e } \Phi_{|_K} = \varphi.$$

In $K(\alpha_1)[X]$, f si fattorizza nella forma $f = (X - \alpha_1)\, g$, con $g \in K(\alpha_1)[X]$. Applicando ad f l'isomorfismo (indotto da Φ) $\Phi' : K(\alpha_1)[X] \to K'(\beta_1)[X]$, si ottiene

$$f' = \varphi'(f) = \Phi'(f) = (X - \beta_1)\, \Phi'(g)$$

[si osservi che $\Phi'(f) = \varphi'(f)$ in quanto $f \in K[X]$ e $\Phi_{|_K} = \varphi$]. Si ponga $g' := \Phi'(g)$. Si nota subito che g' si spezza su L [in quanto g' è un fattore di f' e $K'(\beta_1) \subseteq L'$]. Si ha:

$$\partial g = n - 1; \quad \Sigma_{g, K(\alpha_1)} = \Sigma_{f, K} = E; \quad g' \text{ si spezza su } L'.$$

È quindi possibile applicare a g l'ipotesi induttiva: esiste perciò un omomorfismo $\Psi : E \to L'$ tale che $\Psi_{|_{K(\alpha_1)}} = \Phi$. Ma allora $\Psi_{|_K} = \Psi_{|_{K(\alpha_1)}|_K} = \Phi_{|_K} = \varphi$. Dunque Ψ è l'omomorfismo cercato.

Dim. (Teor. **2.1'**) In base al precedente lemma, esiste un omomorfismo $\Psi : E \to E'$ tale che $\Psi_{|_K} = \varphi$. Bisogna soltanto dimostrare che Ψ è suriettivo, cioè che $\Psi(E) = E'$.

Poiché $K' \subseteq \Psi(E) \subseteq E'$ [infatti $K' = \varphi(K) = \Psi(K) \subseteq \Psi(E)$] in base alla condizione (*ii*) di Def. **2.2** è sufficiente verificare che f' si spezza sul campo $\Psi(E)$.

Ψ induce l'omomorfismo di anelli $\Psi' : E[X] \to E'[X]$, tale che $\Psi'_{|_{K[X]}} = \varphi'$. Se, in $E[X]$, risulta $f = c(X-\alpha_1)\dots(X-\alpha_n)$, allora $f' = \varphi'(f) = \Psi'(f) = \varphi(c)(X-\Psi(\alpha_1))\dots(X-\Psi(\alpha_n))$ e, ovviamente, tale polinomio appartiene a $\Psi(E)[X]$.

L'ultima affermazione è evidente: infatti una base di E su K si trasforma tramite Ψ in una base di E' su K'.

Osservazione 2.1. Se $f \in K[X]$ e L è un campo intermedio tra K e $\Sigma_{f,K}$, risulta: $\Sigma_{f,L} = \Sigma_{f,K}$.

Se infatti $\alpha_1, \dots, \alpha_t$ sono gli zeri di f, risulta $\Sigma_{f,K} = K(\alpha_1, \dots, \alpha_t)$ e $\Sigma_{f,L} = L(\alpha_1, \dots, \alpha_t)$. Poiché $K(\alpha_1, \dots, \alpha_t) \subseteq L(\alpha_1, \dots, \alpha_t) \subseteq \Sigma_{f,K}$, allora $\Sigma_{f,L} = \Sigma_{f,K}$.

Osservazione 2.2. Se E è il campo di spezzamento di f su K, l'estensione $K \subseteq E$ è ovviamente finita (in quanto algebrica e finitamente generata). Se poi $E = K(\alpha_1, \dots, \alpha_n)$ e $\partial f = n$, allora

$$[E : K] = [E : K(\alpha_1, \dots, \alpha_{n-1})]\cdot[K(\alpha_1, \dots, \alpha_{n-1}) : K(\alpha_1, \dots, \alpha_{n-2})]\cdot \dots \cdot[K(\alpha_1) : K] \leq n^n$$

[in quanto ogni estensione $K(\alpha_1, \dots, \alpha_{i-1}) \subseteq K(\alpha_1, \dots, \alpha_i)$ è algebrica semplice, di grado $\leq n$]. Ma tale diseguaglianza può essere molto migliorata, come ora dimostriamo.

Proposizione 2.2. *Sia $f \in K[X]$ un polinomio di grado $n \geq 1$ e sia E il suo campo di spezzamento su K. Se $f = f_1^{s_1} \dots f_r^{s_r}$, con $f_1, \dots, f_r \in K[X]$ componenti irriducibili (a due a due distinte) di f, posto $n_i = \partial f_i$, risulta:*

$$[E : K] \,\big|\, n_1!\; n_2! \dots n_r!.$$

Ne segue in particolare che $[E : K] \,\big|\, n!$.

Dim. Posto $F = f_1 \cdot \dots \cdot f_r$, ovviamente $\Sigma_{F,K} = E$. Possiamo quindi sostituire f con F, o meglio assumere che f abbia tutte componenti f_i di molteplicità $s_i = 1$.

L'ultima tesi del teorema segue subito dalla precedente. Infatti, essendo $n = \sum n_i$, risulta che $\prod n_i! \,\big|\, (\sum n_i)! = n!$ [si noti che, $\forall\, a, b \in \boldsymbol{N}$, $a!\, b! \,\big|\, (a+b)!$, in quanto $\frac{(a+b)!}{a!\, b!} = \binom{a+b}{a}$].

Per dimostrare la prima affermazione procediamo per induzione su n.

Se $n = 1$, allora $E = K$, f è irriducibile e $[E : K] = [K : K] = 1 \,\big|\, 1!$.

Sia $n > 1$ e sia α uno zero di f_1. In $K(\alpha)[X]$ sussiste la fattorizzazione $f_1 = (X - \alpha)g_1$. Se g_1 non è irriducibile, si fattorizza in $K(\alpha)[X]$ nel prodotto di fattori irriducibili

$$g_1 = g_{11} \dots g_{1s_1}, \quad \text{con } \partial g_{1j} = n_{1j} \quad \text{e} \quad \sum n_{1j} = \partial g_1 = n_1 - 1.$$

Analogamente, le altre componenti irriducibili $f_2, \dots, f_r$ si fattorizzano (eventualmente) in $K(\alpha)[X]$. Per $i = 2, \dots, r$, sia

$$f_i = g_{i1} \dots g_{is_i}, \quad \text{con } \partial g_{ij} = n_{ij} \quad \text{e} \quad \sum n_{ij} = \partial f_i = n_i.$$

Si noti che $\prod (n_{ij}!) \,\big|\, (\sum n_{ij})! = n_i!$. Posto

$$h := g_1 f_2 \dots f_r = g_{11} \dots g_{1s_1}\; g_{21} \dots g_{2s_2}\; \dots\dots\; g_{r1} \dots g_{rs_r},$$

si ha $\partial h = n-1$ e dunque ad h può applicarsi l'ipotesi induttiva. Si noti poi che $\Sigma_{h,K(\alpha)} = \Sigma_{f,K} = E$. Dunque (contando anche gli eventuali fattori g_{ij} ripetuti):

$$[E : K(\alpha)] \,\big|\, \prod (n_{1j}!)\; \prod (n_{2j}!) \dots \prod (n_{rj}!) \,\big|\, (\sum n_{1j})!\; (\sum n_{2j})! \dots (\sum (n_{rj})! = (n_1 - 1)!\; n_2! \dots n_r!.$$

Essendo poi $[K(\alpha) : K] = n_1$, allora

$$[E : K] = [E : K(\alpha)]\cdot[K(\alpha) : K] \,\big|\, n_1(n_1 - 1)!\; n_2! \dots n_r! = n_1!\; n_2! \dots n_r!.$$

Il Teor. **2.1** ha inoltre un importante corollario relativo alla struttura dei campi finiti.

Corollario 2.1. *Due campi finiti aventi la stessa cardinalità sono isomorfi.*

Dim. Siano K e $\tilde{K}$ due campi finiti, entrambi di cardinalità p^n (cfr. Prop. **1.1**, Cap. **4**). Tali campi hanno lo stesso sottocampo fondamentale $\boldsymbol{Z}_p$ (cfr. Cap. **4.3**). In base al Teor. **2.1**, basterà dimostrare che entrambi i campi sono campi di spezzamento del polinomio $f = X^{p^n} - X \in \boldsymbol{Z}_p[X]$.

Proviamo che ogni elemento $a \in K$ verifica la relazione $a^{p^n} = a$. Ciò è evidente se $a = 0$; sia invece $a \neq 0$. Poiché $a \in K^{\cdot}$ e $(K^{\cdot}, \cdot)$ è un gruppo di ordine $p^n - 1$, allora $a^{p^n - 1} = 1$ e quindi $a^{p^n} = a$. Abbiamo così provato che $f(a) = 0$, $\forall\, a \in K$. D'altra parte f ha grado p^n e quindi ha al più p^n zeri. Si conclude che $f = \prod_{a \in K} (X - a)$ e dunque K è un campo di spezzamento di f su $\boldsymbol{Z}_p$.

Le stesse considerazioni valgono anche per $\tilde{K}$. Dunque i due campi sono isomorfi.

Veniamo ora alla definizione di *estensione normale*. Esaminiamo l'estensione algebrica semplice

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2}).$$

Il polinomio minimo di $\sqrt[3]{2}$ su $\boldsymbol{Q}$ è ovviamente $f = X^3 - 2$. Tale polinomio non si spezza su $\boldsymbol{Q}(\sqrt[3]{2})$. Infatti, come ben noto, gli altri due suoi zeri sono $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$ [con $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ radice primitiva terza dell'unità]. Trattandosi di numeri complessi non reali, non appartengono a $\boldsymbol{Q}(\sqrt[3]{2})$ [che è invece contenuto in $\boldsymbol{R}$]. Dunque in tale estensione fallisce la seguente "buona" proprietà:

se $f \in K[X]$ è irriducibile ed ha uno zero in L (estensione di K), ha tutti gli zeri in L.

Diremo in tal caso che l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2})$ è non *normale*, in accordo con la seguente definizione.

Definizione 2.3. *Un'estensione di campi $K \subseteq L$ è detta estensione normale se ogni polinomio irriducibile $f \in K[X]$ con uno zero in L si spezza (linearmente) in L [cioè ha tutti gli zeri in L].*

Ogni estensione $K \subseteq \boldsymbol{C}$ è ovviamente normale (in base al Teorema Fondamentale dell'Algebra). Invece ad esempio le estensioni $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2})$ e $\boldsymbol{Q} \subset \boldsymbol{R}$ non sono normali.

Il seguente risultato collega i campi di spezzamento con le estensioni normali.

Teorema 2.2. *Sia $K \subseteq L$ un'estensione finita. Risulta*

$$K \subseteq L \text{ è normale } \iff L \text{ è campo di spezzamento di un polinomio in } K[X].$$

Dim. ($\Longrightarrow$). Essendo $K \subseteq L$ finita, allora $L = K(\alpha_1, \dots, \alpha_t)$, con $\alpha_1, \dots, \alpha_t$ algebrici su K. Denotiamo con m_i il polinomio minimo di α_i su K e poniamo $g = \prod_{i=1}^{t} m_i \in K[X]$. Ogni m_i ha uno zero in L (cioè α_i) ed, essendo $K \subseteq L$ normale, tutti i suoi zeri sono in L. Allora

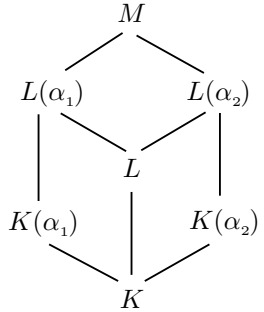
$$L = K(\alpha_1, \dots, \alpha_t) \subseteq K(\alpha_1, \dots, \alpha_2, \dots, \dots, , \alpha_t, \dots) = \Sigma_{g,K} \subseteq L,$$

cioè $L = \Sigma_{g,K}$.

($\Longleftarrow$). Sia $L = \Sigma_{g,K}$, con $g \in K[X]$. Si tratta di verificare che per ogni polinomio irriducibile $f \in K[X]$ risulta: f ha uno zero in $L \implies f$ ha ogni zero in L, ovvero:

$$\forall\, \alpha_1, \alpha_2 \text{ zeri di } f\text{: } \alpha_1 \in L \iff \alpha_2 \in L.$$

Si consideri il campo di spezzamento $M := \Sigma_{fg,K}$. Ovviamente $M \supseteq L$ e sussiste il seguente diagramma di inclusioni di campi:



Si noti che, essendo α_1, α_2 zeri di f (irriducibile su K), in base a a Prop. **2.3** di Cap. **4**, $K(\alpha_1) \cong K(\alpha_2)$. Ne segue:

$(\bullet)$ $\quad [K(\alpha_1) : K] = [K(\alpha_2) : K]$.

Essendo $L = \Sigma_{g,K}$, allora $L(\alpha_1) = \Sigma_{g,K(\alpha_1)}$ [infatti, se $L = K(\beta_1, \dots, \beta_t)$, con $\beta_1, \dots, \beta_t$ zeri di g, allora $\Sigma_{g,K(\alpha_1)} = K(\alpha_1)(\beta_1, \dots, \beta_t) = L(\alpha_1)$]. Analogamente, $L(\alpha_2) = \Sigma_{g,K(\alpha_2)}$.

In base al Teor. **2.1'**, da $K(\alpha_1) \cong K(\alpha_2)$ segue che $\Sigma_{g,K(\alpha_1)} \cong \Sigma_{g,K(\alpha_2)}$, cioè $L(\alpha_1) \cong L(\alpha_2)$ e quindi:

$(\bullet\bullet)$ $\quad [L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)]$.

Il teorema sarà dimostrato se proveremo che $[L(\alpha_1) : L] = 1 \iff [L(\alpha_2) : L] = 1$. Basterà quindi dimostrare che $[L(\alpha_1) : L] = [L(\alpha_2) : L]$.

Calcoliamo $[L(\alpha_1) : K]$ e $[L(\alpha_2) : K]$. Si ha, in base a $(\bullet)$ e $(\bullet\bullet)$:

$$[L(\alpha_1) : K] = [L(\alpha_1) : K(\alpha_1)]\cdot[K(\alpha_1) : K] = [L(\alpha_2) : K(\alpha_2)]\cdot[K(\alpha_2) : K] = [L(\alpha_2) : K].$$

Ne segue che

$$[L(\alpha_1) : L]\cdot[L : K] = [L(\alpha_1) : K] = [L(\alpha_2) : K] = [L(\alpha_2) : L]\cdot[L : K].$$

e pertanto, come richiesto, $[L(\alpha_1) : L] = [L(\alpha_2) : L]$.

Osservazione 2.3. Ogni estensione $K \subseteq L$ di grado 2 è normale.

Sia infatti $\alpha \in L - K$. Allora $L = K(\alpha)$ ed α ha polinomio minimo $m \in K[X]$ di grado 2. In $L[X]$ tale polinomio si fattorizza linearmente e dunque $L = \Sigma_{m,K}$. In base al teorema precedente $K \subseteq L$ è normale.

Osservazione 2.4. Sia $K \subseteq M \subseteq L$ una catena di estensioni finite. Se $K \subseteq L$ è normale, anche $M \subseteq L$ è normale [infatti, se $L = \Sigma_{f,K}$ (con $f \in K[X]$), da Osserv. **2.1** segue che $L = \Sigma_{f,M}$ e dunque $M \subseteq L$ è normale]. Invece $K \subseteq M$ può non essere normale [ad esempio, posto $f = X^3 - 2 \in \boldsymbol{Q}[X]$, si consideri la catena $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2}) \subset \Sigma_{f,\boldsymbol{Q}}$].

Se viceversa $K \subseteq M$ e $M \subseteq L$ sono normali, non è detto che $K \subseteq L$ sia normale. Ad esempio $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2})$ e $\boldsymbol{Q}(\sqrt{2}) \subset \boldsymbol{Q}(\sqrt{1+\sqrt{2}})$ sono estensioni normali (perché di grado 2), mentre $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{1+\sqrt{2}})$ non è normale. Infatti, posto $\alpha := \sqrt{1+\sqrt{2}}$, si osserva subito che α ha polinomio $f = X^4 - 2X^2 - 1 \in \boldsymbol{Q}[X]$ [si noti che $\alpha^2 - 1 = \sqrt{2}$; quadrando, $\alpha^4 - 2\alpha^2 - 1 = 0$]. Tale polinomio ha due zeri non reali [cioè $\pm\sqrt{1-\sqrt{2}} = \pm i\sqrt{\sqrt{2}-1}$] e quindi non appartenenti a $\boldsymbol{Q}(\sqrt{1+\sqrt{2}})$].

Se $K \subseteq L$ è finita ma non normale, esiste sempre, come ora vedremo, un'estensione normale $K \subseteq N$, con $N \supseteq L$. Esiste anzi un unico campo N "minimale" rispetto a tale proprietà: è la *chiusura normale di* $K \subseteq L$, che ora definiamo.

Definizione 2.4. *Sia $K \subseteq L$ un'estensione di campi. Si chiama chiusura normale di $K \subseteq L$ un campo N contenente L tale che:*

(i) l'estensione $K \subseteq N$ è normale;

(ii) sia N' un campo tale che $L \subseteq N' \subseteq N$ e l'estensione $K \subseteq N'$ è normale. Allora $N = N'$.

Teorema 2.3. *Sia $K \subseteq L$ un'estensione finita. Esiste una chiusura normale N di $K \subseteq L$, con $K \subseteq N$ finita. Tale chiusura normale è unica a meno di K-isomorfismi.*

Dim. Sia $L = K(\alpha_1, \dots, \alpha_t)$, con $\alpha_1, \dots, \alpha_t$ algebrici su K. Siano $m_1, \dots, m_t \in K[X]$ i rispettivi polinomi minimi e sia $f = \prod_{i=1}^{t} m_i \in K[X]$. Poniamo $N = \Sigma_{f,L}$: proveremo che N è una chiusura normale di $K \subseteq L$ e che $K \subseteq N$ è finita.

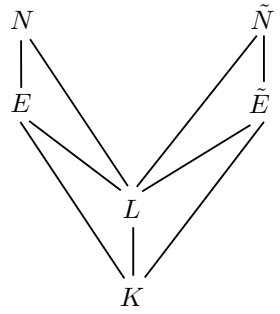
Si osserva subito che $N = \Sigma_{f,K}$. Infatti, denotati con $\alpha_i = \alpha_{i1}, \dots, \alpha_{in_i}$ gli zeri di m_i, allora

$$\Sigma_{f,K} = K(\alpha_1, \dots, \alpha_2, \dots, \dots, \alpha_t, \dots) = K(\alpha_1, \alpha_2, \dots, \alpha_t)(\alpha_{12}, \dots, \alpha_{tn_t}) = L(\dots) = \Sigma_{f,L} = N.$$

In base al Teor. **2.2**, $K \subseteq N$ è normale. Inoltre $K \subseteq N$ è ovviamente finita [è finitamente generata ed algebrica]. Resta da verificare soltanto la condizione (*ii*) di Def. **2.4**.

Sia N' un campo tale che $L \subseteq N' \subseteq N$ e $K \subseteq N'$ è normale. Ogni polinomio m_i ha uno zero in N' [in quanto lo ha in L] e perciò si spezza su N'. Ne segue che anche f si spezza su N'. Poiché $N = \Sigma_{f,K}$, allora $N \subseteq N'$ [per la minimalità del campo di spezzamento] e quindi $N = N'$.

Dimostriamo ora l'unicità (a meno di K-isomorfismi) della chiusura normale. Siano $N, \tilde{N}$ due chiusure normali di $K \subseteq L$ e sia $f = \prod_{i=1}^{t} m_i \in K[X]$, definito come sopra. f si fattorizza linearmente su N e su $\tilde{N}$. Dunque esistono $E, \tilde{E}$ campi di spezzamento di f su K tali che $N \supseteq E$ e $\tilde{N} \supseteq \tilde{E}$. Inoltre, per costruzione, $E \supseteq L$ e $\tilde{E} \supseteq L$.



Per la minimalità della chiusura normale, $N = E$ e $\tilde{N} = \tilde{E}$. Dal Teor. **2.1**, E, $\tilde{E}$ sono K-isomorfi. Ne segue che N e $\tilde{N}$ sono K-isomorfi.

La precedente dimostrazione fornisce il modo per ottenere la chiusura normale di un'estensione finita $K \subseteq L = K(\alpha_1, \dots, \alpha_t)$. Se infatti $f = \prod_{i=1}^{t} m_i$, allora $N = \Sigma_{f,K}$. Ad esempio, la chiusura normale dell'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2})$ è

$$N = \Sigma_{f,\boldsymbol{Q}} = \boldsymbol{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2) = \boldsymbol{Q}(\sqrt[3]{2},\ \zeta_3) = \boldsymbol{Q}(\sqrt[3]{2},\ i\sqrt{3}).$$

Faremo uso del concetto di *chiusura normale di un'estensione* nella dimostrazione del *TFA* (cfr. § **6**) e soprattutto nella dimostrazione del teorema fondamentale della teoria di Galois (cfr. § **5**), dimostrazione che è rinviata all'**Appendice 1**, al termine del presente capitolo. Anche il risultato che segue verrà utilizzato nella stessa appendice [cfr. dim Teor. **B**].

Proposizione 2.3. *Sia $K \subseteq L$ un'estensione finita e sia $x \in L$. Siano N ed N_1 rispettivamente la chiusura normale di $K \subseteq L$ e di $K(x) \subseteq L$. A meno di K-isomorfismi risulta che $N = N_1$.*

Dim. Se (con le notazioni precedenti) $L = K(\alpha_1, \dots, \alpha_t)$ e $f = \prod_{i=1}^{t} m_i \in K[X]$, allora $N = \Sigma_{f,L}$. Ma $L = K(x, \alpha_1, \dots, \alpha_t)$. Detto m il polinomio minimo di x su K e posto $f_1 = fm$, allora N_1 è K-isomorfo a $\Sigma_{f_1,L}$. D'altra parte $\Sigma_{f_1,L} \supseteq \Sigma_{f,L}$, cioè $N_1 \supseteq N$ (a meno di K-isomorfismi). Viceversa, siccome l'estensione $K(x) \subseteq N$ è normale (cfr. Osserv. **2.4**), per la minimalità di N_1 segue che $N_1 = N$.

Osservazione 2.5. In molti testi di teoria di Galois non si fa riferimento alle estensioni normali, ma si definiscono le *estensioni galoisiane*, cioè le estensioni finite $K \subseteq L$ tali che $[L : K] = G(L|K)|$. Nella parte conclusiva dell'**Appendice 1** proveremo che, in caratteristica 0 i due concetti sono equivalenti.

* * * * * * * * * * * * * * * * * *

Esercizio 5.2.1. Verificare che il campo di spezzamento E di $f = X^4 + 1 \in \boldsymbol{Q}[X]$ è $E = \boldsymbol{Q}(i, \sqrt{2})$.

Esercizio 5.2.2. Determinare il campo di spezzamento E di $f = X^6 - 8 \in \boldsymbol{Q}[X]$. Calcolare il grado $[E : \boldsymbol{Q}]$.

Esercizio 5.2.3. Determinare il campo di spezzamento del polinomio $f = X^3 + X^2 + X + \overline{2} \in \boldsymbol{Z}_3[X]$ e fattorizzare f in tale campo.

Esercizio 5.2.4. Determinare il campo di spezzamento E di $f = X^3 + \overline{5} \in \boldsymbol{Z}_7[X]$. Fattorizzare f in $E[X]$ e calcolare $[E : \boldsymbol{Z}_7]$.

Esercizio 5.2.5. Sia $f = X\,T^5 - X^2T^3 - \frac{1}{X^2}T^2 + \frac{1}{X} \in \boldsymbol{Z}_3(X)[T]$. Fattorizzare f e determinare il campo di spezzamento $\Sigma_{f,\boldsymbol{Z}_3(X)}$.

Esercizio 5.2.6. Determinare il campo di spezzamento del polinomio $f = X^8 + X^2 + \overline{1} \in \boldsymbol{Z}_2[X]$.

Esercizio 5.2.7. Determinare la chiusura normale N dell'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{3}, \sqrt[3]{2})$ e calcolare il grado di $\boldsymbol{Q} \subset N$.

Esercizio 5.2.8. Determinare (se esiste) la chiusura normale dell'estensione $\boldsymbol{Q} \subset \boldsymbol{R}$.

Esercizio 5.2.9. Dire perché l'estensione $\boldsymbol{Q}(X) \subset \boldsymbol{Q}(\sqrt[3]{X})$ è non normale e determinarne la chiusura normale.

Esercizio 5.2.10. Sia $K \subseteq L$ un'estensione finita e sia N la sua chiusura normale. Sia M un'estensione di N e sia $\varphi : L \to M$ un K-omomorfismo. Verificare che $Im\,\varphi \subseteq N$.

3. Separabilità

Nella dimostrazione del teorema dell'elemento primitivo (cfr. Teor. **3.1** di Cap. **4**) abbiamo utilizzato un risultato relativo al concetto di *separabilità*, che ora vogliamo dimostrare (cfr. il successivo Teor. **3.1**). Cominciamo con una definizione.

Definizione 3.1. *Un polinomio irriducibile in* $K[X]$ *è detto separabile se tutti i suoi zeri (in un'estensione di* K*) sono semplici ed un polinomio in* $K[X]$ *è detto separabile se tutte le sue componenti irriducibili sono polinomi separabili. Se inoltre* $K \subseteq L$ *è un'estensione di campi e* $\alpha \in L$ *è algebrico su* K*,* α *è detto separabile su* K *se il suo polinomio minimo in* $K[X]$ *è separabile. Infine un'estensione algebrica* $K \subseteq L$ *è detta separabile se ogni* $\alpha \in L$ *è separabile su* K*.*

Teorema 3.1. *Sia* $car(K) = 0$*. Ogni polinomio in* $K[X]$ *è separabile. Ne segue che ogni estensione algebrica* $K \subseteq L$ *è separabile.*

Per dimostrare tale teorema è necessario premettere (cfr. Prop. **3.1**) una caratterizzazione dei polinomi con zeri multipli. A tale scopo serve un'altra definizione.

Definizione 3.2. *Sia* $f \in K[X]$*,* $f = \sum_{i=0}^{n} a_i X^i$*. Si chiama derivata (formale) di* f *(o polinomio derivato di* f*) il polinomio* $Df = \sum_{i=1}^{n} i\, a_i X^{i-1} \in K[X]$*.*

Nota. In luogo di Df viene talvolta utilizzata la notazione $\frac{df}{dx}$.

Si noti che $\partial(Df) \leq \partial f - 1$. In particolare, se $car(K) = 0$ e $\partial f \geq 1$, allora $\partial(Df) = \partial f - 1$ [infatti $na_n \neq 0$, essendo $a_n \neq 0$]. Se invece $car(K) = p > 0$, la precedente diseguaglianza può essere stretta [ad esempio, se $f \in K[X^p]$, allora $Df = 0$].

Osservazione 3.1. (*i*) Se $K = \boldsymbol{R}$, Df coincide con l'usuale derivata di f [intesa come limite del rapporto incrementale]. La Def. **3.1** estende quindi la definizione di derivata di un polinomio ad ogni campo K, usando la regola di calcolo della derivata di un polinomio in $\boldsymbol{R}[X]$.

(*ii*) L'applicazione di derivazione formale $D : K[X] \to K[X]$ verifica le ben note proprietà delle derivate:

(*a*) $D(f+g) = Df + Dg, \ \forall\, f, g \in K[X]$; (*b*) $D(fg) = fDg + gDf, \ \forall\, f, g \in K[X]$;

(*c*) $D(c) = 0, \ \forall\, c \in K$; (*d*) $D(cf) = cDf, \ \forall\, c \in K, \ \forall\, f \in K[X]$.

Di queste quattro proprietà, soltanto la verifica di (*b*) [nota come *regola di Leibnitz*] richiede qualche calcolo (cfr. [AA], Esercizio **3.7**).

Lemma 3.1. *Sia* $f \in K[X]$ *e sia* α *uno zero di* f *(in un'opportuna estensione* L *di* K*). Risulta:*

$$\alpha \text{ è uno zero multiplo di } f \iff (Df)(\alpha) = 0.$$

Dim. ($\Longrightarrow$). Sia $f = (X-\alpha)^2 g$ (in $L[X]$). Allora $Df = 2(X-\alpha)\, g + (X-\alpha)^2 Dg$ e pertanto $(Df)(\alpha) = 0 + 0 = 0$.

($\Longleftarrow$). Sia $f = (X-\alpha)\, h$ (in $L[X]$) e sia $(Df)(\alpha) = 0$. Si ha: $Df = (X-\alpha)\, Dh + h$ e quindi $0 = (Df)(\alpha) = h(\alpha)$. Allora $X - \alpha \,|\, h$ (in $L[X]$), cioè $h = (X-\alpha)\, h_1, \ \exists\, h_1 \in L[X]$. Pertanto $f = (X-\alpha)^2 h_1$, cioè α è uno zero multiplo di f.

Proposizione 3.1. *Sia* $f \in K[X]$*.* f *ha uno zero multiplo* $\iff$ f, Df *hanno un fattore comune non costante in* $K[X]$*.*

Dim. ($\Longrightarrow$). Sia α uno zero multiplo di f. Dal Lemma **3.1**, $f(\alpha) = (Df)(\alpha) = 0$. Detto m il polinomio minimo di α su K, allora $m \,|\, f$ e $m \,|\, Df$. Dunque m è un fattore non costante cercato.

($\Longleftarrow$). Sia $g \in K[X]$ un fattore comune non costante di f e Df. Sia α uno zero di g (in un'estensione L di K). In $L[X]$, $X - \alpha \,|\, Df$ e $X - \alpha \,|\, f$. Ne segue che $f(\alpha) = 0$ e $Df(\alpha) = 0$. Dal Lemma **3.1** segue che α è uno zero multiplo di f.

Possiamo così dimostrare il Teorema **3.1**.

Dim. (Teor. **3.1**) Sia $car(K) = 0$. Bisogna dimostrare che se $f \in K[X]$ è irriducibile, tutti i suoi zeri sono semplici.

Per assurdo, f abbia uno zero multiplo. Dalla Prop. **3.1**, f e Df hanno un fattore comune non costante g. Poiché f è irriducibile e $g \,|\, f$, allora $g = cf$ (con $c \in K^{\cdot}$) e quindi $\partial g = \partial f$. Ma $g \,|\, Df$ e quindi $\partial g \leq \partial Df = \partial f - 1$. Dunque $\partial f \leq \partial f - 1$: assurdo.

Relativamente alla caratteristica p, vale il seguente risultato, anch'esso conseguenza di Prop. **3.1**.

Teorema 3.2. *Sia $car(K) = p > 0$ e sia $f \in K[X]$ un polinomio irriducibile. Risulta:*

$$f \text{ è non separabile } \iff f \in K[X^p].$$

Dim. ($\Longrightarrow$). Sia $f = \sum_{i=0}^{n} a_i X^i$ non separabile, cioè dotato di almeno uno zero multiplo. Da Prop. **3.1**, f e Df hanno un fattore comune non costante g. Ma f è irriducibile e quindi $g = cf$ (con $c \in K^{\cdot}$). Dunque $f \,|\, Df$. Allora, per ragioni di grado, $Df = 0$ e pertanto $i\, a_i = 0$, per ogni $i = 1, \ldots, n$. Se quindi $i \not\equiv 0 \ (mod\ p)$, allora $a_i = 0$. Si conclude che $f \in K[X^p]$.

($\Longleftarrow$). Sia $f = \sum_{i=0}^{t} a_i X^{pi}$. Allora $Df = 0$ e pertanto f, Df hanno in comune un fattore non costante (cioè f). Dalla Prop. **3.1**, f ha uno zero multiplo.

Osservazione 3.2. Costruiamo ora un esempio esplicito di un polinomio irriducibile non separabile (in caratteristica $p > 0$).

Sia $K = \boldsymbol{Z}_p(X)$ il campo delle funzioni razionali su $\boldsymbol{Z}_p$ e sia $f = T^p - X \in K[T]$. Se proviamo che è irriducibile, allora è non separabile (in base a Teor. **3.2**). Ma si può dimostrare qualcosa in più e cioè che f ha un unico zero (di molteplicità p).

Cominciamo col provare quest'ultima affermazione. Siano α, β zeri di f (in un'opportuna estensione di K). Allora $\alpha^p = X = \beta^p$ e dunque $\alpha^p = \beta^p$. Poiché $car(K) = p$, allora $(\alpha - \beta)^p = \alpha^p - \beta^p = 0$. Dunque $\alpha - \beta = 0$, cioè $\alpha = \beta$.

Ora dimostriamo che f è irriducibile in $K[T]$. Per assurdo, sia $f = gh$, con $g, h \in K[T]$ e $\partial g, \partial h \geq 1$. Poiché in $\Sigma_{f,K}[T]$ risulta $f = (T - \alpha)^p$, allora $g = (T - \alpha)^s$, con $1 \leq s < p$. Si noti inoltre che $\alpha^p = X \in K$ e che anche $\alpha^s \in K$ [in quanto $\pm\alpha^s$ è il termine noto di g]. Poiché $MCD(s, p) = 1$, allora $1 = as + bp$, con $a, b \in \boldsymbol{Z}$. Ne segue

$$\alpha = \alpha^1 = (\alpha^s)^a \cdot (\alpha^p)^b \in K\,(= \boldsymbol{Z}_p(X)).$$

Dunque $\alpha = \frac{u(X)}{v(X)}$, con $u = u(X), v = v(X) \in \boldsymbol{Z}_p[X]$. Elevando tale uguaglianza alla p-sima potenza si ottiene $v^p\, \alpha^p = u^p$, cioè $v^p X = u^p$. Confrontando i gradi (in $\boldsymbol{Z}_p[X]$) si ottiene $p\,\partial v + 1 = p\,\partial u$ e quindi $p \,|\, 1$: assurdo.

Nota. L'esempio precedente è probabilmente il più semplice possibile. In effetti possiamo subito verificare che non esistono polinomi irriducibili non separabili in $\boldsymbol{Z}_p[X]$, $\forall p$ primo. Se infatti $f \in \boldsymbol{Z}_p[X]$ fosse irriducibile e non separabile, in base a Teor. **3.2** $f \in \boldsymbol{Z}_p[X^p]$ e quindi si avrebbe

$$f = \sum_{i=0}^{s} a_i X^{ip}.$$

Ma allora, tenuto conto che $a = a^p$, $\forall\, a \in \boldsymbol{Z}_p$, si avrebbe

$$f = \sum_{i=0}^{s} a_i^p X^{ip} = \sum_{i=0}^{s} (a_i X^i)^p = \Big(\sum_{i=0}^{s} a_i X^i\Big)^p$$

e dunque f non sarebbe irriducibile.

Da tale considerazione segue che ogni estensione algebrica $\boldsymbol{Z}_p \subseteq K$ è separabile (perché, $\forall\, \alpha \in K$, il polinomio minimo di α su $\boldsymbol{Z}_p$ è separabile).

Concludiamo con un semplice corollario del Lemma **3.1**.

Teorema 3.3. *Per ogni primo p ed ogni intero $n \geq 1$, esiste, a meno di isomorfismi, un unico campo di cardinalità p^n.*

Dim. L'unicità è già stata dimostrata (cfr. Coroll. **2.1**). Per dimostrare l'esistenza, si consideri il polinomio $f = X^{p^n} - X \in \boldsymbol{Z}_p[X]$ e sia $E = \Sigma_{f,\boldsymbol{Z}_p}$ un suo campo di spezzamento. Si osserva subito che ogni zero di f è semplice [infatti $Df = -\overline{1}$ e quindi, se $\alpha \in E$ è uno zero di f, $(Df)(\alpha) \neq \overline{0}$. Dal Lemma **3.1** segue che α è semplice]. Dunque f possiede (in E) p^n zeri distinti. Denotato con K l'insieme di tali zeri, basterà verificare che K è un sottocampo di E: dunque è il richiesto campo di cardinalità p^n.

Se infatti $\alpha, \beta \in K$, risulta: $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$ e quindi $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$, cioè $\alpha - \beta \in K$. Analogamente, se $\beta \neq \overline{0}$, $(\frac{\alpha}{\beta})^{p^n} = \frac{\alpha^{p^n}}{\beta^{p^n}} = \frac{\alpha}{\beta}$, cioè $\frac{\alpha}{\beta} \in K$.

Nota. Si osservi che, poiché $K \supseteq \boldsymbol{Z}_p$ ed E è generato su $\boldsymbol{Z}_p$ dagli zeri di f, allora $E = K$.

* * * * * * * * * * * * * * * * * * *

Esercizio 5.3.1. Sia $K \subseteq L$ un'estensione algebrica e separabile e sia M un campo intermedio (tra K ed L). Verificare che le estensioni $K \subseteq M$ e $M \subseteq L$ sono separabili.

Esercizio 5.3.2. Sia n un naturale positivo e sia d un suo divisore positivo. Per ogni primo p, verificare che ogni campo di cardinalità p^n contiene un unico campo di cardinalità p^d.

Esercizio 5.3.3. Verificare se un campo L di cardinalità 8 può ammettere un sottocampo K di cardinalità 4.

4. Gruppi risolubili

Ricordiamo (cfr. Def. **1.3**) che un gruppo *risolubile* è un gruppo $(G,\cdot)$ nel quale esiste una catena di sottogruppi

(*) $$\{1\} = G_0 < G_1 < \ldots < G_n = G,$$

tale che, $\forall\, i = 1, \ldots, n$: $G_{i-1} \triangleleft G_i$ e $G_i/_{G_{i-1}}$ è abeliano.

[Per brevità diremo che (*) è una *catena di risolubilità* di G].

Si osserva subito che ogni gruppo abeliano $(G,\cdot)$ è risolubile, con catena di risolubilità $\{1\} < G$. Risulta inoltre:

(**1**) Il gruppo $\boldsymbol{S}_3$ è risolubile, con catena di risolubilità $\{(1)\} < \boldsymbol{A}_3 < \boldsymbol{S}_3$.

(**2**) Il gruppo diedrale $\boldsymbol{D}_n$ è risolubile, $\forall\, n \geq 3$. Infatti, ricordato che

$$\boldsymbol{D}_n = \langle \varphi, \rho \mid \varphi^n = \rho^2 = 1,\ \rho\circ\varphi = \varphi^{n-1}\circ\rho\rangle,$$

$\boldsymbol{D}_n$ possiede la catena di risolubilità $\{1\} < \langle\varphi\rangle < \boldsymbol{D}_n$ [verificare].

(**3**) Il gruppo $\boldsymbol{S}_4$ è risolubile. Infatti ha catena di risolubilità

$$\{(1)\} < \boldsymbol{V} < \boldsymbol{A}_4 < \boldsymbol{S}_4,$$

con $\boldsymbol{V} = \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$ (gruppo di Klein). C'è soltanto da osservare che $\boldsymbol{V} \triangleleft \boldsymbol{A}_4$ (infatti $\boldsymbol{V}$ è l'unico sottogruppo del proprio ordine in $\boldsymbol{A}_4$).

(**4**) Ogni p-gruppo è risolubile. Infatti, se $|G| = p^n$, in base al Coroll. **4.1** di Cap. **2**, G possiede una catena di sottogruppi $\{1\} = H_0 < H_1 < \ldots < H_n = G$, tale che, $\forall\, i = 1, \ldots, n$, $H_{i-1} \triangleleft H_i$ e $H_i/_{H_{i-1}} \cong \boldsymbol{C}_p$ (abeliano).

(**5**) Ogni gruppo semplice non abeliano è non risolubile. Ricordiamo infatti (cfr. Osserv. **1.1**, Cap. **2**) che un gruppo semplice G è un gruppo privo di sottogruppi normali non banali. L'unica catena di risolubilità di G potrebbe essere $\{1\} < G$ [se $G/_{\{1\}}$ fosse abeliano]. Se quindi G è semplice non abeliano, allora non è risolubile.

Il risultato principale che vogliamo provare è il seguente.

Teorema 4.1. *Per ogni $n \geq 5$, il gruppo simmetrico $\boldsymbol{S}_n$ è non risolubile.*

Allo scopo serve il seguente risultato.

Proposizione 4.1. *Se G è risolubile e $H \leq G$, anche H è risolubile.*

Dim. Sia (*) una catena di risolubilità di G. Intersechiamola con H ed otteniamo la catena

(**) $$\{1\} \leq G_1 \cap H \leq \ldots \leq G_{n-1} \cap H \leq H.$$

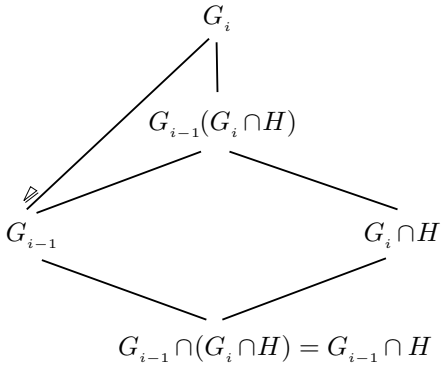
Vogliamo provare che (**) è una catena di risolubilità di H. Bisogna verificare che, $\forall\, i = 1, \ldots, n$:

$$(i)\ \ G_{i-1} \cap H \trianglelefteq G_i \cap H; \qquad\qquad (ii)\ \ G_i \cap H/_{G_{i-1}\cap H} \text{ è abeliano.}$$

La (i) è già stata dimostrata in Esercizio **1.4.2**. Per provare la (ii) basta osservare che $G_i/_{G_{i-1}}$ è abeliano e dimostrare che

$$G_i \cap H/_{G_{i-1}\cap H} \leq G_i/_{G_{i-1}}.$$

Applichiamo il secondo teorema di isomorfismo ai sottogruppi G_{i-1} e $G_i \cap H$ di G_i:



Si ottiene:

$$G_i \cap H \big/ _{G_{i-1} \cap H} \;\cong\; G_{i-1}(G_i \cap H) \big/ _{G_{i-1}} \;\leq\; G_i \big/ _{G_{i-1}} .$$

Osservazione 4.1. Sussistono altri due notevoli risultati sulla risolubilità, analoghi a quello di Prop. **4.1**. La dimostrazione verrà proposta come esercizio (cfr. Esercizio **5.4.3**).

(*i*) Se G è risolubile e $H \trianglelefteq G$, anche $G \big/ _H$ è risolubile.

(*ii*) Sia $H \trianglelefteq G$. Se H e $G \big/ _H$ sono risolubili, anche G è risolubile.

Per dimostrare il Teor. **4.1** basterà dimostrare che il gruppo alterno $\boldsymbol{A}_n$ è semplice, $\forall\, n \geq 5$. In tal caso, infatti, se $\boldsymbol{S}_n$ fosse risolubile, anche $\boldsymbol{A}_n$ lo sarebbe (in base a Prop. **4.1**). Ma $\boldsymbol{A}_n$ non è abeliano e quindi (in base a (**5**)) non è risolubile.

Sia $n \geq 3$. Del gruppo alterno $\boldsymbol{A}_n$ assumiamo noti i seguenti fatti:

(*a*) Se $n \geq 3$, $\boldsymbol{A}_n$ è generato dai 3-cicli (cfr. [AA], Osserv. **4**, pag. 155).

(*b*) Se $n \geq 4$, $\boldsymbol{A}_n$ non è abeliano [si verifichi che $(a\,b\,c)(a\,b\,d) \neq (a\,b\,d)(a\,b\,c)$].

Per provare che $\boldsymbol{A}_n$ è semplice, $\forall\, n \geq 5$, basta dimostrare che se $H \trianglelefteq \boldsymbol{A}_n$ e $H \neq \{(1)\}$, allora H contiene tutti i 3-cicli di $\boldsymbol{S}_n$ [e quindi, in base ad (*a*), $H = \boldsymbol{A}_n$]. Allo scopo è sufficiente dimostrare i due seguenti lemmi.

Lemma 4.1. *Sia $H \trianglelefteq \boldsymbol{A}_n$ e $H \neq \{(1)\}$. Se H contiene un 3-ciclo, li contiene tutti.*

Lemma 4.2. *Sia $H \trianglelefteq \boldsymbol{A}_n$ e $H \neq \{(1)\}$. Se $n \geq 5$, H contiene un 3-ciclo.*

Dim. (Lemma **4.1**). Assumiamo $n \geq 5$ [mentre i casi $n = 3, 4$ possono essere trattati a parte, cfr. Eserc. **5.4.1**]. Sia $(a_0\,b_0\,c_0) \in H$ e sia $(a\,b\,c)$ un arbitrario 3-ciclo di $\boldsymbol{S}_n$: bisogna dimostrare che $(a, b, c) \in H$.

I due 3-cicli $(a_0\,b_0\,c_0)$ e $(a\,b\,c)$ sono coniugati [infatti hanno la stessa struttura ciclica, cfr. [AA], Prop. **5**, pag. 156]. Dunque $\exists\, \sigma \in \boldsymbol{S}_n$ tale che $(a\,b\,c) = \sigma^{-1}(a_0\,b_0\,c_0)\,\sigma$.

Se $\sigma \in \boldsymbol{A}_n$, allora $(a\,b\,c) \in H$ [infatti, essendo $H \trianglelefteq \boldsymbol{A}_n$, allora $\sigma^{-1} H\, \sigma \subseteq H$]. Sia $\sigma \notin \boldsymbol{A}_n$. Poiché $n \geq 5$, esiste un 2-ciclo $(d\,e)$ disgiunto da $(a\,b\,c)$. Allora $\sigma_1 := \sigma\,(d\,e) \in \boldsymbol{A}_n$. Si ha:

$$\sigma_1{}^{-1}(a_0\,b_0\,c_0)\,\sigma_1 = (d\,e)\,\sigma^{-1}(a_0\,b_0\,c_0)\,\sigma\,(d\,e) = (d\,e)\,(a\,b\,c)\,(d\,e) = (d\,e)\,(d\,e)\,(a\,b\,c) = (a\,b\,c)$$

[infatti $(a\,b\,c)$, $(d\,e)$ commutano]. Come nel caso precedente, concludiamo quindi che $(a\,b\,c) \in H$.

Dim. (Lemma **4.2**). Scegliamo in H una permutazione $\sigma \neq (1)$. Poniamo $\sigma = \sigma_1 \ldots \sigma_n$ (prodotto di cicli disgiunti). A priori sono possibili le seguenti alternative:

(A) σ contiene un ciclo σ_1 di lunghezza $k \geq 4$;

(B) σ contiene due 3-cicli disgiunti σ_1, σ_2 ed eventualmente altri 2-cicli o 3-cicli;

(C) σ contiene un solo 3-ciclo σ_1 ed eventualmente altri 2-cicli;

(D) σ è prodotto di soli 2-cicli [almeno due, essendo σ di classe pari].

Dimostriamo che, a partire da ciascuno di tali casi, è possibile concludere che H possiede un 3-ciclo.

(A) Sia ad esempio $\sigma_1 = (1\,2\,3\,4\,...\,k)$ e consideriamo in $\boldsymbol{A}_n$ il 3-ciclo $\tau = (1\,2\,3)$. Poiché $H \trianglelefteq \boldsymbol{A}_n$, $\tau^{-1}\sigma\,\tau \in H$ e quindi anche $\tau^{-1}\sigma\,\tau\,\sigma^{-1} \in H$. Risulta:

$$\tau^{-1}\sigma\,\tau\,\sigma^{-1} = (1\,3\,2)(1\,2\,3\,4\,...\,k)\,\sigma_2\,...\,\sigma_n(1\,2\,3)\,\sigma_n^{-1}\,...\,\sigma_2^{-1}(1\,k\,...\,4\,3\,2).$$

Tenuto conto che $(1\,2\,3)$ commuta con $\sigma_2, \ldots, \sigma_n$ [in quanto disgiunto da essi], allora:

$$\tau^{-1}\sigma\,\tau\,\sigma^{-1} = (1\,3\,2)(1\,2\,3\,4\,...\,k)(1\,2\,3)(1\,k\,...\,4\,3\,2) = (1\,3\,k).$$

Dunque H contiene il 3-ciclo $(1\,3\,k)$.

(B) Si assuma ad esempio $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (4\,5\,6)$. Sia poi $\tau = (2\,3\,4) \in \boldsymbol{A}_n$. Come in (A), risulta $\tau^{-1}\sigma\,\tau\,\sigma^{-1} \in H$ e si ha:

$$\begin{aligned}\tau^{-1}\sigma\,\tau\,\sigma^{-1} &= (2\,4\,3)(1\,2\,3)(4\,5\,6)\,\sigma_3\,...\,\sigma_n(2\,3\,4)\,\sigma_n^{-1}\,...\,\sigma_3^{-1}(4\,6\,5)(1\,3\,2) = \\ &= (2\,4\,3)(1\,2\,3)(4\,5\,6)(2\,3\,4)(4\,6\,5)(1\,3\,2) = (1\,2\,4\,3\,6).\end{aligned}$$

Allora H contiene un 5-ciclo e si conclude utilizzando il caso (A).

Nota. Ovviamente il caso (B) si può presentare solo se $n \geq 6$.

(C) Si assuma ad esempio $\sigma_1 = (1\,2\,3)$. Tenuto conto che i cicli σ_i commutano tra loro, si ha:

$$\sigma^2 = \sigma\,\sigma = (1\,2\,3)\,\sigma_2\,...\,\sigma_n(1\,2\,3)\,\sigma_2\,...\,\sigma_n = (1\,2\,3)(1\,2\,3)\sigma_2^2\,...\,\sigma_n^2 = (1\,2\,3)(1\,2\,3) = (1\,3\,2) \in H.$$

Dunque H contiene il 3-ciclo $(1\,3\,2)$.

(D) Si assuma ad esempio $\sigma_1 = (1\,2)$, $\sigma_2 = (3\,4)$ e si scelga in $\boldsymbol{A}_n$ il 3-ciclo $\tau = (2\,3\,4)$. Allora $\rho := \tau^{-1}\sigma\,\tau\,\sigma^{-1} \in H$ e si ha:

$$\begin{aligned}\rho &= (2\,4\,3)(1\,2)(3\,4)\,\sigma_3\,...\,\sigma_n(2\,3\,4)\,\sigma_n^{-1}\,...\,\sigma_3^{-1}(3\,4)(1\,2) = \\ &= (2\,4\,3)(1\,2)(3\,4)(2\,3\,4)(3\,4)(1\,2) = (1\,4)(2\,3) \in H.\end{aligned}$$

Si consideri ora in $\boldsymbol{A}_n$ il 3-ciclo $\gamma = (1\,4\,5)$. Si ha: $\gamma^{-1}\rho\,\gamma\,\rho^{-1} \in H$ e risulta:

$$\gamma^{-1}\rho\,\gamma\,\rho^{-1} = (1\,5\,4)(1\,4)(2\,3)(1\,4\,5)(2\,3)(1\,4) = (1\,4\,5)(2)(3) = \gamma.$$

Si conclude che H contiene il 3-ciclo $\gamma = (1\,4\,5)$.

* * * * * * * * * * * * * * * * * * *

Esercizio 5.4.1. Dimostrare il Lemma **4.1** nei casi $n = 3$ e $n = 4$.

Esercizio 5.4.2. Dimostrare che, $\forall\, n \geq 2$ risulta: $\boldsymbol{S}_n = \langle (1\,2),\, (1\,2\,3\,...\,n) \rangle$.

Suggerimento. Si ponga $n \geq 3$, $\gamma = (1\,2)$, $\sigma = (1\,2\,3\,...\,n)$ e $H = \langle\, \gamma,\, \sigma\,\rangle$. Ricordato che ogni permutazione di $\boldsymbol{S}_n$ è prodotto di 2-cicli, verificare:

(a) $H \ni (t,\, t+1)$, $\forall\, t = 1,\, \ldots,\, n-1$;

(b) $H \ni (1\,t)$, $\forall\, t = 2,\, \ldots,\, n$;

(c) ogni $(h\,k)$ è prodotto di 2-cicli di tipo $(1\,t)$.

Esercizio 5.4.3. Dimostrare le affermazioni (i) e (ii) enunciate in Osserv **4.1**.

5. La corrispondenza di Galois

Assegnata un'estensione di campi $K \subseteq L$, abbiamo affermato nel paragrafo **1** che l'insieme dei K-automorfismi di L è un gruppo, detto *gruppo di Galois di L su K* e denotato $G(L|K)$. Verifichiamo ora che si tratta effettivamente di un gruppo.

Lemma 5.1. *$G(L|K)$ è un gruppo, rispetto al prodotto operatorio. Si tratta di un sottogruppo del gruppo $\boldsymbol{Aut}(L)$ degli automorfismi di L.*

Dim. Se $\varphi_1, \varphi_2 \in G(L|K)$, allora $\varphi_2 \circ \varphi_1 \in \boldsymbol{Aut}(L)$; inoltre $(\varphi_2 \circ \varphi_1)(c) = c, \ \forall\, c \in K$ e dunque $\varphi_2 \circ \varphi_1 \in G(L|K)$. Analogamente, se $\varphi \in G(L|K)$ allora $\varphi^{-1} \in \boldsymbol{Aut}(L)$ e $\varphi^{-1}(c) = \varphi^{-1}(\varphi(c)) = \mathbf{1}_L(c) = c, \ \forall\, c \in K$; dunque $\varphi^{-1} \in G(L|K)$. Infine ovviamente $\mathbf{1}_L \in G(L|K)$.

Osservazione 5.1. In letteratura sono presenti numerose altre notazioni per indicare il gruppo di Galois. Eccone alcune: $G(L,K)$, $Gal(L|K)$, $Gal(L,K)$, $\Gamma(L|K)$, $\Gamma(L:K)$.

Come già detto nel paragrafo **1**, Galois introdusse il gruppo di Galois limitatamente ad estensioni del tipo $K \subseteq \Sigma_{f,K}$ ed abbiamo già osservato, sempre nel paragrafo **1**, che il gruppo di Galois $G(\Sigma_{f,K}|K)$ [usualmente denotato $G(f|K)$] si identifica ad un sottogruppo del gruppo delle permutazioni $\boldsymbol{S}_t$, se t è il numero degli zeri distinti di f. Ma determinare tale sottogruppo è in generale molto complicato, soprattutto se non si conoscono gli zeri di f; ed ancora più dificile è determinare il gruppo di Galois di un'arbitraria estensione $K \subseteq L$.

Ci limiteremo ora a svolgere qualche considerazione elementare circa il gruppo di Galois di un'estensione semplice, sia trascendente che algebrica.

(A) Assegnata un'estensione trascendente semplice $K \subset K(X)$, si può dimostrare che

$$G(K(X)\,|K) \cong \boldsymbol{GL}_2(K)\big/_{K^\cdot},$$

dove $\boldsymbol{GL}_2(K)$ è il gruppo delle matrici invertibili di ordine 2 a valori in K, mentre $K^\cdot$ si identifica con il sottogruppo (normale in $\boldsymbol{GL}_2(K)$) delle matrici scalari invertibili di ordine 2 (cioè le matrici $cI_2, \ \forall\, c \in K^\cdot$). Tale gruppo quoziente è usualmente denotato $\boldsymbol{PGL}_2(K)$ ed è chiamato *gruppo generale lineare proiettivo di ordine 2 su K*.

Dimostrare che esiste l'isomorfismo sopra indicato non è banale e ci limiteremo solo a qualche accenno. Assegnata una matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{GL}_2(K)$, ad essa si può associare l'omomorfismo

$$\varphi_A : K(X) \to K(X) \ \text{ tale che } \ \varphi_A(X) = \tfrac{aX+b}{cX+d}$$

[e quindi $\varphi_A(\frac{u(X)}{v(X)}) = \frac{u(\varphi_A(X))}{v(\varphi_A(X))}, \ \forall\, \frac{u(X)}{v(X)} \in K(X)$]. Si verifica facilmente che $\varphi_{A^{-1}} = \varphi_A{}^{-1}$ e che $\varphi_{A\,|K} = \mathbf{1}_K$. Dunque è definito un omomorfismo

$$\Phi : \boldsymbol{GL}_2(K) \to G(K(X)\,|K) \ \text{ tale che } \ \Phi(A) = \varphi_A, \ \forall\, A \in \boldsymbol{GL}_2(K),$$

e si dimostra che tale omomorfismo è suriettivo ed ha nucleo $Ker\Phi = K^\cdot$.

(B) Sia ora $K \subseteq K(\alpha)$ un'estensione algebrica semplice. Denotiamo con $m \in K[X]$ il polinomio minimo di α su K e siano $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t$ tutti gli zeri a due a due distinti di m, contenuti in $K(\alpha)$. Ovviamente $K(\alpha_i) = K(\alpha), \ \forall\, i = 1, \ldots, t$. Verificheremo che $G(K(\alpha)\,|K)$ è un sottogruppo di ordine t di $\boldsymbol{S}_t$.

Infatti, in perfetta analogia a quanto avviene in $G(f|K)$, risulta, per ogni $\varphi \in G(K(\alpha)\,|K)$ e per ogni $i, \ 1 \le i \le t$:

$$m(\varphi(\alpha_i)) = \varphi(m(\alpha_i)) = \varphi(0) = 0.$$

Dunque $\varphi(\alpha_i)$ è uno zero di m e φ individua quindi la permutazione

$$\sigma_\varphi = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_t \\ \varphi(\alpha_1) & \varphi(\alpha_2) & \ldots & \varphi(\alpha_t) \end{pmatrix},$$

che è identificabile ad un elemento di $\boldsymbol{S}_t$. L'applicazione

$$\Phi : G(K(\alpha)\,|K) \to \boldsymbol{S}_t\,, \text{ tale che } \varphi \to \sigma_\varphi\,,\ \forall\, \varphi \in G(K(\alpha)|K),$$

è un omomorfismo di gruppi [infatti $\sigma_{\varphi_1}\circ\sigma_{\varphi_2}(\alpha_i) = \sigma_{\varphi_1\circ\varphi_2}(\alpha_i)$]. Inoltre Φ è iniettiva; infatti, se σ_φ è la permutazione identica di $\boldsymbol{S}_t$ allora $\varphi(\alpha) = \alpha$ e dunque, $\forall \sum c_i\alpha^i \in K(\alpha)$, risulta: $\varphi(\sum c_i\alpha^i) = \sum c_i\varphi(\alpha)^i = \sum c_i\alpha^i$, cioè $\varphi = \mathbf{1}$.

Si tratta ora di verificare che $|G(K(\alpha)\,|K)| = t$. Per ogni $\alpha_s \in \{\alpha = \alpha_1, \alpha_2, \dots, \alpha_t\}$, poniamo $\varphi_s(\alpha) = \alpha_s$. Poiché α, α_s hanno lo stesso polinomio minimo, in base alla Prop. **2.3** di Cap. **4** è ben definito il K-isomorfismo

$$\varphi_s : K(\alpha) \to K(\alpha_s) \text{ tale che } \varphi_s(\textstyle\sum c_i\alpha^i) = \sum c_i{\alpha_s}^i,\ \forall \sum c_i\alpha^i \in K(\alpha).$$

Essendo $K(\alpha) = K(\alpha_s)$, $\varphi_s \in G(K(\alpha)\,|K)$. Viceversa, per ogni $\varphi \in G(K(\alpha)\,|K)$, se $\varphi(\alpha) = \alpha_s$, allora $\varphi = \varphi_s$ e dunque $G(K(\alpha)\,|K) = \{\varphi_1, \dots, \varphi_t\}$.

Nota. Come già osservato nel paragrafo **1** a proposito di $G(f|K)$, anche il gruppo $G = G(L|K)$ agisce fedelmente sull'insieme $S = \{\alpha_1, \dots, \alpha_t\}$ [con azione $\omega : G\times S \to S$ tale che $\omega(\varphi, \alpha_i) = \varphi(\alpha_i)$]. Tale azione è anche transitiva: infatti, $\forall\, \alpha_i\,,\ \alpha_j \in S,\ \varphi_j\circ\varphi_i^{-1}(\alpha_i) = \alpha_j$.

Con l'aiuto delle considerazioni svolte, calcoliamo il gruppo di Galois di alcune estensioni algebriche semplici.

Esempio 5.1. $G(\boldsymbol{Q}(i)\,|\boldsymbol{Q}) \cong \boldsymbol{C}_2$.

Il polinomio minimo di i su $\boldsymbol{Q}$ è ovviamente $m = X^2 + 1 \in \boldsymbol{Q}[X]$. I due zeri di m sono $\pm i$, entrambi contenuti in $\boldsymbol{Q}(i)$. Allora $G(\boldsymbol{Q}(i)\,|\boldsymbol{Q}) = \{\mathbf{1}, \varphi\}$, con $\mathbf{1} = \mathbf{1}_{\boldsymbol{Q}(i)}$ e

$$\varphi : \boldsymbol{Q}(i) \to \boldsymbol{Q}(i) \text{ tale che } \varphi(i) = -i \text{ e quindi } \varphi(a + ib) = a - ib,\ \forall\, a + ib \in \boldsymbol{Q}(i),$$

[si tratta della restrizione a $\boldsymbol{Q}(i)$ dell'automorfismo di coniugio di $\boldsymbol{C}$]. Ovviamente $\varphi^2 = \mathbf{1}$ e pertanto $G(\boldsymbol{Q}(i)\,|\boldsymbol{Q}) = \langle\varphi\rangle \cong \boldsymbol{C}_2$.

Esempio 5.2. $G(\boldsymbol{Q}(\sqrt[3]{2})\,|\boldsymbol{Q}) = \{\mathbf{1}\}$.

Il polinomio minimo di $\sqrt[3]{2}$ su $\boldsymbol{Q}$ è $m = X^3 - 2 \in \boldsymbol{Q}[X]$. I suoi tre zeri (in $\boldsymbol{C}$) sono $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$ e $\sqrt[3]{2}\,\zeta_3^2$. Di essi, soltanto il primo è in $\boldsymbol{Q}(\sqrt[3]{2})$ [gli altri due non sono reali]. Pertanto $G(\boldsymbol{Q}(\sqrt[3]{2})|\boldsymbol{Q})$ è formato dalla sola identità $\mathbf{1} = \mathbf{1}_{\boldsymbol{Q}(\sqrt[3]{2})}$.

Esempio 5.3. $G(\boldsymbol{Q}(\sqrt{1+\sqrt{2}})\,|\boldsymbol{Q}) \cong \boldsymbol{C}_2$.

Posto $\alpha = \sqrt{1+\sqrt{2}}$, risulta subito che α è zero del polinomio $m = X^4 - 2X^2 - 1 \in \boldsymbol{Q}[X]$. Per verificare che m è il polinomio minimo di α su $\boldsymbol{Q}$, va verificato che è irriducibile su $\boldsymbol{Q}$ e ciò è lasciato al lettore [si confronti l'Osserv. **2.4**]. Il polinomio m ha soltanto due zeri in $\boldsymbol{Q}(\alpha)$: α e $-\alpha$. Gli altri due zeri di m sono complessi coniugati e si tratta di $\pm i\sqrt{\sqrt{2}-1}$. Segue che $G(\boldsymbol{Q}(\alpha)\,|\boldsymbol{Q}) = \{\mathbf{1}, \varphi\}$, con $\varphi : \boldsymbol{Q}(\alpha) \to \boldsymbol{Q}(\alpha)$ tale che $\varphi(\alpha) = -\alpha$ e dunque

$$\varphi(a + b\alpha + c\alpha^2 + d\alpha^3) = a - b\alpha + c\alpha^2 - d\alpha^3,\ \forall\, a, b, c, d \in \boldsymbol{Q}.$$

Pertanto $G(\boldsymbol{Q}(\alpha)\,|\boldsymbol{Q}) = \langle\varphi\rangle \cong \boldsymbol{C}_2$.

Osservazione 5.2. Cosa si può dire di $G(L|K)$, se $K \subseteq L$ è un'estensione finita non semplice (o almeno se non è presentata come tale)?

Se $L = K(\alpha_1, \dots, \alpha_t)$ e $m_1, \dots, m_t$ sono i polinomi minimi di $\alpha_1, \dots, \alpha_t$ su K, si può senz'altro affermare che, $\forall\, \varphi \in G(L|K)$, $\varphi(\alpha_i)$ varia tra gli zeri di m_i contenuti in L. Ne segue che $G(L|K)$ è un gruppo finito di permutazioni (cfr. Eserc. **5.5.1**). Ma resta ovviamente il problema di individuarlo.

Va comunque detto che, se $K \subseteq L$ è un'estensione finita, $|G(L|K)|$ è un divisore di $[L : K]$. Una dimostrazione di tale fatto è presentata nell'**Appendice 1** al termine di questo capitolo [cfr. *Nota*

in coda alla dimostrazione del Teor. **A**].

Ora vogliamo illustrare la corrispondenza di Galois, tra i campi intermedi dell'estensione $K \subseteq L$ ed i sottogruppi del suo gruppo di Galois $G(L|K)$.

Osserviamo che, per ogni campo intermedio M di $K \subseteq L$, è definito il gruppo di Galois $G(L|M)$. Si tratta di un sottogruppo di $G(L|K)$ [infatti ogni M-automorfismo di L è a fortiori un K-automorfismo di L].

Viceversa, assegnato un sottogruppo H di $G(L|K)$, vogliamo associargli un campo intermedio di $K \subseteq L$. Vale il seguente risultato.

Lemma 5.2. *Sia $K \subseteq L$ un'estensione di campi e sia H un sottogruppo di $G(L|K)$. L'insieme*

$$L^H = \{x \in L \,|\, \varphi(x) = x, \ \forall \varphi \in H\}$$

è un campo intermedio di $K \subseteq L$. Tale campo è detto campo fisso di H.

Dim. Siano $x, y \in L^H$. Si ha, $\forall \varphi \in H$:

$$\varphi(x-y) = \varphi(x) - \varphi(y) = x - y; \qquad \varphi(\tfrac{x}{y}) = \tfrac{\varphi(x)}{\varphi(y)} = \tfrac{x}{y} \ \ (\text{se } y \neq 0).$$

Dunque $L^H - L^H \subseteq L^H$ e $L^H (L^{H\cdot})^{-1} \subseteq L^H$. Pertanto L^H è un campo. Ovviamente $L^H \subseteq L$. D'altra parte, $\forall \varphi \in H$, φ è un K-automorfismo e dunque $\varphi(c) = c$, $\forall c \in K$. Pertanto $K \subseteq L^H$.

Se denotiamo con $\boldsymbol{\mathcal{G}}$ l'insieme dei sottogruppi di $G(L|K)$ e con $\boldsymbol{\mathcal{F}}$ l'insieme dei campi intermedi dell'estensione $K \subseteq L$, da quanto precede restano definite le due seguenti applicazioni che, per economia di scrittura, denoteremo rispettivamente con $\sharp$ (*diesis*) e $\flat$ (*bemolle*):

$\sharp : \boldsymbol{\mathcal{F}} \to \boldsymbol{\mathcal{G}}$ tale che $M \to M^\sharp := G(L|M)$, $\forall M \in \boldsymbol{\mathcal{F}}$;
$\flat : \boldsymbol{\mathcal{G}} \to \boldsymbol{\mathcal{F}}$ tale che $H \to H^\flat := L^H$, $\forall H \in \boldsymbol{\mathcal{G}}$.

È evidente che le due applicazioni $\sharp$, $\flat$ sono inverse l'una dell'altra se e solo se sono verificate le due condizioni:

$$(\bullet) \ \ M^{\sharp\flat} = M, \ \forall M \in \boldsymbol{\mathcal{F}}; \qquad (\bullet\bullet) \ \ H^{\flat\sharp} = H, \ \forall H \in \boldsymbol{\mathcal{G}}.$$

Dai precedenti esempi **5.2** e **5.3** ricaveremo che, in generale, le applicazioni $\sharp$ e $\flat$ non sono inverse tra loro. Ma lo sono se l'estensione $K \subseteq L$ è finita, normale e separabile: questo è il contenuto di parte del *teorema fondamentale della teoria di Galois*, che enunceremo nel seguito (cfr. Teor. **5.1**). Premettiamo alcuni semplici risultati sulle relazioni che sussistono tra le due applicazioni $\sharp$, $\flat$.

Proposizione 5.1. *Sia $K \subseteq L$ un'estensione di campi. Risulta:*

(i) Per ogni $M \in \boldsymbol{\mathcal{F}}$, $M^{\sharp\flat} \supseteq M$.

(ii) Per ogni $H \in \boldsymbol{\mathcal{G}}$, $H^{\flat\sharp} \geq H$.

Dim. (*i*) Risulta:

$$M^{\sharp\flat} = L^{G(L|M)} = \{x \in L \,|\, \varphi(x) = x, \ \forall \varphi \in G(L|M)\}.$$

Se $x \in M$ e $\varphi \in G(L|M)$, allora $\varphi(x) = x$ e dunque $x \in M^{\sharp\flat}$. Pertanto $M \subseteq M^{\sharp\flat}$.

(*ii*) Risulta:

$$H^{\flat\sharp} = G(L|L^H) = \{\, L^H\text{-automorfismi di } L\,\}.$$

Se $\varphi \in H$ e $x \in L^H$, allora $\varphi(x) = x$ e dunque $\varphi \in G(L|L^H)$. Pertanto $H \leq H^{\flat\sharp}$.

Proposizione 5.2. *Sia $K \subseteq L$ un'estensione di campi. Risulta:*

(i) Se $M_1, M_2 \in \boldsymbol{\mathcal{F}}$ e $M_1 \subseteq M_2$, allora $M_1^\sharp \geq M_2^\sharp$.

(ii) Se $H_1, H_2 \in \boldsymbol{\mathcal{G}}$ e $H_1 \leq H_2$, allora $H_1^\flat \supseteq H_2^\flat$.

Dim. (*i*) Sia $\varphi \in M_2^\sharp = G(L|M_2)$. φ è anche un M_1-automorfismo e dunque $\varphi \in M_1^\sharp$.

(*ii*) Sia $x \in H_2^{\flat} = L^{H_2}$. Per ogni $\varphi \in H_1$, $\varphi \in H_2$ e dunque $\varphi(x) = x$. Pertanto $x \in H_1^{\flat}$

Proposizione 5.3. *Sia $K \subseteq L$ un'estensione di campi. Risulta:*

(i) $M^{\sharp\flat\sharp} = M^{\sharp}$, $\forall\, M \in \boldsymbol{\mathcal{F}}$.

(ii) $H^{\flat\sharp\flat} = H^{\flat}$, $\forall\, H \in \boldsymbol{\mathcal{G}}$.

Dim. (*i*) Da Prop. **5.1***(i)*, $M \subseteq M^{\sharp\flat}$; da Prop. **5.2***(i)*, $M^{\sharp} \geq (M^{\sharp\flat})^{\sharp} = M^{\sharp\flat\sharp}$. Viceversa, da Prop. **5.1***(ii)*, $M^{\sharp} \leq (M^{\sharp})^{\flat\sharp} = M^{\sharp\flat\sharp}$.

(*ii*) Da Prop. **5.1***(ii)*, $H \leq H^{\flat\sharp}$; da Prop. **5.2***(ii)*, $H^{\flat} \supseteq (H^{\flat\sharp})^{\flat} = H^{\flat\sharp\flat}$. Viceversa, da Prop. **5.1***(i)*, $H^{\flat} \subseteq (H^{\flat})^{\sharp\flat} = H^{\flat\sharp\flat}$.

Proposizione 5.4. *Sia $K \subseteq L$ un'estensione di campi. Risulta:*

(i) $K^{\sharp} = G(L|K)$ *e* $L^{\sharp} = \{\mathbf{1}_L\}$.

(ii) $\{\mathbf{1}_L\}^{\flat} = L$ *e* $G(L|K)^{\flat} \supseteq K$.

Dim. (*i*) è ovvio.

(*ii*) Risulta: $\{\mathbf{1}_L\}^{\flat} = L^{\{\mathbf{1}_L\}} = \{x \in L \,|\, \mathbf{1}_L(x) = x\} = L$. L'inclusione $G(L|K)^{\flat} \supseteq K$ è semplicemente l'inclusione $K^{\sharp\flat} \supseteq K$ (cfr. Prop. **5.1**(*i*)).

Possiamo riassumere i risultati precedenti nei due seguenti diagrammi:

$$\begin{array}{ccc} L & \overset{\sharp}{\dashrightarrow} & \{\mathbf{1}_L\} \\ \cup & & \shortmid\wedge \\ M & \overset{\sharp}{\dashrightarrow} & M^{\sharp} \\ \cup & & \shortmid\wedge \\ K & \overset{\sharp}{\dashrightarrow} & G(L|K) \end{array} \qquad\qquad \begin{array}{ccc} & & K \\ & & \shortmid\cap \\ G(L|K) & \overset{\flat}{\dashrightarrow} & K^{\sharp\flat} \\ \vee\shortmid & & \shortmid\cap \\ H & \overset{\flat}{\dashrightarrow} & H^{\flat} \\ \vee\shortmid & & \shortmid\cap \\ \{\mathbf{1}_L\} & \overset{\flat}{\dashrightarrow} & L \end{array}$$

L'inclusione $K \subseteq K^{\sharp\flat}$ può essere stretta [nel qual caso le applicazioni $\sharp$ e $\flat$ non sono inverse tra loro]. Nell'Esempio **5.1**, $\boldsymbol{Q}^{\sharp\flat} = \boldsymbol{Q}$, in quanto

$$\boldsymbol{Q}^{\sharp\flat} = \boldsymbol{Q}(i)^{\langle\varphi\rangle} = \{a + ib \in \boldsymbol{Q}(i) \,\big|\, \varphi(a+ib) = a + ib\} = \{a + ib \in \boldsymbol{Q}(i) \,\big|\, a - ib = a + ib\} = \boldsymbol{Q}.$$

Invece, nell'Esempio **5.2** risulta $\boldsymbol{Q}^{\sharp\flat} \supset \boldsymbol{Q}$, in quanto $\boldsymbol{Q}^{\sharp\flat} = \{\mathbf{1}\}^{\flat} = \boldsymbol{Q}(\sqrt[3]{2})$. Anche nell'Esempio **5.3** risulta $\boldsymbol{Q}^{\sharp\flat} \supset \boldsymbol{Q}$. Infatti

$$\boldsymbol{Q}^{\sharp\flat} = \boldsymbol{Q}(\alpha)^{\langle\varphi\rangle} = \{x \in \boldsymbol{Q}(\alpha) \,\big|\, \varphi(x) = x\} = \{a + c\alpha^2,\ \forall\, a, c \in \boldsymbol{Q}\} = \boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\sqrt{2}).$$

Passiamo ora ad enunciare il *teorema fondamentale della teoria di Galois* [abbreviato *TFTG*, nel seguito]. Avvertiamo che la dimostrazione è piuttosto tecnica e l'abbiamo posta nell'**Appendice 1**, al termine di questo capitolo.

Teorema 5.1. *(TFTG) Se $K \subseteq L$ è un'estensione finita, normale e separabile, risulta:*

(i) $|\,G(L|K)\,| = [L : K]$;

(ii) Le applicazioni $\sharp$ e $\flat$ sono inverse l'una dell'altra [cioè valgono le due relazioni:

(•) $M^{\sharp\flat} = M$, $\forall\, M \in \boldsymbol{\mathcal{F}}$; *(••)* $H^{\flat\sharp} = H$, $\forall\, H \in \boldsymbol{\mathcal{G}}$*].*

(iii) Per ogni $M \in \boldsymbol{\mathcal{F}}$, $|G(L|M)| = [L : M]$ e $[M : K] = \frac{|\,G(L|K)\,|}{|\,G(L|M)\,|}$.

(iv) Sia $M \in \boldsymbol{\mathcal{F}}$. L'estensione $K \subseteq M$ è normale $\iff$ $G(L|M) \trianglelefteq G(L|K)$.

(v) Sia $M \in \boldsymbol{\mathcal{F}}$ e $K \subseteq M$ normale. Allora

$$G(M|K) \cong G(L|K)\big/_{G(L|M)}.$$

Osservazione 5.3. Nelle ipotesi del *TFTG*, segue subito da (*i*), (*ii*), (*iii*) che:

(iii') Per ogni $H \in \boldsymbol{\mathcal{G}}$, $[L : H^\flat] = |H|$ *e* $[H^\flat : K] = (G(L|K) : H)$ *[indice di* H *in* $G(L|K)$*].*

Infatti da (*iii*) e (*ii*): $[L : H^\flat] = |(G(L|H^\flat)| = |H^{\flat\sharp}| = |H|$ e da (*i*): $[H^\flat : K] = \frac{[L:K]}{[L:H^\flat]} = \frac{|G(L|K)|}{|H|} = (G(L|K) : H)$.

Il *TFTG* può essere utilizzato per costruire il reticolo dei campi intermedi di una data estensione finita, normale e separabile [di cui sia facile costruire il gruppo di Galois]. Procediamo con un esempio.

Esempio 5.4. Sia $f = X^4 - 2 \in \boldsymbol{Q}[X]$. Si tratta di un polinomio irriducibile su $\boldsymbol{Q}$ (dal criterio di Eisenstein). Posto $E = \Sigma_{f,\boldsymbol{Q}}$, l'estensione $\boldsymbol{Q} \subset E$ è finita, normale e separabile. Ne calcoleremo il gruppo di Galois e poi il reticolo dei campi intermedi.

Sia $\alpha = \sqrt[4]{2}$. In $E[X]$: $f = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha)$. Dunque

$$E = \boldsymbol{Q}(\alpha, -\alpha, i\alpha, -i\alpha) = \boldsymbol{Q}(\alpha, i).$$

Risulta:

$$[E : \boldsymbol{Q}] = [\boldsymbol{Q}(\alpha, i) : \boldsymbol{Q}(\alpha)]\,[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 2 \cdot 4 = 8$$

[infatti $X^2 + 1$ è il polinomio minimo di i su $\boldsymbol{Q}(\alpha)$]. Ogni $\boldsymbol{Q}$-automorfismo $\varphi \in G(E\,|\,\boldsymbol{Q})$ è completamente individuato da $\varphi(\alpha)$ e $\varphi(i)$, che vanno scelti tra gli zeri dei polinomi minimi di α ed i (rispettivamente). Dalla (*i*) del *TFTG* segue che $|G(E\,|\,\boldsymbol{Q})| = 8$ e quindi $\varphi(\alpha)$ può essere scelto arbitrariamente in $\{\alpha, -\alpha, i\alpha, -i\alpha\}$ e $\varphi(i)$ in $\{i, -i\}$.

Passiamo quindi a descrivere gli otto $\boldsymbol{Q}$-automorfismi di $G(E\,|\,\boldsymbol{Q})$. Se poniamo

$$\varphi : \begin{cases} \alpha \to i\alpha \\ i \to i, \end{cases} \qquad \rho : \begin{cases} \alpha \to \alpha \\ i \to -i, \end{cases}$$

da φ, ρ restano definiti:

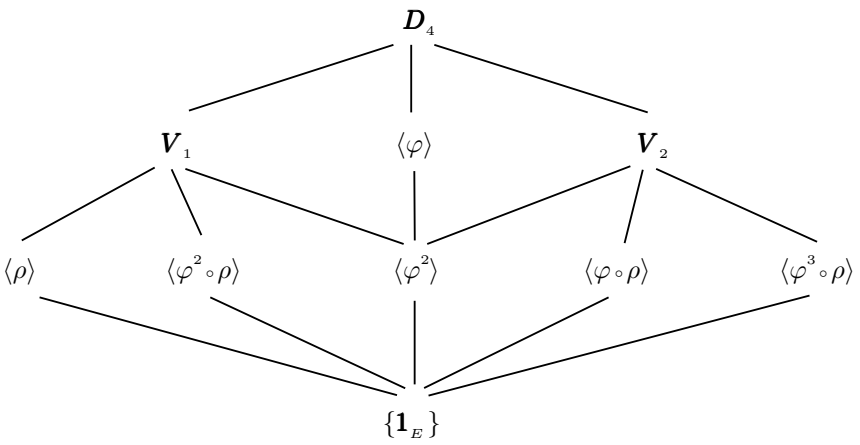
$$\varphi^2 : \begin{cases} \alpha \to -\alpha \\ i \to i, \end{cases} \qquad \varphi^3 : \begin{cases} \alpha \to -i\alpha \\ i \to i, \end{cases} \qquad \varphi^4 = \mathbf{1}_E, \qquad \rho^2 = \mathbf{1}_E,$$

$$\varphi\circ\rho : \begin{cases} \alpha \to i\alpha \\ i \to -i, \end{cases} \qquad \varphi^2\circ\rho : \begin{cases} \alpha \to -\alpha \\ i \to -i, \end{cases} \qquad \varphi^3\circ\rho : \begin{cases} \alpha \to -i\alpha \\ i \to -i. \end{cases}$$

Si osservi poi che $\rho\circ\varphi : \begin{cases} \alpha \to -i\alpha \\ i \to -i \end{cases}$ e dunque $\rho\circ\varphi = \varphi^3\circ\rho$. Si conclude che

$$G(E\,|\,\boldsymbol{Q}) = \langle\, \varphi, \rho \mid \varphi^4 = \rho^2 = 1,\ \rho\circ\varphi = \varphi^3\circ\rho \,\rangle \cong \boldsymbol{D}_4 \text{ (gruppo diedrale del quadrato).}$$

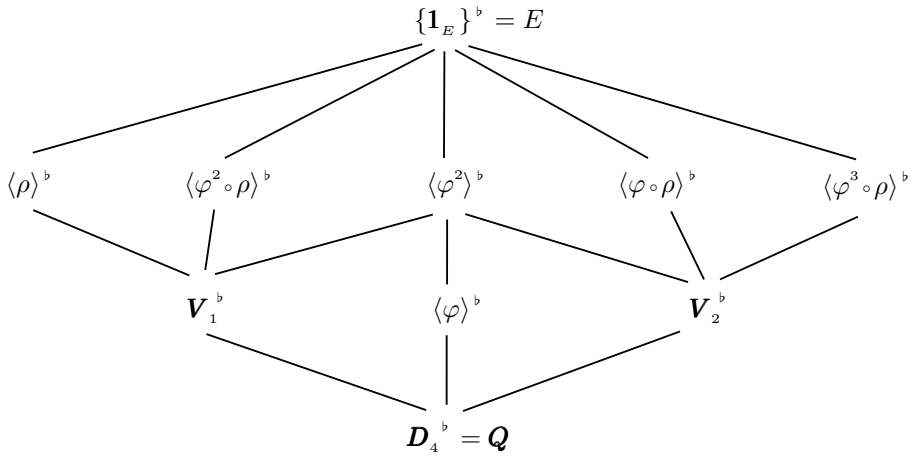
Dal corso di **Alg. 1** è ben noto il reticolo dei sottogruppi di $\boldsymbol{D}_4$:



con $\boldsymbol{V}_1 = \langle \varphi^2, \rho \rangle = \{\mathbf{1}_E, \varphi^2, \rho, \varphi^2\circ\rho\}$ e $\boldsymbol{V}_2 = \langle \varphi^2, \varphi\circ\rho \rangle = \{\mathbf{1}_E, \varphi^2, \varphi\circ\rho, \varphi^3\circ\rho\}$ (gruppi di Klein).

I tre sottogruppi di ordine 4 sono normali [in quanto hanno indice 2] mentre è noto che dei cinque sottogruppi di ordine 2 soltanto $\langle\varphi^2\rangle$ è normale.

Applichiamo ora la biiezione $\flat : \boldsymbol{\mathcal{G}} \to \boldsymbol{\mathcal{F}}$ e passiamo al corrispondente reticolo dei campi fissi, cioè dei campi intermedi dell'estensione $\boldsymbol{Q} \subset E$ [si noti che $\flat$ inverte le inclusioni, cfr. Prop. **5.2**].



Vogliamo presentare gli otto campi fissi intermedi come estensioni di $\boldsymbol{Q}$. Osserviamo preliminarmente che, in base all'Osserv. **5.3**, per ogni sottogruppo H di $\boldsymbol{D}_4$, risulta:

$$[H^\flat : \boldsymbol{Q}] = (G(E|\boldsymbol{Q}) : H) = (\boldsymbol{D}_4 : H) = \tfrac{8}{|H|}.$$

I campi $\langle\varphi\rangle^\flat$, $\boldsymbol{V}_1^\flat$ e $\boldsymbol{V}_2^\flat$ per la formula precedente sono tutte estensioni di grado 2 su $\boldsymbol{Q}$.

Relativamente a $\langle\varphi\rangle^\flat = \{x \in E \,|\, \varphi(x) = x\}$, poiché $\varphi(i) = i$, allora $i \in \langle\varphi\rangle^\flat$ e quindi $\langle\varphi\rangle^\flat = \boldsymbol{Q}(i)$.

Relativamente a $\boldsymbol{V}_1^\flat = \{x \in E \,|\, \varphi^2(x) = \rho(x) = x\}$, poiché

$$\varphi^2(\alpha^2) = (\varphi^2(\alpha))^2 = (-\alpha)^2 = \alpha^2, \qquad \rho(\alpha^2) = \alpha^2,$$

allora $\alpha^2 \in \boldsymbol{V}_1^\flat$ e dunque $\boldsymbol{V}_1^\flat = \boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\sqrt{2})$.

Relativamente a $\boldsymbol{V}_2^\flat = \{x \in E \,|\, \varphi^2(x) = (\varphi\circ\rho)(x) = x\}$, poiché

$$\varphi^2(i\alpha^2) = i\,\varphi^2(\alpha^2) = i\alpha^2, \quad (\varphi\circ\rho)(i\alpha^2) = \varphi(-i\,\alpha^2) = -i\,\varphi(\alpha)^2 = -i(i\,\alpha)^2 = i\,\alpha^2,$$

allora $i\,\alpha^2 \in \boldsymbol{V}_2^\flat$ e dunque (essendo $[\boldsymbol{V}_2^\flat : \boldsymbol{Q}] = 2$), allora $\boldsymbol{V}_2^\flat = \boldsymbol{Q}(i\,\alpha^2) = \boldsymbol{Q}(i\sqrt{2})$.

Veniamo ora ai campi $\langle\varphi^2\rangle^\flat$ e $\langle\rho\rangle^\flat$, entrambi estensioni di grado 4 su $\boldsymbol{Q}$.

Si ha: $\langle\varphi^2\rangle^\flat = \{x \in E \,|\, \varphi^2(x) = x\}$. Si osserva subito che φ^2 fissa i ed α^2. Dunque $i, \alpha^2 \in \langle\varphi^2\rangle^\flat$. Essendo $[\boldsymbol{Q}(\alpha^2, i) : \boldsymbol{Q}] = 4$, allora $\langle\varphi^2\rangle^\flat = \boldsymbol{Q}(\alpha^2, i) = \boldsymbol{Q}(\sqrt{2}, i)$.

Analogamente, $\langle\rho\rangle^\flat = \{x \in E \,|\, \rho(x) = x\}$. Ovviamente ρ fissa α. Dunque, essendo $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 4$, allora $\langle\rho\rangle^\flat = \boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\sqrt[4]{2})$.

Determinare gli ultimi tre campi fissi è meno immediato. Conviene esprimere il generico elemento $x \in E$ rispetto ad una $\boldsymbol{Q}$-base di E, ad esempio $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$, e tradurre rispetto a tale base la condizione che x sia fissato dal generatore del gruppo.

Calcoliamo $\langle\varphi^2\circ\rho\rangle^\flat$. Si ponga:

$$x = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\,i + a_5\,i\alpha + a_6\,i\alpha^2 + a_7\,i\alpha^3, \text{ con } a_0, \ldots, a_7 \in \boldsymbol{Q}.$$

Si ha:

$$(\varphi^2\circ\rho)(x) = a_0 - a_1\alpha + a_2\alpha^2 - a_3\alpha^3 - a_4\,i + a_5\,i\alpha - a_6\,i\alpha^2 + a_7\,i\alpha^3.$$

Imponendo la condizione $(\varphi^2\circ\rho)(x) = x$, si ottiene il sistema di equazioni lineari

$$\begin{cases} a_0 = a_0, \ a_1 = -a_1, \ a_2 = a_2, \ a_3 = -a_3, \\ a_4 = -a_4, \ a_5 = a_5, \ a_6 = -a_6, \ a_7 = a_7, \end{cases}$$

equivalente a $\{a_1 = a_3 = a_4 = a_6 = 0$. Pertanto

$$x \in \langle\varphi^2\circ\rho\rangle^\flat \iff x = a_0 + a_2\alpha^2 + a_5\,i\alpha + a_7\,i\alpha^3.$$

Quindi $\langle\varphi^2\circ\rho\rangle^\flat = \boldsymbol{Q}(1,\,\alpha^2,\,i\alpha,\,i\alpha^3) = \boldsymbol{Q}(\alpha^2,\,i\alpha)$. Ma $\alpha^2 = -(i\alpha)^2$ e quindi

$$\langle\varphi^2\circ\rho\rangle^\flat = \boldsymbol{Q}(i\alpha) = \boldsymbol{Q}(i\sqrt[4]{2}).$$

Procediamo in modo analogo per i campi $\langle\varphi\circ\rho\rangle^\flat$ e $\langle\varphi^3\circ\rho\rangle^\flat$.

Si ha:

$$(\varphi\circ\rho)(x) = a_0 + a_1\,i\alpha - a_2\alpha^2 - a_3\,i\alpha^3 - a_4\,i + a_5\alpha + a_6\,i\alpha^2 - a_7\,\alpha^3.$$

Dunque

$$(\varphi\circ\rho)(x) = x \iff \begin{cases} a_0 = a_0,\ a_1 = a_5,\ a_2 = -a_2,\ a_3 = -a_7\,, \\ a_4 = -a_4,\ a_5 = a_1,\ a_6 = a_6,\ a_7 = -a_3. \end{cases} \iff \begin{cases} a_2 = a_4 = 0 \\ a_7 = -a_3,\ a_5 = a_1. \end{cases}$$

Perciò

$$x \in \langle\varphi\circ\rho\rangle^\flat \iff x = a_0 + a_1(\alpha + i\alpha) + a_3(\alpha^3 - i\alpha^3) + a_6\,i\alpha^2$$

e quindi $\langle\varphi\circ\rho\rangle^\flat = \boldsymbol{Q}(1,\,\alpha + i\alpha,\,\alpha^3 - i\alpha^3,\,i\alpha^2)$. Ma $\alpha^3 - i\alpha^3 = -i\,\alpha^2(\alpha + i\alpha)$ e $i\,\alpha^2 = \frac{1}{2}(\alpha + i\alpha)^2$. Quindi

$$\langle\varphi\circ\rho\rangle^\flat = \boldsymbol{Q}(\alpha + i\alpha) = \boldsymbol{Q}((1+i)\sqrt[4]{2}).$$

Infine si ha:

$$(\varphi^3\circ\rho)(x) = a_0 - a_1\,i\alpha - a_2\alpha^2 + a_3\,i\alpha^3 - a_4\,i - a_5\alpha + a_6\,i\alpha^2 + a_7\,\alpha^3.$$

Pertanto

$$(\varphi^3\circ\rho)(x) = x \iff \begin{cases} a_0 = a_0,\ a_1 = -a_5,\ a_2 = -a_2,\ a_3 = a_7\,, \\ a_4 = -a_4,\ a_5 = -a_1,\ a_6 = a_6,\ a_7 = a_3. \end{cases} \iff \begin{cases} a_2 = a_4 = 0 \\ a_5 = -a_1,\ a_7 = a_3. \end{cases}$$

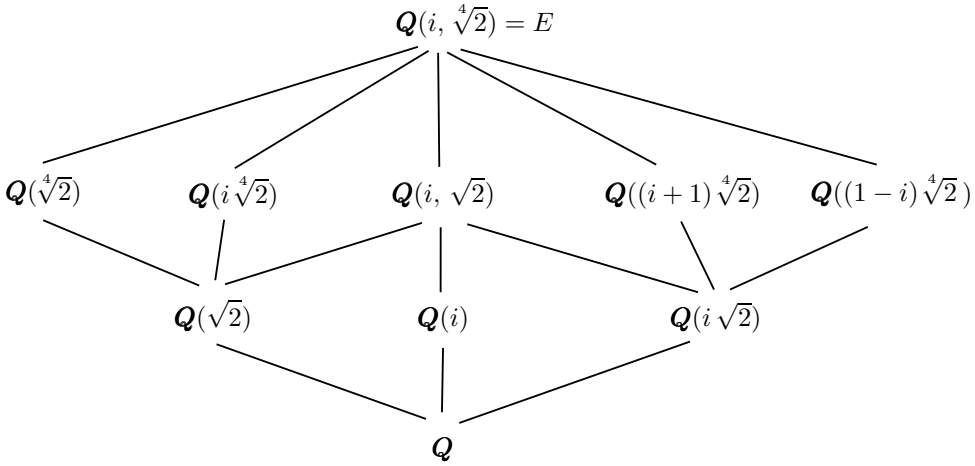
Dunque

$$x \in \langle\varphi^3\circ\rho\rangle^\flat \iff x = a_0 + a_1(\alpha - i\alpha) + a_3(\alpha^3 + i\alpha^3) + a_6\,i\alpha^2.$$

Come nel caso precedente, $\alpha^3 + i\alpha^3 = i\,\alpha^2(\alpha - i\alpha)$, $i\,\alpha^2 = -\frac{1}{2}(\alpha - i\alpha)^2$ e quindi

$$\langle\varphi^3\circ\rho\rangle^\flat = \boldsymbol{Q}(\alpha - i\alpha) = \boldsymbol{Q}((1-i)\sqrt[4]{2}).$$

Riassumendo, il reticolo dei campi intermedi è il seguente:



Nota. (*i*) I campi intermedi normali su $\boldsymbol{Q}$ sono quattro: $\boldsymbol{Q}(i,\,\sqrt{2})$, $\boldsymbol{Q}(\sqrt{2})$, $\boldsymbol{Q}(i)$ e $\boldsymbol{Q}(i\sqrt{2})$ [corrispondenti ai quattro sottogruppi normali propri di $\boldsymbol{D}_4$]. Sono campi di spezzamento rispettivamente dei seguenti polinomi: $(X^2+1)(X^2-2)$, X^2-2, X^2+1, $X^2+2 \in \boldsymbol{Q}[X]$.

(*ii*) Se $M \in \boldsymbol{\mathcal{F}}$ e $\boldsymbol{Q} \subseteq M$ è normale, il gruppo di Galois $G(M\,|\,\boldsymbol{Q})$ può essere facilmente calcolato dalla (*v*) del *TFTG*. Ad esempio, scelto $M = \langle\varphi^2\rangle^\flat = \boldsymbol{Q}(i,\,\sqrt{2})$, si ha:

$$G(\boldsymbol{Q}(i,\,\sqrt{2})\,|\,\boldsymbol{Q}) \cong G(E\,|\,\boldsymbol{Q})\big/_{G(E\,|\,\boldsymbol{Q}(i,\,\sqrt{2}))} \cong \boldsymbol{D}_4\big/_{\langle\varphi^2\rangle^{\flat\sharp}} \cong \boldsymbol{D}_4\big/_{\langle\varphi^2\rangle}.$$

Si tratta di un gruppo di Klein, come facilmente si verifica.

Usando il *TFTG* (ed un semplice risultato sulle funzioni simmetriche elementari) è possibile determinare - con un semplice calcolo aritmetico - il gruppo di Galois di un polinomio irriducibile di grado

3 in $\boldsymbol{Q}[X]$. È quanto vedremo nell'osservazione che segue.

Osservazione 5.4. Sia $f = X^3 + aX^2 + bX + c \in \boldsymbol{Q}[X]$ un polinomio monico irriducibile. Siano α, β, γ i suoi zeri, contenuti nel campo di spezzamento $\Sigma = \boldsymbol{Q}(\alpha, \beta, \gamma)$ [contenuto in $\boldsymbol{C}$]. In $\Sigma[X]$ risulta:

$$f = (X-\alpha)(X-\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\,...\,)X - \alpha\beta\gamma.$$

In particolare, $a = -(\alpha+\beta+\gamma)$ e dunque $\gamma \in \boldsymbol{Q}(\alpha, \beta)$. Pertanto $\Sigma = \boldsymbol{Q}(\alpha, \beta)$.

È poi noto che $G(f|\boldsymbol{Q})$ è isomorfo ad un sottogruppo di $\boldsymbol{S}_3$ e che $|G(f|\boldsymbol{Q})| = [\Sigma : \boldsymbol{Q}]$. Ne segue che $[\Sigma : \boldsymbol{Q}] \,\big|\, 6$. Poiché poi $[\Sigma : \boldsymbol{Q}] = [\Sigma : \boldsymbol{Q}(\alpha)] \cdot [\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = [\Sigma : \boldsymbol{Q}(\alpha)] \cdot 3$, allora $3 \,\big|\, [\Sigma : \boldsymbol{Q}]$. Ne segue che $[\Sigma : \boldsymbol{Q}] = 3$ oppure $= 6$. Pertanto

$$G(f|\boldsymbol{Q}) \cong \boldsymbol{S}_3 \text{ oppure } G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3 \text{ (gruppo alterno).}$$

Ovviamente $[\Sigma : \boldsymbol{Q}(\alpha)] = 1 \iff \beta \in \boldsymbol{Q}(\alpha)$ e quindi

$(*)$ $\qquad G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3 \iff \beta \in \boldsymbol{Q}(\alpha).$

Ma la condizione $\beta \in \boldsymbol{Q}(\alpha)$ non è facile da verificare [specialmente se gli zeri di f non sono noti!]. È quindi opportuno cercare un'altra caratterizzazione. Si consideri il numero complesso

$$\delta := (\beta-\alpha)(\gamma-\beta)(\gamma-\alpha).$$

Ovviamente $\delta \in \Sigma$ e $\delta \neq 0$ [infatti α, β, γ sono a due a due distinti]. Facciamo ora agire $\boldsymbol{S}_3$ su Σ [identificando α, β, γ risp. con $1, 2, 3$ e ponendo: $\omega(\sigma, P(\alpha,\beta,\gamma)) = P(\sigma(\alpha), \sigma(\beta), \sigma(\gamma))$, $\forall\, \sigma \in \boldsymbol{S}_3$, $\forall\, P(\alpha,\beta,\gamma) \in \Sigma$]. Risulta:

$$\begin{cases} \sigma(\delta) = \delta, \text{ se } \sigma \text{ è di classe pari;} \\ \sigma(\delta) = -\delta, \text{ se } \sigma \text{ è di classe dispari.} \end{cases}$$

Ad esempio, se $\sigma = (1\,2\,3)$, allora $\sigma(\delta) = (\gamma-\beta)(\alpha-\gamma)(\alpha-\beta) = \delta$. Se invece $\sigma = (1\,2)$, allora $\sigma(\delta) = (\alpha-\beta)(\gamma-\alpha)(\gamma-\beta) = -\delta$. In modo analogo si verificano gli altri casi.

Ricordato che $\boldsymbol{A}_3$ è il sottogruppo delle permutazioni di classe pari di $\boldsymbol{S}_3$, si ha:

$$G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3 \iff \delta \text{ è fissato da ogni automorfismo } \varphi \in G(f|\boldsymbol{Q}) \iff \delta \in G(f|\boldsymbol{Q})^\flat.$$

Poiché $G(f|\boldsymbol{Q})^\flat = \boldsymbol{Q}^{\sharp\flat} = \boldsymbol{Q}$, si ottiene:

$(**)$ $\qquad G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3 \iff \delta \in \boldsymbol{Q}.$

Osserviamo ora che, $\forall\, \sigma \in \boldsymbol{S}_3$, $\sigma(\delta^2) = \sigma(\delta)^2 = (\pm\delta)^2 = \delta^2$. Pertanto $\delta^2 \in G(f|\boldsymbol{Q})^\flat = \boldsymbol{Q}$, indipendentemente da quale sia il gruppo $G(f|\boldsymbol{Q})$ [se $\boldsymbol{S}_3$ oppure $\boldsymbol{A}_3$]. Il numero razionale δ^2 è detto *discriminante* di f ed è denotato con D. La caratterizzazione $(**)$ si trasforma quindi nella

$(***)$ $\qquad G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3 \iff \sqrt{D} \in \boldsymbol{Q}.$

Per rendere "operativa" tale caratterizzazione è necessario poter calcolare D senza conoscere gli zeri di f. A tal fine ci aiutano alcuni semplici risultati relativi alle funzioni simmetriche elementari [per i quali rinviamo ad esempio ad [Artin], Ch. **14** Sec. **3**]. Si perviene facilmente a questo risultato.

Assegnato un polinomio irriducibile $f \in \boldsymbol{Q}[X]$ di grado 3 e rappresentatolo nella sua "forma incompleta" $f = X^3 + pX + q$, risulta: $D = -4p^3 - 27q^2$.

Dunque D è aritmeticamente calcolabile a partire dai coefficienti di f e senza conoscerne gli zeri. Si ricorda (cfr. ad esempio [AA], pag. 135) che per ottenere la forma incompleta di f basta operare su f con la sostituzione lineare $X \to X - \frac{a}{3}$.

Nota. Si osservi che se f ha un unico zero reale α [e quindi due zeri complessi coniugati β, γ], necessariamente $\beta \notin \boldsymbol{Q}(\alpha)$ [infatti $\boldsymbol{Q}(\alpha) \subset \boldsymbol{R}$] e dunque $G(f|\boldsymbol{Q}) \cong \boldsymbol{S}_3$ in virtù di $(*)$. Si osservi che tale risultato è altresì ottenibile dalla successiva Prop. **5.5**.

Se invece f ha tre zeri reali, $G(f|\boldsymbol{Q})$ può essere isomorfo a $\boldsymbol{A}_3$ o $\boldsymbol{S}_3$, a seconda che $\sqrt{D}$ sia o meno razionale. Ad esempio $f = X^3 - 3X + 1$ è irriducibile su $\boldsymbol{Q}$, ha tre zeri reali e e risulta $D = 81 = 9^2$. Allora $G(f|\boldsymbol{Q}) \cong \boldsymbol{A}_3$. Invece, posto ad esempio $g = 4X^3 - 12X + 3$, si osserva che g è irriducibile su $\boldsymbol{Q}$, ha tre zeri reali e $D = \frac{1485}{16}$ non è un quadrato. Allora $G(g|\boldsymbol{Q}) \cong \boldsymbol{S}_3$.

Concludiamo il paragrafo dimostrando che esistono in $\boldsymbol{Q}[X]$ polinomi di grado ≥ 5 non risolubili per radicali. Tenuto conto di quanto già detto in conclusione del paragrafo **1**, è sufficiente dimostrare

il seguente risultato.

Proposizione 5.5. *Sia p un primo e sia $f \in \boldsymbol{Q}[X]$ un polinomio irriducibile di grado p. Se f ha esattamente $p-2$ zeri reali distinti [e quindi altri due zeri complessi coniugati], allora*

$$G(\Sigma_{f,\boldsymbol{Q}} \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_p$$

[e dunque, se $p \geq 5$, f non è risolubile per radicali].

Dim. Denotiamo con $\alpha, \overline{\alpha}, \alpha_3, \dots, \alpha_p$ gli zeri di f, assumendo i primi due complessi (e coniugati) e gli altri reali (distinti). Poiché

$$\Sigma_{f,\boldsymbol{Q}} = \boldsymbol{Q}(\alpha, \overline{\alpha}, \alpha_3, \dots, \alpha_p),$$

$G := G(\Sigma_{f,\boldsymbol{Q}} \,|\, \boldsymbol{Q})$ è isomorfo ad un sottogruppo di $\boldsymbol{S}_p$. Identifichiamo gli zeri $\alpha, \overline{\alpha}, \alpha_3, \dots, \alpha_p$ rispettivamente con i naturali $1, 2, 3, \dots, p$.

In base alla (i) del *TFTG*, $|\,G\,| = [\Sigma_{f,\boldsymbol{Q}} : \boldsymbol{Q}]$. Inoltre $[\Sigma_{f,\boldsymbol{Q}} : \boldsymbol{Q}] = [\Sigma_{f,\boldsymbol{Q}} : \boldsymbol{Q}(\alpha)] \cdot [\boldsymbol{Q}(\alpha) : \boldsymbol{Q}]$ e $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = p$. Ne segue che che $p \,\big|\, |G|$.

In base al teorema di Cauchy (cfr. Teor. **4.1**, Cap. **2**), G possiede un elemento di periodo p.

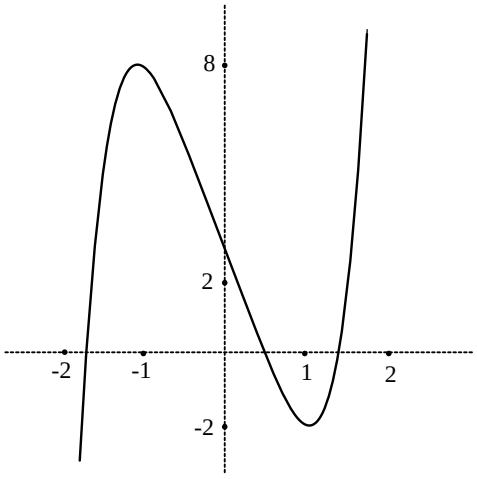
Osserviamo che in $\boldsymbol{S}_p$ i soli elementi di periodo p sono i p-cicli. Infatti, se $\circ(\sigma) = p$ e $\sigma = \sigma_1 \dots \sigma_h$ (prodotto di cicli disgiunti non banali), risulta $p = mcm(\circ(\sigma_1), \dots, \circ(\sigma_h))$ (cfr [AA], Prop. **2***(ii)*, pag. 152). Ne segue che $\circ(\sigma_i) = p$, $\forall\, i = 1, \dots, h$. Poiché i σ_i sono disgiunti, allora σ è prodotto di un unico p-ciclo.

Assumiamo dunque che G contenga il p-ciclo $\sigma = (c_1\, c_2 \dots c_p)$. Si può assumere, sostituendo eventualmente σ con una sua potenza, che risulti $\sigma = (1\, 2\, c_3 \dots c_p)$. Rinumerando eventualmente gli zeri reali di f, si può ulteriormente assumere che sia $\sigma = (1\, 2\, 3 \dots p)$. Dunque $(1\, 2\, 3 \dots p) \in G$.

Ora verifichiamo che anche $(1\, 2) \in G$. Ovviamente $\Sigma_{f,\boldsymbol{Q}} \subseteq \boldsymbol{C}$ e l'automorfismo di coniugio $^- : \boldsymbol{C} \to \boldsymbol{C}$ induce un automorfismo su $\Sigma_{f,\boldsymbol{Q}}$ [infatti $^-$ fissa $\boldsymbol{R}$ e scambia α con $\overline{\alpha}$]. Tale automorfismo corrisponde al 2-ciclo $(1\, 2)$. Pertanto $(1\, 2) \in G$.

In base all'Esercizio **5.4.2**, $\boldsymbol{S}_p = \langle (1\, 2), (1\, 2\, 3 \dots p) \rangle$. Dunque $G = \boldsymbol{S}_p$, come richiesto.

Un esempio di polinomio di grado $p = 5$ in $\boldsymbol{Q}[X]$, verificante le condizioni della proposizione precedente, è il polinomio $f = X^5 - 6X + 3$, il cui grafico ha un andamento come riportato in figura.



* * * * * * * * * * * * * * * * * * *

Esercizio 5.5.1. Se $K \subseteq L$ è un'estensione finita, verificare che $G(L|K)$ è un gruppo finito.

Esercizio 5.5.2. Sia $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, $n \geq 1$. Verificare che $G(\boldsymbol{Q}(\zeta_n) \,|\, \boldsymbol{Q})$ è abeliano e ha ordine $\varphi(n)$.

Esercizio 5.5.3. Posto $f = X^3 - 2 \in \boldsymbol{Q}[X]$, calcolare $G(\Sigma_{f,\,Q} \,|\, \boldsymbol{Q})$ e determinare i campi intermedi

dell'estensione $\boldsymbol{Q} \subset \Sigma_{f,\,Q}$.

Esercizio 5.5.4. Sia N la chiusura normale dell'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{1+\sqrt{2}})$.

(*i*) Determinare il gruppo di Galois $G(N \,|\, \boldsymbol{Q})$.

(*ii*) Verificare che l'unico campo intermedio tra $\boldsymbol{Q}$ e $\boldsymbol{Q}(\sqrt{1+\sqrt{2}})$ è il campo $\boldsymbol{Q}(\sqrt{2})$.

Esercizio 5.5.5. Sia $\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Dimostrare che l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\zeta_5)$ contiene un unico campo intermedio K. Determinare il polinomio minimo di ζ_5 su K.

Esercizio 5.5.6. Sia $f = X^3 + X + \overline{1} \in \boldsymbol{Z}_2[X]$.

(*i*) Determinare il campo di spezzamento $\Sigma = \Sigma_{f,\boldsymbol{Z}_2}$.

(*ii*) Calcolare il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_2)$, esplicitandone tutti gli $\boldsymbol{Z}_2$-automorfismi.

Esercizio 5.5.7. Sia $f = X^3 + \overline{2}X + \overline{1} \in \boldsymbol{Z}_3[X]$. Determinare il campo di spezzamento $\Sigma = \Sigma_{f,\boldsymbol{Z}_3}$ e dedurne il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_3)$.

Esercizio 5.5.8. Si consideri l'estensione di campi $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2},\, \sqrt{3},\, \sqrt{5})$.

(*i*) Determinare il grado di tale estensione e dire se è normale.

(*ii*) Determinare il gruppo di Galois G di tale estensione.

(*iii*) Determinare i campi intermedi di tale estensione contenenti $\boldsymbol{Q}(\sqrt{10})$.

Esercizio 5.5.9. È assegnato il polinomio $f = X^6 + X^3 + \overline{2} \in \boldsymbol{Z}_3[X]$.

(*i*) Verificare che f è il cubo di un polinomio irriducibile $g \in \boldsymbol{Z}_3[X]$.

(*ii*) Determinare il campo di spezzamento Σ di f su $\boldsymbol{Z}_3$ e dire se l'estensione $\boldsymbol{Z}_3 \subset \Sigma$ è finita, normale e separabile.

(*iii*) Determinare il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_3)$.

Esercizio 5.5.10. Determinare le radici ottave dell'unità su $\boldsymbol{Z}_5$. Qual'è la minima estensione di $\boldsymbol{Z}_5$ in cui sono contenute? Qual'è il gruppo di Galois di tale estensione su $\boldsymbol{Z}_5$?

Esercizio 5.5.11. (*i*) Determinare il campo di spezzamento E del polinomio $X^7 - \overline{1} \in \boldsymbol{Z}_2[X]$.

(*ii*) Calcolare il gruppo di Galois $G(E \,|\, \boldsymbol{Z}_2)$.

(*iii*) Determinare i campi intermedi dell'estensione $\boldsymbol{Z}_2 \subset E$.

Esercizio 5.5.12. Sono assegnati i polinomi $f = X^3 - 3X + 1,\ g = X^3 + 3X + 1 \in \boldsymbol{Q}[X]$ [si tratta di polinomi irriducibili, come facilmente si verifica].

(*i*) Posto $\zeta = \zeta_9$ (radice primitiva nona dell'unità), verificare che f ammette i tre zeri reali

$$\alpha = \zeta + \zeta^{-1},\quad \beta = \zeta^2 + \zeta^{-2},\quad \gamma = \zeta^4 + \zeta^{-4}$$

e che $\beta,\, \gamma \in \boldsymbol{Q}(\alpha)$. Dedurne che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{A}_3$.

(*ii*) Verificare che g ammette un unico zero reale. Dedurne che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_3$ e calcolare il campo fisso $\boldsymbol{A}_3^{\flat}$.

6. Il teorema fondamentale dell'Algebra

È noto che un campo K è *algebricamente chiuso* se verifica una delle seguenti condizioni (ovviamente) equivalenti:

(*1*) Ogni polinomio non costante in $K[X]$ si fattorizza linearmente.
(*2*) Ogni polinomio non costante in $K[X]$ ha almeno uno zero in K.
(*3*) Ogni polinomio irriducibile in $K[X]$ ha grado 1.
(*4*) K non possiede estensioni algebriche proprie.

Scopo di questo paragrafo è dimostrare il *Teorema fondamentale dell'Algebra* (come d'abitudine abbreviato *TFA*): $\boldsymbol{C}$ *è un campo algebricamente chiuso.*

Tale teorema, enunciato da D'Alembert (nel 1746), fu provato per la prima volta da Gauss, nella sua tesi di dottorato (1799). Di tale teorema esistono numerose e molto diverse dimostrazioni e nessuna di esse è puramente "algebrica". Infatti tutte rinviano alla definizione ed alle proprietà (non algebriche) dei numeri reali. Tra le varie dimostrazioni ne presenteremo una, attribuita a Legendre (1752-1833), che non è certo la più elementare, ma che ha il pregio - relativamente a questo corso - di avere contenuto prettamente algebrico ed in particolare di sfruttare il *TFTG*.

Cominciamo con il seguente risultato che possiamo riguardare come il primo passo del *TFA*.

Proposizione 6.1. *In* $\boldsymbol{C}[X]$ *non esiste alcun polinomio irriducibile di grado* 2. *Ne segue che* $\boldsymbol{C}$ *non ammette estensioni algebriche di grado* 2.

Dim. L'ultima parte dell'enunciato segue ovviamente dalla prima [infatti ogni estensione di grado 2 di $\boldsymbol{C}$ determina un polinomio irriducibile di grado 2 in $\boldsymbol{C}[X]$].

Sia $f = X^2 + \alpha X + \beta \in \boldsymbol{C}[X]$. Posto $\gamma = \frac{\alpha^2}{4} - \beta$, risulta: $f = (X + \frac{\alpha}{2})^2 - \gamma$. Si scelga $\delta \in \boldsymbol{C}$ tale che $\delta^2 = \gamma$ [se $\gamma = r(\cos t + i\sin t)$, con $r, t \in \boldsymbol{R}$, $r > 0$, basta porre $\delta = \sqrt{r}(\cos\frac{t}{2} + i\sin\frac{t}{2})$]. Allora

$$f = (X + \tfrac{\alpha}{2} + \delta)(X + \tfrac{\alpha}{2} - \delta)$$

e dunque f è riducibile su $\boldsymbol{C}$, come richiesto.

Proposizione 6.2. *Ogni estensione finita di* $\boldsymbol{R}$ *ha grado* 2^h, *con* $h \geq 0$.

Premettiamo il seguente Lemma, che contiene la parte "non algebrica" di questa dimostrazione.

Lemma 6.1. *Ogni estensione finita propria di* $\boldsymbol{R}$ *ha grado pari.*

Dim. (*Lemma* **6.1**). Sia $\boldsymbol{R} \subset L$ un'estensione finita propria. Dal teorema dell'elemento primitivo (cfr. Teor. **3.1**, Cap. **4**) tale estensione è semplice. Se quindi $L = \boldsymbol{R}(\alpha)$, allora $[L : \boldsymbol{R}] = \partial m_\alpha$, con $m_\alpha \in \boldsymbol{R}[X]$ polinomio minimo di α su $\boldsymbol{R}$. Ovviamente $\partial m_\alpha \geq 2$.

Per assurdo, ∂m_α sia dispari. La funzione polinomiale $f = \Phi_{m_\alpha}$ [tale che $f(x) = m_\alpha(x)$, $\forall\, x \in \boldsymbol{R}$] è una funzione reale di variabile reale. Dai corsi di Calcolo è noto che $f(x)$ è una funzione continua e che $f(x) \to +\infty$, per $x \to +\infty$ mentre $f(x) \to -\infty$, per $x \to -\infty$. Per ragioni di continuità, esiste $x_0 \in \boldsymbol{R}$ tale che $f(x_0) = 0$. Pertanto $X - x_0 \,\big|\, m_\alpha$ e ciò contrasta con l'irriducibilità di m_α.

Dim. (*Prop.* **6.2**). Sia $\boldsymbol{R} \subset L$ un'estensione finita propria e sia N la chiusura normale di tale estensione. Poiché $\boldsymbol{R} \subset N$ è finita e propria, in base al lemma precedente $2 \,\big|\, [N : \boldsymbol{R}]$. Essendo $\boldsymbol{R} \subset N$ finita, normale e separabile, dal *TFTG(i)* segue che $\big|G(N|\boldsymbol{R})\big| = [N : \boldsymbol{R}]$ e dunque $G(N|\boldsymbol{R})$ ha ordine pari.

Poniamo $\big|G(N|\boldsymbol{R})\big| = 2^r m$, con $r \geq 1$ e m dispari ≥ 1. In base al teorema di Sylow (cfr. Teor. **4.2**, Cap. **2**), $G(N|\boldsymbol{R})$ contiene un 2-Sylow H (con $|H| = 2^r$). Sia $H^\flat$ il campo fisso di H (campo intermedio dell'estensione $\boldsymbol{R} \subset N$). In base all'Osserv. **5.3**, si ha:

$$[H^\flat : \boldsymbol{R}] = (G(N|\boldsymbol{R}) : H) = \tfrac{|G(N|\boldsymbol{R})|}{|H|} = \tfrac{2^r m}{2^r} = m.$$

Abbiamo così provato che $\boldsymbol{R} \subseteq H^\flat$ è un'estensione finita di grado dispari. Ancora in base al lemma precedente, $m = 1$ e dunque $[N : \boldsymbol{R}] = \big|G(N|\boldsymbol{R})\big| = 2^r$. Ne segue che

$$[L : \boldsymbol{R}] = \tfrac{[N:\boldsymbol{R}]}{[N:L]} = \tfrac{2^r}{[N:L]} = 2^h,$$

con $0 \leq h \leq r$.

Possiamo finalmente dimostrare il *TFA*.

Teorema 6.1. *(TFA). Il campo $\boldsymbol{C}$ dei complessi è algebricamente chiuso.*

Dim. Va dimostrato che, per ogni $f \in \boldsymbol{C}[X]$, risulta $\Sigma_{f,\boldsymbol{C}} = \boldsymbol{C}$.

Si ponga $\Sigma = \Sigma_{f,\boldsymbol{C}}$ e si assuma, per assurdo, che $\boldsymbol{C} \subset \Sigma$ sia un'estensione (finita) propria. Essendo anche $\boldsymbol{R} \subset \Sigma$ un'estensione (finita) propria, in base alla Prop. **6.2** risulta $[\Sigma : \boldsymbol{R}] = 2^h$, con $h \geq 1$. Ne segue che

$$[\Sigma : \boldsymbol{C}] = \tfrac{[\Sigma:\boldsymbol{R}]}{[\boldsymbol{C}:\boldsymbol{R}]} = \tfrac{2^h}{2} = 2^{h-1}.$$

Si noti che $2^{h-1} > 1$ (cioè $h \geq 2$) perché $\boldsymbol{C} \subset \Sigma$ è un'estensione propria. In base al *TFTG(i)*, $|G(\Sigma|\boldsymbol{C})| = [\Sigma : \boldsymbol{C}] = 2^{h-1}$ e dunque $G(\Sigma|\boldsymbol{C})$ è un 2-gruppo. È noto allora (cfr. Prop. **4.1**, Cap. **2**) che $G(\Sigma|\boldsymbol{C})$ possiede un sottogruppo H di indice 2, cioè di ordine 2^{h-2}. Consideriamone il campo fisso $H^\flat$ (campo intermedio tra $\boldsymbol{C}$ e Σ). Risulta, in base all'Osserv. **5.3**:

$$[H^\flat : \boldsymbol{C}] = (G(\Sigma|\boldsymbol{C}) : H) = 2.$$

Dunque $H^\flat$ è un'estensione di grado 2 di $\boldsymbol{C}$: ciò è in contrasto con la Prop. **6.1**.

APPENDICI DEL CAPITOLO 5

1. Dimostrazione del Teorema fondamentale della teoria di Galois

Rienunciamo il *teorema fondamentale della teoria di Galois* (abbr. *TFTG*):

Se $K \subseteq L$ *è un'estensione finita, normale e separabile, risulta:*

(i) $|\,G(L|K)\,| = [L : K]$*;*

(ii) Le applicazioni $\sharp$ *e* $\flat$ *sono inverse l'una dell'altra [cioè valgono le due relazioni*

$(\bullet)$ $M^{\sharp\flat} = M,\ \forall\, M \in \boldsymbol{\mathcal{F}}$*;* $\qquad$ $(\bullet\bullet)$ $H^{\flat\sharp} = H,\ \forall\, H \in \boldsymbol{\mathcal{G}}$*].*

(iii) Per ogni $M \in \boldsymbol{\mathcal{F}}$, $|G(L|M)| = [L : M]$ e $[M : K] = \frac{|\,G(L|K)\,|}{|\,G(L|M)\,|}$.

(iv) Sia $M \in \boldsymbol{\mathcal{F}}$. L'estensione $K \subseteq M$ è normale $\iff$ $G(L|M) \trianglelefteq G(L|K)$.

(v) Sia $M \in \boldsymbol{\mathcal{F}}$ e $K \subseteq M$ normale. Allora

$$G(M|K) \cong G(L|K)\big/_{G(L|M)}.$$

Il *TFTG* può essere dimostrato essenzialmente come conseguenza di tre risultati, che per il momento ci limitiamo ad enunciare e la cui dimostrazione verrà posta in coda a questa appendice.

Teorema A. *Sia* $K \subseteq L$ *un'estensione di campi e sia* H *un sottogruppo finito di* $G(L|K)$*. Risulta:*

$$[L : L^H] = |H|.$$

Ne segue subito che $[L^H : K] = [L : K]\big/_{|H|}$.

Teorema B. *Sia* $K \subseteq L$ *un'estensione finita e separabile. Sia* N *la chiusura normale di* $K \subseteq L$*. Risulta:*

$$\big|\{K\text{-omomorfismi da } L \text{ a } N\}\big| = [L : K].$$

Ne segue che se $K \subseteq L$ *è anche normale, allora* $|G(L|K)| = [L : K]$.

Proposizione C. *Sia* $K \subseteq L$ *un'estensione finita e normale. Siano* $\alpha, \beta \in L$ *zeri di un polinomio irriducibile* $f \in K[X]$*. Esiste* $\varphi \in G(L|K)$ *tale che* $\varphi(\alpha) = \beta$.

Si noti che la Prop. **C** sarà utilizzata per dimostrare il Teor. **B** [e quindi verrà dimostrata prima di tale teorema]. Utilizzando i risultati precedenti, cominciamo col provare le parti (i), (ii) e (iii), del *TFTG*.

Dim. $((i),(ii),(iii))$. La (i) segue immediatamente dalla seconda parte del Teor. **B**.

Proviamo la relazione $(\bullet)$ di (ii). Sia $M \in \boldsymbol{\mathcal{F}}$. L'estensione $M \subseteq L$ è ovviamente finita. Inoltre è normale (cfr. Osserv. **2.4**) e separabile (cfr. Esercizio **3.1**). Dai Teor. **A**, **B** segue che

$$[L : M^{\sharp\flat}] = [L : L^{G(L|M)}] = |G(L|M)| = [L : M].$$

Poiché $M \subseteq M^{\sharp\flat} \subseteq L$, dalla moltiplicatività del grado segue che $[M^{\sharp\flat} : M] = 1$, cioè $M = M^{\sharp\flat}$.

Proviamo ora la relazione $(\bullet\bullet)$ di (ii). Essendo $H \leq H^{\flat\sharp}$ ed essendo tali gruppi finiti [in quanto lo è $G(L\,|\,K)$], basta verificare che $|H| = |H^{\flat\sharp}|$. Infatti, essendo $H^{\flat} = H^{\flat\sharp\flat}$ (cfr. Prop. **5.3**), dal Teor. **A** segue che

$$|H| = [L : H^{\flat}] = [L : H^{\flat\sharp\flat}] = |H^{\flat\sharp}|.$$

La (iii) è pressoché ovvia. Infatti, $\forall\, M \in \boldsymbol{\mathcal{F}}$, essendo $M \subseteq L$ finita, normale e separabile, da (i) segue che $|G(L|M)| = [L : M]$. Infine, da $[L : K] = [L : M]\cdot[M : K]$ segue che

$$|G(L|K)| = |G(L|M)|\cdot[M:K], \text{ cioè } [M:K] = \tfrac{|\,G(L|K)\,|}{|\,G(L|M)\,|}.$$

Per dimostrare (iv) e (v) serve il seguente lemma.

Lemma 1. *Sia $K \subseteq L$ un'estensione finita, normale e separabile. Sia $M \in \boldsymbol{\mathcal{F}}$ e sia $\varphi \in G(L|K)$. Risulta:*

$$\varphi(M)^\sharp = \varphi\, M^\sharp\, \varphi^{-1}.$$

Dim. Proviamo la doppia inclusione tra i due gruppi.

$(\geq)$ Per ogni $\psi \in G(L|M) = M^\sharp$, bisogna verificare che $\varphi\circ\psi\circ\varphi^{-1} \in \varphi(M)^\sharp = G(L|\varphi(M))$.

Sia infatti $y = \varphi(x) \in \varphi(M)$, con $x \in M$. Allora $(\varphi\circ\psi\circ\varphi^{-1})(y) = \varphi(\psi(x)) = \varphi(x) = y$. Dunque $\varphi\circ\psi\circ\varphi^{-1} \in G(L|\varphi(M))$, come richiesto.

$(\leq)$ Sia $\psi \in G(L|\varphi(M)) = \varphi(M)^\sharp$. Basta verificare che $\varphi^{-1}\circ\psi\circ\varphi \in M^\sharp = G(L|M)$. Infatti, $\forall\, x \in M$: $(\varphi^{-1}\circ\psi\circ\varphi)(x) = \varphi^{-1}\big(\psi(\varphi(x))\big) = \varphi^{-1}\big(\varphi(x)\big) = x$.

Dim. $((iv))$. $(\Longrightarrow)$. Assumiamo $K \subseteq M$ normale (con $M \in \boldsymbol{\mathcal{F}}$). Bisogna verificare che $G(L|M) \trianglelefteq G(L|K)$, e cioè che

$$\forall\, \varphi \in G(L|K),\ M^\sharp\varphi = \varphi\, M^\sharp, \text{ ovvero } M^\sharp = \varphi\, M^\sharp\, \varphi^{-1}.$$

In base al Lemma **1**, è sufficiente dimostrare che $\varphi(M) = M$. Sia $x \in M$ e sia m il suo polinomio minimo su K. Si ha: $0 = \varphi(m(x)) = m(\varphi(x))$. Dunque $\varphi(x)$ è uno zero di m. Essendo $K \subseteq M$ normale e m irriducibile su K, allora m ha tutti gli zeri in M. Dunque $\varphi(x) \in M$ ed abbiamo così provato che $\varphi(M) \subseteq M$. Essendo poi φ iniettiva, allora $dim(\varphi(M)) = dim(M)$ e quindi (per la finitezza delle dimensioni di tali spazi vettoriali) $M = \varphi(M)$.

$(\Longleftarrow)$. Per ipotesi $M^\sharp \trianglelefteq G(L|K)$. Per dimostrare che $K \subseteq M$ è normale, bisogna verificare che, se $f \in K[X]$ è irriducibile su K, con uno zero $\alpha \in M$, ogni altro zero β di f appartiene ad M.

Certo $\beta \in L$ (perché $K \subseteq L$ è normale). Si può quindi applicare a $K \subseteq L$ la Prop. **C** e si ottiene un automorfismo $\Phi \in G(L|K)$ tale che $\Phi(\alpha) = \beta$. Si ponga ora $\varphi = \Phi_{|_M}$. Se verifichiamo che $\varphi(M) = M$, allora $\beta = \varphi(\alpha) \in M$, come richiesto.

Poiché $M^\sharp \trianglelefteq G(L|K)$, allora $\Phi\, M^\sharp\, \Phi^{-1} = M^\sharp$. Dal Lemma **1**, $\Phi\, M^\sharp\, \Phi^{-1} = \Phi(M)^\sharp$ e quindi $M^\sharp = \Phi(M)^\sharp$. Applichiamo $\flat$ a tale uguaglianza e utilizziamo (ii). Si ha:

$$\Phi(M) = \Phi(M)^{\sharp\,\flat} = M^{\sharp\,\flat} = M.$$

Dunque $\Phi(M) = M$. Allora $\varphi(M) = \Phi_{|_M}(M) = \Phi(M) = M$, come richiesto.

Dim. $((v))$. Sia $K \subseteq M$ normale, con $M \in \boldsymbol{\mathcal{F}}$. Per determinare un isomorfismo tra $G(M|K)$ e $G(L|K)\big/_{G(L|M)}$ utilizzeremo il *TFO*, creando un omomorfismo suriettivo $F : G(L|K) \to G(M|K)$ tale che $KerF = G(L|M)$.

L'applicazione richiesta è semplicemente la restrizione ad M dei K-automorfismi di L, cioè:

$$F(\varphi) = \varphi_{|_M},\quad \forall\, \varphi \in G(L|K).$$

Si tratta di verificare che

(a) $\varphi_{|_M} \in G(M|K)$; (b) F è un omomorfismo di gruppi;
(c) F è suriettiva; (d) $KerF = G(L|M)$.

(a) Basta ripetere la dimostrazione di $(iv)(\Longrightarrow)$: si ottiene $\varphi_{|_M}(M) = M$, cioè $\varphi_{|_M} \in G(M|K)$.

(b) Per ogni $\varphi_1, \varphi_2 \in G(L|K)$, si ha [tenuto conto che, da (a), $\varphi_2(M) = M$]:

$$F(\varphi_1\circ\varphi_2) = (\varphi_1\circ\varphi_2)_{|_M} = \varphi_1(\varphi_{2_{|_M}}) = \varphi_{1_{|_M}}\circ\varphi_{2_{|_M}} = F(\varphi_1)\circ F(\varphi_2).$$

(c) Assegnato $\psi \in G(M|K)$, va provata l'esistenza di un automorfismo $\varphi \in G(L|K)$ tale che $\varphi_{|_M} = \psi$ [si usa dire che φ è un *sollevamento* di ψ]. Ciò segue subito dal successivo Lemma **2** (un lemma che serve per dimostrare la Prop. **C**).

(*d*) Risulta: $KerF = \{\varphi \in G(L|K) \mid \varphi_{|_M} = \mathbf{1}_{_M}\} = G(L|M)$.

Dimostrazione del Teorema A

Rienunciamo il Teorema **A**: *sia* $K \subseteq L$ *un'estensione di campi e sia* H *un sottogruppo finito di* $G(L|K)$. *Risulta:* $[L : L^{^H}] = |H|$. *Ne segue subito che* $[L^{^H} : K] = [L : K]\Big/_{|H|}$.

L'ultima affermazione segue immediatamente dalla prima, in quanto $[L : K] = [L : L^{^H}]\cdot[L^{^H} : K]$.

Per dimostrare l'uguaglianza $[L : L^{^H}] = |H|$, poniamo: $n := |H|$, $m := [L : L^{^H}]$. Sia inoltre $H = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$. Basterà dimostrare:

$$(i)\ \ n \not< m; \qquad (ii)\ \ m \not< n.$$

(*i*) Per assurdo, sia $n < m$.

Essendo $m = dim_{_{L^H}}(L)$, si possono scegliere $x_1, \dots x_{n+1} \in L$, che siano $L^{^H}$-linearmente indipendenti. Resta definita la matrice

$$A = \begin{pmatrix} \varphi_1(x_1) & \dots & \varphi_1(x_{n+1}) \\ \vdots & \vdots & \vdots \\ \varphi_n(x_1) & \dots & \varphi_n(x_{n+1}) \end{pmatrix} \in \mathfrak{M}_{_{n,n+1}}(L).$$

Si consideri il sistema lineare omogeneo $A\boldsymbol{Y} = 0$, con $\boldsymbol{Y} = \begin{pmatrix} Y_1 \\ \vdots \\ Y_{n+1} \end{pmatrix}$ colonna di incognite. Poiché $n < n+1$, tale sistema ammette autosoluzioni. Se ne può scegliere una avente *il massimo numero possibile di zeri*. Permutando eventualmente le righe di A, si può assumere che tale autosoluzione sia $(y_1, \dots, y_r, 0, \dots, 0)$, con $r \le n+1$ e $y_1, \dots, y_r \neq 0$. Si ottiene quindi il sistema di uguaglianze:

$$(*) \qquad \begin{cases} \sum_{i=1}^{r} \varphi_j(x_i)\, y_i = 0 \\ \quad j = 1, \dots, n. \end{cases}$$

Si scelga ora arbitrariamente $\varphi \in H$ e lo si applichi alle n uguaglianze di $(*)$. Si ottiene

$$\begin{cases} \sum_{i=1}^{r} \varphi\big(\varphi_j(x_i)\big)\, \varphi(y_i) = 0 \\ \quad j = 1, \dots, n. \end{cases}$$

Poiché la moltiplicazione per φ è una biiezione di H, le precedenti uguaglianze si riscrivono [con un'eventuale permutazione] nella forma:

$$(**) \qquad \begin{cases} \sum_{i=1}^{r} \varphi_j(x_i)\, \varphi(y_i) = 0 \\ \quad j = 1, \dots, n. \end{cases}$$

Si moltiplicano ora le uguaglianze di $(*)$ per $\varphi(y_1)$ e quelle di $(**)$ per y_1, ottenendo:

$$(\bullet) \begin{cases} \sum_{i=1}^{r} \varphi_j(x_i)\, y_i\, \varphi(y_1) = 0 \\ \quad j = 1, \dots, n, \end{cases} \qquad (\bullet\bullet) \begin{cases} \sum_{i=1}^{r} \varphi_j(x_i)\, \varphi(y_i)\, y_1 = 0 \\ \quad j = 1, \dots, n. \end{cases}$$

Sottraendo le righe corrispondenti di $(\bullet)$ e $(\bullet\bullet)$ si ottiene:

$$(\bullet\bullet\bullet) \qquad \begin{cases} \sum_{i=1}^{r} \varphi_j(x_i)\, \big[y_i\, \varphi(y_1) - \varphi(y_i)\, y_1\big] = 0 \\ \quad j = 1, \dots, n. \end{cases}$$

Si noti che il coefficiente di $\varphi_j(x_1)$ è nullo. Pertanto $(\bullet\bullet\bullet)$ fornisce una soluzione del sistema $A\boldsymbol{Y} = 0$ avente meno di r elementi non nulli. Per non ottenere una contraddizione, tale soluzione deve essere nulla, cioè:

$$y_i\, \varphi(y_1) = \varphi(y_i)\, y_1, \ \text{ da cui } \ \frac{y_i}{y_1} = \frac{\varphi(y_i)}{\varphi(y_1)} = \varphi\big(\frac{y_i}{y_1}\big).$$

Essendo $\varphi \in H$ un elemento arbitrario, allora $\frac{y_i}{y_1} \in L^H$. Si ponga: $\alpha_i = \frac{y_i}{y_1}$ (e quindi $y_i = \alpha_i y_1$). La generica espressione di $(*)$ diventa (essendo $\alpha_i = \varphi_j(\alpha_i)$):

$$0 = \sum_{i=1}^{r} \varphi_j(x_i)\,\alpha_i\,y_1 = y_1\big(\sum_{i=1}^{r} \varphi_j(x_i)\,\varphi_j(\alpha_i)\big) = y_1\big(\sum_{i=1}^{r} \varphi_j(x_i\,\alpha_i)\big).$$

Cancellando y_1 $(\neq 0)$ e ricordato che φ_j è un automorfismo, allora $\sum_{i=1}^{r} x_i\,\alpha_i = 0$. Poiché ogni $\alpha_i \neq 0$, allora $x_1, \dots, x_r$ sono L^H-linearmente dipendenti, contro l'ipotesi [$x_1, \dots, x_{n+1}$ L^H-linearmente indipendenti].

(*ii*) Per assurdo, sia $m < n$.

Assumiamo che $\{x_1, \dots, x_m\}$ sia una base di L (come L^H-spazio vettoriale). E' definita la matrice:

$$B = \begin{pmatrix} \varphi_1(x_1) & \dots & \varphi_n(x_1) \\ \vdots & \vdots & \vdots \\ \varphi_1(x_m) & \dots & \varphi_n(x_m) \end{pmatrix} \in \mathfrak{M}_{m,n}(L),$$

e quindi il sistema lineare omogeneo $B\boldsymbol{Y} = 0$. Poiché $m < n$, tale sistema ammette autosoluzioni. Sia $(y_1, \dots, y_n)$ un'autosoluzione del sistema: dunque

$$\begin{cases} \sum_{i=1}^{n} \varphi_i(x_j)\,y_i = 0 \\ \quad j = 1, \dots, m. \end{cases}$$

Dimostreremo ora che $\sum_{i=1}^{n} y_i\,\varphi_i = \mathbf{0}$ (omomorfismo nullo). Si tratta di verificare che

$$\sum_{i=1}^{n} y_i\,\varphi_i(x) = 0, \quad \forall\, x \in L.$$

Sia $x = \sum_{j=1}^{m} \alpha_j\,x_j$ (con $\alpha_j \in L^H$). Allora [tenuto conto che $\varphi_i(\alpha_j) = \alpha_j$]:

$$\sum_{i=1}^{n} y_i\varphi_i(x) = \sum_{i=1}^{n} y_i\varphi_i\big(\sum_{j=1}^{m} \alpha_j\,x_j\big) = \sum_{i=1}^{n} y_i \sum_{j=1}^{m} \alpha_j\,\varphi(x_j) = \sum_{j=1}^{m} \big(\sum_{i=1}^{n} \varphi_i(x_j)\,y_i\big)\alpha_j = \sum_{j=1}^{m} 0\,\alpha_j = 0.$$

Gli automorfismi $\varphi_1, \dots, \varphi_n$ sono quindi L-linearmente dipendenti. Ma tale fatto contrasta con il seguente risultato (noto come *Lemma di Dedekind*) e da ciò segue l'assurdo.

Teorema. *(Lemma di Dedekind). Siano M, L due campi e siano $\varphi_1, \dots, \varphi_n$ omomorfismi distinti e non banali di campi. Risulta: $\varphi_1, \dots, \varphi_n$ sono L-linearmente indipendenti. Ne segue in particolare che ogni insieme finito di automorfismi distinti di L è L-linearmente indipendente.*

Dim. Per assurdo, $\varphi_1, \dots, \varphi_n$ siano L-linearmente dipendenti, con relazione di dipendenza lineare $\sum_{i=1}^{n} a_i\,\varphi_i = \mathbf{0}$ $(a_1, \dots, a_n \in L)$. Possiamo assumere (permutando eventualmente i φ_i) che i coefficienti non nulli di tale relazione siano i primi r $(1 \leq r \leq n)$ e che *non esistano relazioni di dipendenza lineare tra $\varphi_1, \dots, \varphi_n$ con meno di r addendi.*

Essendo $\varphi_1 \neq \varphi_r$, esiste $y \in M$ tale che $\varphi_1(y) \neq \varphi_r(y)$. Per ogni $x \in M$, si ha:

$$(\bullet)\ \begin{cases} \sum_{i=1}^{r} a_i\,\varphi_i(x) = 0; \end{cases} \qquad (\bullet\bullet)\ \begin{cases} \sum_{i=1}^{r} a_i\,\varphi_i(xy) = 0. \end{cases}$$

Da $(\bullet\bullet)$ segue: $(\bullet\bullet')$ $\begin{cases} \sum_{i=1}^{r} a_i\,\varphi_i(x)\,\varphi_i(y) = 0. \end{cases}$.

Da $(\bullet)$, moltiplicando per $\varphi_1(y)$, segue: $(\bullet')$ $\begin{cases} \sum_{i=1}^{r} a_i\,\varphi_i(x)\,\varphi_1(y) = 0. \end{cases}$.

Sottraendo $(\bullet')$ da $(\bullet\bullet')$, si ottiene: $(\bullet\bullet\bullet)$ $\begin{cases} \sum_{i=1}^{r} a_i\,\big[\varphi_i(y) - \varphi_1(y)\big]\varphi_i(x) = 0 \end{cases}$.

Osservato che $a_1\big[\varphi_1(y) - \varphi_1(y)\big] = 0$ e che $a_r\big[\varphi_r(y) - \varphi_1(y)\big] \neq 0$, la $(\bullet\bullet\bullet)$ fornisce la relazione di dipendenza lineare

$$\sum_{i=2}^{r} a_i\,\big[\varphi_i(y) - \varphi_1(y)\big]\,\varphi_i = \mathbf{0}$$

formata da $r-1$ addendi. Ciò è assurdo per le ipotesi di minimalità fatte.

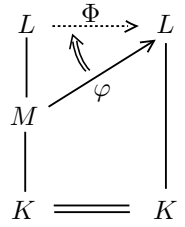
Nota. Sia $K \subseteq L$ un'estensione finita. Dal Teor. **A** [applicato a $G(L|K)$] segue che $|G(L|K)| = [L : K^{\sharp\flat}]$. Ne segue che $|G(L|K)| \,\big|\, [L : K]$.

Dimostrazione della Proposizione C

Rienunciamo la Proposizione **C**: *sia $K \subseteq L$ un'estensione finita e normale. Siano $\alpha, \beta \in L$ zeri di un polinomio irriducibile $f \in K[X]$. Esiste $\varphi \in G(L|K)$ tale che $\varphi(\alpha) = \beta$.*

La dimostrazione della Prop. **C** segue da questo lemma (di "*sollevamento*" di un K-omomorfismo).

Lemma 2. *Sia $K \subseteq L$ un'estensione finita e normale. Sia $M \in \boldsymbol{\mathcal{F}}$. Ogni K-omomorfismo $\varphi : M \to L$ si estende ad un K-automorfismo Φ di L [cioè $\Phi_{|_M} = \varphi$].*



Dim. (Lemma **2**). L'applicazione suriettivizzata $\varphi_{su} : M \to \varphi(M)$ è un K-isomorfismo; inoltre $\varphi(M) \subseteq L$. Essendo $K \subseteq L$ finita e normale, dal Teor. **2.2**, $L = \Sigma_{f,K}$, per un opportuno $f \in K[X]$. Dall'Osserv. **2.2**, $L = \Sigma_{f,M} = \Sigma_{f,\varphi(M)}$.

Considerato l'isomorfismo d'anelli $\varphi' : M[X] \to \varphi(M)[X]$ (indotto da φ_{su}), risulta (essendo $f \in K[X]$) $\varphi'(f) = f$. In base al Teor. **2.1'**, esiste un isomorfismo di campi $\Phi : L \to L$ tale che $\Phi_{|_M} = \varphi_{su}$. Ma allora $\Phi_{|_K} = \Phi_{|_M|_K} = \varphi_{|_K} = \mathbf{1}_K$, cioè Φ è un K-automorfismo di L che estende φ.

Dim. (Prop. **C**). In base a Prop. **2.4** di Cap. **4**, esiste un K-isomorfismo $K(\alpha) \to K(\beta)$ che trasforma α in β. Lo si componga con l'inclusione canonica $K(\beta) \hookrightarrow L$. Si ottiene il K-omomorfismo $\varphi : K(\alpha) \to K(\beta) \hookrightarrow L$. In base al Lemma **2**, φ si estende ad un K-automorfismo Φ di L tale che $\Phi_{|_{K(\alpha)}} = \varphi$. In particolare $\Phi(\alpha) = \beta$, come richiesto.

Dimostrazione del Teorema B

Rienunciamo il Teorema **B**: *Sia $K \subseteq L$ un'estensione finita e separabile. Sia N la chiusura normale di $K \subseteq L$. Risulta:*

$$\big|\{K\text{-omomorfismi da } L \text{ a } N\}\big| = [L : K].$$

Ne segue che se $K \subseteq L$ è anche normale, allora $|G(L|K)| = [L : K]$.

Possiamo subito dimostrare (utilizzando la prima parte del teorema) l'ultima e più significativa affermazione.

Poiché $K \subseteq L$ è normale, $N = L$. Ogni K-omomorfismo $\varphi : L \to L$ è necessariamente suriettivo [infatti, essendo φ iniettivo e $dim_K(L)$ finita, allora $Im\,\varphi = L$]. Pertanto φ è un K-automorfismo di L. Dalla prima parte del teor. **B** segue:

$$|G(L|K)| = \big|\{K\text{-omomorfismi da } L \text{ a } L\}\big| = [L : K].$$

Dimostriamo ora la prima parte del teorema, procedendo per induzione forte su $t = [L : K]$.

Sia $t = 1$. In tal caso $K = L = N$. Allora $\{K\text{-omomorfismi da } K \text{ a } K\} = \{\mathbf{1}_K\}$ e pertanto $|\{\mathbf{1}_K\}| = 1 = [K : K]$ [la tesi è ovvia].

Sia $t > 1$ ed assumiamo vero il risultato per ogni estensione finita e separabile di grado $< t$.

Sia $\alpha \in L - K$ e sia $m \in K[X]$ il suo polinomio minimo. Sia $r = \partial m$ (> 1) e si consideri il campo intermedio $K(\alpha)$ (tra K ed L). Essendo $[K(\alpha) : K] = r$, dalla moltiplicatività del grado segue subito che $[L : K(\alpha)] = \frac{t}{r} < t$. Poniamo $s := \frac{t}{r}$ ed osserviamo che l'estensione $K(\alpha) \subseteq L$ è finita e separabile (cfr. Esercizio **3.1**). Dalla Prop. **2.3** la chiusura normale di $K(\alpha) \subseteq L$ è ancora N. Applicando l'ipotesi induttiva,

$$\left|\{K(\alpha)\text{-omomorfismi da } L \text{ a } N_1\}\right| = [L : K(\alpha)] = s.$$

Denotiamo tali $K(\alpha)$-omomorfismi con $\psi_1, \dots, \psi_s$.

Per ipotesi, il polinomio $m \in K[X]$ è separabile. Inoltre ha zero $\alpha \in L \subseteq N$. Poiché $K \subseteq N$ è normale, i suoi r zeri - tutti distinti - sono in N. Li denotiamo $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$.

Dalla Prop. **C**, applicata all'estensione finita e normale $K \subseteq N$, segue che esistono $\varphi_1, \dots, \varphi_r$ K-automorfismi di N, tali che $\varphi_i(\alpha) = \alpha_i \quad (1 \le i \le r)$.

Consideriamo le seguenti composizioni:

$$\varphi_i \circ \psi_j : L \to N \to N, \quad 1 \le i \le r,\ 1 \le j \le s.$$

Si tratta di K-omomorfismi a due a due distinti. Sono complessivamente $rs = t$. Per concludere la dimostrazione basta provare che non esistono altri K-omomorfismi da L a N.

Sia quindi $\varphi : L \to N$ un K-omomorfismo. Poiché $\varphi(\alpha)$ è uno zero di m, allora $\varphi(\alpha) = \alpha_h$, $\exists\, h \in \boldsymbol{N}$, $1 \le h \le r$. Consideriamo allora

$$\varphi_h^{-1} \circ \varphi : L \to N.$$

Risulta: $(\varphi_h^{-1} \circ \varphi)(\alpha) = \varphi_h^{-1}(\alpha_h) = \alpha$. Dunque $\varphi_h^{-1} \circ \varphi$ è un $K(\alpha)$-omomorfismo da L a N e dunque è uno degli s omomorfismi $\psi_1, \dots, \psi_s$ sopra considerati. Se ad esempio $\varphi_h^{-1} \circ \varphi = \psi_\ell$, allora $\varphi = \varphi_h \circ \psi_\ell$, cioè φ è uno dei t K-omomorfismi sopra considerati.

Come accennato nell'Osserv. **2.5** del Cap. **5**, la definizione di estensione normale è equivalente, per estensioni finite e separabili, a quella di *estensione galoisiana*, molto diffusa in letteratura (cfr. ad esempio [Artin]): *un'estensione finita $K \subseteq L$ è detta galoisiana se* $[L : K] = |G(L|K)|$.

Nella proposizione che segue intendiamo giustificare tale affermazione.

Proposizione 1. *Sia $K \subseteq L$ un'estensione finita e separabile. Risulta:*

$$K \subseteq L \text{ è normale} \iff K \subseteq L \text{ è galoisiana.}$$

Dim. L'implicazione $(\Longrightarrow)$ è dimostrata dal $TFTG(i)$. Per dimostrare $(\Longleftarrow)$ bisogna verificare che se $f \in K[X]$ è un polinomio irriducibile con uno zero $\alpha \in L$, allora f si spezza su L.

Osserviamo che $K = K^{\sharp\flat}$. Infatti, dal Teor. **A** applicato a $G(L|K)$ segue $[L : K^{\sharp\flat}] = |G(L|K)|$. Ma, per ipotesi, $|G(L|K)| = [L : K]$ e quindi, essendo $K \subseteq K^{\sharp\flat} \subseteq L$, $K = K^{\sharp\flat}$.

Sia ora $\boldsymbol{O}(\alpha)$ l'orbita di α rispetto all'azione

$$\omega : G(L|K) \times L \to L \text{ tale che } \omega(\varphi, x) = \varphi(x),\ \forall\, \varphi \in G(L|K),\ \forall\, x \in L.$$

Essendo l'estensione finita, $G(L|K)$ è un gruppo finito. Se $G(L|K) = \{\varphi_1 = \mathbf{1}, \varphi_2, \dots, \varphi_r\}$, risulta $\boldsymbol{O}(\alpha) = \{\alpha, \varphi_2(\alpha), \dots, \varphi_r(\alpha)\} \subset L$. Poniamo $\alpha_i := \varphi_i(\alpha)$ $(1 \le i \le r)$ e

$$g := (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_r) \in L[X].$$

Se proviamo che $g \in K[X]$ e che $g \,|\, f$, dall'irriducibilità di f segue che $f = g$ e dunque f si spezza in $L[X]$, come richiesto.

Ogni automorfismo $\varphi_i \in G(L|K)$ induce una permutazione di $\alpha_1, \dots \alpha_r$ [infatti $G(L|K) = \{\varphi_i \circ \varphi_1, \varphi_i \circ \varphi_2, \dots, \varphi_i \circ \varphi_r\}$]. Indicato con $\varphi_i' : L[X] \to L[X]$ l'automorfismo di anelli associato a φ_i, allora φ_i' fissa g. Se poi $g = \sum_h c_h X^h$, si ha:

$$g = \varphi_i'(g) = \sum_h \varphi_i(c_h) X^h \quad \text{e quindi} \quad \varphi_i(c_h) = c_h,\ \forall\, h,$$

cioè $c_h \in K^{\sharp\flat} = K$. Dunque $g \in K[X]$. Inoltre ogni α_i è uno zero di f. Infatti , essendo $\alpha_i = \varphi_i(\alpha)$, allora $f(\alpha_i) = f(\varphi_i(\alpha)) = \varphi_i(f(\alpha)) = 0$. Pertanto $X - \alpha_i \,|\, f$ $(1 \le i \le r)$ e quindi $g \,|\, f$. Essendo f irriducibile, allora $f = g$, come richiesto.

2. Il Teorema di Galois sulla risolubilità per radicali

Scopo della presente appendice è dimostrare il teorema di Galois sulla risolubilità per radicali di un polinomio. Come noto (cfr. Cap. **5**, Teor **1.1**) tale teorema afferma che, assegnato un polinomio $f \in K[X]$, con $car(K) = 0$, risulta:

$$f \text{ è risolubile per radicali } \iff \text{ il gruppo di Galois } G(\Sigma_{f,K}|K) \text{ è risolubile.}$$

Cominciamo col provare l'implicazione $(\Longrightarrow)$.

Per definizione, se f è risolubile per radicali esiste un campo M tale che $K \subseteq \Sigma_{f,K} \subseteq M$ e $K \subseteq M$ è un'estensione radicale. L'implicazione $(\Longrightarrow)$ è quindi dimostrata dal seguente teorema.

Teorema 1. *Sia $car(K) = 0$ e sia $K \subseteq M$ un'estensione radicale. Per ogni campo intermedio L di tale estensione, il gruppo di Galois $G(L|K)$ è risolubile.*

La dimostrazione del Teor. **1** poggia sul seguente analogo risultato, che ha ipotesi più forti.

Teorema 1'. *Sia $car(K) = 0$ e sia $K \subseteq L$ un'estensione finita, normale e radicale. Il gruppo di Galois $G(L|K)$ è risolubile.*

Prima di dimostrare questo teorema, vogliamo dimostrare che dal Teor. **1'** segue il Teor. **1**. A tale scopo enunciamo due risultati preliminari, che dimostreremo successivamente.

Lemma 1. *Sia $K \subseteq L$ un'estensione radicale e sia N la chiusura normale di $K \subseteq L$. Anche $K \subseteq N$ è un'estensione radicale.*

Proposizione 1. *Se $K \subseteq L$ è un'estensione finita, considerato il campo fisso $K^{\sharp\flat} = L^{G(L|K)}$, si ha che l'estensione $K^{\sharp\flat} \subseteq L$ è normale.*

Abbiamo ora gli strumenti per dimostrare che Teor. **1'** $\Longrightarrow$ Teor. **1**.

Sia $K \subseteq M$ un'estensione radicale ed L un campo intermedio di tale estensione. Si consideri il campo $K^{\sharp\flat} = L^{G(L|K)}$. In base a Prop. **1**, $K^{\sharp\flat} \subseteq L$ è normale. Inoltre, da Prop. **5.3**, $G(L|K) = K^{\sharp} = K^{\sharp\flat\sharp} = G(L|K^{\sharp\flat})$. Infine l'estensione $K^{\sharp\flat} \subseteq M$ è radicale (con la stessa sequenza radicale di $K \subseteq M$). Pertanto non è restrittivo sostituire K con $K^{\sharp\flat}$, ovvero supporre direttamente che l'estensione $K \subseteq L$ sia normale.

Sia ora N la chiusura normale di $K \subseteq M$. Dal Lemma **1**, essendo $K \subseteq M$ radicale, anche $K \subseteq N$ è radicale. Infine, considerato L come campo intermedio dell'estensione (finita, normale e separabile) $K \subseteq N$ ed essendo $K \subseteq L$ normale, dal $TFTG(v)$ segue che $G(L|K) \cong G(N|K)/_{G(N|L)}$. Se quindi dimostriamo che $G(N|K)$ è risolubile, in base a Osserv. **4.1**, anche $G(L|K)$ è risolubile. Quindi il Teor. **1** può essere dimostrato direttamente per l'estensione $K \subseteq N$ che è finita, normale e radicale. Siamo così nelle ipotesi del Teor. **1'**.

Per dimostrare il Teor. **1'** enunciamo un altro lemma (che poi dimostreremo).

Lemma 2. *Sia n un naturale positivo, sia p un primo e sia K un campo con $car(K) = 0$.*
(i) Posto $f = X^p - 1 \in K[X]$, il gruppo di Galois $G(\Sigma_{f,K}|K)$ è abeliano.

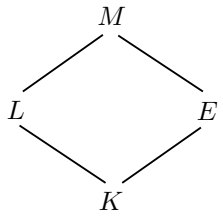
(ii) Se K contiene tutte le radici n-sime dell'unità, per ogni $f = X^n - a \in K[X]$, il gruppo di Galois $G(\Sigma_{f,K}|K)$ è abeliano.

Dim. (Teor. **1'**). Sia $L = K(\alpha_1, \dots, \alpha_n)$, con $\alpha_i^{t_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ (per $1 \leq i \leq n$). Non è restrittivo assumere che ogni esponente t_i sia primo. Basta altrimenti aggiungere alla sequenza radicale $\{\alpha_1, \dots, \alpha_n\}$ ulteriori potenze degli α_i, come chiarito dal seguente esempio: se $\{\alpha_1, \alpha_2, ...\}$ è una sequenza radicale di $K \subseteq L$, con $\alpha_1^6 \in K$, $\alpha_2^{10} \in K(\alpha_1)$, ... , la si può sostituire con la sequenza radicale $\{\alpha_1^3, \alpha_1^2, \alpha_2^5, \alpha_2^2, \alpha_3, \dots\}$ [che genera ancora L].

Denoteremo in particolare con p il primo esponente della sequenza radicale $\{\alpha_1, \dots, \alpha_n\}$ [a esponenti primi]. Dunque $\alpha_1^p \in K$. Sia ora $f := X^p - 1 \in K[X]$ e si ponga:

$$E := \Sigma_{f,K}, \quad M := \Sigma_{f,L}.$$

Sussiste quindi il seguente diagramma di estensioni



ed ovviamente risulta: $M = E(\alpha_1, \dots, \alpha_n)$. Inoltre l'estensione $K \subseteq M$ è normale [se infatti $L = \Sigma_{g,K}$, allora : $M = \Sigma_{fg,K}$] ed è ovviamente finita e separabile. Dal $TFTG\,(v)$, essendo $K \subseteq L$ normale,

$$G(L \,|\, K) \cong G(M \,|\, K)/_{G(M \,|\, L)}.$$

In base ad Osserv.**4.1** (i), basta dimostrare che $G(M \,|\, K)$ è risolubile. Dal Lemma **2** (i), $G(E \,|\, K)$ è abeliano e quindi risolubile. Inoltre (essendo $K \subseteq E$ normale), sempre dal $TFTG\,(v)$,

$$G(E \,|\, K) \cong G(M \,|\, K)/_{G(M \,|\, E)}.$$

In base ad Osserv.**4.1** (ii), se proviamo che $G(M \,|\, E)$ è risolubile, anche $G(M \,|\, K)$ lo è. La tesi diventa quindi: $G(M \,|\, E)$ è risolubile, e la proveremo per induzione su n.

Sia $n = 1$. Allora: $L = K(\alpha_1)$; $\alpha_1^p \in K$; $M = E(\alpha_1)$. Possiamo applicare il Lemma **2** (ii) al polinomio $X^p - \alpha_1^p \in E[X]$ [si noti che $E = \Sigma_{f,K}$ contiene le radici p-sime dell'unità]. Ne segue che $G(M \,|\, E)$ è abeliano e quindi, come richiesto, risolubile.

Sia ora $n > 1$ e consideriamo l'estensione $E \subseteq M$. Si tratta di un'estensione normale (in quanto $K \subseteq M$ è normale) ed ovviamente finita e separabile. Se ne consideri il campo intermedio $E(\alpha_1)$ ed il relativo gruppo di Galois $E(\alpha_1)^\sharp = G(M \,|\, E(\alpha_1))$. Poiché $E(\alpha_1)$ è campo di spezzamento su E del polinomio $X^p - \alpha_1^p$, allora l'estensione $E \subseteq E(\alpha_1)$ è normale e quindi, dal $TFTG\,(v)$,

$$G(E(\alpha_1) \,|\, E) \cong G(M \,|\, E)/_{G(M \,|\, E(\alpha_1))}.$$

Il gruppo $G(E(\alpha_1) \,|\, E)$ è abeliano per il Lemma **2** (ii) e quindi è risolubile. Il gruppo $G(M \,|\, E(\alpha_1))$ è risolubile per ipotesi induttiva [infatti $E(\alpha_1) \subseteq E(\alpha_1)(\alpha_2, \dots, \alpha_n)$ è un'estensione normale e radicale con $n-1$ generatori]. Si conclude, in base a Osserv. **4.1** (ii), che $G(M \,|\, E)$ è risolubile.

Completiamo la dimostrazione dell'implicazione ($\Longrightarrow$) del teorema di Galois sulla risolubilità per radicali, dimostrando tutti i risultati precedentemente enunciati ed utilizzati.

Dim. (Lemma **1**). Premettiamo due osservazioni

(a) Date due estensioni isomorfe $K \subseteq L$ e $K \subseteq L'$, se una è radicale, anche l'altra lo è.

Infatti, se $\varphi : L \to L'$ è un K-isomorfismo e $\{\alpha_1, \dots, \alpha_m\}$ è una sequenza radicale di $K \subseteq L$, allora $\{\varphi(\alpha_1), \dots, \varphi(\alpha_m)\}$ è una sequenza radicale di $K \subseteq L'$ (con gli stessi esponenti).

(b) Se $K \subseteq L_1, \dots, K \subseteq L_s$, sono estensioni radicali, anche $K \subseteq \langle L_1 \cup \dots \cup L_s \rangle$ è radicale.

Se infatti $\{\alpha_{i1}, ..., \alpha_{im_i}\}$ è una sequenza radicale di $K \subseteq L_i$ $(1 \leq i \leq s)$, si verifica subito che $\{\alpha_{11}, ..., \alpha_{1m_1}, \alpha_{21}, ..., \alpha_{2m_2}, ..., \alpha_{s1}, ..., \alpha_{sm_s}\}$ è una sequenza radicale di $K \subseteq \langle L_1 \cup ... \cup L_s \rangle$.

Veniamo ora alla dimostrazione del lemma. Sia $L = K(\alpha_1, ..., \alpha_m)$, con $\{\alpha_1, ..., \alpha_m\}$ sequenza radicale di $K \subseteq L$. Indichiamo con $\alpha_i = \alpha_{i,1}, ..., \alpha_{i,n_i}$ gli zeri del polinomio minimo di α_i su K. È ben noto che

$$N = K(\alpha_1, \alpha_{1,2}, ..., ..., \alpha_m, \alpha_{m,2}, ...)$$

Poiché $K(\alpha_i) \cong K(\alpha_{i,j})$, allora $L \cong K(\alpha_1, ..., \alpha_{i,j}, ..., \alpha_m)$. In base ad (a), l'estensione $K \subseteq K(\alpha_1, ..., \alpha_{i,j}, ..., \alpha_m)$ è radicale. Da (b) segue che l'estensione $K \subseteq K(\alpha_1, ..., \alpha_i, \alpha_{i,j}, ..., \alpha_m)$ è radicale. Ripetendo questo ragionamento per ogni i e per ogni $\alpha_{i,j}$ si conclude che $K \subseteq N$ è radicale.

Per dimostrare la Prop. **1** occorre una caratterizzazione delle estensioni normali, che dimostriamo in questa proposizione.

Proposizione 1'. *Sia $K \subseteq L$ un'estensione finita. Le seguenti affermazioni sono equivalenti:*

(i) $K \subseteq L$ è normale

(ii) per ogni campo M tale che $K \subseteq L \subseteq M$ e $K \subseteq M$ è normale, si ha che, per ogni K-omomorfismo $\varphi : L \to M$, $\varphi(L) = L$.

(iii) esiste un campo M tale che $K \subseteq L \subseteq M$, $K \subseteq M$ è normale e, per ogni K-omomorfismo $\varphi : L \to M$, $\varphi(L) = L$.

Dim. (Prop. **1'**). $(i \Longrightarrow ii)$. Si consideri un campo M tale che $K \subseteq L \subseteq M$ e $K \subseteq M$ è normale. Sia $\varphi : L \to M$ un K-omomorfismo. Sia $\alpha \in L$, con polinomio minimo $m_\alpha \in K[X]$. Si ha: $m_\alpha(\varphi(\alpha)) = \varphi(m_\alpha(\alpha)) = \varphi(0) = 0$ e dunque $\varphi(\alpha)$ è uno zero di m_α. Essendo $K \subseteq L$ normale, allora $\varphi(\alpha) \in L$. Dunque $\varphi(L) \subseteq L$ e quindi, per ragioni di grado, $\varphi(L) = L$.

$(ii \Longrightarrow iii)$ è evidente.

$(iii \Longrightarrow i)$. Sia $K \subseteq L$ un'estensione finita e sia M un campo verificante le ipotesi di (iii). Sia $f \in K[X]$ un polinomio irriducibile con uno zero $\alpha \in L$. Sia $\beta \in M$ un altro zero di f. Applichiamo all'estensione finita $K \subseteq M$ la Prop. **C** della precedente appendice. Esiste $\varphi \in G(M \,|\, K)$ tale che $\varphi(\alpha) = \beta$. Essendo $\varphi_{|_L} : L \to M$ un K-omomorfismo, per ipotesi $\varphi(L) = L$ e dunque $\beta \in L$. È così provato che l'estensione $K \subseteq L$ è normale.

Dim. (Prop **1**). Applichiamo il Teor. **A** dell'Appendice **1** all'estensione $K \subseteq L$ ed all'intero gruppo $G(L \,|\, K)$. Si ottiene:

$$[L : K^{\sharp\flat}] = |G(L \,|\, K)|.$$

Dal Teor. **B** dell'Appendice **1**, applicato all'estensione $K^{\sharp\flat} \subseteq L)$, si ottiene (indicata con N la chiusura normale di tale estensione):

$$\left|\{K^{\sharp\flat}\text{-omomorfismi da } L \text{ a } N\}\right| = [L : K^{\sharp\flat}].$$

Tenuto conto che $G(L \,|\, K^{\sharp\flat}) = G(L \,|\, K)$, ne segue:

$$(*) \qquad \left|\{K^{\sharp\flat}\text{-omomorfismi da } L \text{ a } N\}\right| = |G(L \,|\, K^{\sharp\flat})|.$$

Evidentemente ogni $\varphi \in G(L \,|\, K^{\sharp\flat})$ definisce un $K^{\sharp\flat}$-omomorfismo $\varphi \equiv i \circ \varphi : L \to N$. In base ad $(*)$, ogni $K^{\sharp\flat}$-omomorfismo $\varphi : L \to N$ proviene da un automorfismo $\varphi \in G(L \,|\, K^{\sharp\flat})$. Ne segue che $\varphi(L) = L$, come richiesto dalla Prop. **1'**.

Dim. (Lemma **2**). (i) Risulta: $\Sigma_{f,K} = K(\zeta_p)$; ogni automorfismo $\varphi \in G(K(\zeta_p) \,|\, K)$ è completamente individuato da $\varphi(\zeta_p)$ e $\varphi(\zeta_p) = \zeta_p^{\,i}$ (con $1 \leq i < p$). Se quindi $\varphi, \psi \in G(K(\zeta_p) \,|\, K)$, con $\varphi(\zeta_p) = \zeta_p^{\,i}$, $\psi(\zeta_p) = \zeta_p^{\,j}$, si ha:

$$(\psi \circ \varphi)(\zeta_p) = \zeta_p^{\,ij} = (\varphi \circ \psi)(\zeta_p).$$

Dunque $\psi\circ\varphi=\varphi\circ\psi$, cioè $G(\Sigma_{f,K}\,|\,K)$ è abeliano.

(*ii*) Sia α uno zero di f (in $\Sigma_{f,K}$). Gli altri zeri di f sono gli elementi $\alpha\,\zeta_n^{\,i}$ (con $1\le i<n$). Essendo per ipotesi $\zeta_n^{\,i}\in K$, allora $\Sigma_{f,K}=K(\alpha)$. Ogni $\varphi\in G(K(\alpha)\,|\,K)$ è completamente definito da $\varphi(\alpha)$ e $\varphi(\alpha)=\alpha\,\zeta_n^{\,i}$ (con $0\le i<n$).

Se quindi $\varphi,\psi\in G(K(\alpha)\,|\,K)$ e $\varphi(\alpha)=\alpha\,\zeta_n^{\,i}$, $\psi(\alpha)=\alpha\,\zeta_n^{\,j}$, allora:

$(\varphi\circ\psi)(\alpha)=\varphi(\alpha\,\zeta_n^{\,j})=\varphi(\alpha)\varphi(\zeta_n^{\,j})=\alpha\,\zeta_n^{\,i}\,\zeta_n^{\,j}=\alpha\,\zeta_n^{\,i+j}$. Analogamente, $(\psi\circ\varphi)(\alpha)=\alpha\,\zeta_n^{\,j+i}$ e quindi si conclude che $\psi\circ\varphi=\varphi\circ\psi$, cioè $G(\Sigma_{f,K}\,|\,K)$ è abeliano.

Ora veniamo alla dimostrazione dell'implicazione ($\Longleftarrow$) del teorema di Galois sulla risolubiltà per radicali: *se* $car(K)=0$, $f\in K[X]$ *ed il gruppo di Galois* $G(\Sigma_{f,K}\,|\,K)$ *è risolubile, allora* f *è risolubile per radicali, cioè esiste un campo* R *tale che* $\Sigma_{f,K}\subseteq R$ *e* $K\subseteq R$ *è radicale.*

Per ottenere tale risultato dimostreremo, più generalmente il seguente teorema.

Teorema 2. *Sia* $car(K)=0$ *e* $K\subseteq L$ *un'estensione finita e normale (ovviamente separabile). Se il gruppo di Galois* $G(L\,|\,K)$ *è risolubile, esiste un'estensione* R *di* L *tale che* $K\subseteq R$ *è radicale.*

Premettiamo una proposizione, che, al solito, dimostreremo dopo.

Proposizione 2. *Sia* K *un campo, con* $car(K)=0$, *ed assumiamo che il polinomio* $f=X^p-1\in K[X]$, *con* p *primo, si spezzi su* K. *Sia poi* $K\subseteq L$ *un'estensione finita normale (ed ovviamente separabile), con gruppo di Galois* $G(L\,|\,K)$ *ciclico di ordine* p.

Risulta: $L=K(\alpha)$, *dove* $\alpha\in L$ *è uno zero di un polinomio della forma* $X^p-a\in K[X]$.

Dim. (Teor. **2**). Procediamo per induzione sull'ordine di $G(L\,|\,K)$. Se $|G(L\,|\,K)|=1$, allora $L=K$ e basta porre $R=L$.

Sia $|G(L\,|\,K)|=n>1$ e fissiamo arbitrariamente un primo p [che verrà poi determinato nella parte conclusiva della dimostrazione]. Procedendo come nella dimostrazione di Teor. **1'**, poniamo:

$$f:=X^p-1\in K[X],\quad E:=\Sigma_{f,K},\quad M:=\Sigma_{f,L}.$$

Verifichiamo che il gruppo di Galois $G(M\,|\,E)$ è risolubile. Infatti per ipotesi lo è $G(L\,|\,K)$; inoltre $G(L\,|\,K)\cong G(M\,|\,K)\big/_{G(M\,|\,L)}$ e $G(M\,|\,L)$ è abeliano [basta verificarlo, dopo aver osservato che $M=\Sigma_{f,L}=L(\zeta_p)$] e quindi risolubile. Da Osserv. **4.1** (*ii*) segue che $G(M\,|\,K)$ è risolubile. Poiché $G(M\,|\,E)\le G(M\,|\,K)$, anche $G(M\,|\,E)$ è risolubile (cfr. Prop. **4.1**).

Per dimostrare la tesi, basterà determinare un'estensione R di M tale che $E\subseteq R$ è radicale. Infatti anche $K\subseteq E$ è radicale [essendo $E=\Sigma_{f,K}=K(\zeta_p)$ e $\zeta_p^{\,p}\in K$] e la composizione di due estensioni radicali è radicale, come subito si verifica.

Si definisce la seguente applicazione:

$$F:G(M\,|\,E)\to G(L\,|\,K)\ \text{ tale che }\ F(\varphi)=\varphi_{|_L},\ \ \forall\,\varphi\in G(M\,|\,E).$$

Si noti che F è ben definita, in quanto $\varphi(L)=L$ [basta applicare la Prop. **1'** all'estensione normale $K\subseteq L$]. Inoltre F è un omomorfismo ed è un'applicazione iniettiva [se infatti $\varphi_{|_L}=\mathbf{1}_L$, allora φ agisce come identità su $L\cup E$ e quindi $\varphi=\mathbf{1}_M$, essendo $M=\langle L\cup E\rangle$].

Consideriamo il sottogruppo $Im(F)$ di $G(L\,|\,K)$. Sono possibili due casi:

$$(a)\ \ Im(F)<G(L\,|\,K);\qquad (b)\ \ Im(F)=G(L\,|\,K).$$

Nel caso (a), $|G(M\,|\,E)|=|Im(F)|<n$; l'estensione $E\subseteq M$ è finita, normale, separabile ed ha gruppo di Galois risolubile (come sopra osservato). Per ipotesi induttiva esiste un'estensione R di M tale che $E\subseteq R$ è radicale.

Nel caso (b), $F:G(M\,|\,E)\to G(L\,|\,K)$ è un isomorfismo. Essendo $G(L\,|\,K)$ un gruppo finito, possiamo scegliere in esso un sottogruppo proprio H, normale e "massimale rispetto alla normalità". Allora $G(L\,|\,K)\big/_H$ è semplice. Inoltre è risolubile (come lo è $G(L\,|\,K)$). Ma un gruppo semplice e

risolubile è abeliano ed i gruppi abeliani semplici sono ciclici di ordine primo. Dunque $G(L \,|\, K)/_H \cong \boldsymbol{C}_p$, con p primo. Ne segue che $F^{-1}(H)$ è un sottogruppo ciclico di indice p di $G(M \,|\, E)$.

Consideriamo nell'estensione $E \subseteq M$ [che è finita, normale e separabile] il campo fisso $F^{-1}(H)^\flat = M^{F^{-1}(H)}$, che denoteremo P. Si ha:

(*1*) L'estensione $E \subseteq P$ è radicale. Per provare tale fatto osserviamo che $E \subseteq P$ è finita, separabile ed anche normale [infatti $F^{-1}(H) \trianglelefteq G(M \,|\, E)$]. Inoltre

$$G(P \,|\, E) \cong G(M \,|\, E)/_{G(M \,|\, P)} = G(M \,|\, E)/_{F^{-1}(H)} \cong G(L \,|\, K)/_H \cong \boldsymbol{C}_p .$$

Infine $f = X^p - 1$ si spezza su E $(= \Sigma_{f,K})$. Siamo nelle ipotesi della Prop. **2** (applicata all'estensione $E \subseteq P$) e dunque $P = E(\alpha)$, con $\alpha^p \in E$, ovvero $E \subseteq P$ è radicale.

(*2*) L'estensione $P \subseteq M$ è finita, separabile e normale. Il suo gruppo di Galois $G(M \,|\, P)$ è risolubile [infatti è sottogruppo di $G(M \,|\, E)$]. Poiché

$$|G(M \,|\, P)| < |G(M \,|\, E)| = |G(L \,|\, K)| = n,$$

per ipotesi induttiva esiste un campo $R \supseteq M$ tale che $P \subseteq R$ è radicale.

Componendo le due estensioni radicali $E \subseteq P$ e $P \subseteq R$, si ottiene l'estensione radicale $E \subseteq R$, con $M \subseteq R$, come richiesto.

Resta da dimostrarne la Prop. **2**. A tale scopo è necessario premettere un altro risultato, noto come *Teorema 90 di Hilbert* [in quanto dimostrato da Hilbert nel 1890]. Tale teorema necessita a sua volta di una definizione.

Definizione 1. *Sia $K \subseteq L$ un'estensione finita e sia $G(L \,|\, K) = \{\varphi_1, \dots, \varphi_n\}$. Per ogni $\alpha \in L$ l'elemento*

$$\mathcal{N}(\alpha) := \prod_{i=1}^{n} \varphi_i(\alpha)$$

è detto norma di α. [Si tratta di un elemento di L e si osserva facilmente che $\mathcal{N}(\alpha) \in L^{G(L|K)} = K^{\sharp\flat}$. Inoltre, se $\alpha \in K$, $\mathcal{N}(\alpha) = \alpha^n$.]

Proposizione 2'. *(Teorema 90 di Hilbert) Sia $K \subseteq L$ un'estensione finita il cui gruppo di Galois $G(L \,|\, K)$ è ciclico (finito, di ordine $n \geq 1$), con generatore φ. Per ogni $\alpha \in L$, risulta:*

$$\mathcal{N}(\alpha) = 1 \iff \alpha = \tfrac{\beta}{\varphi(\beta)},\ \exists\, \beta \in L^{\cdot}.$$

Dim. (Prop. **2'**). Per ipotesi, $G(L \,|\, K) = \langle\varphi\rangle = \{\mathbf{1}, \varphi, \dots, \varphi^{n-1}\}$.

($\Longleftarrow$). Per definizione di norma,

$$\mathcal{N}(\tfrac{\beta}{\varphi(\beta)}) = \prod_{i=0}^{n-1} \varphi^i(\tfrac{\beta}{\varphi(\beta)}) = \prod_{i=0}^{n-1} \tfrac{\varphi^i(\beta)}{\varphi^{i+1}(\beta)} = \tfrac{\mathcal{N}(\beta)}{\mathcal{N}(\beta)} = 1.$$

($\Longrightarrow$). Fissato arbitrariamente $c \in L$, si definiscono in L gli n elementi

$$d_i := \alpha \cdot \varphi(\alpha) \cdot \varphi^2(\alpha) \cdot \dots \cdot \varphi^i(\alpha) \cdot \varphi^i(c), \quad \forall\, i = 0, \dots n-1.$$

In particolare, $d_0 = \alpha \cdot c$, $d_{n-1} = \mathcal{N}(\alpha) \cdot \varphi^{n-1}(c) = \varphi^{n-1}(c)$ [essendo, per ipotesi, $\mathcal{N}(\alpha) = 1$].

Si verifica con facilità che

$$d_{i+1} = \alpha \cdot \varphi(d_i), \quad \forall\, i = 0, \dots n-2.$$

Si ponga ora, $\forall\, i = 0, \dots, n-1$, $\lambda_i := \alpha \cdot \varphi(\alpha) \cdot \dots \cdot \varphi^i(\alpha)$ [in particolare $\lambda_0 = \alpha \neq 0$] e si consideri la combinazione lineare di automorfismi:

$$\sum_{i=0}^{n-1} \lambda_i \varphi^i : L \to L.$$

In base al Lemma di Dedekind (cfr. Appendice **1**), gli automorfismi $\mathbf{1}, \varphi, \dots, \varphi^{n-1}$ sono linearmente indipendenti e quindi $\sum_{i=0}^{n-1} \lambda_i \varphi^i \neq \mathbf{0}$. Pertanto esiste $c \in L$ tale che $(\sum_{i=0}^{n-1} \lambda_i \varphi^i)(c) \neq 0$. Essendo

$$(\sum_{i=0}^{n-1} \lambda_i \varphi^i)(c) = \sum_{i=0}^{n-1} d_i\,,$$

esiste in L un elemento non nullo $\beta = \sum_{i=0}^{n-1} d_i$.

Verifichiamo allora che $\varphi(\beta) = \frac{\beta}{\alpha}$ (da cui la tesi). Si ha infatti:

$$\varphi(\beta) = \varphi(\sum_{i=0}^{n-1} d_i) = \varphi(d_0) + \varphi(d_1) + \ ... \ + \varphi(d_{n-1}) = \frac{d_1}{\alpha} + \frac{d_2}{\alpha} + \ ... \ + \frac{d_{n-1}}{\alpha} + \varphi^{n-1}(c) =$$
$$= \tfrac{1}{\alpha}(d_1 + \ ... \ + d_{n-1}) + c = \tfrac{1}{\alpha}(d_0 + d_1 + \ ... \ + d_{n-1}) = \tfrac{\beta}{\alpha}.$$

Dim. (Prop. **2**). Sia $G(L \,|\, K) = \langle \varphi \rangle$ [e quindi $\varphi^p = \mathbf{1}$].

Le radici p-sime dell'unità formano, come ben noto, un gruppo ciclico di ordine p, generato da $\zeta := \zeta_p$ [con $\zeta^p = 1$]. Per ipotesi, $\zeta \in K$ e dunque $\mathcal{N}(\zeta) = \zeta^p = 1$. In base alla Prop. **2'**, esiste $\alpha \in L^{\cdot}$ tale che $\zeta = \frac{\alpha}{\varphi(\alpha)}$.

Verifichiamo che $\alpha^p \in K$. Poiché $K = K^{\sharp\flat}$, basta verificare che $\varphi^i(\alpha^p) = \alpha^p$, $\forall\, i = 0, \ ..., p-1$. Infatti, da $\varphi(\alpha) = \zeta^{-1}\alpha$ segue subito che $\varphi^i(\alpha) = \zeta^{-i}\alpha$ e dunque $\varphi^i(\alpha^p) = \zeta^{-ip}\alpha^p = \alpha^p$.

Si ponga $a := \alpha^p$ e si consideri il polinomio $g := X^p - a \in K[X]$. Gli zeri di g sono gli elementi $\zeta^i\alpha$ $(0 \leq i < p)$, tutti in $K(\alpha)$, e dunque $K(\alpha) = \Sigma_{g,K}$.

Ovviamente $K(\alpha) \subseteq L$ e dunque resta solo da verificare che $K(\alpha) = L$. L'estensione $K \subseteq L$ è finita, normale e, ovviamente, separabile. Quindi per il $TFTG\,(i)$ risulta $[L : K] = |G(L \,|\, K)| = p$. Inoltre $\alpha \notin K$, perché altrimenti avremmo $\zeta = \frac{\alpha}{\varphi(\alpha)} = \frac{\alpha}{\alpha} = 1$: assurdo. Quindi $K \subseteq K(\alpha)$ è un'estensione propria e $[K(\alpha) : K] \,|\, [L : K] = p$, da cui $[K(\alpha) : K] = p$ e quindi $K(\alpha) = L$.

SOLUZIONI DEGLI ESERCIZI

DEL CAPITOLO 1

Esercizio 1.1.1. Verificare che le seguenti sette condizioni sono equivalenti:

(i) $H \trianglelefteq G$; (ii) $aH \subseteq Ha,\ \forall\, a \in G$; (iii) $Ha \subseteq aH,\ \forall\, a \in G$;

(iv) $aHa^{-1} = H,\ \forall\, a \in G$; (v) $aHa^{-1} \subseteq H,\ \forall\, a \in G$; (vi) $aHa^{-1} \supseteq H,\ \forall\, a \in G$.

(vii) $\forall\, x, y \in G,\ xy \in H \implies yx \in H$.

Soluzione. $(i) \implies (ii)$ e $(i) \implies (iii)$ sono ovvie.

$(ii) \implies (i)$. Basta verificare che $Ha \subseteq aH,\ \forall\, a \in G$, ovvero che $ha \in aH,\ \forall\, a \in G,\ \forall\, h \in H$. Per ipotesi, $a^{-1}H \subseteq Ha^{-1}$ e dunque $a^{-1}h = h_1 a^{-1}, \exists\, h_1 \in H$. Moltiplicando a destra ed a sinistra per a si ottiene $a(a^{-1}h)a = a(h_1 a^{-1})a$, da cui $ha = ah_1 \in aH$.

$(iii) \implies (i)$ si dimostra nello stesso modo.

$(i) \iff (iv)$. Si ha: $H \trianglelefteq G \iff aH = Ha,\ \forall\, a \in G \iff aHa^{-1} = H,\ \forall\, a \in G$.

$(iv) \implies (v)$ e $(iv) \implies (vi)$ sono ovvie.

$(v) \implies (ii)$. Si ha, $\forall\, a \in G$: $aHa^{-1} \subseteq H \implies aHa^{-1}a \subseteq Ha \implies aH \subseteq Ha$.

$(vi) \implies (iii)$. Si ha, $\forall\, a \in G$: $aHa^{-1} \supseteq H \implies aHa^{-1}a \supseteq Ha \implies aH \supseteq Ha$.

$(i) \implies (vii)$. Sia $H \trianglelefteq G$ e sia $h := xy \in H$. Allora $x = hy^{-1} \in Hy^{-1} = y^{-1}H$. Dunque $x = y^{-1}h_1, \exists\, h_1 \in H$. Allora $yx = h_1 \in H$.

$(vii) \implies (ii)$. Scelto $ah \in aH$, bisogna provare che $ah \in Ha$. Si ha: $h = (a^{-1}a)h = a^{-1}(ah) \in H$. Per l'ipotesi, $(ah)a^{-1} \in H$ e dunque $\exists\, h_1 \in H$ tale che $aha^{-1} = h_1$. Allora $ah = h_1 a \in Ha$.

* * *

Esercizio 1.1.2. Sia $\mathbf{Q}$ il gruppo (delle unità) dei quarternioni (cfr. [AA] pag. 174). Verificare che il gruppo quoziente $\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle}$ è isomorfo ad un gruppo di Klein.

Soluzione. È noto che

$$\mathbf{Q} = \{\underline{\mathbf{1}}, -\underline{\mathbf{1}}, \underline{\boldsymbol{i}}, -\underline{\boldsymbol{i}}, \underline{\boldsymbol{j}}, -\underline{\boldsymbol{j}}, \underline{\boldsymbol{k}}, -\underline{\boldsymbol{k}}\},$$

con $\underline{\boldsymbol{i}}^2 = \underline{\boldsymbol{j}}^2 = \underline{\boldsymbol{k}}^2 = -\underline{\mathbf{1}},\ (-\underline{\mathbf{1}})^2 = \underline{\mathbf{1}},\ \underline{\boldsymbol{i}}\underline{\boldsymbol{j}} = \underline{\boldsymbol{k}} = -\underline{\boldsymbol{j}}\underline{\boldsymbol{i}},\ \underline{\boldsymbol{j}}\underline{\boldsymbol{k}} = \underline{\boldsymbol{i}} = -\underline{\boldsymbol{k}}\underline{\boldsymbol{j}},\ \underline{\boldsymbol{k}}\underline{\boldsymbol{i}} = \underline{\boldsymbol{j}} = -\underline{\boldsymbol{i}}\underline{\boldsymbol{k}}$.

Verifichiamo che $\langle -\underline{\mathbf{1}} \rangle = \{\underline{\mathbf{1}}, -\underline{\mathbf{1}}\}$ è normale in $\mathbf{Q}$. Si ha infatti:

$$\underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle = \{\underline{\boldsymbol{i}}, -\underline{\boldsymbol{i}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{i}}, \quad \underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle = \{\underline{\boldsymbol{j}}, -\underline{\boldsymbol{j}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{j}}, \quad \underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle = \{\underline{\boldsymbol{k}}, -\underline{\boldsymbol{k}}\} = \langle -\underline{\mathbf{1}} \rangle \underline{\boldsymbol{k}}$$

[ma tale verifica è inutile, in quanto $\langle -\underline{\mathbf{1}} \rangle$ è l'unico sottogruppo di $\mathbf{Q}$ di ordine 2].

Il gruppo quoziente è:

$$\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle} = \{\langle -\underline{\mathbf{1}} \rangle, \underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle, \underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle\}, \underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle\}.$$

Si ha: $(\underline{\boldsymbol{i}}\langle -\underline{\mathbf{1}} \rangle)^2 = (\underline{\boldsymbol{j}}\langle -\underline{\mathbf{1}} \rangle)^2 = (\underline{\boldsymbol{k}}\langle -\underline{\mathbf{1}} \rangle)^2 = \langle -\underline{\mathbf{1}} \rangle$. Dunque $\mathbf{Q}/_{\langle -\underline{\mathbf{1}} \rangle}$ ha tre elementi di periodo 2 ed è pertanto un gruppo di Klein.

* * *

Esercizio 1.1.3. Verificare che $\boldsymbol{S}_n/_{\boldsymbol{A}_n} \cong \boldsymbol{C}_2$, con $\boldsymbol{A}_n$ gruppo alterno di $\boldsymbol{S}_n$ e $\boldsymbol{C}_2$ gruppo ciclico di ordine 2.

Soluzione. $\boldsymbol{A}_n$ è il sottogruppo di $\boldsymbol{S}_n$ formato dalle permutazioni pari. Risulta:

$$(1\,2)\boldsymbol{A}_n = \boldsymbol{S}_n - \boldsymbol{A}_n$$

[infatti la moltiplicazione per $(1\,2)$ trasforma le permutazioni pari in dispari e viceversa]. Ne segue che $\boldsymbol{A}_n$ ha indice 2 e quindi è un sottogruppo normale di $\boldsymbol{S}_n$. Il gruppo quoziente

$$\boldsymbol{S}_n/_{\boldsymbol{A}_n} = \{\boldsymbol{A}_n,\, (1\,2)\boldsymbol{A}_n\}$$

è necessariamente isomorfo a $\boldsymbol{C}_2$ [in quanto unico gruppo di ordine 2, a meno di isomorfismi].

* * *

Esercizio 1.1.4. Sia $n \geq 3$ e sia $H_i = \boldsymbol{S}(\{1, 2, .., \not{i}, .., n\})$ (con $1 \leq i \leq n$). Verificare che H_i è un sottogruppo non normale di $\boldsymbol{S}_n$. Verificare che gli H_i sono a due a due coniugati.

Soluzione. Consideriamo $H_1 = \boldsymbol{S}(\{2, 3, .., n\}) < \boldsymbol{S}_n$. Si ha:

$$(1\,2)H_1(1\,2)^{-1} \ni (1\,2)(2\,3\,...\,n)(1\,2) = (1\,3\,4\,...\,n)(2).$$

Poiché $(1\,3\,4\,...\,n) \notin H_1$, allora $(1\,2)H_1(1\,2)^{-1} \not\subseteq H_1$ e dunque $H_1 \not\trianglelefteq \boldsymbol{S}_n$.

Analogamente:

$$(1\,2)H_2(1\,2)^{-1} \ni (1\,2)(1\,3\,...\,n)(1\,2) = (2\,3\,4\,...\,n) \notin H_2;$$
$$(1\,3)H_3(1\,3)^{-1} \ni (1\,3)(1\,2\,4\,...\,n)(1\,3) = (2\,4\,...\,n\,3) \notin H_3;$$

$$(1\,n)H_n(1\,n)^{-1} \ni (1\,n)(1\,2\,...\,n-1)(1\,n) = (2\,3\,...\,n-1\,n) \notin H_n.$$

Ne segue che, per $i = 1, ...\,n$, $(1\,i)H_i(1\,i)^{-1} \not\subseteq H_i$ e dunque $H_i \not\trianglelefteq \boldsymbol{S}_n$.

Per provare l'ultima affermazione verifichiamo che, per $i = 2, ...\,n$, $H_i \sim H_1$.

Calcoliamo $(1\,i)H_1(1\,i)^{-1}$. Per ogni permutazione $\sigma \in H_1$: $(1\,i)\sigma(1\,i)^{-1}$ fissa l'elemento i. Dunque $(1\,i)\sigma(1\,i)^{-1} \in H_i$ e quindi $(1\,i)H_1(1\,i)^{-1} \subseteq H_i$. Ma i due gruppi hanno lo stesso ordine e quindi coincidono. Pertanto $H_1 \sim H_i$ tramite $(1\,i)$.

* * *

Esercizio 1.1.5. Verificare che, $\forall\, n \geq 2$ $\boldsymbol{SO}_n(\boldsymbol{R}) \not\trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$ [con

$$\boldsymbol{SO}_n(\boldsymbol{R}) = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \,:\, A^{-1} = A^t \ \text{ e } \ det(A) = 1\}$$ (*gruppo ortogonale speciale*).

Soluzione. Si noti che $\boldsymbol{SO}_n(\boldsymbol{R})$ è un sottogruppo di $\boldsymbol{GL}_n(\boldsymbol{R})$. Se infatti $A, B \in \boldsymbol{SO}_n(\boldsymbol{R})$, allora $(AB^{-1})^t = (B^{-1})^t A^t = (B^t)^{-1}A^{-1} = BA^{-1} = (AB^{-1})^{-1}$. Inoltre $det(AB^{-1}) = \frac{det(A)}{det(B)} = \frac{1}{1} = 1$.

Per verificare che $\boldsymbol{SO}_n(\boldsymbol{R}) \not\trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$, basta determinare una matrice $A \in \boldsymbol{SO}_n(\boldsymbol{R})$ ed una matrice $B \in \boldsymbol{GL}_n(\boldsymbol{R})$ tali che $BAB^{-1} \notin \boldsymbol{SO}_n(\boldsymbol{R})$.

Si ponga provvisoriamente $n = 2$ e si scelgano

$$A_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\pi}{2} & -\sin\frac{\pi}{2} \\ \sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{pmatrix} \in \boldsymbol{SO}_2(\boldsymbol{R}) \ \text{ e } \ B_0 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \boldsymbol{GL}_2(\boldsymbol{R}).$$

Si ha:

$$A'_0 := B_0 A_0 B_0^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}.$$

La matrice A'_0 ottenuta non è ortogonale [infatti si verifica che $(A'_0)^{-1} \neq (A'_0)^t$].

Sia ora $n \geq 3$ e si ponga

$$A = \begin{pmatrix} I_{n-2} & \mathbf{0} \\ \mathbf{0}^t & A_0 \end{pmatrix},\ B = \begin{pmatrix} I_{n-2} & \mathbf{0} \\ \mathbf{0}^t & B_0 \end{pmatrix}$$

[si tratta di matrici quadrate di ordine n; $\mathbf{0}$ denota la matrice nulla di $n-2$ righe e 2 colonne ed I_{n-2} la matrice unità di ordine $n-2$]. Ovviamente $A \in \boldsymbol{SO}_n(\boldsymbol{R})$ e $B \in \boldsymbol{GL}_n(\boldsymbol{R})$. Come prima,

$$BAB^{-1} = \begin{pmatrix} I_{n-2} & \mathbf{0} \\ \mathbf{0}^t & A'_0 \end{pmatrix} \notin \boldsymbol{SO}_n(\boldsymbol{R}).$$

Si conclude che $\boldsymbol{SO}_n(\boldsymbol{R}) \not\trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$ [e con la stessa dimostrazione si prova che $\boldsymbol{O}_n(\boldsymbol{R}) \not\trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$].

* * *

Esercizio 1.1.6. Determinare una catena di gruppi $H < K < G$ tali che

$$H \triangleleft K, \quad K \triangleleft G, \quad \text{ma } H \not\triangleleft G.$$

Soluzione. Si consideri il gruppo diedrale $\boldsymbol{D}_4 = \langle \varphi, \rho \mid \varphi^4 = \rho^2 = 1, \ \rho\circ\varphi = \varphi^3\circ\rho \rangle$. In esso si considerino i sottogruppi

$$H = \langle \rho \rangle \text{ (gruppo ciclico di ordine 2)}, \quad K = \langle \rho, \varphi^2 \rangle \text{ (gruppo di Klein)}.$$

Poiché $(K : H) = (\boldsymbol{D}_4 : K) = 2$, allora $H \triangleleft K$, $K \triangleleft \boldsymbol{D}_4$. Proviamo che $H \not\triangleleft \boldsymbol{D}_4$. Infatti:

$$\varphi\circ\langle \rho \rangle = \{\varphi, \varphi\circ\rho\} \text{ mentre } \langle \rho \rangle\circ\varphi = \{\varphi, \varphi^3\circ\rho\}.$$

Nota. L'esempio considerato è il più semplice possibile, nel senso che è minimo rispetto all'ordine di G. Il successivo esempio più semplice si ottiene considerando nel gruppo alterno $\boldsymbol{A}_4$ (di ordine 12) la catena di sottogruppi $H := \langle (1\,2)(3\,4) \rangle < K := \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle < \boldsymbol{A}_4$

* * *

Esercizio 1.2.1. Verificare che, per ogni campo K, l'anello $K[X]$ possiede soltanto ideali principali e risulta $K[X]/_{(P)} = K[X]/_{\equiv_P}$, $\forall P \in K[X]$.

Soluzione. Sia I un ideale di $K[X]$. Se $I = \{0\}$, $I = 0K[X]$ (ideale principale). Sia quindi $I \neq \{0\}$ e si scelga in I un polinomio di grado minimo. Sia P un tale polinomio. Ovviamente $PK[X] \subseteq I$. Viceversa, $\forall F \in I$, si divida F per P:

$$F = PQ + R, \text{ con } \partial R < \partial P.$$

Poiché $R = F - PQ \in I - I \subseteq I$, allora necessariamente $R = 0$ [altrimenti sarebbe contraddetta la minimalità di ∂P in I]. Dunque $F \in PK[X]$ e pertanto $I = PK[X]$.

Si osservi infine che la classe di congruenza $[F]$ di F *mod* P coincide con $F + PK[X]$. Dunque $K[X]/_{\equiv_P} = K[X]/_{(P)}$.

* * *

Esercizio 1.2.2. Verificare che un campo possiede soltanto i due ideali banali. Viceversa, verificare che ogni anello commutativo unitario che ha solo gli ideali banali è un campo.

Soluzione. Sia K un campo ed I un suo ideale, $I \neq \{0\}$. Bisogna dimostrare che $I = K$. Allo scopo basta verificare che $1 \in I$. Infatti, scelto $x \in I^{\cdot}$, risulta: $1 = x^{-1}x \in KI \subseteq I$. Dunque $1 \in I$.

Sia A un anello commutativo unitario, privo di ideali propri. Per provare che A è un campo, basta dimostrare che $a^{-1} \in A$, $\forall a \in A^{\cdot}$. Infatti, essendo $a \neq 0$, $(a) = A$ e dunque $1 \in (a)$. Allora $1 = ab$, $\exists b \in A$ e quindi $a^{-1} = b \in A$.

* * *

Esercizio 1.2.3. Siano I, J ideali di un anello A. Verificare che l'insieme

$$I + J = \{x + y, \ \forall x \in I, \ \forall y \in J\}$$

è un ideale di A, detto *ideale somma di I e J*. Verificare che si tratta del più piccolo ideale contenente $I \cup J$, cioè $(I \cup J)$ [se A è commutativo e unitario].

Soluzione. Si tratta di verificare che:

$$(I + J) - (I + J) \subseteq I + J, \quad (I + J)A \subseteq I + J, \quad A(I + J) \subseteq I + J.$$

Infatti, $\forall x, x_1, x_2 \in I$, $\forall y, y_1, y_2 \in J$, $\forall a \in A$:

$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) \in I + J$;
$(x + y)a = xa + ya \in IA + JA \subseteq I + J$;
$a(x + y) = ax + ay \in AI + AJ \subseteq I + J$.

Si osserva subito che $I \cup J \subseteq I + J$ [infatti $\forall x \in I : \ x = x + 0 \in I + J$; $\forall y \in J : \ y = 0 + y \in I + J$].

Sia ora K un ideale di A tale che $K \supseteq I \cup J$. Per ogni $x \in I$ ed $y \in J$, allora $x, y \in K$ e quindi $x + y \in K + K \subseteq K$. Dunque $I + J \subseteq K$. Abbiamo così dimostrato che $I + J = (I \cup J)$.

* * *

Esercizio 1.2.4. Siano I, J ideali di un anello A.

(*i*) Verificare che l'insieme

$$IJ = \Big\{ \sum_{i=1}^{n} x_i y_i \,,\ \forall\, n \geq 1,\ \forall\, x_i \in I,\ \forall\, y_i \in J \Big\}$$

è un ideale di A, detto *ideale prodotto di* I *e* J.

(*ii*) Verificare che $IJ \subseteq I \cap J$.

(*iii*) Sia A commutativo unitario e sia $I + J = A$. Verificare che in tal caso risulta: $IJ = I \cap J$.

(*iv*) Determinare due ideali I, $J \subseteq \boldsymbol{Z}$ tali che $IJ \subset I \cap J$.

Soluzione. (*i*) Risulta:

$IJ - IJ \subseteq IJ$ [ovvio]; $(IJ)A \subseteq IJ$ [infatti $(\sum_{i=1}^{n} x_i y_i)a = \sum_{i=1}^{n} x_i (y_i a) \in IJ$];

$A(IJ) \subseteq IJ$ [infatti $a(\sum_{i=1}^{n} x_i y_i)a = \sum_{i=1}^{n} (a x_i) y_i \in IJ$].

(*ii*) Sia $\sum_{i=1}^{n} x_i y_i \in IJ$. Si ha: $x_i y_i \in IA \cap AJ \subseteq I \cap J$. Dunque $\sum_{i=1}^{n} x_i y_i \in I \cap J$. Pertanto $IJ \subseteq I \cap J$.

(*iii*) Sia $1 = r + s$, con $r \in I$, $s \in J$. Per ogni $x \in I \cap J$: $x = x1 = xr + xs$. Si ha: $xr \in JI = IJ$, $xs \in IJ$. Dunque $x = xr + xs \in IJ + IJ \subseteq IJ$. Pertanto $I \cap J \subseteq IJ$. Da (*ii*), $I \cap J = IJ$.

(*iv*) Si ponga ad esempio $I = 4\boldsymbol{Z}$, $J = 6\boldsymbol{Z}$. Verifichiamo che $IJ = 24\boldsymbol{Z}$ mentre $I \cap J = 12\boldsymbol{Z}$ (e dunque $IJ \subset I \cap J$).

Si ha: $24 = 4 \cdot 6 \in IJ$ e dunque $24\boldsymbol{Z} \subseteq IJ$. Viceversa, $\forall\, x = \sum 4 t_i 6 s_i \in IJ$, risulta $x = 24(\sum t_i s_i) \in 24\boldsymbol{Z}$. Dunque $IJ \subseteq 24\boldsymbol{Z}$.

Si ha: $12 \in I \cap J$ e dunque $12\boldsymbol{Z} \subseteq I \cap J$. Viceversa, sia $x \in I \cap J$. Allora $x = 4n = 6m$. Poiché $3 \,|\, 4n$ e $MCD(3, 4) = 1$, allora $3 \,|\, n$ e quindi $n = 3r$, da cui $x = 12r \in 12\boldsymbol{Z}$. Dunque $I \cap J \subseteq 12\boldsymbol{Z}$.

* * *

Esercizio 1.2.5. Sia I il sottoinsieme di $\boldsymbol{Z}[X]$ formato dai polinomi a termine noto pari. Verificare che I è un ideale non principale di $\boldsymbol{Z}[X]$.

Soluzione. Verifichiamo che I è un ideale di $\boldsymbol{Z}[X]$:

$I - I \subseteq I$. Infatti, $\forall\, f, g \in I$, con $f = 2a + X f_1$, $g = 2b + X g_1$, $a, b \in \boldsymbol{Z}$, $f_1, g_1 \in \boldsymbol{Z}[X]$, allora $f - g = 2(a - b) + X(f_1 - g_1) \in I$.

$I \cdot \boldsymbol{Z}[X] \subseteq I$. Infatti, $\forall\, f = 2a + X f_1 \in I$, $g \in \boldsymbol{Z}[X]$, risulta $fg = 2a\, g(0) + X(\,\ldots\,) \in I$.

Per assurdo, I sia un ideale principale, con generatore $h \in \boldsymbol{Z}[X]^{\cdot}$. Poiché $2 \in I$, allora $2 = hf$, $\exists\, f \in \boldsymbol{Z}[X]$. Ne segue che $\partial h = 0$, cioè $h \in \boldsymbol{Z}^{\cdot}$. Poiché $\pm 1 \notin I$ allora $h \neq \pm 1$. Infine, poiché $X \in I$, allora $X = hg$, $\exists\, g \in \boldsymbol{Z}[X]$ e $h \neq 0, \pm 1$. Ma allora X non sarebbe primitivo: assurdo.

* * *

Esercizio 1.2.6. Sia $\mathcal{F}$ l'insieme delle funzioni continue da $\boldsymbol{R}$ a $\boldsymbol{R}$.

(*i*) Verificare che $(\mathcal{F}, +, \cdot)$ è un anello commutativo unitario rispetto alle due seguenti operazioni:

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x) \cdot g(x), \ \forall\, f, g \in \mathcal{F}, \ \forall\, x \in \boldsymbol{R}.$$

(*ii*) Si ponga: $\mathcal{I}_0 = \{f \in \mathcal{F} \mid f(0) = 0\}$, $\mathcal{I}_1 = \{f \in \mathcal{F} \mid f(1) = 0\}$, $\mathcal{I} = \mathcal{I}_0 \cap \mathcal{I}_1$. Verificare che $\mathcal{I}$ è un ideale di $\mathcal{F}$ e che l'anello $\mathcal{F}/_{\mathcal{I}}$ è non integro (cfr. [AA], Def. **8**, pag. 22).

Soluzione. (*i*) Dal Calcolo è noto che la somma ed il prodotto di funzioni continue sono funzioni continue. L'applicazione costante nulla è elemento neutro della somma e l'applicazione costante di valore 1 è elemento neutro del prodotto. Inoltre $-f$ è continua ed è l'opposta di f. Infine $fg = gf$ e valgono le proprietà associative e distributive. Dunque $\mathcal{F}$ è un anello commutativo unitario.

(*ii*) Si ha: $\mathcal{I} = \{f \in \mathcal{F} \mid f(0) = f(1) = 0\}$. Risulta:

$\mathcal{I} - \mathcal{I} \subseteq \mathcal{I}$ [infatti, se $f(0) = f(1) = 0, g(0) = g(1) = 0$, allora $(f-g)(0) = 0 = (f-g)(1)$];

$\mathcal{I}\mathcal{F} \subseteq \mathcal{I}$ [infatti, se $f(0) = f(1) = 0$, $g \in \mathcal{F}$, allora $(fg)(0) = 0\,g(0) = 0$, $(fg)(1) = 0\,g(1) = 0$].

Analogamente, $\mathcal{F}\mathcal{I} \subseteq \mathcal{I}$. Dunque $\mathcal{I}$ è un ideale di $\mathcal{F}$.

Si scelgano in $\mathcal{F}$ le funzioni $f(x) = x$, $g(x) = x - 1$. Risulta subito $(fg)(0) = (fg)(1) = 0$ e dunque $fg \in \mathcal{I}$. Ma $f(1) \neq 0$, $g(0) \neq 0$ e dunque $f, g \notin \mathcal{I}$. Quindi

$$f + \mathcal{I} \neq \mathcal{I},\ g + \mathcal{I} \neq \mathcal{I} \text{ e } fg + \mathcal{I} = \mathcal{I}.$$

I due elementi $f + \mathcal{I}$, $g + \mathcal{I}$ sono zero-divisori di $\mathcal{F}/_{\mathcal{I}}$.

* * *

Esercizio 1.3.1. Verificare che $\boldsymbol{GL}_n(\boldsymbol{R})/_{\boldsymbol{SL}_n(\boldsymbol{R})} \cong (\boldsymbol{R}^{\cdot}, \cdot)$ [dove $\boldsymbol{SL}_n(\boldsymbol{R})$ è il gruppo delle matrici quadrate di ordine n, a valori in $\boldsymbol{R}$ e a determinante $= 1$].

Soluzione. Utilizzando il *TFO*, basta determinare un omomorfismo suriettivo da $\boldsymbol{GL}_n(\boldsymbol{R})$ a $\boldsymbol{R}^{\cdot}$, il cui nucleo sia $\boldsymbol{SL}_n(\boldsymbol{R})$. Si definisce l'applicazione

$$det : \boldsymbol{GL}_n(\boldsymbol{R}) \to \boldsymbol{R}^{\cdot} \text{ tale che } det : A \to det(A),\ \forall\, A \in \boldsymbol{GL}_n(\boldsymbol{R}).$$

det è un omomorfismo di gruppi. Infatti, per il teorema di Binet:

$$det(AB) = det(A)\, det(B),\ \forall\, A, B \in \boldsymbol{GL}_n(\boldsymbol{R}).$$

L'omomorfismo *det* è suriettivo. Infatti, $\forall\, a \in \boldsymbol{R}^{\cdot}$, risulta:

$$det \begin{pmatrix} a & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = a.$$

Infine $Ker(det) = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) = 1\} = \boldsymbol{SL}_n(\boldsymbol{R})$.

* * *

Esercizio 1.3.2. Sia $\boldsymbol{\mathcal{H}} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) \in \boldsymbol{Q}^{\cdot}\}$.

(*i*) Verificare che $\boldsymbol{\mathcal{H}} \trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$.

(*ii*) Verificare che $\boldsymbol{GL}_n(\boldsymbol{R})/_{\boldsymbol{\mathcal{H}}} \cong \boldsymbol{R}^{\cdot}/_{\boldsymbol{Q}^{\cdot}}$.

Soluzione. (*i*) Verifichiamo che $\boldsymbol{\mathcal{H}}$ è un sottogruppo di $\boldsymbol{GL}_n(\boldsymbol{R})$. Risulta, $\forall\, A, B \in \boldsymbol{\mathcal{H}}$:

$$det(AB^{-1}) = \tfrac{det(A)}{det(B)} \in \boldsymbol{Q}^{\cdot} \text{ [in quanto } det(A), det(B) \in \boldsymbol{Q}^{\cdot}].$$

Dunque $AB^{-1} \in \boldsymbol{\mathcal{H}}$.

Verifichiamo che $\boldsymbol{\mathcal{H}} \trianglelefteq \boldsymbol{GL}_n(\boldsymbol{R})$, cioè che $A\boldsymbol{\mathcal{H}}A^{-1} \subseteq \boldsymbol{\mathcal{H}}$, $\forall\, A \in \boldsymbol{GL}_n(\boldsymbol{R})$. Infatti, $\forall\, B \in \boldsymbol{\mathcal{H}}$:

$$det(ABA^{-1}) = det(A)\, det(B)\, det(A)^{-1} = det(B) \in \boldsymbol{Q}^{\cdot}.$$

Dunque $ABA^{-1} \in \boldsymbol{\mathcal{H}}$.

(*ii*) Sia $f : \boldsymbol{GL}_n(\boldsymbol{R}) \to \boldsymbol{R}^{\cdot}/_{\boldsymbol{Q}^{\cdot}}$ la composizione delle due applicazioni

$$det : \boldsymbol{GL}_n(\boldsymbol{R}) \to \boldsymbol{R}^{\cdot} \mid A \to det(A); \qquad \pi : \boldsymbol{R}^{\cdot} \to \boldsymbol{R}^{\cdot}/_{\boldsymbol{Q}^{\cdot}} \text{ (proiezione canonica).}$$

Dunque $f(A) = det(A)\boldsymbol{Q}^{\cdot}$, $\forall\, A \in \boldsymbol{GL}_n(\boldsymbol{R})$. f è un omomorfismo suriettivo (perché *det*, π lo sono). Si ha infine:

$$Ker f = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid f(A) \in \boldsymbol{Q}^{\cdot}\} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A)\boldsymbol{Q}^{\cdot} = \boldsymbol{Q}^{\cdot}\} =$$
$$= \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) \in \boldsymbol{Q}^{\cdot}\} = \boldsymbol{\mathcal{H}}.$$

Applicando ad f il *TFO* si conclude.

* * *

Esercizio 1.3.3. In $\boldsymbol{GL}_n(\boldsymbol{R})$ si consideri il sottoinsieme $\boldsymbol{\mathcal{K}} = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \mid det(A) > 0\}$.
(*i*) Verificare che $\boldsymbol{\mathcal{K}}$ è un sottogruppo normale di $\boldsymbol{GL}_n(\boldsymbol{R})$.
(*ii*) Determinare il gruppo $\boldsymbol{GL}_n(\boldsymbol{R})/_{\boldsymbol{\mathcal{K}}}$.

Soluzione. (*i*) $\boldsymbol{\mathcal{K}}$ è un sottogruppo di $G = \boldsymbol{GL}_n(\boldsymbol{R})$. Infatti, $\forall\, A, B \in \boldsymbol{\mathcal{K}}$, $det(AB^{-1}) = \frac{det(A)}{det(B)} > 0$ e quindi $AB^{-1} \in \boldsymbol{\mathcal{K}}$. Per provare che $\boldsymbol{\mathcal{K}} \triangleleft G$, basta verificare che, $\forall\, A \in G$ risulta: $A\boldsymbol{\mathcal{K}}A^{-1} \subseteq \boldsymbol{\mathcal{K}}$. Infatti, $\forall\, B \in \boldsymbol{\mathcal{K}}$:

$$det(ABA^{-1}) = det(A)\, det(B)\, \tfrac{1}{det(A)} = det(B) > 0.$$

(*ii*) Si consideri l'applicazone

$$f : G \to \boldsymbol{C}_2 \text{ tale che } f(A) = \begin{cases} +1, \text{ se } det(A) > 0 \\ -1, \text{ se } det(A) < 0. \end{cases}$$

Si ha: $f(AB) = \begin{cases} +1, \text{ se } det(A)\, det(B) > 0 \\ -1, \text{ se } det(A)\, det(B) < 0 \end{cases}$
$= \begin{cases} +1, \text{ se } det(A),\, det(B) \text{ hanno lo stesso segno} \\ -1, \text{ se } det(A),\, det(B) \text{ hanno segno opposto} \end{cases}$
$= f(A)f(B).$

Dunque f è un omomorfismo di gruppi. Risulta infine:

$$Ker f = \{A \in G \;\big|\; det(A) > 0\} = \boldsymbol{\mathcal{K}}.$$

Applicando ad f il *TFO*, si conclude che $G/_{\boldsymbol{\mathcal{K}}} \cong \boldsymbol{C}_2$.

* * *

Esercizio 1.3.4. Dimostrare che $(\boldsymbol{R}, +)/_{(\boldsymbol{Z},+)}$ è isomorfo al sottogruppo moltiplicativo dei complessi di norma 1.

Soluzione. Sia $U = \{z \in \boldsymbol{C} :\ |z| = 1\}$. $(U, \cdot)$ è un sottogruppo di $(\boldsymbol{C}^{\cdot}, \cdot)$ [infatti, se $|z| = |w| = 1$, allora $|\frac{z}{w}| = \frac{|z|}{|w|} = 1$]. Si ponga:

$$\varphi : (\boldsymbol{R}, +) \to (U, \cdot) \text{ tale che } \varphi(t) = \cos 2\pi t + i \sin 2\pi t,\ \forall\, t \in \boldsymbol{R}.$$

Risulta, in base alle formule di addizione di seno e coseno, $\forall\, t, s \in \boldsymbol{R}$:

$$\varphi(t+s) = \cos(2\pi t + 2\pi s) + i \sin(2\pi t + 2\pi s) = (\cos 2\pi t + i \sin 2\pi t)(\cos 2\pi s + i \sin 2\pi s) = \varphi(t)\varphi(s).$$

Dunque φ è un omomorfismo di gruppi. Inoltre è suriettivo [se infatti $z = a + ib \in U$, risulta $z = \varphi(\frac{1}{2\pi} \arccos a)$]. Si ha infine:

$$Ker\varphi = \{t \in \boldsymbol{R} :\ \cos 2\pi t = 1,\, \sin 2\pi t = 0\} = \boldsymbol{Z}.$$

Applicando a φ il *TFO*, $U \cong \boldsymbol{R}/_{\boldsymbol{Z}}$, come richiesto.

* * *

Esercizio 1.3.5. (*i*) Esprimere il gruppo $\boldsymbol{SO}_2(\boldsymbol{R})$ come quoziente di $(\boldsymbol{R}, +)$.
(*ii*) Sia $C_2 = \langle -I_2 \rangle$. Verificare che $C_2 \trianglelefteq \boldsymbol{SO}_2(\boldsymbol{R})$ ed esprimere $\boldsymbol{SO}_2(\boldsymbol{R})/_{C_2}$ come quoziente di $(\boldsymbol{R}, +)$.

Soluzione. (*i*) È noto dai corsi di Algebra Lineare che

$$\boldsymbol{SO}_2(\boldsymbol{R}) = \Big\{ \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix},\ \forall\, t \in \boldsymbol{R} \Big\}.$$

Si ponga:

$$\varphi : \boldsymbol{R} \to \boldsymbol{SO}_2(\boldsymbol{R}) \text{ tale che } \varphi(t) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix},\ \forall\, t \in \boldsymbol{R}.$$

Dalle formule di addizione del seno e del coseno segue che φ è un omomorfismo. Inoltre φ è suriettivo e si ha:

$$Ker\varphi = \{t \in \boldsymbol{R} \mid \cos t = 1, \sin t = 0\} = \{2k\pi, \ \forall\, k \in \boldsymbol{Z}\} = 2\pi\boldsymbol{Z}.$$

Dal *TFO*, $\boldsymbol{SO}_2(\boldsymbol{R}) \cong \boldsymbol{R}/_{2\pi\boldsymbol{Z}}$.

(*ii*) Si ha: $-I_2 = \varphi(\pi) \in \boldsymbol{SO}_2(\boldsymbol{R})$. Inoltre $(-I_2)^2 = I_2$ e dunque C_2 è un gruppo ciclico di ordine 2. Si noti inoltre che $-I_2$ commuta con ogni matrice quadrata di ordine 2. Ne segue che, $\forall\, A \in \boldsymbol{SO}_2(\boldsymbol{R})$, $AC_2 = C_2 A$. Dunque $C_2 \trianglelefteq \boldsymbol{SO}_2(\boldsymbol{R})$.

Sia $\tilde{\varphi} = \pi \circ \varphi : \boldsymbol{R} \to \boldsymbol{SO}_2(\boldsymbol{R}) \to \boldsymbol{SO}_2(\boldsymbol{R})/_{C_2}$. Tale omomorfismo è suriettivo e

$$Ker\tilde{\varphi} = \{t \in \boldsymbol{R} \mid \cos t = \pm 1, \sin t = 0\} = \pi\boldsymbol{Z}.$$

Dunque $\boldsymbol{SO}_2(\boldsymbol{R})/_{C_2} \cong \boldsymbol{R}/_{\pi\boldsymbol{Z}}$.

* * *

Esercizio 1.3.6. Sia A un anello commutativo. Verificare che gli anelli $A[X,Y]/_{(Y)}$ e $A[X]$ sono isomorfi.

Soluzione. Sia

$$\varphi : A[X,Y] \to A[X] \ \text{ tale che } \ \varphi(P) = P(X,0), \ \forall\, P \in A[X,Y].$$

Si noti che, se $P = \sum_{i+j=0}^{n} a_{ij} X^i Y^j$, allora $\varphi(P) = \sum_{i=0}^{n} a_{i0} X^i$. È evidente che φ è suriettiva [infatti, $\forall\, f \in A[X]$, risulta $\varphi(f) = f$]. Proviamo che φ è un omomorfismo di anelli, cioè:

$$\varphi(P+Q) = \varphi(P) + \varphi(Q), \quad \varphi(PQ) = \varphi(P)\varphi(Q), \ \forall\, P, Q \in A[X,Y].$$

Posto $P = \sum_{i+j=0}^{n} a_{ij} X^i Y^j$, $Q = \sum_{h+k=0}^{m} b_{hk} X^h Y^k$, allora

$$P+Q = \sum_{r+s=0}^{max(n,m)} (a_{rs} + b_{rs}) X^r Y^s, \quad PQ = \sum_{h+k=0}^{m} b_{hk} \big(\sum_{i+j=0}^{n} a_{ij} X^i Y^j \big) X^h Y^k.$$

Quindi:

$$\varphi(P+Q) = \sum_{r=0}^{max(n,m)} (a_{r0} + b_{r0}) X^r = \sum_{i=0}^{n} a_{i0} X^i + \sum_{h=0}^{m} b_{h0} X^h = \varphi(P) + \varphi(Q);$$

$$\varphi(PQ) = \sum_{h=0}^{m} b_{h0} \big(\sum_{i=0}^{n} a_{i0} X^i \big) X^h = \big(\sum_{h=0}^{m} b_{h0} X^h \big) \big(\sum_{i=0}^{n} a_{i0} X^i \big) = \varphi(P)\varphi(Q).$$

Risulta infine:

$$Ker\varphi = \{P \in A[X,Y] : \ P(X,0) = 0\} = \{P \in A[X,Y] : \ Y \,\big|\, P\} = (Y).$$

Dal *TFO* si conclude.

* * *

Esercizio 1.3.7. Verificare che $\boldsymbol{Z}[X,Y]/_{(XY)}$ è isomorfo ad un sottoanello B di $\boldsymbol{Z}[X] \times \boldsymbol{Z}[Y]$. Individuare B come immagine di un opportuno omomorfismo.

Soluzione. Si ponga:

$$\varphi : \boldsymbol{Z}[X,Y] \to \boldsymbol{Z}[X] \times \boldsymbol{Z}[Y] \ \text{ tale che } \ \varphi(P) = \big(P(X,0), P(0,Y)\big), \ \forall\, P \in \boldsymbol{Z}[X,Y].$$

Si noti che φ è un omomorfismo di anelli, in quanto lo sono le sue due componenti:

$$\varphi_1 : \boldsymbol{Z}[X,Y] \to \boldsymbol{Z}[X] \ \big| \ P \to P(X,0), \quad \varphi_2 : \boldsymbol{Z}[X,Y] \to \boldsymbol{Z}[Y] \ \big| \ P \to P(0,Y)$$

(cfr. esercizio precedente). Verifichiamo che $Ker\varphi = (XY)$.

Certo $XY \in Ker\varphi$ e dunque $(XY) \subseteq Ker\varphi$. Viceversa, sia $P \in Ker\varphi$. Allora $P(X,0) = 0 = P(0,Y)$ e quindi $X \,\big|\, P$ e $Y \,\big|\, P$, cioè $P = XQ_1 = YQ_2$, per opportuni $Q_1, Q_2 \in \boldsymbol{Z}[X,Y]$. Accettiamo come evidente il fatto che $\boldsymbol{Z}[X,Y]$ è un *UFD* (cfr. Cap. **3** Teor. **3.1**) e che X è irriducibile in $\boldsymbol{Z}[X,Y]$. Poiché $X \not| Y$, allora $X \,\big|\, Q_2$, cioè $Q_2 = XQ_3$, $\exists\, Q_3 \in \boldsymbol{Z}[X,Y]$. Allora $P = XYQ_3 \in (XY)$.

Per rispondere all'ultima domanda, basta determinare $Im\varphi$.
Si osservi che, $\forall\, P = \sum a_{ij} X^i Y^j \in \boldsymbol{Z}[X,Y]$,

$$\varphi(P) = (a_{00} + Xf_1,\, a_{00} + Yg_1),\ \text{ con }\ f_1 \in \boldsymbol{Z}[X],\ g_1 \in \boldsymbol{Z}[Y].$$

Tale fatto suggerisce di considerare in $\boldsymbol{Z}[X]\times\boldsymbol{Z}[Y]$ il sottoinsieme

$$B := \Delta_{\boldsymbol{Z}} + (X\boldsymbol{Z}[X] \times Y\boldsymbol{Z}[Y]),\ \text{ con }\ \Delta_{\boldsymbol{Z}} = \{(a,a),\ \forall\, a \in \boldsymbol{Z}\}.$$

Si verifica facilmente che B è un sottoanello di $\boldsymbol{Z}[X]\times\boldsymbol{Z}[Y]$ [infatti $B - B \subseteq B,\ BB \subseteq B$]. Per quanto sopra osservato, $Im\varphi \subseteq B$. Viceversa, $\forall\,(a,a) + (Xf_1, Yg_1) \in B$, risulta:

$$\varphi(a + Xf_1 + Yg_1) = (a + Xf_1, a + Yg_1) = (a,a) + (Xf_1, Yg_1).$$

Dunque $B \subseteq Im\varphi$ e si conclude che $B = Im\varphi$ è il sottoanello cercato.

* * *

Esercizio 1.3.8. Fissato un intero non nullo b, si denoti con $(\boldsymbol{Z})_b$ il sottoinsieme di $\boldsymbol{Q}$ così definito:

$$(\boldsymbol{Z})_b := \big\{ \tfrac{a}{b^k},\ \forall\, a \in \boldsymbol{Z},\ \forall\, k \in \boldsymbol{N} \big\}.$$

(*i*) Verificare che $(\boldsymbol{Z})_b$ è un anello contenente $\boldsymbol{Z}$.

(*ii*) Dimostrare che $(\boldsymbol{Z})_b \cong \boldsymbol{Z}[X]\big/_{(bX-1)}$.

Soluzione. Per comodità di notazioni, poniamo $B = (\boldsymbol{Z})_b$.

(*i*) Verifichiamo che B è un anello. Si ha:

$$B - B \subseteq B \ \text{ [infatti } \tfrac{a}{b^k} - \tfrac{a'}{b^h} = \tfrac{ab^h - a'b^k}{b^{h+k}} \in B\text{]}; \qquad B\,B \subseteq B \ \text{ [infatti } \tfrac{a}{b^k} \cdot \tfrac{a'}{b^h} = \tfrac{aa'}{b^{h+k}} \in B\text{]}.$$

Per provare che $\boldsymbol{Z} \subseteq B$ occorre verificare che l'applicazione $f : \boldsymbol{Z} \to B$ tale che $f(a) = \frac{a}{1},\ \forall\, a \in \boldsymbol{Z}$ è un omomorfismo iniettivo. Che sia un omomorfismo è evidente. Se poi $\frac{a}{1} = \frac{a'}{1}$ allora $a = a'$. Dunque f è iniettiva.

(*ii*) Si ponga:

$$\varphi : \boldsymbol{Z}[X] \to B \ \text{ tale che } \ \varphi(P) = P(\tfrac{1}{b}),\ \forall\, P \in \boldsymbol{Z}[X].$$

φ è un omomorfismo di anelli. Infatti, $\forall\, P, Q \in \boldsymbol{Z}[X]$:

$$\varphi(P+Q) = (P+Q)(\tfrac{1}{b}) = P(\tfrac{1}{b}) + Q(\tfrac{1}{b}) = \varphi(P) + \varphi(Q) \quad \text{e}$$
$$\varphi(PQ) = (PQ)(\tfrac{1}{b}) = P(\tfrac{1}{b}) \cdot Q(\tfrac{1}{b}) = \varphi(P)\,\varphi(Q).$$

φ è suriettivo [infatti $\frac{a}{b^k} = \varphi(aX^k)$]. Ovviamente $bX - 1 \in Ker\varphi$. Viceversa, vogliamo provare che $Ker\varphi \subseteq (bX-1)$ [e da ciò segue la tesi, applicando il *TFO* a φ].

Per ogni $P = \sum_{i=0}^{n} a_i X^i \in \boldsymbol{Z}[X]$, poniamo $\tilde{P} = \sum_{i=0}^{n} a_{n-i} X^i \in \boldsymbol{Z}[X]$. Ovviamente $\tilde{\tilde{P}} = P$. Inoltre risulta $\tilde{PQ} = \tilde{P}\,\tilde{Q}$. Proviamo tale affermazione. Sia infatti $P = \sum_{i=0}^{n} a_i X^i,\ Q = \sum_{j=0}^{m} a_j X^j$. Allora:

$$\begin{aligned}\tilde{PQ} &= \tilde{}\,[a_0b_0 + (a_0b_1 + a_1b_0)X + \,...\, + (a_nb_{m-1} + a_{n-1}b_m)X^{n+m-1} + a_nb_mX^{n+m}] = \\ &= a_nb_m + (a_nb_{m-1} + a_{n-1}b_m)X + \,...\, + (a_0b_1 + a_1b_0)X^{n+m-1} + a_0b_0X^{n+m} = \\ &= (a_n + a_{n-1}X + \,...\, + a_0X^n)(b_m + b_{m-1}X + \,...\, + b_0X^m) = \tilde{P}\,\tilde{Q}.\end{aligned}$$

Verifichiamo ora che, $\forall\, P = \sum_{i=0}^{n} a_i X^i \in Ker\varphi$, risulta $P \in (bX-1)$. Infatti:

$$\begin{aligned}P(\tfrac{1}{b}) = 0 \implies \sum_{i=0}^{n} a_i \tfrac{1}{b^i} = 0 \implies \tfrac{1}{b^n}\big(\sum_{i=0}^{n} a_i b^{n-i}\big) = 0 \implies \tfrac{1}{b^n}\big(\sum_{i=0}^{n} a_{n-i} b^{i}\big) = 0 \implies \\ \implies \sum_{i=0}^{n} a_{n-i} b^i = 0 \implies \tilde{P}(b) = 0 \implies X - b \,\big|\, \tilde{P} \implies \tilde{P} = (X-b)G,\ \exists\, G \in \boldsymbol{Z}[X] \implies \\ \implies P = \tilde{\tilde{P}} = \tilde{(X-b)}\,\tilde{G} \implies P = (1-bX)\tilde{G} = (bX-1)(-\tilde{G}) \in (bX-1).\end{aligned}$$

Dunque $Ker\varphi = (bX-1)$, come richiesto.

Nota. L'esercizio può essere risolto anche in ipotesi più generali, sostituendo cioè l'anello $\boldsymbol{Z}$ con un anello commutativo unitario A e l'intero b con un elemento non zero-divisore di A. In tal caso

l'insieme $(A)_b = \left\{\frac{a}{b^k},\ \forall a \in A,\ \forall k \in \boldsymbol{N}\right\}$ è un anello in quanto l'insieme $\{b^k,\ \forall k \in \boldsymbol{N}\}$ è una *parte moltiplicativa di* A (cfr. Cap. **3.2**).

* * *

Esercizio 1.3.9. Siano A, B due anelli e sia $A\times B$ il loro prodotto diretto. Sia I un ideale di A. Verificare che $I\times B$ è un ideale di $A\times B$ e calcolare il quoziente $A\times B/_{I\times B}$.

Soluzione. Per provare che $I\times B$ è un ideale di $A\times B$ bisogna verificare che
$(I\times B)-(I\times B)\subseteq I\times B$ [infatti $I-I\subseteq I$];
$(I\times B)(A\times B)\subseteq I\times B$ [infatti $IA\subseteq I$];
$(A\times B)-(I\times B)\subseteq I\times B$ [infatti $AI\subseteq I$].

Si denoti con $f: A\times B\to A/_I$ la composizione dei due omomorfismi suriettivi:

$$p_1: A\times B\to A \text{ tale che } p_1((a,b))=a; \quad \pi: A\to A/_I \text{ tale che } \pi(a)=a+I.$$

f è un omomorfismo suriettivo e risulta: $f((a,b))=a+I,\ \forall (a,b)\in A\times B$. Si ha:

$$Kerf=\{(a,b)\in A\times B \mid a+I=I\}=\{(a,b)\in A\times B \mid a\in I\}=I\times B.$$

Dal *TFO* si conclude che $A\times B/_{I\times B}\cong A/_I$.

* * *

Esercizio 1.3.10. Sia $f: A\to B$ un omomorfismo di anelli. Sia J un ideale di B e sia $I=f^{-1}(J)$.
(*i*) Verificare che I è nucleo di un omomorfismo.
(*ii*) Dimostrare che $A/_I$ è isomorfo ad un sottoanello di $B/_J$
(*iii*) Cosa avviene se f è suriettivo?.

Soluzione. (*i*) Già è noto da Osserv. **2.5** che $I=f^{-1}(J)$ è un ideale di A. Per dimostrare che I è nucleo di un omomorfismo, si ponga:

$$\varphi=\pi\circ f: A\to B\to B/_J.$$

φ è un omomorfismo di anelli e risulta:

$$Ker\varphi=\{a\in A \mid f(a)+J=J\}=\{a\in A \mid f(a)\in J\}=f^{-1}(J)=I.$$

Dunque $I=Ker\varphi$.

(*ii*) Dal *TFO* applicato a φ, esiste un isomorfismo da $A/_I$ a $Im\varphi$, sottoanello di $B/_J$.

(*iii*) Se f è suriettiva, anche φ lo è e quindi $A/_I\cong B/_J$.

* * *

Esercizio 1.4.1. Siano $n, m\in \boldsymbol{Z}$ e siano $d=MCD(n,m)$, $h=mcm(n,m)$. Applicando il secondo teorema di isomorfismo, dimostrare che $d\boldsymbol{Z}/_{n\boldsymbol{Z}}\cong m\boldsymbol{Z}/_{h\boldsymbol{Z}}$.

Soluzione. Applichiamo il secondo teorema di isomorfismo ai sottogruppi additivi $n\boldsymbol{Z}$, $m\boldsymbol{Z}$ di $(\boldsymbol{Z},+)$ [ma si può anche applicare il secondo teorema di isomorfismo (per gli anelli) agli ideali $n\boldsymbol{Z}$, $m\boldsymbol{Z}$ dell'anello $\boldsymbol{Z}$]. Si ha:

$$(n\boldsymbol{Z}+m\boldsymbol{Z})/_{n\boldsymbol{Z}}\cong m\boldsymbol{Z}/_{(n\boldsymbol{Z}\cap m\boldsymbol{Z})}.$$

Per concludere, bisogna verificare che

$$n\boldsymbol{Z}+m\boldsymbol{Z}=d\boldsymbol{Z},\ \text{con } d=MCD(n,m); \quad n\boldsymbol{Z}\cap m\boldsymbol{Z}=h\boldsymbol{Z},\ \text{con } h=mcm(n,m).$$

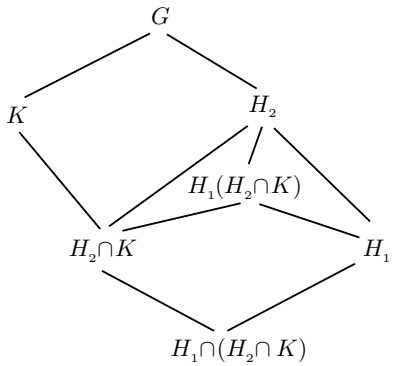
Poiché $d\,\Big|\begin{matrix}n\\m\end{matrix}$ allora $\begin{matrix}d\boldsymbol{Z}\supseteq n\boldsymbol{Z}\\ d\boldsymbol{Z}\supseteq m\boldsymbol{Z}\end{matrix}$ e quindi $d\boldsymbol{Z}\supseteq n\boldsymbol{Z}+m\boldsymbol{Z}$. Viceversa, risulta: $d=nx+my$ (identità di Bézout), da cui $d\boldsymbol{Z}\subseteq n\boldsymbol{Z}+m\boldsymbol{Z}$.

Poiché $\begin{matrix} n \\ m \end{matrix} \Big| h$ allora $\begin{matrix} n\boldsymbol{Z} \supseteq h\boldsymbol{Z} \\ m\boldsymbol{Z} \supseteq h\boldsymbol{Z} \end{matrix}$ e quindi $n\boldsymbol{Z} \cap m\boldsymbol{Z} \supseteq h\boldsymbol{Z}$. Viceversa, sia $x \in n\boldsymbol{Z} \cap m\boldsymbol{Z}$, cioè $x = na = mb, \exists\, a, b \in \boldsymbol{Z}$. Allora $\begin{matrix} n \\ m \end{matrix} \Big| x$ e quindi, per definizione di mcm, $h \,|\, x$, cioè $x \in h\boldsymbol{Z}$. Pertanto $n\boldsymbol{Z} \cap m\boldsymbol{Z} \subseteq h\boldsymbol{Z}$.

* * *

Esercizio 1.4.2. Siano $H_1 \trianglelefteq H_2 \leq G$ e $K \leq G$. Verificare che $H_1 \cap K \trianglelefteq H_2 \cap K$.

Soluzione. Poiché $H_1 \trianglelefteq H_2$, è possibile applicare il secondo teorema di isomorfismo ai sottogruppi H_1, $H_2 \cap K$ di H_2.



Tenuto conto che $H_1 \cap (H_2 \cap K) = H_1 \cap K$, si ottiene:

$$H_1(H_2 \cap K)\big/_{H_1} \cong (H_2 \cap K)\big/_{H_1 \cap (H_2 \cap K)} = (H_2 \cap K)\big/_{(H_1 \cap K)}.$$

Ne segue che $H_1 \cap K \trianglelefteq H_2 \cap K$.

* * *

Esercizio 1.4.3. Utilizzando il terzo teorema di isomorfismo, determinare un isomorfismo tra il gruppo additivo $(\boldsymbol{Z}_{12}, +)$ ed un opportuno quoziente di $(\boldsymbol{Z}_{60}, +)$. Esplicitare un siffatto isomorfismo.

Soluzione. Si ha: $60\boldsymbol{Z} \subset 12\boldsymbol{Z} \subset \boldsymbol{Z}$. Applicando il terzo teorema di isomorfismo:

$$\boldsymbol{Z}_{12} = \boldsymbol{Z}\big/_{12\boldsymbol{Z}} \cong \frac{\boldsymbol{Z}\big/_{60\boldsymbol{Z}}}{12\boldsymbol{Z}\big/_{60\boldsymbol{Z}}} = \boldsymbol{Z}_{60}\big/_{\langle \overline{12} \rangle},$$

con $\langle \overline{12} \rangle = \overline{12}\boldsymbol{Z}_{60} = \{\overline{0}, \overline{12}, \overline{24}, \overline{36}, \overline{48}\}$.

Per esplicitare un isomorfismo $\varphi : \boldsymbol{Z}_{12} \to \boldsymbol{Z}_{60}\big/_{\langle \overline{12} \rangle}$, basta porre, $\forall\, \tilde{x} \in \boldsymbol{Z}_{12}$:

$$\varphi(\tilde{x}) = \overline{x} + \langle \overline{12} \rangle \in \boldsymbol{Z}_{60}\big/_{\langle \overline{12} \rangle} \quad (\text{con } \overline{x} \in \boldsymbol{Z}_{60}).$$

Nota. Si osservi che lo stesso risultato vale per gli anelli $(\boldsymbol{Z}_{12}, +, \cdot)$ e $(\boldsymbol{Z}_{60}, +, \cdot)$.

* * *

Esercizio 1.4.4. In $G = \boldsymbol{GL}_n(\boldsymbol{R})$ si considerino il sottogruppo normale $H = \boldsymbol{SL}_n(\boldsymbol{R})$ ed il sottogruppo $K = \boldsymbol{O}_n(\boldsymbol{R})$. Si calcoli HK e si verifichi se è normale in G.

Soluzione. È noto da un precedente esercizio (cfr. Esercizio **1.3.1**) che $H \lhd G$ e che $G\big/_H \cong (\boldsymbol{R}^\cdot, \cdot)$, applicando il *TFO* all'omomorfismo $det : G \to \boldsymbol{R}^\cdot$ (che associa ad ogni matrice invertibile il suo determinante). Poiché $H \lhd G$, HK è un sottogruppo di G e risulta $HK = \pi^{-1}(\pi(K))$, con $\pi : G \to G\big/_H$ proiezione canonica (identificata con det, se $G\big/_H$ viene identificato con $\boldsymbol{R}^\cdot$).

È noto che, $\forall\, A \in \boldsymbol{O}_n(\boldsymbol{R})$, $det(A) = \pm 1$ [infatti, essendo $A^{-1} = A^t$, allora $1 = det(A)\, det(A^t) = det(A)^2$ e quindi $det(A) = \pm 1$]. Risulta: $\pi(K) \equiv det(\boldsymbol{O}_n(\boldsymbol{R})) = \{\pm 1\} = \boldsymbol{C}_2$ e quindi

$$HK = \pi^{-1}(\pi(K)) = \{A \in G \mid det(A) = \pm 1\}.$$

In base al teorema di corrispondenza, i sottogruppi normali di $G/_H$ corrispondono ai sottogruppi normali di G contenenti H. Ma in $(\boldsymbol{R}^*, \cdot)$ ogni sottogruppo è normale. Dunque $HK \lhd G$.

* * *

Esercizio 1.4.5. Nel gruppo diedrale $\boldsymbol{D}_8 = \langle \varphi, \rho \mid \varphi^8 = \rho^2 = 1,\ \rho\circ\varphi = \varphi^7\circ\rho \rangle$ si consideri il sottogruppo $H = \langle \varphi^2 \rangle$.

(*i*) Verificare che $H \lhd \boldsymbol{D}_8$.

(*ii*) Determinare i sottogruppi di $\boldsymbol{D}_8$ contenenti H.

(*iii*) Quanti sono i gruppi diedrali del quadrato contenuti in $\boldsymbol{D}_8$?

Soluzione. (*i*) Si ha: $(\boldsymbol{D}_8 : H) = \frac{16}{4} = 4$. I quattro laterali destri modulo H sono:

$$H1 = H = \{1, \varphi^2, \varphi^4, \varphi^6\}, \qquad H\rho = \{\rho, \varphi^2\circ\rho, \varphi^4\circ\rho, \varphi^6\circ\rho\},$$
$$H\varphi = \{\varphi, \varphi^3, \varphi^5, \varphi^7\}, \quad H(\varphi\circ\rho) = \{\varphi\circ\rho, \varphi^3\circ\rho, \varphi^5\circ\rho, \varphi^7\circ\rho\}.$$

Ovviamente $1H = H1$ e $\varphi H = H\varphi$. Se verifichiamo che $\rho H = H\rho$, allora necessariamente $(\varphi\circ\rho)H = H(\varphi\circ\rho)$ e quindi $H \lhd \boldsymbol{D}_8$. Poiché $\rho\circ\varphi^k = \varphi^{8-k}\circ\rho$, si ha infatti:

$$\rho H = \{\rho,\ \rho\circ\varphi^2 = \varphi^6\circ\rho,\ \rho\circ\varphi^4 = \varphi^4\circ\rho,\ \rho\circ\varphi^6 = \varphi^2\circ\rho\} = H\rho.$$

(*ii*) Per ottenere i sottogruppi cercati conviene utilizzare il teorema di corrispondenza e calcolare i sottogruppi di $\boldsymbol{D}_8/_H$. Risulta:

$$\boldsymbol{D}_8/_H = \{H, H\rho, H\varphi, H(\varphi\circ\rho)\}.$$

Si verifica che $H\rho \cdot H\rho = H$, $H\varphi \cdot H\varphi = H$. Dunque $\boldsymbol{D}_8/_H$ ha almeno due elementi di periodo 2: quindi è un gruppo di Klein ed ha perciò tre sottogruppi propri di ordine 2. I sottogruppi di $\boldsymbol{D}_8$ contenenti H sono quindi tre (escludendo quelli banali). Si ha:

$$\frac{\boldsymbol{D}_8/_H}{\langle H\rho\rangle} = \frac{\boldsymbol{D}_8/_H}{\langle\rho\rangle H/_H} \cong \boldsymbol{D}_8/_{\langle\rho\rangle H}, \quad \frac{\boldsymbol{D}_8/_H}{\langle H\varphi\rangle} \cong \boldsymbol{D}_8/_{\langle\varphi\rangle H}, \quad \frac{\boldsymbol{D}_8/_H}{\langle H(\varphi\circ\rho)\rangle} \cong \boldsymbol{D}_8/_{\langle\varphi\circ\rho\rangle H}.$$

I tre sottogruppi cercati sono quindi:

$$\langle\varphi\rangle H = \langle\varphi\rangle \cong \boldsymbol{C}_8 \ \text{ (ciclico di ordine 8)}, \ \langle\rho\rangle H = \langle\varphi^2, \rho\rangle \ \text{ e } \ \langle\varphi\circ\rho\rangle H = \langle\varphi^2, \varphi\circ\rho\rangle.$$

Gli ultimi due sottogruppi hanno cinque elementi di periodo 2 e quindi sono isomorfi a $\boldsymbol{D}_4$ (gruppo diedrale del quadrato).

(*iii*) E' noto che $\boldsymbol{D}_4$ ogni possiede due elementi di periodo 4. Poiché in $\boldsymbol{D}_8$ esistono esattamente due elementi di periodo 4 (cioè φ^2, $|f^6$), segue che ogni $\boldsymbol{D}_4$ in $\boldsymbol{D}_8$ contiene H. Pertanto $\boldsymbol{D}_8$ possiede esattamente due soli $\boldsymbol{D}_4$: $\langle\varphi^2, \rho\rangle$ e $\langle\varphi^2, \varphi\circ\rho\rangle$.

* * *

Esercizio 1.5.1. In $A = K[X, Y]$ si considerino il sottoanello $B = K[Y]$ e l'ideale $I = (XY)$ (ideale generato dal polinomio $XY \in A$). Determinare l'anello $(I + B)/_I$.

Soluzione. Dal secondo teorema di isomorfismo: $(I + B)/_I \cong B/_{I\cap B}$.

Sia XYF un elemento di I ($\forall F \in A$). Si ha:

$$XYF \in I \cap B \iff XYF \in K[Y] \iff F = 0.$$

Ne segue che $I \cap B = \{0\}$. Pertanto $B/_{I\cap B} \cong B$ e dunque $(I + B)/_I \cong B$.

* * *

Esercizio 1.5.2. Sia $\mathcal{A} = \mathfrak{M}_n(\boldsymbol{Z})$ l'anello delle matrici di interi, quadrate e di ordine n. In $\mathcal{A}$ si considerino i sottoinsiemi

$$\mathcal{I} = \{\text{matrici di } A \text{ ad elementi pari}\}, \qquad \mathcal{R} = \{A \in \mathcal{A} \mid \text{la prima riga di } A \text{ è nulla}\}.$$

(*i*) Verificare che $\mathcal{I}$ è un ideale di $\mathcal{A}$ e che $\mathcal{R}$ è un sottoanello ma non un ideale di $\mathcal{A}$.

(*ii*) Dimostrare che $\mathcal{A}/_{\mathcal{I}} \cong \mathfrak{M}_n(\boldsymbol{Z}_2)$.

(*iii*) Verificare che $\mathcal{I} \cap \mathcal{R}$ è un ideale di $\mathcal{R}$ e determinare l'anello $\mathcal{R}/_{\mathcal{I}\cap\mathcal{R}}$.

Soluzione. (*i*) Risulta: $\mathcal{I} - \mathcal{I} \subseteq \mathcal{I}$ [se A, B sono formate da interi pari, anche $A - B$ lo è]. Si noti che

$$A \in \mathcal{I} \iff A = (2I_n)\, A_1,\ \exists\, A_1 \in \mathcal{A}$$

[con I_n matrice unità in $\mathcal{A}$]. Ne segue:

$\mathcal{A}\mathcal{I} \subseteq \mathcal{I}$ [se infatti $B \in \mathcal{A}$ e $A = (2I_n)\, A_1 \in \mathcal{I}$, allora $BA = B(2I_n)A_1 = (2I_n)BA_1 \in \mathcal{I}$; si ricordi che $2I_n$ commuta con ogni matrice].

$\mathcal{I}\,\mathcal{A} \subseteq \mathcal{I}$ [se infatti $A \in \mathcal{I}$ e $B \in \mathcal{A}$, allora $AB = (2I_n)\, A_1 B \in \mathcal{I}$]. Abbiamo così provato che $\mathcal{I}$ è un ideale di $\mathcal{A}$.

Verifichiamo che $\mathcal{R}$ è un sottoanello di $\mathcal{A}$. Si ha:

$\mathcal{R} - \mathcal{R} \subseteq \mathcal{R}$ [se A, B hanno prima riga nulla, anche $A - B$ ha prima riga nulla];

$\mathcal{R}\,\mathcal{R} \subseteq \mathcal{R}$ [se A ha prima riga nulla, AB ha prima riga nulla; si noti quindi che $\mathcal{R}\,\mathcal{A} \subseteq \mathcal{R}$].

Ma $\mathcal{A}\,\mathcal{R} \not\subseteq \mathcal{R}$ [ad esempio $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 4 & 4 \end{pmatrix} \notin \mathcal{R}$]. Dunque $\mathcal{R}$ non è un ideale di $\mathcal{A}$.

(*ii*) Sia $\varphi : \mathcal{A} \to \mathfrak{M}_n(\boldsymbol{Z}_2)$ tale che, $\forall\, (a_{ij}) \in \mathcal{A}$:

$$\varphi\big((a_{ij})\big) = (\overline{a}_{ij}),\ \text{con}\ \overline{a}_{ij} \in \boldsymbol{Z}_2$$

[φ è la "riduzione *mod* 2" degli elementi di ogni matrice in $\mathcal{A}$]. Si verifica che φ è un omomorfismo di anelli. Infatti:

$$\varphi\big((a_{ij}) + (b_{ij})\big) = (\overline{a_{ij} + b_{ij}}) = (\overline{a_{ij}}) + (\overline{b_{ij}}) = \varphi\big((a_{ij})\big) + \varphi\big((b_{ij})\big);$$

$$\varphi\big((a_{ij}) \cdot (b_{ij})\big) = \varphi\big((\textstyle\sum a_{ik}\, b_{kj})\big) = \big(\overline{\textstyle\sum a_{ik}\, b_{kj}}\big) = \big(\textstyle\sum \overline{a_{ik}}\ \overline{b_{kj}}\big) = \varphi\big((a_{ij})\big) \cdot \varphi\big((b_{ij})\big).$$

φ è ovviamente suriettivo. Inoltre

$$Ker\,\varphi = \{A \in \mathcal{A} \mid \varphi(A) = 0\ (mod\ 2)\} = \mathfrak{M}_n(2\boldsymbol{Z}) = \mathcal{I}.$$

Dal *TFO*, $\mathcal{A}/_{\mathcal{I}} \cong \mathfrak{M}_n(\boldsymbol{Z}_2)$.

(*iii*) Dal secondo teorema di isomorfismo:

$$\mathcal{R}/_{\mathcal{I}\cap\mathcal{R}} \cong (\mathcal{I} + \mathcal{R})/_{\mathcal{I}}.$$

Ovviamente $\mathcal{I} \cap \mathcal{R}$ è un ideale di $\mathcal{R}$. Inoltre $(\mathcal{I} + \mathcal{R})/_{\mathcal{I}}$ è un sottoanello di $\mathcal{A}/_{\mathcal{I}} \cong \mathfrak{M}_n(\boldsymbol{Z}_2)$. Si ha:

$$\varphi(\mathcal{I} + \mathcal{R}) = \{\text{matrici di } \mathfrak{M}_n(\boldsymbol{Z}_2) \text{ la cui prima riga è nulla (in } \boldsymbol{Z}_2)\}$$

[infatti $\mathcal{I} + \mathcal{R} = \{$matrici di $\mathcal{A}$ la cui prima riga è pari$\}$]. Poiché $\varphi(\mathcal{I} + \mathcal{R})$ si identifica a $(\mathcal{I} + \mathcal{R})/_{\mathcal{I}}$ in $\mathfrak{M}_n(\boldsymbol{Z}_2)$, abbiamo ottenuto che

$$\mathcal{R}/_{\mathcal{I}\cap\mathcal{R}} \cong \{\text{matrici di } \mathfrak{M}_n(\boldsymbol{Z}_2) \text{ la cui prima riga è nulla}\}.$$

* * *

Esercizio 1.5.3. Determinare l'anello $\boldsymbol{Z}[X]/_{(X,2)}$ [dove $(X, 2)$ è l'ideale di $\boldsymbol{Z}[X]$ generato dagli elementi X, 2].

Soluzione. Si può applicare il terzo teorema di isomorfismo ad una delle seguenti due catene di ideali:

$$(i)\ \ (2) \subset (X, 2) \subset \boldsymbol{Z}[X]; \qquad (ii)\ \ (X) \subset (X, 2) \subset \boldsymbol{Z}[X].$$

(*i*) Risulta:

$$\boldsymbol{Z}[X]/_{(X,2)} \cong \frac{\boldsymbol{Z}[X]/_{(2)}}{(X,2)/_{(2)}}.$$

Ora $\boldsymbol{Z}[X]/_{(2)} \cong \boldsymbol{Z}_2[X]$ [applicando il *TFO* alla "riduzione *mod* 2" cioè all'omomorfismo suriettivo $\boldsymbol{Z}[X] \to \boldsymbol{Z}_2[X]$ tale che $\sum a_i X^i \to \sum \overline{a_i} X^i$]. Tramite tale isomorfismo, l'ideale $(X, 2)/_{(2)}$ si trasforma nell'ideale $(X) = X\boldsymbol{Z}_2[X]$. Allora

$$\boldsymbol{Z}[X]/_{(X,2)} \cong \boldsymbol{Z}_2[X]/_{X\boldsymbol{Z}_2[X]} \cong \boldsymbol{Z}_2$$

[dove l'ultimo isomorfismo è indotto dall'omomorfismo $\boldsymbol{Z}_2[X] \to \boldsymbol{Z}_2$, tale che $f \to f(\overline{0})$].

(*ii*) Risulta:

$$\boldsymbol{Z}[X]/_{(X,2)} \cong \frac{\boldsymbol{Z}[X]/_{(X)}}{(X,2)/_{(X)}}.$$

Ora $\boldsymbol{Z}[X]/_{(X)} \cong \boldsymbol{Z}$ [tramite l'omomorfismo $\boldsymbol{Z}[X] \to \boldsymbol{Z}$, tale che $f \to f(0)$]. Tramite tale isomorfismo, l'ideale $(X,2)/_{(X)}$ corrisponde a $2\boldsymbol{Z}$ e quindi:

$$\boldsymbol{Z}[X]/_{(X,2)} \cong \boldsymbol{Z}/_{2\boldsymbol{Z}} \cong \boldsymbol{Z}_2.$$

* * *

Esercizio 1.5.4. Assegnato un campo K, determinare gli eventuali ideali propri dell'anello $A = K[X]/_{(X^3)}$. Di ciascuno calcolare il quoziente rispetto ad A.

Soluzione. Risulta:

$$A = K[X]/_{(X^3)} = \{a + bx + cx^2,\ \forall\, a, b \in K;\ x^3 = 0\}$$

(con $x := X + (X^3)$).

In base al teorema di corrispondenza, l'insieme $\mathcal{I}(A)$ degli ideali di A è in corrispondenza biunivoca con l'insieme $\mathcal{I}_{(X^3)}$ degli ideali di $K[X]$ contenenti (X^3). Gli ideali di $K[X]$ sono principali. Per ogni $F \in K[X]$:

$$(F) \supseteq (X^3) \iff F \,\big|\, X^3 \iff F = cX^i,\ 0 \leq i \leq 3,\ \forall\, c \in K^{\cdot}.$$

Ne segue che $\mathcal{I}_{(X^3)} = \{(1), (X), (X^2), (X^3)\}$. Dunque A ha quattro ideali, formanti la seguente catena (decrescente):

$$A \supset (x) \supset (x^2) \supset (0)\ [= (x^3)].$$

Ovviamente $A/_A = 0$ e $A/_{(0)} = A$. Gli ideali propri di A sono (x) e (x^2). Risulta:

$$A/_{(x)} \cong \frac{K[X]/_{(X^3)}}{(X)/_{(X^3)}} \cong K[X]/_{(X)} \cong K;$$

$$A/_{(x^2)} \cong \frac{K[X]/_{(X^3)}}{(X^2)/_{(X^3)}} \cong K[X]/_{(X^2)} = K[\zeta \mid \zeta^2 = 0] = \{a + b\zeta,\ \forall\, a, b \in K;\ \zeta^2 = 0\}\ \text{(non integro)}.$$

* * *

Esercizio 1.5.5. Sia d un intero positivo tale che $X^2 - d \in \boldsymbol{Z}[X]$ sia irriducibile. Verificare che

$$\boldsymbol{Z}[\sqrt{d}]/_{(2d)} \cong \boldsymbol{Z}[\sqrt{-d}]/_{(2d)},$$

dove, come noto dal corso di **Alg. 1**, $\boldsymbol{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ \forall\, a, b \in \boldsymbol{Z}\}$ è isomorfo a $\boldsymbol{Z}[X]/_{(X^2-d)}$ (cfr. anche Cap. **3**, Osserv. **2.1**(*iv*)).

Soluzione. Risulta:

$$\boldsymbol{Z}[\sqrt{d}]/_{(2d)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2-d)}}{(X^2-d,\,2d)/_{(X^2-d)}} \cong \boldsymbol{Z}[X]/_{(X^2-d,\,2d)} \cong \frac{\boldsymbol{Z}[X]/_{(2d)}}{(X^2-d,\,2d)/_{(2d)}} \cong \boldsymbol{Z}_{2d}[X]/_{(X^2-\overline{d})},$$

con $\overline{d} \in \boldsymbol{Z}_{2d}$. Osservato che, in $\boldsymbol{Z}_{2d}$, $\overline{d} = -\overline{d}$, allora

$$\boldsymbol{Z}[\sqrt{d}]/_{(2d)} \cong \boldsymbol{Z}_{2d}[X]/_{(X^2+\overline{d})} \cong \boldsymbol{Z}[X]/_{(X^2+d,\,2d)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+d)}}{(X^2+d,\,2d)/_{(X^2+d)}} \cong \boldsymbol{Z}[\sqrt{-d}]/_{(2d)}.$$

Nota. Non è detto che $\boldsymbol{Z}[\sqrt{d}]$ sia isomorfo a $\boldsymbol{Z}[\sqrt{-d}]$. In effetti si potrebbe ad esempio dimostrare che $\boldsymbol{Z}[\sqrt{3}]$ è un dominio a fattorizzazione unica, mentre $\boldsymbol{Z}[\sqrt{-3}]$ non lo è (cfr. Cap. **3.3**).

* * *

Esercizio 1.5.6. Utilizzando il terzo teorema di isomorfismo, verificare che $\boldsymbol{Z}[i]/_{(1+3i)} \cong \boldsymbol{Z}_{10}$. Esplicitare un siffatto isomorfismo.

Soluzione. Si ha: $(1+3i) = (i-3)$. Infatti $i(1+3i) = i-3$ e $i \in \mathcal{U}(\boldsymbol{Z}[i])$. Ne segue che

$$\boldsymbol{Z}[i]/_{(1+3i)} = \boldsymbol{Z}[i]/_{(i-3)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(X-3,\, X^2+1)/_{(X^2+1)}} \cong \boldsymbol{Z}[X]/_{(X-3,\, X^2+1)} \cong \frac{\boldsymbol{Z}[X]/_{(X-3)}}{(X-3,\, X^2+1)/_{(X-3)}}.$$

Ora $\boldsymbol{Z}[X]/_{(X-3)} \cong \boldsymbol{Z}$, tramite l'isomorfismo $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{Z}$ tale che $\varphi(f) = f(3),\ \forall\, f \in \boldsymbol{Z}[X]$, [il cui nucleo è $(X-3)$]. Poiché $\varphi(X^2+1) = 10$, l'ideale $(X-3,\, X^2+1)/_{(X-3)}$ viene trasformato in $10\boldsymbol{Z}$. Dunque

$$\boldsymbol{Z}[i]/_{(1+3i)} \cong \boldsymbol{Z}_{10}.$$

Per esplicitare un isomorfismo F tra tali anelli, conviene procedere da $\boldsymbol{Z}_{10}$ a $\boldsymbol{Z}[i]/_{(1+3i)}$, tenendo conto che, $\forall\, t = 0, \ldots, 9,\ F(\overline{t}) = F(t\,\overline{1})$ e $F(\overline{1}) = 1 + (1+3i)$. Si ponga, per abbreviare le notazioni, $J = (1+3i)$. Allora:

$$\begin{aligned}
&F(\overline{0}) = J, \quad F(\overline{1}) = 1 + J, \quad F(\overline{2}) = 2 + J,\\
&F(\overline{3}) = F(\overline{1}) + F(\overline{2}) = 3 + J = i + J \ \text{ (perché } i - 3 \in J);\\
&F(\overline{4}) = F(\overline{1}) + F(\overline{3}) = 1 + i + J, \quad F(\overline{5}) = F(\overline{2}) + F(\overline{3}) = 2 + i + J,\\
&F(\overline{6}) = F(\overline{3}) + F(\overline{3}) = 2i + J, \quad F(\overline{7}) = F(\overline{1}) + F(\overline{6}) = 1 + 2i + J,\\
&F(\overline{8}) = F(\overline{4}) + F(\overline{4}) = 2 + 2i + J, \quad F(\overline{9}) = F(\overline{1}) + F(\overline{8}) = 3 + 2i + J = 3i + J
\end{aligned}$$

(in quanto $3 + 2i - 3i = 3 - i \in J$).

* * *

Esercizio 1.5.7. Dimostrare che $\boldsymbol{Z}[i]/_{(2)}$ è un anello non integro con quattro elementi. Indicarne gli zero-divisori (non banali).

Soluzione. Risulta, usando il terzo teorema di isomorfismo:

$$\begin{aligned}
\boldsymbol{Z}[i]/_{(2)} &\cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(2,X^2+1)/_{(X^2+1)}} \cong \boldsymbol{Z}[X]/_{(2,X^2+1)} \cong \frac{\boldsymbol{Z}[X]/_{(2)}}{(2,X^2+1)/_{(2)}} \cong \boldsymbol{Z}_2[X]/_{(X^2+\overline{1})} =\\
&= \boldsymbol{Z}_2[x \mid x^2 = \overline{1}] = \{a + bx,\ \ \forall\, a, b \in \boldsymbol{Z}_2;\ x^2 = \overline{1}\} = \{\overline{0},\, \overline{1},\, x,\, \overline{1} + x;\ x^2 = \overline{1}\}
\end{aligned}$$

[dove si è posto $x := X + (X^2 + \overline{1})$].

Risulta: x è invertibile [infatti $x \cdot x = \overline{1}$], mentre $(\overline{1} + x)^2 = \overline{1} + x^2 = \overline{0}$ e quindi $\overline{1} + x$ è uno zero-divisore non banale. Si conclude che

$$\boldsymbol{Z}[i]/_{(2)} = \{(2),\ 1 + (2),\ i + (2),\ 1 + i + (2)\}$$

e che $1 + i + (2)$ è l'unico zero-divisore non banale.

* * *

Esercizio 1.5.8. Dimostrare che $\boldsymbol{Z}_6[X]/_{(\overline{2}X - \overline{1})} \cong \boldsymbol{Z}_3$.

Soluzione. Si verifica facilmente che $(\overline{2}X - \overline{1}) = (\overline{3},\, X + \overline{1})$. Infatti si ha:

($\supseteq$). $\overline{3} = (\overline{2}X - \overline{1})(-\overline{3}),\ X + \overline{1} = (\overline{2}X - \overline{1})(-\overline{1} - \overline{3}X)$.

($\subseteq$). $\overline{2}X - \overline{1} = \overline{2}(X + \overline{1}) - \overline{3}$.

Allora:

$$\begin{aligned}
\boldsymbol{Z}_6[X]/_{(\overline{2}X - \overline{1})} &\cong \boldsymbol{Z}_6[X]/_{(\overline{3},\, X + \overline{1})} \cong \frac{\boldsymbol{Z}[X]/_{6\boldsymbol{Z}[X]}}{(3,X+1,6)/_{6\boldsymbol{Z}[X]}} \cong \boldsymbol{Z}[X]/_{(3,X+1,6)} = \boldsymbol{Z}[X]/_{(3,X+1)} \cong\\
&\cong \frac{\boldsymbol{Z}[X]/_{3\boldsymbol{Z}[X]}}{(3,X+1)/_{3\boldsymbol{Z}[X]}} \cong \boldsymbol{Z}_3[X]/_{(X+\overline{1})} \cong \boldsymbol{Z}_3
\end{aligned}$$

[dove l'ultimo isomorfismo è ottenuto applicando il *TFO* all'epimorfismo $\boldsymbol{Z}_3[X] \to \boldsymbol{Z}_3$ tale che $P \to P(-\overline{1}),\ \ \forall\, P \in \boldsymbol{Z}_3[X]$].

* * *

Esercizio 1.5.9. (*i*) Sia $z = a + ib$ un elemento non nullo e non invertibile di $\boldsymbol{Z}[i]$ e sia $n = \mathcal{N}(z)$. Esprimere $\boldsymbol{Z}[i]/_{(z)}$ come quoziente di $\boldsymbol{Z}_n[X]$.

(*ii*) Verificare che $\boldsymbol{Z}[i]/_{(3+4i)} \cong \boldsymbol{Z}_{25}$.

Soluzione. (*i*) Si noti che, posto $z = a + ib$: $n = \mathcal{N}(z) = z\,\overline{z} = a^2 + b^2 \in (z)$. Dunque $(n) \subseteq (z)$. Pertanto, dal terzo teorema di isomorfismo:

$$\boldsymbol{Z}[i]/_{(z)} \cong \frac{\boldsymbol{Z}[i]/_{(n)}}{(z)/_{(n)}}.$$

Si ha:

$$\boldsymbol{Z}[i]/_{(n)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(n,\, X^2+1)/_{(X^2+1)}} \cong \boldsymbol{Z}[X]/_{(n,\, X^2+1)} \cong \boldsymbol{Z}_n[X]/_{(X^2+\overline{1})}$$

(con $X^2 + \overline{1} \in \boldsymbol{Z}_n[X]$).
In particolare, l'ideale $(z)/_{(n)}$ di $\boldsymbol{Z}[i]/_{(n)}$ corrisponde all'ideale $(\overline{a} + \overline{b}X,\, X^2 + \overline{1})/_{(X^2+\overline{1})}$ di $\boldsymbol{Z}_n[X]/_{(X^2+\overline{1})}$. Pertanto

$$\boldsymbol{Z}[i]/_{(z)} \cong \frac{\boldsymbol{Z}_n[X]/_{(X^2+\overline{1})}}{(\overline{a}+\overline{b}X,\, X^2+\overline{1})/_{(X^2+\overline{1})}} \cong \boldsymbol{Z}_n[X]/_{(\overline{a}+\overline{b}X,\, X^2+\overline{1})}.$$

(*ii*) Da (*i*),

$$\boldsymbol{Z}[i]/_{(3+4i)} \cong \boldsymbol{Z}_{25}[X]/_{(\overline{3}+\overline{4}X,\, X^2+\overline{1})}.$$

Si noti che $\overline{3} + \overline{4}X = \overline{4}(X + \overline{7})$ e $\overline{4}$ è invertibile in $\boldsymbol{Z}_{25}$ (con inverso $\overline{-6} = \overline{19}$). Risulta inoltre $X^2 + \overline{1} = (X + \overline{7})(X - \overline{7})$. Ne segue che

$$(\overline{3} + \overline{4}X,\, X^2 + \overline{1}) = (X + \overline{7}) = (X - \overline{18}).$$

Pertanto

$$\boldsymbol{Z}_{25}[X]/_{(\overline{3}+\overline{4}X,\, X^2+\overline{1})} \cong \boldsymbol{Z}_{25}[X]/_{(X-\overline{18})}.$$

Tale anello è isomorfo a $\boldsymbol{Z}_{25}$, tramite l'omomorfismo suriettivo

$$\boldsymbol{Z}_{25}[X] \to \boldsymbol{Z}_{25} \ \text{ tale che } \ P \to P(\overline{18}),\ \ \forall\, P \in \boldsymbol{Z}_{25}[X].$$

È così provato che $\boldsymbol{Z}[i]/_{(3+4i)} \cong \boldsymbol{Z}_{25}$.

* * *

Esercizio 1.5.10. Esplicitare un isomorfismo tra gli anelli $\boldsymbol{Z}_6[X]/_{\overline{2}\boldsymbol{Z}_6[X]}$ e $\boldsymbol{Z}_2[X]$. Dedurne che $\boldsymbol{Z}_6[X]/_{(\overline{3}X+\overline{1})} \cong \boldsymbol{Z}_2$.

Soluzione. Che i due anelli siano isomorfi è facilmente verificabile:

$$\boldsymbol{Z}_6[X]/_{\overline{2}\boldsymbol{Z}_6[X]} \cong \frac{\boldsymbol{Z}[X]/_{6\boldsymbol{Z}[X]}}{(2,6)/_{6\boldsymbol{Z}[X]}} \cong \boldsymbol{Z}[X]/_{(2,6)} = \boldsymbol{Z}[X]/_{(2)} \cong \boldsymbol{Z}_2[X]$$

Per esplicitare un isomorfismo tra i due anelli, si consideri l'applicazione

$$\varphi : \boldsymbol{Z}_6[X] \to \boldsymbol{Z}_2[X] \ \text{ tale che } \ \varphi(\textstyle\sum \overline{a}_i X^i) = \sum \tilde{a}_i X^i,$$

con $\overline{a}_i = a_i + 6\boldsymbol{Z},\ \tilde{a}_i = a_i + 2\boldsymbol{Z}$.

φ è ben definita [infatti $\overline{a}_i = \overline{b}_i \implies \tilde{a}_i = \tilde{b}_i$]. Inoltre è un omomorfismo suriettivo di anelli. Calcoliamone il nucleo.

Se $f = \overline{2}g \in \boldsymbol{Z}_6[X]$, allora $\varphi(f) = \tilde{2}\,\varphi(g) = \tilde{0}\,\varphi(g) = \tilde{0}$. Pertanto $\overline{2}\boldsymbol{Z}_6[X] \subseteq Ker\varphi$. Viceversa, se $f = \sum \overline{a}_i X^i \in Ker\varphi$, allora $\tilde{a}_i = \tilde{0}$ e quindi $\overline{a}_i = \overline{2}\,\overline{b}_i,\ \forall\, i$. Dunque $f \in \overline{2}\,\boldsymbol{Z}_6[X]$.

Dal *TFO* segue che $\boldsymbol{Z}_6[X]/_{\overline{2}\boldsymbol{Z}_6[X]} \cong \boldsymbol{Z}_2[X]$ ed un isomorfismo tra i due anelli è il seguente:

$$\sum \overline{a}_i X^i + (\overline{2}) \to \sum \tilde{a}_i X^i, \ \ \forall \sum \overline{a}_i X^i \in \boldsymbol{Z}_6[X].$$

Dimostriamo ora l'ultima affermazione. Si noti che, in $\boldsymbol{Z}_6[X]$, $\overline{2} = \overline{2}(\overline{3}X + \overline{1})$. Dunque $(\overline{2}) \subseteq (\overline{3}X + \overline{1})$. Dal terzo teorema di isomorfismo:

$$\boldsymbol{Z}_6[X]/_{(\overline{3}X+\overline{1})} \cong \frac{\boldsymbol{Z}_6[X]/_{(\overline{2})}}{(\overline{3}X+\overline{1})/_{(\overline{2})}} \cong \boldsymbol{Z}_2[X]/_{(\tilde{3}X+\tilde{1})} = \boldsymbol{Z}_2[X]/_{(X+\tilde{1})} \cong \boldsymbol{Z}_2.$$

* * *

Esercizio 1.5.11. (*i*) Dimostrare che $\boldsymbol{Z}[\sqrt{-2}]/_{(3-\sqrt{-2})}$ è un campo e indicarne la cardinalità.
(*ii*) Dimostrare che per ogni $a \in \boldsymbol{N}$, a pari, $a \geq 4$, l'anello $\boldsymbol{Z}[\sqrt{2}]/_{(a-\sqrt{2})}$ non è integro.

Soluzione. (*i*) Risulta: $\boldsymbol{Z}[\sqrt{-2}] \cong \boldsymbol{Z}[X]/_{(X^2+2)}$. Allora

$$\boldsymbol{Z}[\sqrt{-2}]/_{(3-\sqrt{-2})} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+2)}}{(3-X, X^2+2)/_{(X^2+2)}} \cong \boldsymbol{Z}[X]/_{(X^2+2,\, 3-X)} \cong \frac{\boldsymbol{Z}[X]/_{(3-X)}}{(X^2+2, 3-X)/_{(3-X)}} \cong \boldsymbol{Z}/_{(3^2+2,\, 0)} \cong \boldsymbol{Z}_{11}.$$

Poiché $\boldsymbol{Z}_{11}$ è un campo con 11 elementi, lo stesso vale per il quoziente assegnato.

(*ii*) Risulta: $\boldsymbol{Z}[\sqrt{2}] \cong \boldsymbol{Z}[X]/_{(X^2{}_2)}$. Allora

$$\boldsymbol{Z}[\sqrt{2}]/_{(a-\sqrt{2})} \cong \frac{\boldsymbol{Z}[X]/_{(X^2-2)}}{(a-X, X^2-2)/_{(X^2-2)}} \cong \frac{\boldsymbol{Z}[X]/_{(a-X)}}{(a-X, X^2-2)/_{(a-X)}} \cong \boldsymbol{Z}/_{(0,\, a^2-2)} \cong \boldsymbol{Z}_{a^2-2}.$$

Sia $a \in \boldsymbol{N}$, $a \geq 4$, $a = 2n$. Allora $a^2 - 2 = 2(2n^2 - 1)$ non è primo. Pertanto $\boldsymbol{Z}_{a^2-2}$ non è integro.

* * *

SOLUZIONI DEGLI ESERCIZI

DEL CAPITOLO 2

Esercizio 2.1.1. Assumendo nota la struttura dei sottogruppi del gruppo alterno $\boldsymbol{A}_4$ [cfr. [AA] pag. 175], determinare un sottogruppo H di $\boldsymbol{A}_4$, di ordine massimo per cui l'omomorfismo del teorema di Cayley generalizzato sia iniettivo.

Soluzione. È noto che $\boldsymbol{A}_4$ è privo di sottogruppi di ordine 6. Inoltre $\boldsymbol{A}_4$ possiede un unico sottogruppo di Klein $\boldsymbol{V}$, quattro sottogruppi ciclici di ordine 3 e tre sottogruppi ciclici di ordine 2.

$\boldsymbol{V}$ è ovviamente normale in $\boldsymbol{A}_4$ [in quanto unico del proprio ordine] e quindi non può essere scelto come sottogruppo H [in quanto $KerT$ non sarebbe $\{1\}$ ma $\boldsymbol{V}$].

Esaminiamo un gruppo ciclico di ordine 3, ad esempio $\langle(1\,2\,3)\rangle$.

Tale sottogruppo non ha sottogruppi propri. Basta allora provare che tale sottogruppo non è normale in $\boldsymbol{A}_4$. Infatti si verifica facilmente che $(12)(34)\langle(1\,2\,3)\rangle \neq \langle(1\,2\,3)\rangle(12)(34)$. Poiché $|\mathcal{L}_s\big(\langle(1\,2\,3)\rangle\big)| = (\boldsymbol{A}_4 : \langle(1\,2\,3)\rangle) = \frac{12}{3} = 4$, allora $T : \boldsymbol{A}_4 \to \boldsymbol{S}_4$ è l'omorfismo iniettivo cercato.

Nota. Ovviamente $\boldsymbol{A}_4$ è, per definizione, un sottogruppo di $\boldsymbol{S}_4$. Abbiamo quindi ottenuto solo un fatto ovvio. Si noti infine che, per ovvie ragioni di cardinalità, $\boldsymbol{A}_4$ non potrebbe essere un sottogruppo di $\boldsymbol{S}_3$. Dunque l'immersione ottenuta è la migliore possibile.

* * *

Esercizio 2.1.2. Sia G un gruppo di ordine 20. Tenuto conto che G possiede un sottogruppo H di ordine 5 [in base al teorema di Cauchy, cfr. § 4], dimostrare che G non è semplice.

Soluzione. Sia H un sottogruppo di G di ordine 5. Si ha: $|\mathcal{L}_s(H)| = (G : H) = \frac{20}{5} = 4$.

Si consideri l'omomorfismo:

$$T : G \to \boldsymbol{S}(\mathcal{L}_s(H)) \cong \boldsymbol{S}_4, \text{ tale che } T : g \to T_g \text{ e } T_g(xH) = gxH, \ \forall\, xH \in \mathcal{L}_s(H).$$

Se T fosse iniettivo, $|G| = |Im\,T|$ e, in base al teorema di Lagrange, $|Im\,T| \,\big|\, |\boldsymbol{S}_4| = 4!$, cioè $20 \,\big|\, 24$: assurdo. Dunque T non è iniettivo, cioè $KerT$ è un sottogruppo proprio di G. Poiché $KerT \lhd G$, allora G è non semplice.

* * *

Esercizio 2.1.3. Dimostrare che se G è un gruppo abeliano finito, il teorema di Cayley ed il teorema di Cayley generalizzato forniscono la stessa rappresentazione di G [come sottogruppo di un gruppo simmetrico].

Soluzione. Se G è un gruppo abeliano, ogni sottogruppo H di G è normale. Se quindi $H \neq \{1\}$, l'omomorfismo $T : G \to \boldsymbol{S}(\mathcal{L})$ definito dal teorema di Cayley generalizzato non può essere iniettivo (essendo $KerT = H$). Se invece $H = \{1\}$, allora $|\mathcal{L}| = |G|$ e dunque $T : G \to \boldsymbol{S}(G)$. In tal caso T è iniettivo, in base alla dimostrazione del teorema di Cayley.

L'unica immersione T fornita dal teorema di Cayley generalizzato coincide con quella fornita dal teorema di Cayley.

* * *

Esercizio 2.2.1. Considerati i seguenti gruppi:

$$\boldsymbol{C}_6, \quad \boldsymbol{S}_3, \quad \boldsymbol{A}_4, \quad \boldsymbol{S}_4, \quad \boldsymbol{D}_4, \quad \boldsymbol{D}_5,$$

quale/i di essi è isomorfo al prodotto diretto di due suoi sottogruppi propri ?

Soluzione. (*i*) Poniamo: $\boldsymbol{C}_6 = \langle a \,\big|\, a^6 = 1\rangle$. Si verifica subito che

$$\boldsymbol{C}_6 \cong \langle a^3\rangle \times \langle a^2\rangle \cong \boldsymbol{C}_2 \times \boldsymbol{C}_3.$$

Infatti $a = a^3a^4 \in \langle a^3\rangle \cdot \langle a^2\rangle$ e quindi $\langle a^3\rangle \cdot \langle a^2\rangle = \boldsymbol{C}_6$. Inoltre $\langle a^3\rangle \cap \langle a^2\rangle = \{1\}$.

(*ii*) Se un gruppo finito G è prodotto diretto di due sottogruppi propri, possiede almeno un sottogruppo normale proprio. Poiché $\boldsymbol{S}_3$ ha un solo sottogruppo normale [cioè $\boldsymbol{A}_3$] e non può essere isomorfo ad $\boldsymbol{A}_3 \times \boldsymbol{A}_3$, allora non è prodotto diretto di due suoi sottogruppi propri.

(*iii*) È noto che $\boldsymbol{A}_4$ non ha sottogruppi di ordine 6, mentre ha un sottogruppo di Klein $\boldsymbol{V}$ e quattro sottogruppi ciclici H_i di ordine 3.

Se $\boldsymbol{A}_4$ fosse prodotto diretto di due suoi sottogruppi propri, necessariamente $\boldsymbol{A}_4 \cong \boldsymbol{V} \times H_i$. Ma se proviamo che tutti gli H_i sono non normali, possiamo concludere che $\boldsymbol{A}_4$ non è prodotto diretto di due suoi sottogruppi propri. I quattro sottogruppi ciclici H_i sono:

$$\langle (1\,2\,3)\rangle,\ \langle (1\,2\,4)\rangle,\ \langle (1\,3\,4)\rangle,\ \langle (2\,3\,4)\rangle.$$

Poniamo $\sigma = (1\,2)(3\,4)$. Si verifica facilmente che, $\forall\, H_i$, $\sigma H_i \sigma^{-1} \not\subseteq H_i$. Ad esempio

$$\sigma(1\,2\,3)\,\sigma^{-1} = (1\,4\,2) \notin \langle (1\,2\,3)\rangle.$$

Dunque gli H_i non sono normali in $\boldsymbol{A}_4$.

(*iv*) Siano H, K eventuali sottogruppi propri di $\boldsymbol{S}_4$ tali che $H \times K \cong \boldsymbol{S}_4$. I possibili ordini di H, K sono:

$$(|H|, |K|) = (2, 12),\ (3, 8),\ (4, 6).$$

Ma se dimostriamo che $\boldsymbol{S}_4$ non possiede sottogruppi <u>normali</u> di ordini 2, 3, 6, allora $\boldsymbol{S}_4$ non è prodotto diretto di due suoi sottogruppi propri.

Sia $|H| = 2$. Allora $H = \langle (a\,b)\rangle$. Scelto $c \neq a, b$, si ha: $(a\,c)(a\,b)(a\,c)^{-1} = (b\,c) \notin H$ e quindi $H \not\lhd \boldsymbol{S}_4$.

Sia $|H| = 3$. Certo $H = \langle (a\,b\,c)\rangle$. Scelto $d \neq a, b, c$, si ha: $(a\,d)(a\,b\,c)(a\,d)^{-1} = (b\,c\,d) \notin H$. Dunque $H \not\lhd \boldsymbol{S}_4$.

Sia $|H| = 6$. Certo $H \ncong \boldsymbol{C}_6$ [$\boldsymbol{S}_4$ non ha elementi di periodo 6]. Dunque $H \cong \boldsymbol{S}_3$. In $\boldsymbol{S}_4$ di sottogruppi isomorfi a $\boldsymbol{S}_3$ ne esistono almeno quattro:

$$H_1 = \boldsymbol{S}(\{2,3,4\}),\ H_2 = \boldsymbol{S}(\{1,3,4\}),\ H_3 = \boldsymbol{S}(\{1,2,4\}),\ H_4 = \boldsymbol{S}(\{1,2,3\}).$$

Verifichiamo che non ce ne sono altri. Sia $H < \boldsymbol{S}_4$, $H \cong \boldsymbol{S}_3$. H è generato da un 2-ciclo σ e da un 3-ciclo τ. Sia $\tau = (a\,b\,c)$ e $\sigma = (a\,b)$ [oppure $(a\,c)$, $(b\,c)$]; in tal caso $H = H_i$, con $1 \leq i \leq 4$. Se invece $\tau = (a\,b\,c)$ e $\sigma = (a\,d)$, allora $\tau\sigma = (a\,b\,c\,d) \notin H$.

Per concludere resta da verificare che $H_i \not\lhd \boldsymbol{S}_4$, con $1 \leq i \leq 4$. Per questo si rinvia ad un esercizio precedente (cfr. Esercizio **1.1.4**).

(*v*) $\boldsymbol{D}_4$ è un gruppo non abeliano di ordine 8. Se fosse prodotto diretto di due suoi sottogruppi propri, tali sottogruppi avrebbero necessariamente ordine 2, 4. Ma è noto che tutti i gruppi di ordine 2, 4 sono abeliani. Dunque $\boldsymbol{D}_4$ sarebbe abeliano: assurdo.

(*vi*) Analoghe considerazioni valgono per $\boldsymbol{D}_5$. Tale gruppo non abeliano ha ordine 10 e quindi potrebbe essere prodotto diretto di sottogruppi di ordine 2, 5. Ma tutti i gruppi di ordine 2, 5 sono abeliani e quindi anche $\boldsymbol{D}_5$ lo sarebbe.

* * *

Esercizio 2.2.2. Determinare in $\boldsymbol{S}_5$ un sottogruppo non abeliano di ordine 12, prodotto diretto di due suoi sottogruppi propri.

Soluzione. Si scelgano in $\boldsymbol{S}_5$ i due sottogruppi

$$\langle (1\,2)\rangle,\ \langle (3\,4),\,(3\,4\,5)\rangle,$$

rispettivamente isomorfi a $\boldsymbol{C}_2$ ed $\boldsymbol{S}_3$. Poichè sono generati da permutazioni disgiunte, commutano (elemento per elemento). Dunque $H = \langle (1\,2)\rangle \cdot \langle (3\,4),\,(3\,4\,5)\rangle$ è un gruppo di ordine 12, non abeliano.

Si noti che H contiene i due sottogruppi $\langle (1\,2)\rangle$, $\langle (3\,4),\,(3\,4\,5)\rangle$. Entrambi sono normali in H (perché commutano elemento per elemento) e la loro intersezione è $\{(1)\}$. Si conclude che $H \cong \langle (1\,2)\rangle \times \langle (3\,4),\,(3\,4\,5)\rangle$, come richiesto.

* * *

Esercizio 2.2.3. Verificare che il gruppo $\boldsymbol{Z}\times\boldsymbol{Z}$ non è ciclico.

Soluzione. $\boldsymbol{Z}\times\boldsymbol{Z}$ è il prodotto diretto di $(\boldsymbol{Z},+)$ per se stesso. L'operazione di tale gruppo è quindi:

$$(n,m)+(n',m')=(n+n',m+m'),\ \ \forall\,(n,m),(n',m')\in\boldsymbol{Z}\times\boldsymbol{Z}.$$

Per assurdo, $\boldsymbol{Z}\times\boldsymbol{Z}$ sia ciclico. Dunque $\exists\,(a,b)\in\boldsymbol{Z}\times\boldsymbol{Z}$ tale che

$$\boldsymbol{Z}\times\boldsymbol{Z}=(a,b)\boldsymbol{Z}=\{(an,bn),\ \ \forall\,n\in\boldsymbol{Z}\}.$$

Scegliamo $(r,s)\in\boldsymbol{Z}\times\boldsymbol{Z}$ tale che $MCD(r,s)=1$ e $(r,s)\neq\pm(a,b)$. Risulta: $(r,s)=(an,bn)$, con $n\in\boldsymbol{Z}$. Poiché $r=an,\ s=bn,$ allora

$$1=MCD(r,s)=MCD(an,bn)=|n|MCD(a,b).$$

Dunque $n=\pm1,$ cioè $(r,s)=\pm(a,b)$: assurdo.

* * *

Esercizio 2.2.4. (*i*) Verificare che, per ogni n naturale dispari, $\boldsymbol{O}_n(\boldsymbol{R})\cong\boldsymbol{SO}_n(\boldsymbol{R})\times\boldsymbol{C}_2$.

(*ii*) Verificare che invece $\boldsymbol{O}_2(\boldsymbol{R})\ncong\boldsymbol{SO}_2(\boldsymbol{R})\times\boldsymbol{C}_2$.

[*Suggerimento*. Il gruppo $\boldsymbol{O}_2(\boldsymbol{R})$ possiede un'infinità continua di elementi di periodo 2].

Soluzione. (*i*) Per comodità di notazione poniamo $\boldsymbol{O}_n:=\boldsymbol{O}_n(\boldsymbol{R})$, $\boldsymbol{SO}_n:=\boldsymbol{SO}_n(\boldsymbol{R})$. Il gruppo ciclico $\boldsymbol{C}_2$ si identifica in $\boldsymbol{O}_n$ al gruppo $\langle -I_n\rangle$ [dove I_n è la matrice unità di ordine n. Si noti che $(-I_n)(-I_n)=I_n$]. Basta verificare che:

(*a*) $\boldsymbol{SO}_n\lhd\boldsymbol{O}_n$ e $\boldsymbol{C}_2\lhd\boldsymbol{O}_n$;

(*b*) $\boldsymbol{SO}_n\cdot\boldsymbol{C}_2=\boldsymbol{O}_n$;

(*c*) $\boldsymbol{SO}_n\cap\boldsymbol{C}_2=\{I_n\}$.

(*a*) $\forall\,A\in\boldsymbol{O}_n$ e $\forall\,B\in\boldsymbol{SO}_n$ si ha: $det(ABA^{-1})=det(B)=+1$. Dunque $ABA^{-1}\in\boldsymbol{SO}_n$. Pertanto $\boldsymbol{SO}_n\lhd\boldsymbol{O}_n$. Inoltre, $\forall\,A\in\boldsymbol{O}_n,\ A(-I_n)=-A=(-I_n)A$. Dunque $A\boldsymbol{C}_2=\boldsymbol{C}_2A$ e pertanto $\boldsymbol{C}_2\lhd\boldsymbol{O}_n$.

(*b*) Se $A\in\boldsymbol{O}_n-\boldsymbol{SO}_n,$ allora $-A\in\boldsymbol{SO}_n$. Infatti:

$$\begin{cases}(-A)^{-1}=((-I_n)A)^{-1}=A^{-1}(-I_n)^{-1}=A^{-1}(-I_n)=-(A^{-1})=-(A^{t})=(-A)^{t}.\\ det(-A)=(-1)^{n}det(A)=(-1)^{n+1}=1\quad\text{(essendo } n \text{ dispari)}.\end{cases}$$

Ne segue: $A=(-A)(-I_n)\in\boldsymbol{SO}_n\cdot\boldsymbol{C}_2$. È così provato che $\boldsymbol{O}_n=\boldsymbol{SO}_n\cdot\boldsymbol{C}_2$.

(*c*) Poiché $-I_n\in\boldsymbol{O}_n-\boldsymbol{SO}_n$ (essendo n dispari), allora $\boldsymbol{SO}_n\cap\boldsymbol{C}_2=\{I_n\}$.

(*ii*) È noto che $\boldsymbol{O}_2(\boldsymbol{R})$ è formato da tutte e sole le matrici

$$A_t=\begin{pmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{pmatrix},\quad B_t=\begin{pmatrix}\cos t & \sin t\\ \sin t & -\cos t\end{pmatrix},\ \ \forall\,t\in\boldsymbol{R}.$$

Inoltre $\boldsymbol{SO}_2(\boldsymbol{R})=\{A_t,\ \forall\,t\in\boldsymbol{R}\}$. Ovviamente $A_t=A_{t+2k\pi},\ B_t=B_{t+2k\pi},\ \forall\,k\in\boldsymbol{Z}$. Inoltre si verifica subito che

$$(B_t)^2=I_2,\ \ (A_t)^2=A_{2t},\ \ \forall\,t\in\boldsymbol{R}.$$

Per assurdo, assumiamo che esista un isomorfismo $\Phi:\boldsymbol{O}_2(\boldsymbol{R})\to\boldsymbol{SO}_2(\boldsymbol{R})\times\boldsymbol{C}_2$. Poniamo inoltre $\boldsymbol{C}_2=\{1,-1\}$. Sia $B\in\boldsymbol{O}_2(\boldsymbol{R})-\boldsymbol{SO}_2(\boldsymbol{R})$ e sia $\Phi(B)=(A,x)$, con $A\in\boldsymbol{SO}_2(\boldsymbol{R})$ e $x\in\boldsymbol{C}_2$ $(x=\pm1)$. Poiché $\circ(B)=2$, allora $\circ((A,x))=2$ e dunque $A^2=I_2$ (e $x^2=1$). Se $A=A_t$, allora $A^2=A_{2t}=I_2$ e dunque $2t\in2\pi\boldsymbol{Z}$, cioè $t\in\pi\boldsymbol{Z}$. Allora

$$\Phi(\boldsymbol{O}_2(\boldsymbol{R})-\boldsymbol{SO}_2(\boldsymbol{R}))\subseteq\{A_{k\pi},\ \forall\,k\in\boldsymbol{Z}\}\times\boldsymbol{C}_2$$

ed ha quindi cardinalità al più numerabile, mentre $\boldsymbol{O}_2(\boldsymbol{R})-\boldsymbol{SO}_2(\boldsymbol{R})=\{B_t,\ \forall\,t\in\boldsymbol{R}\}$ ha cardinalità del continuo, essendo in corrispondenza biunivoca con l'intervallo reale $[0,2\pi)$. Essendo Φ biiettiva si ha un assurdo.

* * *

Esercizio 2.2.5. (*i*) Sia G un gruppo finito verificante la seguente proprietà:

per ogni d divisore positivo di $|G|$, G ha al più un solo sottogruppo di ordine d.

Verificare che G è un gruppo ciclico.

(*ii*) Se K è un campo finito, verificare che il gruppo moltiplicativo $(K^{\cdot}, \cdot)$ è ciclico. [*Suggerimento*: se $H \leq K^{\cdot}$ e $|H| = m$, applicare il teorema di Ruffini al polinomio $X^m - 1 \in K[X]$ e dedurne che G non ha altri sottogruppi di ordine m.]

Soluzione. (*i*) Cfr. [AA], Esercizio **4.19**.

(*ii*) Per ogni $x \in H$, $x^{|H|} = 1$ e quindi x è uno zero del polinomio $X^m - 1 \in K[X]$. Gli zeri di tale polinomio sono al più m [dal teorema di Ruffini] e dunque sono tutti e soli gli elementi di H. Se H' è un altro sottogruppo di $(K^{\cdot}, \cdot)$ dello stesso ordine m, i suoi elementi sono zeri di $X^m - 1$ e quindi coincidono con quelli di H. Dunque $H' = H$ [cfr. [AA], Coroll. **5**, pag. 168].

* * *

Esercizio 2.3.1. (*i*) Sia $*$ l'azione di coniugio su un gruppo G. Quando tale azione è fedele?

(*ii*) Sia ω l'azione di coniugio su G, ristretta ad un sottogruppo H. Quando tale azione è fedele?

Soluzione. (*i*) L'azione di coniugio $* : G \times G \to G$ [tale che $g * s = gsg^{-1}$, $\forall\, g, s \in G$] definisce l'omomorfismo $\varphi_* : G \to \boldsymbol{S}(G)$ tale che, $\forall\, g \in G$,

$$\varphi_*(g)(s) = g * s = gsg^{-1}, \ \forall\, s \in G.$$

Dunque $\varphi_*(g)$ coincide con l'automorfismo interno $\gamma_g : G \to G$. Risulta quindi:

$$Ker\,\varphi_* = \{g \in G \mid \gamma_g = \mathbf{1}_G\}$$

e dunque $g \in Ker\,\varphi_* \iff gsg^{-1} = s, \ \forall\, s \in G \iff gs = sg, \ \forall\, s \in G \iff g \in \boldsymbol{Z}(G)$ (centro di G). Dunque $Ker\,\varphi_* = \boldsymbol{Z}(G)$ e quindi $*$ è un'azione fedele $\iff \boldsymbol{Z}(G) = \{1\}$.

(*ii*) L'azione $\omega = *_{|H \times G}$ è così definita:

$$\omega(h, g) = h * g = hgh^{-1}, \ \forall\, h \in H, \ \forall\, g \in G.$$

ω definisce l'omomorfismo $\varphi_\omega : H \to \boldsymbol{S}(G)$ tale che

$$\varphi_\omega(h) = \gamma_h : G \to G, \ \forall\, h \in H.$$

Ovviamente :

$$Ker\,\varphi_\omega = \{h \in H \mid \gamma_h = \mathbf{1}_G\} = H \cap Ker\varphi_* = H \cap \boldsymbol{Z}(G).$$

Dunque ω è fedele $\iff$ H interseca $\boldsymbol{Z}(G)$ soltanto nell'unità 1 di G.

* * *

Esercizio 2.3.2. Sia ω un'azione di G su S.

(*i*) Verificare che ω induce un'azione $\tilde{\omega}$ sull'insieme delle parti $\mathfrak{P}(S)$, così definita: $\forall\, T \in \mathfrak{P}(S)$,

$$\tilde{\omega}(g, T) = g \cdot T := \{g \cdot t, \ \forall\, t \in T\}, \text{ se } T \neq \emptyset; \qquad \tilde{\omega}(g, \emptyset) = \emptyset.$$

(*ii*) Sia $|S| \geq n$ e sia $\boldsymbol{\Sigma}_n$ l'insieme dei sottoinsiemi di S di cardinalità n. Verificare che ω induce un'azione di G su $\boldsymbol{\Sigma}_n$.

Soluzione. (*i*) Risulta, $\forall\, g_1, g_2 \in G$:

$1 \cdot T = \{1 \cdot t = t, \ \forall\, t \in \mathfrak{P}(S)\} = T, \ \forall\, T \in \mathfrak{P}(S)$ [e in particolare si ponga $1 \cdot \emptyset = \emptyset$];

$g_1 \cdot (g_2 \cdot T) = \{g_1 \cdot (g_2 \cdot t), \ \forall\, t \in T\} = \{g_1 g_2 \cdot t, \ \forall\, t \in T\} = g_1 g_2 \cdot T$.

Dunque $\tilde{\omega}$ è un'azione di G su $\mathfrak{P}(S)$.

(*ii*) Sia $T \in \boldsymbol{\Sigma}_n$, $T = \{t_1, \ldots, t_n\}$. Per ogni $g \in G$, $g_- : S \to S$ è una biiezione. Quindi $|g \cdot T| = |T|$, cioè $g \cdot T \in \boldsymbol{\Sigma}_n$. Resta allora definita la restrizione di $\tilde{\omega}$:

$$\overline{\omega} := \tilde{\omega}_{\,\big|\, G \times \boldsymbol{\Sigma}_n} : G \times \boldsymbol{\Sigma}_n \to \boldsymbol{\Sigma}_n.$$

Pertanto $\overline{\omega}$ è un'azione di G su $\boldsymbol{\Sigma}_n$.

* * *

Esercizio 2.3.3. Sia $*$ l'azione di coniugio su un gruppo G e sia H un sottogruppo di G.

(*i*) Determinare l'orbita $\tilde{\boldsymbol{O}}(H)$ rispetto all'azione $\tilde{*}$ indotta su $\mathfrak{P}(G)$ da $*$ (cfr. esercizio precedente).

(*ii*) Denotato con $\tilde{\boldsymbol{S}}t_{_H}$ lo stabilizzatore di tale azione indotta, verificare che

$$\tilde{\boldsymbol{S}}t_{_H} = \{g \in G \mid gH = Hg\}.$$

Tale gruppo è detto *normalizzante di* H *in* G ed è denotato $\mathcal{N}(H)$.

(*iii*) Verificare che $\mathcal{N}(H)$ è il più grande sottogruppo di G in cui H è normale.

Soluzione. (*i*) L'azione $\tilde{*}$ indotta da $*$ sull'insieme delle parti $\mathfrak{P}(G)$ di G è così definita:

$$\tilde{*} : G\times\mathfrak{P}(G) \to \mathfrak{P}(G), \text{ tale che } \tilde{*}(g, X) = g * X = gXg^{-1}, \ \forall\, g \in G, \ \forall\, X \subseteq G.$$

Sia $H \leq G$. $H \in \mathfrak{P}(G)$ e l'orbita di H rispetto a $\tilde{*}$ è

$$\tilde{\boldsymbol{O}}(H) = \{g * H, \ \forall\, g \in G\} = \{gHg^{-1}, \ \forall\, g \in G\}.$$

Dunque $\tilde{\boldsymbol{O}}(H)$ è l'insieme dei sottogruppi coniugati ad H.

(*ii*) Risulta:

$$\tilde{\boldsymbol{S}}t_{_H} = \{g \in G \mid g * H = H\} = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\} =: \mathcal{N}(H).$$

(*iii*) Il normalizzante $\mathcal{N}(H) = \{g \in G \mid gH = Hg\}$ è ovviamente un sottogruppo di G [in quanto è uno stabilizzatore]. Risulta:

$H \leq \mathcal{N}(H)$ [infatti $hH = H = Hh, \ \forall\, h \in H$]; $H \trianglelefteq \mathcal{N}(H)$ [infatti $\forall\, g \in \mathcal{N}(H), \ gH = Hg$].

Sia infine K un sottogruppo di G tale che $H \leq K$ e $H \trianglelefteq K$. Si ha, $\forall\, c \in K$: $cH = Hc$. Dunque $c \in \mathcal{N}(H)$ e quindi $K \leq \mathcal{N}(H)$.

Nota. Se G è finito, essendo $|G| = |\tilde{\boldsymbol{O}}(H)|\cdot|\tilde{\boldsymbol{S}}t_{_H}|$, da (*i*) e (*ii*) segue che $\frac{|G|}{|\mathcal{N}(H)|}$ è il numero dei sottogruppi coniugati di H.

* * *

Esercizio 2.3.4. Sia H un sottogruppo di G e sia $\mathcal{L} = \mathcal{L}_s(H)$ l'insieme delle sue classi laterali sinistre. È definita l'applicazione

$$\omega : G\times\mathcal{L} \to \mathcal{L} \text{ tale che } \omega(g, aH) = ga\,H, \ \forall\, g \in G, \ \forall\, aH \in \mathcal{L}.$$

(*i*) Verificare che ω è un'azione su $\mathcal{L}$.

(*ii*) Verificare che ω è transitiva.

(*iii*) ω è fedele?

Soluzione. (*i*) Risulta, $\forall\, g_1, g_2 \in G, \ \forall\, aH \in \mathcal{L}$:

$$\omega(1, aH) = 1\,aH = aH; \quad \omega(g_1, \omega(g_2, aH)) = g_1g_2\,aH = \omega(g_1g_2, aH).$$

(*ii*) Siano $aH, bH \in \mathcal{L}$. Risulta: $bH = b(a^{-1}a)H = (ba^{-1})aH = \omega(ba^{-1}, aH)$. Pertanto l'azione è transitiva.

(*iii*) Risulta:

$$Ker\,\varphi_\omega = \{g \in G \,|\, \omega(g,\_) = \mathbf{1}_{\mathcal{L}}\} = \{g \in G \,|\, gaH = aH, \ \forall\, a \in G\} = \{g \in G \,|\, a^{-1}ga \in H, \ \forall\, a \in G\}.$$

Se ad esempio $H \trianglelefteq G$ e $h \in H$, risulta $a^{-1}ha \in H, \ \forall\, a \in G$. Dunque $H \subseteq Ker\,\varphi_\omega$ e pertanto in generale ω non è fedele.

Nota. φ_ω è l'omomorfismo T considerato in Teor. **1.2**. Dunque ω è fedele $\iff$ H è privo di sottogruppi normali in G (oltre a $\{1\}$).

* * *

Esercizio 2.3.5. Sia ω l'azione di moltiplicazione (righe per colonne) delle matrici ortogonali $\boldsymbol{O}_n(\boldsymbol{R})$ su $\boldsymbol{R}^n$. Determinare le orbite di tale azione e dire se l'azione è fedele.

Soluzione. Si ponga $G := \boldsymbol{O}_n(\boldsymbol{R}) = \{A \in \boldsymbol{GL}_n(\boldsymbol{R}) \,\big|\, A^t = A^{-1}\}$. L'azione ω è così definita:

$$\omega : G \times \boldsymbol{R}^n \text{ tale che } \omega(A, \underline{x}) = A\,\underline{x}, \ \forall\, A \in G, \ \forall\, \underline{x} \in \boldsymbol{R}^n.$$

Ovviamente l'orbita di $\underline{x}$ è

$$\boldsymbol{O}(\underline{x}) = \{A\,\underline{x}, \ \forall\, A \in G\}.$$

Si noti che, essendo A ortogonale: $A\,\underline{x} \cdot A\,\underline{x} = \underline{x}^t A^t A\,\underline{x} = \underline{x}^t\,\underline{x}$ e quindi $\|A\,\underline{x}\| = \|\underline{x}\|$ ["le matrici ortogonali fissano la norma dei vettori"].

Se $\underline{x} = \underline{0}$, $\boldsymbol{O}(\underline{0}) = \{\underline{0}\}$. Sia $\underline{x} \neq \underline{0}$ e sia $\|\underline{x}\| = r\ (> 0)$. Posto $\mathbf{S}_r = \{\underline{y} \in \boldsymbol{R}^n \,\big|\, \|\underline{y}\| = r\}$ [sfera di centro $\underline{0}$ e raggio r], risulta subito che $\boldsymbol{O}(\underline{x}) \subseteq \mathbf{S}_r$ [infatti $\|A\,\underline{x}\| = \|\underline{x}\| = r, \ \forall\, A \in G$].

Proviamo l'inclusione opposta. Sia $\underline{y} \in \mathbf{S}_r$. Se $\underline{y} = \underline{x}$, ovviamente $\underline{y} \in \boldsymbol{O}(\underline{x})$. Sia invece $\underline{y} \neq \underline{x}$ e sia π l'iperpiano normale alla retta per $\underline{x}, \underline{y}$, passante per il punto medio del segmento congiungente $\underline{x}, \underline{y}$. Poiché π è il luogo dei punti equidistanti da $\underline{x}, \underline{y}$, allora $\underline{0} \in \pi$. Si consideri la riflessione ρ di asse l'iperpiano π. Tale riflessione ha equazione $Y = AX$, per un'opportuna matrice $A \in G$. Poiché $\rho(\underline{x}) = \underline{y}$, allora $\underline{y} = A\,\underline{x}$. Dunque $\underline{y} \in \boldsymbol{O}(\underline{x})$. Abbiamo così provato che

$$\boldsymbol{O}(\underline{x}) = \mathbf{S}_r, \text{ se } \underline{x} \neq \underline{0} \text{ e } r = \|\underline{x}\|.$$

Si ha: $Ker\varphi_\omega = \{A \in \boldsymbol{O}_n(\boldsymbol{R}) \,\big|\, A\underline{x} = \underline{x}, \ \forall\, \underline{x} \in \boldsymbol{R}^n\}$. Poiché l'autospazio di A associato all'autovalore 1 è tutto $\boldsymbol{R}^n$, allora $A = I_n$. Pertanto l'azione è fedele.

* * *

Esercizio 2.3.6. Verificare che gli stabilizzatori di elementi di una stessa orbita sono sottogruppi coniugati.

Soluzione. Se $y = g \cdot x$ (con $g \in G$), dobbiamo verificare che $\boldsymbol{St}_y \sim \boldsymbol{St}_x$. Si ha, $\forall\, h \in G$:

$$h \in \boldsymbol{St}_y \iff h \cdot y = y \iff h \cdot g \cdot x = g \cdot x \iff hg \cdot x = g \cdot x \iff g^{-1}hg \cdot x = x \iff g^{-1}hg \in \boldsymbol{St}_x.$$

Pertanto $g^{-1}\boldsymbol{St}_y\, g \subseteq \boldsymbol{St}_x$, cioè $\boldsymbol{St}_y\, g \subseteq g\boldsymbol{St}_x$. Analogamente, $\forall\, \ell \in G$, si verifica che $\ell \in \boldsymbol{St}_x \iff g\ell g^{-1} \in \boldsymbol{St}_y$ e quindi $g\boldsymbol{St}_x\, g^{-1} \subseteq \boldsymbol{St}_y$, cioè $g\boldsymbol{St}_x \subseteq \boldsymbol{St}_y\, g$. Si conclude che $\boldsymbol{St}_y = g\,\boldsymbol{St}_x\, g^{-1}$.

* * *

Esercizio 2.3.7. (*i*) Calcolare il numero delle orbite rispetto all'azione di coniugio in $\boldsymbol{D}_6$. Determinare ciascuna orbita.

(*ii*) Verificare la formula di Burnside (per il coniugio) e l'equazione delle classi per $\boldsymbol{A}_4$.

Soluzione. (*i*) Dalla formula di Burnside, il numero delle orbite rispetto all'azione di coniugio in $\boldsymbol{D}_6$ è:

$$n := \tfrac{1}{12} \sum_{g \in \boldsymbol{D}_6} |(\boldsymbol{D}_6)_g\,|,$$

dove $(\boldsymbol{D}_6)_g = \{h \in \boldsymbol{D}_6 \,\big|\, g * h = h\} = \{h \in \boldsymbol{D}_6 \,\big|\, ghg^{-1} = h\} = \boldsymbol{C}(g)$ (centralizzante di g).

Calcoliamo quindi il centralizzante di ogni elemento di $\boldsymbol{D}_6$. Ricordiamo che:

$$\boldsymbol{D}_6 = \langle \varphi, \rho \mid \varphi^6 = \rho^2 = 1; \ \rho \circ \varphi = \varphi^5 \circ \rho \rangle = \{1, \varphi, \varphi^2, \varphi^3, \varphi^4, \varphi^5, \rho, \varphi \circ \rho, \varphi^2 \circ \rho, \varphi^3 \circ \rho, \varphi^4 \circ \rho, \varphi^5 \circ \rho\}.$$

Poiché $\boldsymbol{Z}(\boldsymbol{D}_6) = \{1, \varphi^3\}$, allora $\boldsymbol{C}(1) = \boldsymbol{C}(\varphi^3) = \boldsymbol{D}_6$.

Per $k = 1, 2, 4, 5$: $\boldsymbol{C}(\varphi^k) \geq \langle \varphi \rangle$ e $\rho \notin \boldsymbol{C}(\varphi^k)$. Dunque

$$\boldsymbol{C}(\varphi^k) = \langle \varphi \rangle, \text{ per } k = 1, 2, 4, 5.$$

Si ha: $\boldsymbol{C}(\rho) \ni 1, \rho, \varphi^3, \varphi^3 \circ \rho$ mentre $\boldsymbol{C}(\rho) \not\ni \varphi, \varphi^2, \varphi^4, \varphi^5, \varphi \circ \rho, \varphi^2 \circ \rho, \varphi^4 \circ \rho, \varphi^5 \circ \rho$. Pertanto:

$$\boldsymbol{C}(\rho) = \{1, \rho, \varphi^3, \varphi^3 \circ \rho\} = \langle \rho, \varphi^3 \rangle \ (\cong \boldsymbol{V} \text{ gruppo di Klein}).$$

Analogamente:

$$\boldsymbol{C}(\varphi^3 \circ \rho) = \boldsymbol{C}(\rho) \cong \boldsymbol{V};$$
$$\boldsymbol{C}(\varphi \circ \rho) = \langle \varphi^3, \varphi \circ \rho \rangle = \{1, \varphi^3, \varphi \circ \rho, \varphi^4 \circ \rho\} = \boldsymbol{C}(\varphi^4 \circ \rho) \cong \boldsymbol{V};$$
$$\boldsymbol{C}(\varphi^2 \circ \rho) = \langle \varphi^3, \varphi^2 \circ \rho \rangle = \{1, \varphi^3, \varphi^2 \circ \rho, \varphi^5 \circ \rho\} = \boldsymbol{C}(\varphi^5 \circ \rho) \cong \boldsymbol{V}.$$

In base alla formula di Burnside:

$$n = \tfrac{1}{12}(12 + 12 + 6 + 6 + 6 + 6 + 4 + 4 + 4 + 4 + 4 + 4) = \tfrac{72}{12} = 6.$$

Vogliamo ora determinare le sei orbite. Si utilizzi il fatto che $|\boldsymbol{O}(s)| = \frac{12}{|\boldsymbol{C}(s)|}$. Si ha:

$|\boldsymbol{O}(1)| = |\boldsymbol{O}(\varphi^3)| = \frac{12}{12} = 1$. Quindi: $\boldsymbol{O}(1) = \{1\}$, $\boldsymbol{O}(\varphi^3) = \{\varphi^3\}$;

$|\boldsymbol{O}(\varphi)| = \frac{12}{6} = 2$. Allora $\boldsymbol{O}(\varphi) = \{\varphi, \varphi^5\}$ [infatti $\rho\circ\varphi\circ\rho^{-1} = \varphi^5$];

$|\boldsymbol{O}(\varphi^2)| = \frac{12}{6} = 2$. Allora $\boldsymbol{O}(\varphi^2) = \{\varphi^2, \varphi^4\}$ [infatti $\rho\circ\varphi^2\circ\rho^{-1} = \varphi^4$];

$|\boldsymbol{O}(\rho)| = \frac{12}{4} = 3$. Allora $\boldsymbol{O}(\rho) = \{\rho, \varphi^2\circ\rho, \varphi^4\circ\rho\}$ [infatti $\varphi\circ\rho\circ\varphi^{-1} = \varphi^2\circ\rho$, $\varphi^2\circ\rho\circ\varphi^{-2} = \varphi^4\circ\rho$];

$|\boldsymbol{O}(\varphi\circ\rho)| = \frac{12}{4} = 3$. Allora $\boldsymbol{O}(\varphi\circ\rho) = \{\varphi\circ\rho, \varphi^3\circ\rho, \varphi^5\circ\rho\}$ [necessariamente].

(*ii*) Le classi di coniugio di $\boldsymbol{A}_4$ formano una sottopartizione delle classi di coniugio di $\boldsymbol{S}_4$, che, come noto da **Alg. 1**, corrispondono biunivocamente alle possibili strutture cicliche. Le permutazioni di $\boldsymbol{A}_4$ sono quelle pari e quindi dei seguenti tre tipi:

$$(\_),\quad (\_\,\_)(\_\,\_),\quad (\_\,\_\,\_).$$

Ovviamente $\boldsymbol{O}((1)) = \{(1)\}$. Calcoliamo l'orbita di $(1\,2)(3\,4)$. Poiché $(1\,2)(3\,4)$ commuta con $(1\,3)(2\,4)$, allora $(1\,3)(2\,4) \in \boldsymbol{C}((1\,2)(3\,4))$. Essendo $\boldsymbol{C}((1\,2)(3\,4)) \neq \boldsymbol{A}_4$, allora

$$\boldsymbol{C}((1\,2)(3\,4)) = \{(1),\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} = \boldsymbol{V}\ \text{(gruppo di Klein)}.$$

Ne segue che

$$|\boldsymbol{O}\big((1\,2)(3\,4)\big)| = \tfrac{12}{|\boldsymbol{C}((1\,2)(3\,4))|} = \tfrac{12}{4} = 3$$

e quindi $\boldsymbol{O}\big((1\,2)(3\,4)\big) = \{(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$.

Restano da esaminare le orbite dei 3-cicli. Consideriamo $\boldsymbol{O}\big((1\,2\,3)\big)$. Poiché $\boldsymbol{C}((1\,2\,3)) \neq \boldsymbol{A}_4$, allora $\boldsymbol{C}((1\,2\,3)) = \langle(1\,2\,3)\rangle$ e quindi

$$|\boldsymbol{O}\big((1\,2\,3)\big)| = \tfrac{12}{|\boldsymbol{C}((1\,2\,3))|} = \tfrac{12}{3} = 4.$$

Con facili calcoli, risulta:

$$\boldsymbol{O}\big((1\,2\,3)\big) = \{(1\,2\,3),\ (1\,4\,2),\ (1\,3\,4),\ (2\,4\,3)\}$$

[ad esempio $(1\,4\,2) = (1\,2)(3\,4)(1\,2\,3)[(1\,2)(3\,4)]^{-1}$, ecc.]. L'altra orbita degli altri quattro 3-cicli è:

$$\boldsymbol{O}\big((1\,3\,2)\big) = \{(1\,3\,2),\ (1\,2\,4),\ (1\,4\,3),\ (2\,3\,4)\}.$$

Abbiamo ottenuto che $\boldsymbol{A}_4$ ha quattro orbite. Si ha infatti (formula di Burnside):

$$\tfrac{1}{12}\sum_{\sigma\in\boldsymbol{A}_4} |(\boldsymbol{A}_4)_\sigma| = \tfrac{1}{12}\sum_{\sigma\in\boldsymbol{A}_4} |\boldsymbol{C}(\sigma)| = \tfrac{1}{12}(1\cdot 12 + 3\cdot 4 + 8\cdot 3) = 4.$$

Infine, l'equazione delle classi è verificata. Infatti:

$$\sum_{\sigma\in\ldots} \tfrac{12}{|\boldsymbol{C}(\sigma)|} = \tfrac{12}{12} + \tfrac{12}{|\boldsymbol{C}((1\,2)(3\,4))|} + \tfrac{12}{|\boldsymbol{C}((1\,2\,3))|} + \tfrac{12}{|\boldsymbol{C}((1\,3\,2))|} = 1 + \tfrac{12}{4} + \tfrac{12}{3} + \tfrac{12}{3} = 12.$$

* * *

Esercizio 2.3.8. Verificare l'equazione delle classi e la formula di Burnside per il gruppo $\boldsymbol{S}_4$.

Soluzione. Le classi di coniugio di $\boldsymbol{S}_4$ sono, come noto da **Alg. 1**, in corrispondenza biunivoca con le diverse strutture cicliche di $\boldsymbol{S}_4$. Pertanto sono le seguenti cinque:

$$(\_),\ (\_\,\_),\ (\_\,\_)(\_\,\_),\ (\_\,\_\,\_),\ (\_\,\_\,\_\,\_).$$

Scegliamo come rappresentante in ciascuna di esse rispettivamente le permutazioni:

$$(1),\ (1\,2),\ (1\,2)(3\,4),\ (1\,2\,3),\ (1\,2\,3\,4).$$

Deve risultare:

$$|\boldsymbol{S}_4| = 24 = \tfrac{24}{|\boldsymbol{C}((1))|} + \tfrac{24}{|\boldsymbol{C}((1\,2))|} + \tfrac{24}{|\boldsymbol{C}((1\,2)(3\,4))|} + \tfrac{24}{|\boldsymbol{C}((1\,2\,3))|} + \tfrac{24}{|\boldsymbol{C}((1\,2\,3\,4))|}.$$

Si ha:

$\boldsymbol{C}((1)) = \boldsymbol{S}_4$,

$\boldsymbol{C}((1\,2)) = \langle(1\,2),\ (3\,4)\rangle \cong \boldsymbol{V}$ (gruppo di Klein),

$\boldsymbol{C}((1\,2)(3\,4)) = \langle(1\,2)(3\,4),\ (1\,3\,2\,4)\rangle \cong \boldsymbol{D}_4$ (gruppo diedrale),

$\boldsymbol{C}((1\,2\,3)) = \langle(1\,2\,3)\rangle \cong \boldsymbol{C}_3$,

$\boldsymbol{C}((1\,2\,3\,4)) = \langle(1\,2\,3\,4)\rangle \cong \boldsymbol{C}_4$.

Pertanto l'equazione delle classi è verificata, essendo:

$$\tfrac{24}{24} + \tfrac{24}{4} + \tfrac{24}{8} + \tfrac{24}{3} + \tfrac{24}{4} = 1 + 6 + 3 + 8 + 6 = 24$$

Le orbite (rispetto all'azione di coniugio su $\boldsymbol{S}_4$) sono le classi di coniugio. Dunque in $\boldsymbol{S}_4$ sono cinque (corrispondenti alle strutture cicliche). La formula di Burnside ci dice che

$$5 = \tfrac{1}{24} \sum_{\sigma \in \boldsymbol{S}_4} |(\boldsymbol{S}_4)_\sigma|.$$

Si ha: $(\boldsymbol{S}_4)_\sigma = \{\tau \in \boldsymbol{S}_4 \,\big|\, \tau * \sigma = \sigma\} = \{\tau \in \boldsymbol{S}_4 \,\big|\, \tau \circ \sigma = \sigma \circ \tau\} = \boldsymbol{C}(\sigma)$. Basta allora calcolare gli ordini dei centralizzanti (che sono invarianti all'interno di ogni struttura ciclica).

In $\boldsymbol{S}_4$ ci sono: un 1-ciclo, sei 2-cicli, tre coppie di 2-cicli disgiunti, otto 3-cicli e sei 4-cicli. Pertanto la formula di Burnside fornisce:

$$\tfrac{1}{24}\big(1\cdot 24 + 6\cdot 4 + 3\cdot 8 + 8\cdot 3 + 6\cdot 4\big) = \tfrac{1}{24}(24\cdot 5) = 5$$

* * *

Esercizio 2.3.9. Sia ω un'azione di un gruppo G su un anello unitario A.

(*i*) Verificare che ω si estende in modo naturale ad un'azione $\overline{\omega}$ su $A[X]$.

(*ii*) Verificare che $\overline{\omega}$ non è mai transitiva, ma anzi ha sempre infinite orbite.

(*iii*) Verificare che $\boldsymbol{St}_X$ (rispetto a $\overline{\omega}$) coincide con $\boldsymbol{St}_{1_A}$.

Soluzione. (*i*) Si definisce:

$$\overline{\omega} : G \times A[X] \to A[X] \text{ tale che } \overline{\omega}\big(g, \sum_{i=0}^{n} a_i X^i\big) = \sum_{i=0}^{n} g \cdot a_i X^i, \ \ \forall\, g \in G, \ \forall \sum_{i=0}^{n} a_i X^i \in A[X].$$

Si ha:

$$\overline{\omega}\big(1, \sum_{i=0}^{n} a_i X^i\big) = \sum_{i=0}^{n} 1 \cdot a_i X^i = \sum_{i=0}^{n} a_i X^i;$$

$$\overline{\omega}\big(g, \overline{\omega}\big(h, \sum_{i=0}^{n} a_i X^i\big)\big) = \sum_{i=0}^{n} g \cdot (h \cdot a_i) X^i = \sum_{i=0}^{n} gh \cdot a_i X^i = \overline{\omega}\big(gh, \sum_{i=0}^{n} a_i X^i\big).$$

Dunque $\overline{\omega}$ è un'azione di G su $A[X]$.

(*ii*) Posto $1_A = 1$, si ha:

$$\overline{\boldsymbol{O}}(1) = \{g\cdot 1, \ \forall\, g \in G\} \subseteq A; \ \ \overline{\boldsymbol{O}}(X^k) = \{g \cdot X^k, \ \forall\, g \in G\} = \{(g\cdot 1)X^k, \ \forall\, g \in G\} \subseteq AX^k.$$

Ne segue che $\overline{\omega}$ ammette le infinite orbite $\overline{\boldsymbol{O}}(X^k)$, $\forall\, k \geq 0$.

(*iii*) Si ha:

$$\boldsymbol{St}_X = \{g \in G \,|\, g \cdot X = X\}.$$

Ma $g\cdot X = (g\cdot 1)X$ e $(g\cdot 1)X = X \iff g\cdot 1 = 1 \iff g \in \boldsymbol{St}_{1_A}$. Dunque $\boldsymbol{St}_X = \boldsymbol{St}_{1_A}$.

* * *

Esercizio 2.3.10. Sia G un gruppo non abeliano di ordine p^3, con p primo. Verificare che il suo centro $\boldsymbol{Z}(G)$ ha ordine p.

Soluzione. G è un p-gruppo e quindi $\boldsymbol{Z}(G) \neq \{1\}$. Poiché G non è abeliano, $|\boldsymbol{Z}(G)| \neq p^3$. Si hanno quindi due sole possibilità:

$$|\boldsymbol{Z}(G)| = p \ \text{ oppure } \ |\boldsymbol{Z}(G)| = p^2.$$

Per assurdo, sia $|\boldsymbol{Z}(G)| = p^2$. Si scelga un elemento $a \in G - \boldsymbol{Z}(G)$. Ovviamente $\boldsymbol{Z}(G) \leq \boldsymbol{C}(a)$. Inoltre $a \in \boldsymbol{C}(a)$ e $a \notin \boldsymbol{Z}(G)$. Dunque $\boldsymbol{Z}(G) < \boldsymbol{C}(a)$ e pertanto $|\boldsymbol{C}(a)| = p^3$, cioè $\boldsymbol{C}(a) = G$. Ma allora $a \in \boldsymbol{Z}(G)$: assurdo.

Nota. Con la stessa argomentazione si può verificare che se G è un p-gruppo non abeliano, con $|G| = p^n$, allora

$$p \leq |\boldsymbol{Z}(G)| \leq p^{n-2}.$$

* * *

Esercizio 2.3.11. Sia $H \leq G$. Definiamo *centralizzante di* H *in* G l'insieme

$$\mathcal{C}(H) = \{x \in G \mid xh = hx, \ \forall\, h \in H\}.$$

(*i*) Verificare che $\mathcal{C}(H)$ è un sottogruppo di G e che $\mathcal{C}(H) \leq \mathcal{N}(H)$.

(*ii*) Verificare che $\mathcal{C}(H) \trianglelefteq \mathcal{N}(H)$. *Suggerimento*: costruire un opportuno omomorfismo da $\mathcal{N}(H)$ ad $\boldsymbol{Aut}(H)$, di cui $\mathcal{C}(H)$ sia il nucleo.

Soluzione. (*i*) Proviamo che $\mathcal{C}(H) \leq G$. Presi comunque $x, y \in \mathcal{C}(H)$, si ha, $\forall\, h \in H$:
$1h = h = h1$ e quindi $1 \in \mathcal{C}(H)$;
$h(xy) = (hx)y = (xh)y = x(hy) = x(yh) = (xy)h$ e quindi $xy \in \mathcal{C}(H)$;
$h^{-1}x = xh^{-1}$ e quindi $x^{-1}h = (h^{-1}x)^{-1} = (xh^{-1})^{-1} = hx^{-1}$. Allora $x^{-1} \in \mathcal{C}(H)$.

Sia $x \in \mathcal{C}(H)$. Poiché $xh = hx, \ \forall\, h \in H$, allora $xH = Hx$ e quindi $x \in \mathcal{N}(H)$. Pertanto $\mathcal{C}(H) \leq \mathcal{N}(H)$.

(*ii*) Si ponga:

$$\varphi : \mathcal{N}(H) \to \boldsymbol{Aut}(H) \ \text{ tale che } \ \varphi(x) = \gamma_x, \ \forall\, x \in \mathcal{N}(H)$$

[si noti che, a priori, $\gamma_x \in \boldsymbol{Aut}(G)$. Ma $\gamma_x(H) = xHx^{-1} = H, \ \forall\, x \in \mathcal{N}(H)$. Dunque $\gamma_x \in \boldsymbol{Aut}(H)$]. L'applicazione φ è un omomorfismo di gruppi, cioè $\varphi(xy) = \varphi(x) \circ \varphi(y), \ \forall\, x, y \in \mathcal{N}(H)$. Infatti

$$(\gamma_x \circ \gamma_y)(h) = \gamma_x(yhy^{-1}) = x(yhy^{-1})x^{-1} = (xy)h(xy)^{-1}) = \gamma_{xy}(h), \ \forall\, h \in H.$$

Risulta:

$$x \in Ker\varphi \iff \gamma_x = \mathbf{1}_H \iff xhx^{-1} = h, \ \forall\, h \in H \iff x \in \mathcal{C}(H).$$

Ne segue che $\mathcal{C}(H) \trianglelefteq \mathcal{N}(H)$ (essendo un nucleo).

* * *

Esercizio 2.4.1. Quanti sono, a meno di isomorfismi, i gruppi di ordine 33 ?

Soluzione. Sia $|G| = 33$. Poiché $33 = 3 \cdot 11$, dal primo teorema di Sylow, G contiene 3-Sylow (di ordine 3) e 11-Sylow (di ordine 11). Sia r il numero dei 3-Sylow e s il numero degli 11-Sylow. Dal terzo teorema di Sylow,

$$r \,\big|\, 11, \ r \equiv 1 \ (mod\, 3) \quad \text{e} \quad s \,\big|\, 3, \ s \equiv 1 \ (mod\, 11).$$

Ne segue subito che $r = s = 1$.

Sia $H = \langle a \mid a^3 = 1 \rangle$ l'unico 3-Sylow e sia $K = \langle b \mid b^{11} = 1 \rangle$ l'unico 11-Sylow di G. Tali sottogruppi sono normali in G (perché unici del rispettivo ordine). Inoltre $HK = G$ e $H \cap K = \{1\}$. Pertanto: $G \cong H \times K \cong \boldsymbol{C}_3 \times \boldsymbol{C}_{11} \cong \boldsymbol{C}_{33}$. Abbiamo così provato che, a meno di isomorfismi, esiste un unico gruppo di ordine 33: $\boldsymbol{C}_{33}$.

* * *

Esercizio 2.4.2. Sia G un gruppo di ordine 20.

(*i*) Dimostrare che G ha un unico sottogruppo normale di ordine 5.

(*ii*) Quanti e quali sottogruppi di ordine 4 può ammettere ?

Soluzione. (*i*) Sia r il numero dei 5-Sylow. Risulta:

$$r \,\big|\, 4 \quad \text{e} \quad r \equiv 1 \ (mod\, 5).$$

Dunque $r = 1$, cioè G ha un unico 5-Sylow, di ordine 5. Trattandosi dell'unico sottogruppo di ordine 5, è normale.

(*ii*) I 2-Sylow hanno ordine 4. Dunque sono gruppi ciclici o di Klein. Poiché sono coniugati tra loro (per il teorema di Sylow), sono necessariamente tutti ciclici o tutti di Klein. Sia s il numero dei 2-Sylow. Risulta:

$$s \,\big|\, 5 \quad \text{e} \quad s \equiv 1 \ (mod\, 2). \ \text{Allora } \ s = 1 \ \text{ oppure } \ s = 5.$$

Esempi di gruppi con $s = 1$ sono: il gruppo ciclico $\boldsymbol{C}_{20}$ (che ammette un unico $\boldsymbol{C}_4$) ed il gruppo $\boldsymbol{C}_2 \times \boldsymbol{C}_2 \times \boldsymbol{C}_5$ (isomorfo a $\boldsymbol{C}_2 \times \boldsymbol{C}_{10}$), che ammette un solo sottogruppo di di Klein (isomorfo a $\boldsymbol{C}_2 \times \boldsymbol{C}_2$): infatti si può facilmente verificare che tale gruppo ha esattamente tre elementi di periodo 2.

Veniamo ad esempi di gruppi (sempre di ordine 20), con $s = 5$. Innanzitutto c'è il gruppo diedrale $\boldsymbol{D}_{10} = \langle \varphi, \rho \mid \varphi^{10} = \rho^2 = 1;\ \rho \circ \varphi = \varphi^9 \circ \rho \rangle$, che ammette esattamente cinque sottogruppi di Klein:

$$\langle \varphi^5, \rho \rangle, \quad \langle \varphi^5, \varphi \circ \rho \rangle, \quad \langle \varphi^5, \varphi^2 \circ \rho \rangle, \quad \langle \varphi^5, \varphi^3 \circ \rho \rangle, \quad \langle \varphi^5, \varphi^4 \circ \rho \rangle.$$

Esiste anche un gruppo che ammette cinque cicli $\boldsymbol{C}_4$. Si tratta del seguente gruppo:

$$\mathbf{Q}_{10} = \left\langle x, y \,\middle|\, x^{10} = 1,\ y^2 = x^5 = (xy)^2 \right\rangle = \{1,\ x,\ x^2,\ ...,\ x^9,\ y,\ xy,\ x^2y,\ ...,\ x^9y\}.$$

Si verifica infatti che tale gruppo ammette almeno tre elementi di periodo 4: y, xy, x^2y. Dunque ha almeno due sottogruppi ciclici $\boldsymbol{C}_4$ e quindi ne ha cinque.

Nota. Il gruppo $\mathbf{Q}_{10}$ fa parte della famiglia dei *gruppi diciclici* $\mathbf{Q}_n$, con n pari ≥ 2, così definiti:

$$\mathbf{Q}_n = \left\langle x, y \,\middle|\, x^n = 1,\ y^2 = (xy)^2 = x^{n/2} \right\rangle.$$

Si verifica facilmente che $yx = x^{n-1}y$ e quindi $\mathbf{Q}_n = \{x^k y^i,\ 0 \leq k < n,\ 0 \leq i \leq 1\}$. Ne segue che $|\mathbf{Q}_n| = 2n$. È immediato verificare che $\mathbf{Q}_2 \cong \boldsymbol{C}_4$.

* * *

Esercizio 2.4.3. Determinare tutti i sottogruppi di ordine 8 di $\boldsymbol{S}_4$.

Soluzione. Poiché $|\boldsymbol{S}_4| = 24 = 3 \cdot 8$, $\boldsymbol{S}_4$ possiede 2-Sylow (di ordine 8). Denotato con s il numero di tali sottogruppi, dal terzo teorema di Sylow segue che

$$s \,\big|\, 3 \quad \text{e} \quad s \equiv 1 \ (mod\ 2).$$

Pertanto $s = 1$ oppure $s = 3$. Poiché i p-Sylow sono sempre a due a due coniugati, trovatone uno, per ottenere gli altri basta coniugarlo; se ne troviamo un altro, allora sono tre.

$\boldsymbol{S}_4$ contiene il sottogruppo $\boldsymbol{D}_4 = \langle (1\,2\,3\,4),\ (2\,4) \rangle$. Si tratta di un 2-Sylow di $\boldsymbol{S}_4$, che denotiamo H. Si ha:

$$H = \{(1),\ (1\,2\,3\,4),\ (1\,3)(2\,4),\ (1\,4\,3\,2),\ (2\,4),\ (1\,4)(2\,3),\ (1\,3),\ (1\,2)(3\,4)\}.$$

Risulta:

$$(1\,2)H(1\,2)^{-1} \ni (1\,2)(1\,2\,3\,4)(1\,2) = (1\,3\,4\,2), \ \text{ ma } \ (1\,3\,4\,2) \notin H.$$

Dunque $(1\,2)H(1\,2)^{-1} \neq H$. Si tratta di un ulteriore 2-Sylow, che denotiamo H_1. Si ha:

$$H_1 = \{(1),\ (1\,3\,4\,2),\ (1\,4)(2\,3),\ (1\,2\,4\,3),\ (1\,4),\ (1\,3)(2\,4),\ (2\,3),\ (1\,2)(3\,4)\} = \langle (1\,2\,4\,3),\ (2\,3) \rangle.$$

Per ottenere l'ultimo 2-Sylow, si osservi che:

$$(1\,4)H(1\,4)^{-1} \ni (1\,4\,2\,3), \ \text{ ma } \ (1\,4\,2\,3) \notin H \cup H_1.$$

Allora $H_2 := (1\,4)H(1\,4)^{-1}$ è il terzo ed ultimo 2-Sylow di $\boldsymbol{S}_4$. Si ha:

$$H_2 = \{(1),\ (1\,4\,2\,3),\ (1\,2)(3\,4),\ (1\,3\,2\,4),\ (1\,2),\ (1\,4)(2\,3),\ (3\,4),\ (1\,3)(2\,4)\} = \langle (1\,3\,2\,4),\ (3\,4) \rangle.$$

* * *

Esercizio 2.4.4. È assegnato il gruppo $G = \langle x, y \mid x^4 = y^3 = 1,\ xy = y^2x \rangle$.

(*i*) Scriverne i dodici elementi e di ciascuno indicare il periodo.

(*ii*) Dall'esame dei periodi degli elementi di G dedurre che G ha soltanto sottogruppi ciclici e determinarne il reticolo.

Soluzione. (*i*) Risulta:

$$G = \{1,\ x,\ x^2,\ x^3,\ y,\ y^2,\ yx,\ yx^2,\ yx^3,\ y^2x,\ y^2x^2,\ y^2x^3\}.$$

Dalle relazioni di definizione del gruppo G, segue che ogni prodotto del tipo $x^k y^h$ o $y^h x^k$ può essere espresso tramite i 12 elementi di G sopra elencati.

Ovviamente: $\circ(1) = 1$, $\circ(x) = \circ(x^3) = 4$, $\circ(x^2) = 2$, $\circ(y) = \circ(y^2) = 3$. Inoltre:

$(yx)^2 = y(xy)x = y\,y^2x\,x = x^2$. Dunque $\circ(yx) = 4$.

$(yx^2)^2 = y(x^2y)x^2 = y(yx^2)x^2 = y^2$ e quindi $(yx^2)^6 = 1$; inoltre $(yx^2)^3 = y^2\,(yx^2) = x^2 \neq 1$.

Dunque $\circ(yx^2) = 6$.

$(yx^3)^2 = y(x^3y)x^3 = y(y^2x^3)x^3 = x^2$. Dunque $\circ(yx^3) = 4$.

Procedendo in modo analogo si ottiene:

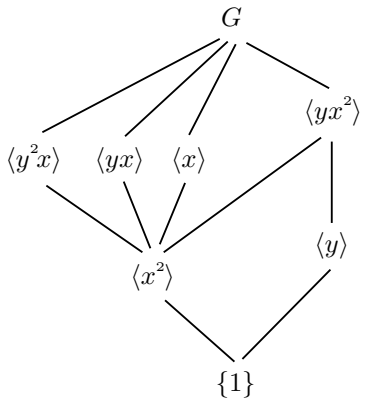
$$\circ(y^2x) = \circ(y^2x^3) = 4, \quad \circ(y^2x^2) = 6.$$

(*ii*) In base al teorema di Lagrange, G può avere soltanto sottogruppi propri di ordine $2, 3, 4, 6$. Da (*i*) si osserva che G ha un solo elemento di periodo 2. Ne segue che G non possiede sottogruppi isomorfi ad $\boldsymbol{S}_3$ né sottogruppi di Klein. Pertanto G può possedere soltanto sottogruppi ciclici. Precisamente G possiede:

- un solo sottogruppo ciclico di ordine 2: $\langle x^2\rangle$;
- un solo sottogruppo ciclico di ordine 3: $\langle y\rangle$;
- un solo sottogruppo ciclico di ordine 6: $\langle yx^2\rangle$;
- tre sottogruppi ciclici di ordine 4: $\langle x^2\rangle$, $\langle yx\rangle$, $\langle y^2x\rangle$.

Nota. I tre 2-Sylow sono ovviamente non normali, mentre tutti gli altri sottogruppi sono normali (in quanto unici del loro ordine).

Conoscendo il reticolo dei gruppi ciclici finiti, possiamo disegnare il reticolo dei sottogruppi di G:



Nota. Esaminando i periodi degli elementi, si può osservare che il gruppo G coincide con il gruppo diciclico $\mathbf{Q}_6$ (cfr. Eserc. **2.4.2**), per quanto i generatori siano assegnati con relazioni diverse.

* * *

Esercizio 2.4.5. È assegnato il gruppo "diciclico" $\mathbf{Q}_4 = \langle\, x, y \mid x^4 = 1;\ y^2 = (xy)^2 = x^2\rangle$.

(*i*) Verificare che $|\mathbf{Q}_4| = 8$ e individuarne gli elementi.

(*ii*) Dimostrare che $\mathbf{Q}_4 \cong \mathbf{Q}$ (gruppo delle unità dei quaternioni).

Soluzione. (*i*) Si noti che il gruppo non è abeliano [se lo fosse, dall'ultima relazione seguirebbe $x^2 = 1$, contro la prima relazione].

In $\mathbf{Q}_4$ sono contenuti gli elementi (a due a due distinti)

$$1,\ x,\ x^2,\ x^3,\ y,\ xy,\ x^2y,\ x^3y.$$

Si noti in particolare che $\circ(y) = 4$ [infatti $y^2 = x^2$ e $\circ(x^2) = 2$].

Per escludere che esistano in $\mathbf{Q}_4$ ulteriori elementi, basta verificare che $yx = x^3y$ [infatti, dalla relazione $(xy)^2 = x^2$ segue: $xy\,xy = x^2 \implies yxy = x \implies yxy\,y^3 = xy^3 \implies yx = x\,x^2\,y = x^3y$]. Come anticipato, $\mathbf{Q}_4$ non contiene ulteriori elementi, oltre a quelli sopra considerati [infatti ogni elemento y^ix^j è di tipo x^hy^k, con $h = 0, 1, 2, 3$, $k = 0, 1$].

(*ii*) Tenuto conto della struttura dei gruppi di ordine 8, $\mathbf{Q}_4$ (non abeliano) può essere isomorfo o al gruppo diedrale $\boldsymbol{D}_4$ o al gruppo delle unità dei quaternioni $\mathbf{Q}$. Mentre $\boldsymbol{D}_4$ ha due soli elementi di periodo 4 (e quindi cinque di periodo 2), $\mathbf{Q}_4$ ha almeno tre elementi di periodo 4, e cioè x, x^3, y. Quindi $\mathbf{Q}_4 \cong \mathbf{Q}$ e la dimostrazione è conclusa. Possiamo comunque verificare che $\mathbf{Q}_4$ ha esattamente

sei elementi di periodo 4 (come $\mathbf{Q}$) e dunque che $\circ(xy) = \circ(x^2y) = \circ(x^3y) = 4$. A tale scopo si verifichi che

$$yx^2 = x^2y,\ yx^3 = xy$$

e, utilizzando tali uguaglianze, che

$$(xy)^2 = y^2,\ (x^2y)^2 = y^2,\ (x^3y)^2 = y^2.$$

* * *

Esercizio 2.4.6. Tenuto conto della classificazione dei gruppi di ordine 12 (cfr. Osserv. **4.3**), dimostrare che $\boldsymbol{C}_2 \times \boldsymbol{S}_3 \cong \boldsymbol{D}_6$ ed esplicitare un isomorfismo tra i due gruppi.

Soluzione. Si ponga:

$$\boldsymbol{S}_3 = \langle x, y \,|\, x^2 = y^3 = 1,\ yx = xy^2 \rangle = \{1, x, y, y^2, xy, xy^2\}, \quad \boldsymbol{C}_2 = \langle \alpha \,|\, \alpha^2 = 1 \rangle = \{1, \alpha\}.$$

Allora

$\boldsymbol{C}_2 \times \boldsymbol{S}_3 = \{(1,1),\ (1,x),\ (1,y),\ (1,y^2),\ (1,xy),\ (1,xy^2),\ (\alpha,1),\ (\alpha,x),\ (\alpha,y),\ (\alpha,y^2),\ (\alpha,xy),\ (\alpha,xy^2)\}$.

Essendo $\boldsymbol{C}_2 \times \boldsymbol{S}_3$ un gruppo non abeliano di ordine 12, potrebbe essere isomorfo ad $\boldsymbol{A}_4$, $\boldsymbol{D}_6$ oppure a $G = \langle x, y \,|\, x^4 = y^3 = 1,\ xy = y^2x \rangle$. Esaminiamo i periodi degli elementi di $\boldsymbol{C}_2 \times \boldsymbol{S}_3$. Risulta subito che tale gruppo ha:

- sette elementi di periodo 2: $(1,x),\ (1,xy),\ (1,xy^2),\ (\alpha,1),\ (\alpha,x),\ (\alpha,xy),\ (\alpha,xy^2)$;
- due elementi di periodo 3: $(1,y),\ (1,y^2)$;
- due elementi di periodo 6: $(\alpha,y),\ (\alpha,y^2)$.

Poiché $\boldsymbol{A}_4$ non ha elementi di periodo 6 e G ha un solo elemento di periodo 2 (cfr. l'esercizio precedente), allora necessariamente $\boldsymbol{C}_2 \times \boldsymbol{S}_3 \cong \boldsymbol{D}_6$.

Ricordiamo che $\boldsymbol{D}_6 = \langle \varphi, \rho \,|\, \varphi^6 = \rho^2 = 1,\ \rho \circ \varphi = \varphi^5 \circ \rho \rangle$. Per ottenere un isomorfismo F da $\boldsymbol{D}_6$ a $\boldsymbol{C}_2 \times \boldsymbol{S}_3$, dobbiamo far corrispondere ai due generatori φ, ρ di $\boldsymbol{D}_6$ elementi di ugual periodo di $\boldsymbol{C}_2 \times \boldsymbol{S}_3$ e verificare che la relazione diedrale $\rho \circ \varphi = \varphi^5 \circ \rho$ venga soddisfatta da $F(\varphi)$, $F(\rho)$. Si ponga:

$$F(\varphi) = (\alpha, y), \quad F(\rho) = (\alpha, x).$$

Deve risultare: $F(\rho) \circ F(\varphi) = F(\varphi^5) \circ F(\rho)$. Infatti si ha: $F(\varphi^5) = F(\varphi)^5 = (\alpha, y)^5 = (\alpha, y^2)$ e

$$F(\rho) \circ F(\varphi) = (\alpha, x)(\alpha, y) = (1, xy), \quad F(\varphi^5) \circ F(\rho) = (\alpha, y^2)(\alpha, x) = (1, y^2x) = (1, xy).$$

Nota. Come visto nella soluzione di **Eserc. 2.2.2**, il sottogruppo $\langle (12) \rangle \cdot \langle (34), (345) \rangle$ di $\boldsymbol{S}_5$ è isomorfo a $\boldsymbol{C}_2 \times \boldsymbol{S}_3$ e quindi, per quanto sopra dimostrato, a $\boldsymbol{D}_6$. Ne segue che $\boldsymbol{D}_6$ si immerge in $\boldsymbol{S}_5$.

Si noti che il teorema di Cayley generalizzato fornisce soltanto immersioni di $\boldsymbol{D}_6$ in $\boldsymbol{S}_6$. Infatti, esaminando il reticolo dei sottogruppi di $\boldsymbol{D}_6$ (cfr. [AA], pag. 173), si osserva che i sottogruppi di $\boldsymbol{D}_6$ privi di sottogruppi normali ($\neq \{1\}$) in $\boldsymbol{D}_6$ sono soltanto di ordine 2 (e quindi di indice 6).

* * *

Esercizio 2.4.7. Verificare che un gruppo G di ordine 30 non è semplice e contiene un sottogruppo di indice 2.

Soluzione. Poiché $30 = 2 \cdot 3 \cdot 5$, G ammette un 3-Sylow H ed un 5-Sylow K, di ordini rispettivamente 3, 5. Trattandosi di sottogruppi di ordine primo (e quindi privi di sottogruppi propri), $H \cap K = \{1\}$. Inoltre sono normali in G (in quanto unici del loro ordine, in base al Coroll. **4.3**). Ne segue che G non è semplice.

Applicando il secondo teorema di isomorfismo,

$$HK/_H \cong K/_{H \cap K} = K/_{\{1\}} \cong K$$

e dunque $|HK| = |H| \cdot |K| = 15$. Allora $(G : HK) = 2$ ed HK è il sottogruppo richiesto.

Si noti che HK è ciclico di ordine 15, come noto dal Coroll. **4.2**).

* * *

Esercizio 2.4.8. Perché un gruppo G di ordine 12 non può avere contemporaneamente tre 2-Sylow e quattro 3-Sylow?

Soluzione. Indicato con s il numero dei 2-Sylow (che hanno ordine 4) e con t e il numero dei 3-Sylow, risulta dal terzo teorema di Sylow che $s = 1, 3$ e $t = 1, 4$.

Per assurdo assumiamo $s = 3$ e $t = 4$. Poiché G ammette quattro 3-Sylow, ammette otto elementi di periodo 3 e quindi ammette esattamente tre elementi di periodo pari. Dunque G non può contenere né tre sottogruppi ciclici $\boldsymbol{C}_4$ [che necessitano di sei elementi di periodo 4], né tre sottogruppi di Klein $\boldsymbol{V}$ [che necessitano di almeno quattro elementi di periodo 2]. Ne segue l'assurdo.

Nota. Da Osserv. **4.3** è noto che, a meno di isomorfismo, i gruppi di ordine 12 sono:

$$\boldsymbol{C}_{12}, \quad \boldsymbol{V}\times\boldsymbol{C}_3, \quad \boldsymbol{A}_4, \quad \boldsymbol{D}_6, \quad \mathbf{Q}_6 = \langle\, x, y \mid x^4 = y^3 = 1,\ xy = y^2x\rangle.$$

Esaminando tali gruppi, si constata che:

$\boldsymbol{C}_{12}$ ha $(s,t) = (1,1)$, con un ciclico $\boldsymbol{C}_4$;

$\boldsymbol{V}\times\boldsymbol{C}_3$ ha $(s,t) = (1,1)$, con un sottogruppo di Klein;

$\boldsymbol{A}_4$ ha $(s,t) = (1,4)$, con un sottogruppo di Klein;

$\boldsymbol{D}_6$ ha $(s,t) = (3,1)$, con tre sottogruppi di Klein;

$\mathbf{Q}_6$ ha $(s,t) = (3,1)$, con tre sottogruppi ciclici $\boldsymbol{C}_4$.

Come si può notare, non si presenta il caso di un gruppo G con $(s,t) = (1,4)$ ed avente come unico 2-Sylow un sottogruppo $\boldsymbol{C}_4$.

* * *

Esercizio 2.4.9. Assegnato il gruppo G, prodotto diretto di $\boldsymbol{S}_3$ per se stesso, determinare i sottogruppi di Sylow di G. [Si ponga $\boldsymbol{S}_3 = \langle x, y \,\big|\, x^2 = y^3 = 1,\ yx = xy^2\rangle$].

Soluzione. Poiché $G = \boldsymbol{S}_3\times\boldsymbol{S}_3$ ha ordine $36 = 2^2 3^2$, G possiede 2-Sylow (di ordine 4) e 3-Sylow (di ordine 9). Indicati rispettivamente con r, s il numero dei 2-Sylow e dei 3-Sylow, risulta, in base al terzo teorema di Sylow:

$$r \,\big|\, 9,\ r \equiv 1\ (mod\ 2); \quad s \,\big|\, 4,\ s \equiv 1\ (mod\ 3)$$

e dunque i possibili valori di r, s sono: $r = 1, 3, 9$ ed $s = 1, 4$.

Osservato che $\boldsymbol{S}_3$ ha due elementi di periodo 3 (y, y^2) e tre elementi di periodo 2 (x, xy, xy^2), allora G ha elementi di periodo 1, 2, 3, 6. Precisamente G ha:

- 15 elementi di periodo 2: $(1,x)$, $(1,xy)$, $(1,xy^2)$, $(x,1)$, (x,x), (x,xy), (x,xy^2), $(xy,1)$, (xy,x), (xy,xy), (xy,xy^2), $(xy^2,1)$, (xy^2,x), (xy^2,xy), (xy^2,xy^2);
- 8 elementi di periodo 3: $(1,y)$, $(1,y^2)$, $(y,1)$, (y,y), (y,y^2), $(y^2,1)$, (y^2,y), (y^2,y^2);
- 12 elementi di periodo 6: (x,y), (x,y^2), (xy,y), (xy,y^2), (xy^2,y), (xy^2,y^2), (y,x), (y,xy), (y,xy^2), (y^2,x), (y^2,xy), (y^2,xy^2).

Ogni 3-Sylow, avendo ordine 9, è isomorfo a $\boldsymbol{C}_9$ o a $\boldsymbol{C}_3\times\boldsymbol{C}_3$. Ma G non ha elementi di periodo 9 e dunque è isomorfo a $\boldsymbol{C}_3\times\boldsymbol{C}_3$. Ogni siffatto gruppo possiede otto elementi di periodo 3. Ma G ha solo otto elementi di periodo 3 e quindi esiste un unico 3-Silow: $\langle y\rangle\times\langle y\rangle$.

I 2-Sylow, avendo ordine 4, sono isomorfi a $\boldsymbol{C}_4$ o a $\boldsymbol{V}$ (gruppo di Klein). Ma G non ha elementi di periodo 4 e dunque sono isomorfi a $\boldsymbol{V}$. Ogni gruppo di Klein possiede tre elementi di periodo 2, che commutano tra loro. Basta allora esaminare i centralizzanti dei vari elementi di periodo 2.

Si osservi che in un prodotto diretto $G_1\times G_2$ risulta $\boldsymbol{C}((g_1,g_2)) = \boldsymbol{C}((g_1))\times\boldsymbol{C}((g_2))$, $\forall\,(g_1,g_2) \in G_1\times G_2$. Inoltre in $\boldsymbol{S}_3$ risulta: $\boldsymbol{C}(x) = \langle x\rangle$, $\boldsymbol{C}(xy) = \langle xy\rangle$, $\boldsymbol{C}(xy^2) = \langle xy^2\rangle$. Ne segue allora che, scelta una coppia di elementi entrambi di periodo 2, il centralizzante ha ordine 4 e dunque è un gruppo di Klein. Ad esempio $\boldsymbol{C}((x,x)) = \langle (1,x),\,(x,1)\rangle$. Esistono nove coppie formate da elementi di periodo 2 e conseguentemente esistono nove 2-Sylow (gruppi di Klein). Sono:

$$\boldsymbol{C}((x,x)),\ \boldsymbol{C}((x,xy)),\ \boldsymbol{C}((x,xy^2)),\ \boldsymbol{C}((xy,x)),\ \boldsymbol{C}((xy,xy)),$$
$$\boldsymbol{C}((xy,xy^2)),\ \boldsymbol{C}((xy^2,x)),\ \boldsymbol{C}((xy^2,xy)),\ \boldsymbol{C}((xy^2,xy^2)).$$

* * *

Esercizio 2.4.10. (*i*) Se $|G| = p\,q$, con p, q primi, verificare che G non è semplice.
(*ii*) Se $|G| = pq$, con $p < q$ e $q \not\equiv 1 \ (mod\, p)$, verificare che G è ciclico.

Soluzione. (*i*) Se $p = q$, G è un p-gruppo di ordine p^2. Quindi G è abeliano. Poiché G ammette sottogruppi propri (di ordine p), allora G non è semplice.

Sia $p \neq q$, con $p < q$. Fissiamo in G un q-Sylow H (che ha ordine q). Per provare che G non è semplice basta verificare (cfr. Osserv. **1.2**) che $|G| \not| (G : H)!$. Infatti

$$(G : H)! = \left(\tfrac{|G|}{|H|}\right)! = \tfrac{pq}{q}\,! = p! \ \text{ e } \ pq = |G| \not| p! \ \text{ (essendo } \ p < q).$$

(*ii*) Sia r il numero dei p-Sylow ed s il numero dei q-Sylow. In base al terzo teorema di Sylow:

$$r \,|\, q \ \text{ e } \ r \equiv 1 \ (mod\, p); \quad s \,|\, p \ \text{ e } \ s \equiv 1 \ (mod\, q).$$

A priori, $r = 1, q$. Ma, per ipotesi, $q \not\equiv 1 \ (mod\, p)$ e dunque $r = 1$. A priori, $s = 1, p$. Ma, poiché $1 < p < q$, allora $p \not\equiv 1 \ (mod\, q)$ e dunque anche $s = 1$.

Consideriamo in G l'unico p-Sylow H e l'unico q-Sylow K. Si tratta di due sottogruppi ciclici di G, entrambi normali in G. Ovviamente $H \cap K = \{1\}$ e $HK = G$ [infatti $|HK| = |H|\,|K| = pq = |G|$]. In base al Teor. **2.1** ed al Cor. **2.1** del Cap. **2**, $G \cong H \times K$ è ciclico.

* * *

Esercizio 2.4.11. Sia S un p-Sylow di un gruppo (finito) G. Verificare che $\mathcal{N}(\mathcal{N}(S)) = \mathcal{N}(S)$.

Soluzione. Poiché $\mathcal{N}(\mathcal{N}(S)) \geq \mathcal{N}(S)$, basta verificare che $x \in \mathcal{N}(\mathcal{N}(S)) \implies x \in \mathcal{N}(S)$.

Per ipotesi, $x\mathcal{N}(S) = \mathcal{N}(S)x$, cioè $\mathcal{N}(S) = x\mathcal{N}(S)x^{-1}$. Allora, posto $T := xSx^{-1}$, risulta:

$$T \subseteq x\mathcal{N}(S)x^{-1} = \mathcal{N}(S).$$

Ovviamente S è normale in $\mathcal{N}(S)$ e dunque è l'unico p-Sylow di $\mathcal{N}(S)$. Ma anche T (che ha lo stesso ordine di S) è un p-Sylow di $\mathcal{N}(S)$. Dunque $T = S$ e pertanto $xSx^{-1} = S$, cioè $x \in \mathcal{N}(S)$.

Nota. Più generalmente, con la stessa dimostrazione si può provare che, per ogni sottogruppo H di G tale che $\mathcal{N}(S) \leq H$ (con S p-Sylow di G), risulta: $\mathcal{N}(H) = H$.

[Infatti S è anche un p-Sylow di H. Sia $x \in \mathcal{N}(H)$ e $T := xSx^{-1}$. Per l'ipotesi, T è un altro p-Sylow di H e quindi $S = yTy^{-1}$, $\exists\, y \in H$. Allora $S = yxS(yx^{-1})$. Quindi $yx \in \mathcal{N}(S) \leq H$ e anche $x = y^{-1}(yx) \in H$. Si conclude che $\mathcal{N}(H) = H$].

* * *

Esercizio 2.4.12. Sia p un primo e G un gruppo finito. Verificare che

$$G \text{ è } p\text{-gruppo} \iff \forall\, x \in G, \ \circ(x) \text{ è una potenza di } p.$$

Soluzione. ($\Longrightarrow$). Sia $|G| = p^n$. Per ogni $x \in G$, $|\langle x\rangle| \,|\, p^n$, cioè $\circ(x) \,|\, p^n$. Dunque $\circ(x)$ è una potenza di p.

($\Longleftarrow$). Per assurdo, $|G|$ ammetta un altro divisore primo q ($\neq p$). Dal teorema di Cauchy, G contiene un elemento x di periodo q. Ma $\circ(x) = p^t$, con $t \geq 0$. Dunque $p^t = q$: assurdo.

* * *

SOLUZIONI DEGLI ESERCIZI

DEL CAPITOLO 3

Esercizio 3.1.1. Sia $A = 2\boldsymbol{Z}$ (anello non unitario) e sia $M = 4\boldsymbol{Z}$.

(*i*) Verificare che M è un ideale massimale di A.

(*ii*) Verificare che $A/_M$ non è un campo.

Soluzione. (*i*) Evidentemente $M - M \subseteq M$ e $MA \subseteq M$. Dunque M è un ideale di A. Sia ora I un ideale di A tale che $M \subset I \subseteq A$. Vogliamo dimostrare che $I = A$.

Si scelga $x \in I - M$. Allora $x = 2(2h+1)$, $\exists\, h \in \boldsymbol{Z}$. Ne segue che $2 = x - 4h \in I + M \subseteq I + I \subseteq I$ e pertanto $2 + 4\boldsymbol{Z} \subseteq I + M \subseteq I$. Allora $2\boldsymbol{Z} = 4\boldsymbol{Z} \cup (2 + 4\boldsymbol{Z}) \subseteq I$ cioè $A = I$, come richiesto.

(*ii*) $A/_M$ è formato da due elementi:

$$M = 4\boldsymbol{Z} \text{ (elemento neutro)}, \; 2 + 4\boldsymbol{Z}.$$

Si ha: $(2+4\boldsymbol{Z})(2+4\boldsymbol{Z}) = 4\boldsymbol{Z}$. Pertanto $2+4\boldsymbol{Z}$ è uno 0-divisore non banale di $A/_M$. Quindi $A/_M$ non è un campo.

* * *

Esercizio 3.1.2. (*i*) Verificare che $\mathfrak{M}_2(2\boldsymbol{Z})$ è un ideale massimale dell'anello unitario (non commutativo) $\mathfrak{M}_2(\boldsymbol{Z})$.

(*ii*) Verificare che $\mathfrak{M}_2(\boldsymbol{Z})/_{\mathfrak{M}_2(2\boldsymbol{Z})}$ non è un corpo.

Soluzione. (*i*) Si ponga $A = \mathfrak{M}_2(\boldsymbol{Z})$ e $M = \mathfrak{M}_2(2\boldsymbol{Z})$. Si verifica facilmente che

$$M - M \subseteq M, \quad MA \subseteq M, \quad AM \subseteq M.$$

Dunque M è un ideale di A. Sia ora I un ideale di A tale che $M \subset I \subseteq A$. Basta verificare che la matrice unità $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$ [da cui $I = A$ e quindi M è massimale].

Poiché $M \subset I$, I contiene una matrice in cui un elemento è dispari. Affermiamo che non è restrittivo supporre che un tale elemento sia quello di posto $(1,1)$ [cioè nella prima riga e prima colonna].

Sia infatti a dispari e si consideri in A la matrice $\delta := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Si ha:

se $\alpha := \begin{pmatrix} r & a \\ s & t \end{pmatrix} \in I$, allora $\alpha\delta = \begin{pmatrix} a & r \\ t & s \end{pmatrix} \in I$;

se $\beta := \begin{pmatrix} r & s \\ a & t \end{pmatrix} \in I$, allora $\delta\beta = \begin{pmatrix} a & t \\ r & s \end{pmatrix} \in I$;

se $\gamma := \begin{pmatrix} r & s \\ t & a \end{pmatrix} \in I$, allora $\delta\gamma\delta = \begin{pmatrix} a & t \\ s & r \end{pmatrix} \in I$.

Scegliamo quindi in I la matrice $\alpha := \begin{pmatrix} a & r \\ s & t \end{pmatrix}$, con a dispari. Denotiamo con r_1 il più grande intero pari $\leq r$ e analogamente definiamo s_1, t_1, rispetto ad s, t. Allora $\alpha' = \begin{pmatrix} a-1 & r_1 \\ s_1 & t_1 \end{pmatrix} \in M$ e quindi $\beta := \alpha - \alpha' \in I$. Risulta:

$$\beta = \begin{pmatrix} 1 & x \\ y & z \end{pmatrix}, \text{ con } x, y, z \in \{0, 1\}.$$

Moltiplicando opportunamente ciascuna di queste otto matrici con la matrice $\zeta := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, si prova che I contiene la matrice ζ [ad esempio, scelto $\beta = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, risulta $\zeta\beta\zeta = \zeta$; poiché $\zeta\beta\zeta \in AIA \subseteq I$, allora $\zeta \in I$. In modo analogo si verificano gli altri sette casi].

Si osserva ora che $\zeta + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \zeta \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (matrice unità). Dunque $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I$, come richiesto.

(*ii*) Si ricorda che un corpo è un anello unitario (non commutativo), in cui ogni elemento non nullo è invertibile. Dunque un corpo è privo di 0-divisori (non banali), cioè è integro.

Si ponga: $x := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $y := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Ovviamente $x, y \notin M$, ma $xy = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \in M$. Posto $\overline{x} = x + M$, $\overline{y} = y + M \in A/_M$, si ha: $\overline{x}\,\overline{y} = \overline{0}$ $(= M)$, con $\overline{x}, \overline{y} \neq \overline{0}$. Dunque $A/_M$ non è integro e quindi non è un corpo.

* * *

Esercizio 3.1.3. Sia K un campo e sia $P = (a, b) \in K^2$.

(*i*) Verificare che $(X - a, Y - b)$ è un ideale massimale di $K[X, Y]$.

(*ii*) Sia $F \in K[X, Y]$ tale che $F(P) = 0$. Verificare che $(F) \subseteq (X - a, Y - b)$.

Soluzione. (*i*) Risulta:

$$K[X,Y]/_{(X-a,\,Y-b)} \cong \frac{K[X,Y]/_{(X-a)}}{(X-a,\,Y-b)/_{(X-a)}} \cong K[Y]/_{(Y-b)} \cong K.$$

Dunque $(X - a,\, Y - b)$ è un ideale massimale di $K[X, Y]$.

(*ii*) Sia $\Phi : K[X, Y] \to K[X, Y]$ la *sostituzione lineare* tale che $X \to X + a,\ Y \to Y + b$. Si ricorda che Φ fissa gli elementi di K e trasforma i polinomi di $K[X, Y]$ con le due sostituzioni assegnate. Si tratta di un'applicazione biiettiva [con inversa Φ^{-1} tale che $X \to X - a,\ Y \to Y - b$] e di un omomorfismo di anelli.

Sia ora $\Phi(F) = \tilde{F}$. Si ha:

$$\tilde{F}(0, 0) = F(0 + a, 0 + b) = F(P) = 0.$$

Poiché $\tilde{F}$ ha termine noto nullo, allora $\tilde{F} \in (X,\, Y)$. Quindi $\exists\, A = A(X, Y)$, $B = B(X, Y) \in K[X, Y]$ tali che $\tilde{F} = XA + YB$. Si ha:

$$F = \Phi^{-1}(\Phi(F)) = \Phi^{-1}(\tilde{F}) = (X - a)\, A(X - a, Y - b) + (Y - b)\, B(X - a, Y - b).$$

Dunque $F \in (X - a,\, Y - b)$ e pertanto $(F) \subseteq (X - a,\, Y - b)$.

Nota. Si verificherà nel prossimo § **3** che $K[X, Y]$ è un *UFD*. Ne segue subito che, se F è un polinomio irriducibile in $K[X, Y]$, (F) è un ideale primo.

* * *

Esercizio 3.1.4. Verificare che l'ideale $I = (X^2 + 1, Y)$:

è massimale in $\boldsymbol{R}[X, Y]$, è primo in $\boldsymbol{Z}[X, Y]$, non è primo in $\boldsymbol{C}[X, Y]$.

Calcolarne i rispettivi quozienti.

Soluzione. Risulta:

$$\boldsymbol{R}[X,Y]/_{(X^2+1,\,Y)} \cong \frac{\boldsymbol{R}[X,Y]/_{(Y)}}{(X^2+1,\,Y)/_{(Y)}} \cong \boldsymbol{R}[X]/_{(X^2+1)}.$$

Siccome $\boldsymbol{R}[X]/_{(X^2+1)} \cong \boldsymbol{C}$ (campo), allora I è massimale in $\boldsymbol{R}[X, Y]$.

Analogamente,

$$\boldsymbol{Z}[X,Y]/_{(X^2+1,\,Y)} \cong \boldsymbol{Z}[X]/_{(X^2+1)} \cong \boldsymbol{Z}[i]$$

e $\boldsymbol{Z}[i]$ è un dominio (non campo). Allora I è primo (non massimale) in $\boldsymbol{Z}[X, Y]$.

Infine,

$$\boldsymbol{C}[X,Y]/_{(X^2+1,\,Y)} \cong \boldsymbol{C}[X]/_{(X^2+1)}.$$

In $\boldsymbol{C}[X]$, $X^2 + 1 = (X + i)(X - i)$ (riducibile). Allora $\boldsymbol{C}[X]/_{(X^2+1)} = \boldsymbol{C}[x \mid x^2 = -1]$ non è integro [ha 0-divisori $x + i$, $x - i$]. Perciò I non è primo in $\boldsymbol{C}[X, Y]$.

Nota. Si osserva subito che $(X+i,\, X-i) = \boldsymbol{C}[X]$. Infatti tale ideale contiene ad esempio $2i$ e $2i \in \mathcal{U}(\boldsymbol{C}[X])$ $(= \boldsymbol{C}^{\cdot})$. Ne segue (cfr. Coroll. **3.2** e Coroll. **3.1**, Cap. **1**) che

$$\boldsymbol{C}[X]\big/_{(X^2+1)} \cong \boldsymbol{C}[X]\big/_{(X+i)(X-i)} \cong \boldsymbol{C}[X]\big/_{(X+i)} \times \boldsymbol{C}[X]\big/_{(X-i)} \cong \boldsymbol{C}\times\boldsymbol{C}.$$

* * *

Esercizio 3.1.5. Per ogni $n \geq 2$, determinare $Spec(\boldsymbol{Z}_n)$.

Soluzione. È noto che $\boldsymbol{Z}$ ha soltanto ideali principali. Essendo $\boldsymbol{Z}_n \cong \boldsymbol{Z}\big/_{n\boldsymbol{Z}}$, dal teorema di corrispondenza segue che gli ideali di $\boldsymbol{Z}_n$ sono tutti e soli gli ideali

$$\overline{m}\boldsymbol{Z}_n = m\boldsymbol{Z}\big/_{n\boldsymbol{Z}}, \;\; \forall\; m\boldsymbol{Z} \supseteq n\boldsymbol{Z},$$

cioè $\forall\, m \in \boldsymbol{N}$, con m divisore di n. Inoltre, dal terzo teorema di isomorfismo,

$$\boldsymbol{Z}_n\big/_{\overline{m}\boldsymbol{Z}_n} \cong \frac{\boldsymbol{Z}\big/_{n\boldsymbol{Z}}}{m\boldsymbol{Z}\big/_{n\boldsymbol{Z}}} \cong \boldsymbol{Z}\big/_{m\boldsymbol{Z}} = \boldsymbol{Z}_m\,,$$

Ne segue che

$$\overline{m}\boldsymbol{Z}_n \text{ è primo } \iff \boldsymbol{Z}_m \text{ è integro } \iff m \text{ è primo (con } m \text{ divisore di } n).$$

Pertanto:

$$Spec(\boldsymbol{Z}_n) = \{\overline{p}\boldsymbol{Z}_n,\; \forall\, p \text{ primo: } p \,\big|\, n\}.$$

Ad esempio: $Spec(\boldsymbol{Z}_{12}) = \{\overline{2}\boldsymbol{Z}_{12}, \overline{3}\boldsymbol{Z}_{12}\}$, $\quad Spec(\boldsymbol{Z}_{25}) = \{\overline{5}\boldsymbol{Z}_{12}\}$, $\quad Spec(\boldsymbol{Z}_7) = \{\overline{0}\boldsymbol{Z}_7\}$.

Nota. Poiché $\boldsymbol{Z}_n$ è integro $\iff$ $\boldsymbol{Z}_n$ è un campo, allora $Spec(\boldsymbol{Z}_n) = Max(\boldsymbol{Z}_n)$, $\forall\, n \geq 2$.

* * *

Esercizio 3.1.6. Sia A un anello c.u. e sia $Spec(A)$ il suo spettro. Per ogni $S \subseteq A$ si definisce:

$$V(S) = \{\mathfrak{p} \in Spec(A) \,\big|\, \mathfrak{p} \supseteq S\},$$

detto *chiuso di* $Spec(A)$ *definito da* S. Verificare che:

(*i*) $V(A) = \emptyset$ e $V(\emptyset) = Spec(A)$.

(*ii*) $V(S_1) \cup V(S_2) = V(S_1S_2)$, con $S_1S_2 := \{s_1s_2,\; \forall\, s_1 \in S_1,\; \forall\, s_2 \in S_2\}$.

(*iii*) $\bigcap\limits_{i\in I} V(S_i) = V\big(\bigcup\limits_{i\in I} S_i\big)$.

Nota. Poiché le tre proprietà precedenti corrispondono agli assiomi dei chiusi di uno spazio topologico, si è provato che la famiglia $\{V(S),\; \forall\, S \subseteq A\}$ è la famiglia dei chiusi di una topologia su $Spec(A)$. Tale topologia è detta *topologia di Zariski di* $Spec(A)$.

Soluzione. (*i*) è del tutto ovvio. Si noti che risulta anche $V(A) = V(\{1\})$ e $V(\emptyset) = V(\{0\})$.

(*ii*) ($\subseteq$). Se ad esempio $\mathfrak{p} \in V(S_1)$, allora $\mathfrak{p} \supseteq S_1$. Ne segue che $\mathfrak{p} \supseteq S_1A \supseteq S_1S_2$ e quindi $\mathfrak{p} \in V(S_1S_2)$.

($\supseteq$). Sia $\mathfrak{p} \in V(S_1S_2)$ e, ad esempio, $\mathfrak{p} \notin V(S_1)$. Allora $\mathfrak{p} \not\supseteq S_1$ e quindi esiste $s_1 \in S_1 - \mathfrak{p}$. Ma $\mathfrak{p} \supseteq S_1S_2$ e quindi $\mathfrak{p} \ni s_1s_2,\; \forall\, s_2 \in S_2$. Dalla definizione di ideale primo, $\mathfrak{p} \ni s_2,\; \forall\, s_2 \in S_2$. Dunque $\mathfrak{p} \supseteq S_2$, cioè $\mathfrak{p} \in V(S_2)$.

(*iii*) Si ha: $\mathfrak{p} \in \bigcap\limits_{i\in I} V(S_i) \iff \mathfrak{p} \supseteq S_i,\; \forall\, i \in I \iff \mathfrak{p} \supseteq \bigcup\limits_{i\in I} S_i \iff \mathfrak{p} \in V\big(\bigcup\limits_{i\in I} S_i\big)$.

* * *

Esercizio 3.1.7. Sia $f : A \to B$ un omomorfismo di anelli c. u..

(*i*) Dimostrare che f definisce la seguente applicazione

$$\varphi_f : Spec(B) \to Spec(A) \;\text{ tale che }\; \varphi_f(\mathfrak{q}) = f^{-1}(\mathfrak{q}),\;\; \forall\, \mathfrak{q} \in Spec(B)$$

[la controimmagine $f^{-1}(\mathfrak{q})$ è detta *contrazione* o *fibra di* $\mathfrak{q}$].

(*ii*) Determinare un esempio di omomorfismo f in cui un massimale di B ha contrazione non massimale in A.

(*iii*) Verificare che $\varphi_f : Spec(B) \to Spec(A)$ è una funzione continua, rispetto alle topologie di Zariski di $Spec(A)$, $Spec(B)$ (cfr. l'esercizio precedente).

Soluzione. (*i*) È noto che $f^{-1}(\mathfrak{q})$ è un ideale di A [cfr. Cap. **1** Osserv. **2.5**]. Verifichiamo che $f^{-1}(\mathfrak{q})$ è primo in A, se $\mathfrak{q}$ è primo in B. Sia $xy \in f^{-1}(\mathfrak{q})$, con $x \notin f^{-1}(\mathfrak{q})$. Allora $f(xy) = f(x)f(y) \in \mathfrak{q}$. Poiché $f(x) \notin \mathfrak{q}$, allora $f(y) \in \mathfrak{q}$, cioè $y \in f^{-1}(\mathfrak{q})$.

(*ii*) Sia $i : \boldsymbol{Z} \hookrightarrow \boldsymbol{Q}$ l'inclusione canonica. L'ideale (0) è massimale in $\boldsymbol{Q}$, mentre $i^{-1}(0) = (0)$ non è massimale (ma è primo) in $\boldsymbol{Z}$.

(*iii*) Basta provare che la controimmagine di un chiuso di $Spec(A)$ è un chiuso di $Spec(B)$, cioè basta verificare che $\forall\, V(S) \subseteq Spec(A)$, $\varphi_f^{-1}(V(S)) \in Spec(B)$. Proveremo infatti che

$$\varphi_f^{-1}(V(S)) = V(f(S)).$$

Per definizione, $\mathfrak{q} \in \varphi_f^{-1}(V(S)) \iff f^{-1}(\mathfrak{q}) \in V(S) \iff f^{-1}(\mathfrak{q}) \supseteq S$; viceversa, $\mathfrak{q} \in V(f(S)) \iff \mathfrak{q} \supseteq f(S)$. In base a proprietà insiemistiche elementari, se $f^{-1}(\mathfrak{q}) \supseteq S$, allora $\mathfrak{q} \supseteq f(f^{-1}(\mathfrak{q})) \supseteq f(S)$; se invece $\mathfrak{q} \supseteq f(S)$, allora $f^{-1}(\mathfrak{q}) \supseteq f^{-1}(f(S)) \supseteq S$.

* * *

Esercizio 3.1.8. Sia A un anello c.u. e sia $I \in \mathfrak{I}(A)$ tale che $A - I \subseteq \mathcal{U}(A)$. Verificare che I è l'unico ideale massimale di A. [Un anello c.u. con un unico ideale massimale è detto *anello locale*].

Soluzione. Osserviamo che un ideale proprio I di un anello c.u. A non contiene alcun elemento invertibile di A [altrimenti, se $x \in \mathcal{U}(A) \cap I$, allora $1 = x\,x^{-1} \in I$ e dunque $I = A$]. Allora, se $A - I \subseteq \mathcal{U}(A)$, necessariamente $A - I = \mathcal{U}(A)$.

Sia ora J un ideale proprio di A. Allora $J \cap \mathcal{U}(A) = \emptyset$ e dunque $J \subseteq A - \mathcal{U}(A) = I$. Pertanto I è massimale e contiene ogni ideale proprio: quindi è l'unico ideale massimale di A.

* * *

Esercizio 3.1.9. Sia A un anello c.u. e sia I un suo ideale.

(*i*) Verificare che $Spec(A/I) = \{\mathfrak{p}/I,\ \forall\, \mathfrak{p} \in V(I)\}$ [dove $V(I) = \{\mathfrak{p} \in Spec(A) \,|\, \mathfrak{p} \supseteq I\}$].

(*ii*) Posto $I = (X^3, Y) \subset \boldsymbol{Q}[X, Y]$, determinare $Spec(\boldsymbol{Q}[X, Y]/I)$.

Soluzione. (*i*) Sia $\mathfrak{p} \in V(I)$. Allora, dal terzo teorema di isomorfismo, $\frac{A/I}{\mathfrak{p}/I} \cong A/\mathfrak{p}$. Poiché $A/\mathfrak{p}$ è un dominio, anche $\frac{A/I}{\mathfrak{p}/I}$ lo è e quindi $\mathfrak{p}/I \in Spec(A/I)$.

Viceversa, ogni ideale proprio di A/I è di tipo J/I, con $J \in \mathfrak{I}(A)$, $J \supseteq I$. Se J/I è primo, l'anello $\frac{A/I}{J/I}$ è un dominio e quindi anche A/J è un dominio, cioè J è primo. Dunque $J \in V(I)$.

(*ii*) Risulta: $\boldsymbol{Q}[X, Y]/I \cong \boldsymbol{Q}[X]/(X^3)$. Inoltre gli ideali di $\boldsymbol{Q}[X]$ sono tutti principali. Per ogni ideale primo (f) in $\boldsymbol{Q}[X]$ contenente (X^3), f è un divisore di X^3. Essendo f irriducibile, risulta, a meno di un fattore invertibile, $f = X$. Dunque

$$Spec(\boldsymbol{Q}[X]/(X^3)) = \{(X)/(X^3)\} \text{ e quindi } Spec(\boldsymbol{Q}[X, Y]/I) = \{(X, Y)/I\}.$$

* * *

Esercizio 3.1.10. (*i*) Sia A un anello c.u.. Verificare che i chiusi della topologia di Zariski di $Spec(A)$ sono tutti e soli della forma $V(I)$, con I ideale di A.

(*ii*) Determinare i chiusi di $Spec(\boldsymbol{Z})$.

Soluzione. (*i*) Basta verificare che, $\forall\, S \subseteq A$, $V(S) = V((S))$, con (S) ideale di A generato da S. Ovviamente $V(S) \supseteq V((S))$ [se $\mathfrak{p} \supseteq (S)$, allora $\mathfrak{p} \supseteq S$]; viceversa, se $\mathfrak{p} \supseteq S$, allora $\mathfrak{p} \supseteq (S)$ (più piccolo ideale contenente S).

(*ii*) È noto che gli ideali di $\boldsymbol{Z}$ sono tutti e soli della forma $n\boldsymbol{Z}$, $\forall\, n \in \boldsymbol{N}$. Da (*i*) segue quindi che i chiusi di $Spec(\boldsymbol{Z})$ sono tutti e soli i chiusi $V(n\boldsymbol{Z})$, $\forall\, n \in \boldsymbol{N}$.

Risulta: $V((0)) = Spec(\boldsymbol{Z})$ e $V((1)) = V(\boldsymbol{Z}) = \emptyset$. Per ogni $n \geq 2$, se n ha come fattori primi $p_1, \dots, p_n$, allora $V(n\boldsymbol{Z}) = \{(p_1), \dots, (p_n)\}$ [infatti $(p) \supseteq (n) \iff p \,|\, n$]. Dunque i chiusi propri di $Spec(\boldsymbol{Z})$ corrispondono biunivocamente ai sottoinsiemi finiti di numeri primi.

Nota. I singoli primi sono punti chiusi [infatti $V(p\boldsymbol{Z}) = \{(p)\}$. Invece $\{(0)\}$ non è chiuso [ed ha chiusura $Spec(\boldsymbol{Z})$].

* * *

Esercizio 3.1.11. Sia A un anello commutativo unitario. È noto da **Alg. 1** che due elementi $a, b \in A$ sono detti *associati* (e si scrive $a \sim b$) se $b = au$, $\exists\, u \in \mathcal{U}(A)$.

(*i*) Verificare che $\sim$ è una relazione di equivalenza su A, che $a \sim b \implies (a) = (b)$ e che, se A è integro, $a \sim b \iff (a) = (b)$.

(*ii*) Verificare che, se $a \sim b$, risulta: a irriducibile [risp. primo] $\implies b$ irriducibile [risp. primo].

Soluzione. (*i*) Che la relazione $\sim$ sia una relazione di equivalenza è una banalissima verifica.

Se $a \sim b$ e $b = au$, allora $b \in (a)$ e $a = bu^{-1} \in (b)$. Dunque $(a) = (b)$.

Sia A integro e $(a) = (b)$. Allora $b = ax$, $a = by$ e quindi $a = axy$. Allora $a(1 - xy) = 0$. Se $a = 0$, allora $b = 0$; se $a \neq 0$ allora $1 - xy = 0$, cioè $x, y \in \mathcal{U}(A)$. Allora $a \sim b$.

Nota. Se A non è integro, può risultare $(a) = (b)$ e $a \not\sim b$. Ad esempio si scelgano in $\boldsymbol{Z}_{60}$ $a = \overline{4}$, $b = \overline{8}$ (e si verifichi).

(*ii*) Sia $a = bu$ e $b = av$, con $u, v \in \mathcal{U}(A)$.

Sia a irriducibile e $b = xy$. Allora $a = uxy = (ux)y$ e quindi $ux \in \mathcal{U}(A)$ oppure $y \in \mathcal{U}(A)$. Se $ux \in \mathcal{U}(A)$, anche $x \in \mathcal{U}(A)$. Dunque b è irriducibile.

Sia a un elemento primo. Allora $(b) = (a)$ è un ideale primo e quindi b è un elemento primo.

* * *

Esercizio 3.2.1. Siano A, B due domini d'integrità e sia $f : A \to B$ un omomorfismo iniettivo.

(*i*) Verificare che f induce un omomorfismo iniettivo $F : \boldsymbol{Q}(A) \to \boldsymbol{Q}(B)$.

(*ii*) Sia S una parte moltiplicativa di A. Verificare che $f(S)$ è una parte moltiplicativa di B e che f induce un omomorfismo iniettivo $F : A_S \to B_{f(S)}$.

Soluzione. (*i*) Si ponga:

$$F(\tfrac{a}{b}) = \tfrac{f(a)}{f(b)},\ \forall\, \tfrac{a}{b} \in \boldsymbol{Q}(A).$$

F è ben posta ed iniettiva. Infatti:

$$\tfrac{a}{b} = \tfrac{a_1}{b_1} \iff ab_1 = a_1 b \iff f(a)f(b_1) = f(a_1)f(b) \iff \tfrac{f(a)}{f(b)} = \tfrac{f(a_1)}{f(b_1)} \iff F(\tfrac{a}{b}) = F(\tfrac{a_1}{b_1})$$

[si noti che $f(b), f(b_1) \neq 0$, essendo f iniettiva].

F è un omomorfismo di anelli. Si ha infatti, $\forall\, \frac{a}{b}, \frac{c}{d} \in \boldsymbol{Q}(A)$:

$$F(\tfrac{a}{b} + \tfrac{c}{d}) = F(\tfrac{ad+bc}{bd}) = \tfrac{f(ad+bc)}{f(bd)} = \tfrac{f(a)f(d)+f(b)f(c)}{f(b)f(d)} = \tfrac{f(a)}{f(b)} + \tfrac{f(c)}{f(d)} = F(\tfrac{a}{b}) + F(\tfrac{c}{d}).$$

Analogamente si verifica che $F(\frac{a}{b} \cdot \frac{c}{d}) = F(\frac{a}{b}) \cdot F(\frac{c}{d})$

(*ii*) Si ha:

$$1_B = f(1_A) \in f(S);\ \ f(s_1) \cdot f(s_2) = f(s_1 s_2) \in f(S),\ \ \forall\, s_1, s_2 \in S.$$

Abbiamo così provato che $f(S)$ è una parte moltiplicativa di B. Si ponga:

$$F : A_S \to B_{f(S)} \ \text{ tale che } \ F(\tfrac{a}{s}) = \tfrac{f(a)}{f(s)},\ \forall\, \tfrac{a}{s} \in A_S.$$

Si procede come in (i) e si ottiene che F è un omomorfismo iniettivo.

* * *

Esercizio 3.2.2. Sia A un anello c.u..

(i) Verificare che l'insieme $\mathcal{U}(A)$ degli elementi invertibili di A è una parte moltiplicativa di A e determinare l'anello $A_{\mathcal{U}(A)}$.

(ii) Sia S una parte moltiplicativa di A. Verificare che $S\cdot\mathcal{U}(A) \subseteq \mathcal{U}(A_S)$.

(iii) Sia K un campo, $A = K[X]$ e $S = A - (X)$. Verificare che $S\cdot\mathcal{U}(A) \subset \mathcal{U}(A_S)$.

Soluzione. (i) Ovviamente $1 \in \mathcal{U}(A)$. Se $u, v \in \mathcal{U}(A)$, con $uu_1 = 1 = vv_1$, allora $uv\,u_1v_1 = 1$ e quindi $uv \in \mathcal{U}(A)$. Dunque $\mathcal{U}(A)$ è una parte moltiplicativa di A.

Sia $f : A \to A_{\mathcal{U}(A)}$ l'omomorfismo tale che $f(a) = \frac{a}{1}$, $\forall\, a \in A$. Verifichiamo che f è un isomorfismo (e quindi $A \cong A_{\mathcal{U}(A)}$). Per ogni $\frac{a}{s} \in A_{\mathcal{U}(A)}$, se $st = 1$, allora $\frac{a}{s} = \frac{at}{st} = \frac{at}{1} = f(at)$. Dunque f è suriettivo. Sia poi $f(a) = \frac{a}{1} = 0$. Allora $as = 0$, $\exists\, s \in \mathcal{U}(A)$. Dunque $a = 0$ e pertanto f è iniettivo.

(ii) Sia $s \in S$ e sia $u \in \mathcal{U}(A)$, con inverso $v \in A$. Allora $\frac{1}{s}\,v \in A_S$ e $su\cdot\frac{1}{s}\,v = s\,\frac{1}{s}\,uv = 1\cdot 1 = 1$. Dunque $su \in \mathcal{U}(A_S)$.

(ii) Risulta: $A_S = K[X]_{(X)} = \{\frac{F}{G},\ \forall\, F, G \in K[X],\, G(0) \neq 0\}$. Ad esempio $\frac{X+1}{X-1} \in \mathcal{U}(A_S)$.

Invece $S\cdot\mathcal{U}(A) = \big(K[X] - (X)\big)\cdot K^{\cdot} =$ polinomi in $K[X]$ a termine noto non nullo. Dunque $\frac{X+1}{X-1} \notin S\cdot\mathcal{U}(A)$ e quindi $S\cdot\mathcal{U}(A) \subset \mathcal{U}(A_S)$.

* * *

Esercizio 3.2.3. In $\boldsymbol{Z}_{12}$ sia $S = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\}$.

(i) Verificare che S è una parte moltiplicativa di $\boldsymbol{Z}_{12}$ e che l'omomorfismo $f : \boldsymbol{Z}_{12} \to (\boldsymbol{Z}_{12})_S$ non è iniettivo.

(ii) Dimostrare che $(\boldsymbol{Z}_{12})_S \cong \boldsymbol{Z}_3$ (campo).

Soluzione. (i) Che S sia una parte moltiplicativa in $\boldsymbol{Z}_{12}$ segue dal fatto che $S = \overline{1} + \overline{3}\boldsymbol{Z}_{12}$ [e $\overline{3}\boldsymbol{Z}_{12}$ è un ideale di $\boldsymbol{Z}_{12}$]. Risulta ad esempio: $f(\overline{3}) = \frac{\overline{3}}{\overline{1}} = \overline{0}$ [in quanto $(\overline{3}\cdot\overline{1} - \overline{0}\cdot\overline{1})\overline{4} = \overline{0}$]. Dunque l'omomorfismo f non è iniettivo.

(ii) Se verifichiamo che f è suriettivo e $Kerf = \overline{3}\boldsymbol{Z}_{12}$, allora, dal *TFO*:

$$(\boldsymbol{Z}_{12})_S \cong \boldsymbol{Z}_{12}\big/_{\overline{3}\boldsymbol{Z}_{12}} \cong \boldsymbol{Z}_3.$$

Verifichiamo che f è suriettivo. Sia $\frac{a}{s} \in (\boldsymbol{Z}_{12})_S$, con $s = \overline{1} + \overline{3}t$, $t \in \boldsymbol{Z}_{12}$. Si hanno tre possibili casi:

$a \equiv \overline{0}\ (mod\ \overline{3})$. Allora $\frac{a}{s} = \overline{0} = f(\overline{0})$ [infatti $a = \overline{3}h$ e $\overline{4}\,a = \overline{12}h = \overline{0}$];

$a \equiv \overline{1}\ (mod\ \overline{3})$. Allora $\frac{a}{s} = \overline{1} = f(\overline{1})$ [infatti $a = \overline{3}h + \overline{1}$ e $\overline{4}\,(a - s) = \overline{4}(\overline{3}h + \overline{1} - \overline{1} - \overline{3}t) = \overline{0}$];

$a \equiv \overline{2}\ (mod\ \overline{3})$. Allora $\frac{a}{s} = \overline{2} = f(\overline{2})$ [infatti $a = \overline{3}h + \overline{2}$ e $\overline{4}\,(a - \overline{2}s) = \overline{4}(\overline{3}h + \overline{2} - \overline{2} - \overline{6}t) = \overline{0}$].

Verifichiamo che $Kerf = (\overline{3})$. Certo $(\overline{3}) \subseteq Kerf$ [in quanto $f(\overline{3}) = \overline{0}$]. Inoltre $(\overline{3})$ è massimale in $\boldsymbol{Z}_{12}$. Poiché l'omomorfismo f non è nullo [infatti $f(\overline{1}) \neq \overline{0}$], allora $Ker \neq \boldsymbol{Z}_{12}$ e dunque $Kerf = (\overline{3})$, come richiesto.

* * *

Esercizio 3.2.4. (i) Sia A un anello c. u. e sia $\mathfrak{p}$ suo ideale primo. Verificare che $A_{\mathfrak{p}}$ possiede un unico ideale massimale M [usualmente denotato $\mathfrak{p}A_{\mathfrak{p}}$].

(ii) Scelto in $\boldsymbol{Z}$ l'ideale primo (2), determinare il campo $\boldsymbol{Z}_{(2)}\big/_M$.

Soluzione. (i) Per definizione, $A_{\mathfrak{p}} = \{\frac{x}{s},\ \forall\, x \in A,\ \forall\, s \notin \mathfrak{p}\}$. L'insieme

$$M = \{\tfrac{a}{s},\ \forall\, a \in \mathfrak{p},\ \forall\, s \notin \mathfrak{p}\}$$

è un ideale di $A_{\mathfrak{p}}$. Infatti:

$M - M \subseteq M$ [infatti $\frac{a_1}{s_1} - \frac{a_2}{s_2} = \frac{a_1 s_2 - a_2 s_1}{s_1 s_2}$ e $a_1 s_2 - a_2 s_1 \in \mathfrak{p},\ s_1 s_2 \notin \mathfrak{p}$];

$MA_{\mathfrak{p}} \subseteq M$ [infatti $\frac{a}{s}\frac{x}{t} = \frac{ax}{st}$ e $ax \in \mathfrak{p},\ st \notin \mathfrak{p}$].

L'insieme complementare $A_{\mathfrak{p}} - M$ è formato da elementi invertibili di $A_{\mathfrak{p}}$. Infatti, $\forall\, \frac{x}{s} \in A_{\mathfrak{p}} - M$, risulta $x \notin \mathfrak{p}$ e dunque $\frac{s}{x} \in A_{\mathfrak{p}}$. Ovviamente $\frac{x}{s} \cdot \frac{s}{x} = 1$, cioè $\frac{x}{s} \in \mathcal{U}(A_{\mathfrak{p}})$. Dal precedente Esercizio **3.1.8**, M è l'unico ideale massimale di $A_{\mathfrak{p}}$. Usualmente M viene denotato $\mathfrak{p}A_{\mathfrak{p}}$.

(*ii*) Si ha:

$$\boldsymbol{Z}_{(2)} = \{\tfrac{a}{2h+1},\ \forall\, a, h \in \boldsymbol{Z}\} \text{ ed } M = \{\tfrac{2k}{2h+1},\ \forall\, h, k \in \boldsymbol{Z}\}.$$

Sia $\alpha \in \boldsymbol{Z}_{(2)}/_M$. Se $\alpha = \frac{2k}{2h+1} + M$, allora $\alpha = 0 + M$ [infatti $\frac{2k}{2h+1} - 0 \in M$]. Se invece $\alpha = \frac{2k+1}{2h+1} + M$, allora $\alpha = 1 + M$ [infatti $\frac{2k+1}{2h+1} - 1 = \frac{2k+1}{2h+1} - \frac{2h+1}{2h+1} = \frac{2(k-h)}{2h+1} \in M$]. Dunque

$$\boldsymbol{Z}_{(2)}/_M = \{M,\, 1+M\} \cong \boldsymbol{Z}_2.$$

* * *

Esercizio 3.2.5. (*i*) Sia S una parte moltiplicativa di un anello c. u. A. Verificare che

$$Spec(A_S) = \{\mathfrak{p}_S,\ \forall\, \mathfrak{p} \in Spec(A) \mid \mathfrak{p} \cap S = \emptyset\}.$$

(*ii*) Posto $S = \{6^h,\ \forall\, h \geq 0\}$, verificare che ogni ideale di $\boldsymbol{Z}_S$ è principale e determinare $Spec(\boldsymbol{Z}_S)$.

(*iii*) In $\boldsymbol{Z}_{16}$ sia $S = \{\overline{2}^{\,h},\ \forall\, h \geq 0\}$. Determinare $Spec((\boldsymbol{Z}_{16})_S)$.

Soluzione. (*i*) Sia $\mathfrak{p} \in Spec(A)$, con $\mathfrak{p} \cap S = \emptyset$. Certo $\mathfrak{p}_S \neq A_S$ [altrimenti $1 \in \mathfrak{p}_S$ e quindi $\exists\, x \in \mathfrak{p}, \exists\, s, t \in S$ tali che $(s-x)t = 0$; allora $st = xt \in S \cap \mathfrak{p} = \emptyset$]. Verifichiamo che $\mathfrak{p}_S$ è primo: se $\frac{x}{s}\frac{y}{t} \in \mathfrak{p}_S$, allora $xy \in \mathfrak{p}$ e quindi (ad esempio) $x \in \mathfrak{p}$; allora $\frac{x}{s} \in \mathfrak{p}_S$.

Viceversa, assumiamo che $P \in Spec(A_S)$. Considerato l'omomorfismo canonico $f : A \to A_S$, dall' Esercizio **3.1.7**(*i*) è noto che $f^{-1}(P) \in Spec(A)$. Inoltre $f^{-1}(P) \cap S = \emptyset$ [se altrimenti $s \in f^{-1}(P) \cap S$, allora $\frac{s}{1} \in P$ e quindi $1 = \frac{s}{1} \cdot \frac{1}{s} \in P$]. Risulta infine [come per ogni ideale di A_S, cfr. Prop. **3.2.3**] $f^{-1}(P)_S = P$.

(*ii*) È noto che $S = \{6^h,\ \forall\, h \geq 0\}$ è una parte moltiplicativa di $\boldsymbol{Z}$ e che ogni ideale J di $\boldsymbol{Z}_S$ è del tipo $J = (n\boldsymbol{Z})_S$, per un opportuno $n \in \boldsymbol{Z}$.

Ovviamente $\frac{n}{1} \in J$ e dunque $\frac{n}{1}\boldsymbol{Z}_S \subseteq J$. Viceversa, $\forall\, \frac{x}{6^h} \in J$, risulta $x = nt$, $\exists\, t \in \boldsymbol{Z}$ e quindi $\frac{x}{6^h} = \frac{n}{1}\frac{t}{6^h} \in \frac{n}{1}\boldsymbol{Z}_S$. Quindi $J = \frac{n}{1}\boldsymbol{Z}_S$ è un ideale principale.

In base a (*i*), $Spec(\boldsymbol{Z}_S) = \{(0),\ (p)_S,\ \forall\, p \text{ primo, tale che } (p) \cap S = \emptyset\}$. Gli unici primi che non verificano tale condizione sono (2), (3). Pertanto $Spec(\boldsymbol{Z}_S) = \{(0),\ (p)_S,\ \forall\, p \text{ primo} \geq 5\}$.

(*iii*) Poiché $S \ni \overline{2}^{\,4} = \overline{0}$, $(\boldsymbol{Z}_{16})_S = 0$ (anello nullo). Dunque $Spec((\boldsymbol{Z}_{16})_S) = \emptyset$.

* * *

Esercizio 3.2.6. (*i*) Sia S una parte moltiplicativa di un anello c. u. A. Verificare che $Spec(A_S)$ può essere immerso in $Spec(A)$.

(*ii*) Se $a \in A$ e $S = \{a^h,\ \forall\, h \geq 0\}$, verificare che $Spec(A_S)$ si identifica ad un aperto di $Spec(A)$ (rispetto alla topologia di Zariski).

Soluzione. (*i*) Dall'esercizio precedente è noto che $Spec(A_S) = \{\mathfrak{p}_S,\ \forall\, \mathfrak{p} \in Spec(A) \,|\, \mathfrak{p} \cap S = \emptyset\}$. Sia $f : A \to A_S$ l'omomorfismo canonico. Tale omomorfismo induce l'applicazione continua

$$\varphi_f : Spec(A_S) \to Spec(A) \text{ tale che } \varphi_f(\mathfrak{p}_S) = f^{-1}(\mathfrak{p}_S),\ \forall\, \mathfrak{p}_S \in Spec(A_S).$$

Risulta: $f^{-1}(\mathfrak{p}_S) = \mathfrak{p}$ [infatti: $x \in f^{-1}(\mathfrak{p}_S) \iff \frac{x}{1} \in \mathfrak{p}_S \iff \frac{x}{1} = \frac{a}{s}, \exists\, a \in \mathfrak{p}, \exists\, s \in S \iff$ $\iff xst \in \mathfrak{p}, \exists\, s, t \in S \iff x \in \mathfrak{p}$ (essendo $st \notin \mathfrak{p}$)]. Pertanto

$$\varphi_f(Spec(A_S)) = \{\mathfrak{p} \in Spec(A) \,|\, \mathfrak{p} \cap S = \emptyset\}.$$

Per concludere la dimostrazione facciamo vedere che l'applicazione φ_f è iniettiva. Sia $\mathfrak{p}_S = \mathfrak{q}_S$, con $\mathfrak{p}$, $\mathfrak{q}$ disgiunti da S. Per ogni $x \in \mathfrak{p}$, sia $\frac{x}{1} = \frac{y}{s}$, con $y \in \mathfrak{q}$. Allora $xst = yt$ con $s, t \in S$. Poichè $xst \in \mathfrak{q}$ e $st \notin \mathfrak{q}$, allora $x \in \mathfrak{q}$. Dunque $\mathfrak{p} \subseteq \mathfrak{q}$ e, analogamente, si verifica che $\mathfrak{q} \subseteq \mathfrak{p}$.

Nota. Si potrebbe anche dimostrare che l'applicazione φ_f induce un omeomorfismo tra $Spec(A_S)$ e la sua immagine in $Spec(A)$, verificando che $\varphi_f(V(I_S)) = V(I)$, $\forall\, I$ ideale di A.

(*ii*) Sia A_a l'anello delle frazioni di A rispetto alla parte moltiplicativa $S = \{a^h,\ \forall\, h \geq 0\}$. Da (*i*),

$$\varphi_f(Spec(A_a)) = \{\mathfrak{p} \in Spec(A) \,\big|\, \mathfrak{p} \cap S = \emptyset\} = \{\mathfrak{p} \in Spec(A) \,\big|\, \mathfrak{p} \not\ni a\} = Spec(A) - V(\{a\}).$$

Dunque $\varphi_f(Spec(A_a))$ è un aperto di $Spec(A)$.

* * *

Esercizio 3.2.7. (*i*) Sia A un anello c. u. e sia $S_0 = A - \mathcal{Z}(A)$ l'insieme dei non 0-divisori di A. Verificare che S_0 è una parte moltiplicativa di A e che A è un sottoanello di A_{S_0}.

(*ii*) Sia S una parte moltiplicativa di A tale che l'omomorfismo canonico sia iniettivo. Verificare che $S \subseteq S_0$ [per questo motivo A_{S_0} è detto *anello totale delle frazioni di* A].

(*iii*) Calcolare $(\boldsymbol{Z}_{12})_{S_0}$.

Soluzione. (*i*) Ovviamente $1 \notin \mathcal{Z}(A)$ e quindi $1 \in S_0$. Siano $a, b \in S_0$, cioè $a, b \notin \mathcal{Z}(A)$. Verifichiamo che $ab \notin \mathcal{Z}(A)$ [e quindi $ab \in S_0$]. Infatti: $(ab)c = 0 \implies a(bc) = 0 \implies bc = 0$ [perché $a \notin \mathcal{Z}(A)$] $\implies c = 0$ [perché $b \notin \mathcal{Z}(A)$]. Abbiamo così provato che S_0 è una parte moltiplicativa di A.

Sia $f : A \to A_{S_0}$ tale che $f(a) = \frac{a}{1}$, $\forall\, a \in A$. Proviamo che f è iniettivo. Se infatti $\frac{a}{1} = 0$, esiste $s \in S_0$ tale che $as = 0$. Ma $s \notin \mathcal{Z}(A)$ e quindi $a = 0$. Allora l'omomorfismo f immerge A in A_{S_0}.

(*ii*) Per assurdo, sia $S \not\subseteq S_0$. Esiste quindi $s \in S$ tale che $s \notin S_0$. Allora $s \in \mathcal{Z}(A)$. Se $sa = 0$, con $a \neq 0$, risulta $f(a) = \frac{a}{1} = 0$ e dunque l'omomorfismo f non è iniettivo.

(*iii*) Sia $A = \boldsymbol{Z}_{12}$. Risulta: $\mathcal{Z}(A) = \{\overline{0}, \overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}\}$. Dunque $S_0 = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Si noti che $S_0 = \mathcal{U}(\boldsymbol{Z}_{12})$. Ne segue che $(\boldsymbol{Z}_{12})_{S_0} = \boldsymbol{Z}_{12}$ [infatti, se $\frac{a}{s} \in (\boldsymbol{Z}_{12})_{S_0}$, allora $\frac{a}{s} = a \cdot s^{-1} \in \boldsymbol{Z}_{12}$].

* * *

Esercizio 3.2.8. In $\boldsymbol{Z}$ siano assegnati i numeri primi distinti $p_1, p_2, \ldots, p_n$. Determinare una parte moltiplicativa S di $\boldsymbol{Z}$ tale che il dominio $\boldsymbol{Z}_S$ ammetta come ideali primi non nulli esattamente $(p_1)_S, (p_2)_S, \ldots, (p_n)_S$.

Soluzione. Sia $m = p_1 p_2 \cdot \ldots \cdot p_n$ e si consideri la parte moltiplicativa $S = 1 + m\boldsymbol{Z}$. Si osserva subito che per ogni primo p risulta

$$(p) \cap S = \emptyset \iff p \in \{p_1, p_2, \ldots, p_n\}.$$

Infatti: $(p) \cap S \neq \emptyset \iff \exists\, x, y \in \boldsymbol{Z} \,\big|\, px = 1 + my \iff \exists\, x, y \in \boldsymbol{Z} \,\big|\, 1 = px - my \iff$

$\iff MCD(p, m) = 1 \iff p \neq p_1, p_2, \ldots, p_n$.

Poiché $Spec(\boldsymbol{Z}_S) = \{\mathfrak{p}_S,\ \forall\, \mathfrak{p} \in Spec(\boldsymbol{Z}) \,\big|\, \mathfrak{p} \cap S = \emptyset\}$, allora

$$Spec(\boldsymbol{Z}_S) = \{(0)_S, (p_1)_S, (p_2)_S, \ldots, (p_n)_S\}.$$

Nota. Un altro esempio è ottenuto scegliendo come parte moltiplicativa l'insieme $\boldsymbol{Z} - \big(\bigcup_{i=1}^{n} (p_i)\big)$ (contenente S).

* * *

Esercizio 3.2.9. Sia A un anello c. u. e sia $\mathfrak{p}$ un suo ideale primo. Dimostrare che

$$\boldsymbol{Q}\big(A/_{\mathfrak{p}}\big) \cong A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$$

[dove $\mathfrak{p}A_{\mathfrak{p}} = \{\frac{a}{s},\ \forall a \in \mathfrak{p},\ \forall s \in A - \mathfrak{p}\}$ è l'unico ideale massimale di $A_{\mathfrak{p}}$, cfr. Esercizio **3.2.4**].

Soluzione. Si consideri la composizione di applicazioni $\varphi = \pi \circ f : A \to A_{\mathfrak{p}} \to A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$, con

$$f : A \to A_{\mathfrak{p}} \text{ tale che } f(a) = \tfrac{a}{1},\ \forall a \in A; \quad \pi : A_{\mathfrak{p}} \to A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}} \text{ (proiezione canonica).}$$

Verifichiamo che $Ker\varphi = \mathfrak{p}$.

Ovviamente, $\forall a \in \mathfrak{p}$, si ha: $\varphi(a) = \frac{a}{1} + \mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ e quindi $\mathfrak{p} \subseteq Ker\varphi$. Viceversa, sia $a \in Ker\varphi$ e quindi $\frac{a}{1} + \mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. Allora $\frac{a}{1} = \frac{x}{s}$, $\exists x \in \mathfrak{p}$, $\exists s \notin \mathfrak{p}$. Dunque $\exists t \notin \mathfrak{p}$ tale che $(as - x)t = 0$, cioè $ast = xt$. Ne segue che $a(st) \in \mathfrak{p}$ e $st \notin \mathfrak{p}$. Allora $a \in \mathfrak{p}$.

Poiché $Ker\varphi = \mathfrak{p}$, resta definito l'omomorfismo iniettivo $\Phi : A/_{\mathfrak{p}} \to A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$. Inoltre, poiché $A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$ è un campo, esiste un omomorfismo iniettivo $F : \boldsymbol{Q}(A/_{\mathfrak{p}}) \to A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$ tale che:

$$F(\tfrac{a+\mathfrak{p}}{b+\mathfrak{p}}) = (\tfrac{a}{1} + \mathfrak{p}A_{\mathfrak{p}})(\tfrac{b}{1} + \mathfrak{p}A_{\mathfrak{p}})^{-1} = \tfrac{a}{b} + \mathfrak{p}A_{\mathfrak{p}},\ \forall \tfrac{a+\mathfrak{p}}{b+\mathfrak{p}} \in \boldsymbol{Q}(A/_{\mathfrak{p}}).$$

Per concludere basta osservare che F è anche suriettivo. Infatti, $\forall \frac{a}{s} + \mathfrak{p}A_{\mathfrak{p}} \in A_{\mathfrak{p}}/_{\mathfrak{p}A_{\mathfrak{p}}}$, si ha: $F(\frac{a+\mathfrak{p}}{s+\mathfrak{p}}) = \frac{a}{s} + \mathfrak{p}A_{\mathfrak{p}}$.

* * *

Esercizio 3.3.1. Dimostrare che ogni dominio d'integrità finito è un campo.

Soluzione. Sia $A = \{0, x_1, \dots, x_n\}$ un dominio d'integrità (finito). Ovviamente $1 \in \{x_1, \dots, x_n\}$.

Si scelga arbitrariamente un elemento non nullo, ad esempio x_1. Gli elementi

$$x_1^2,\ x_1x_2,\ \dots, x_1x_n$$

sono a due a due distinti [infatti $x_1x_i = x_1x_j \implies x_i = x_j$]. Esiste pertanto un elemento x_i tale che $x_1x_i = 1$. Quindi $x_1 \in \mathcal{U}(A)$.

Ripetendo lo stesso ragionamento per ogni x_i si ottiene che $x_i \in \mathcal{U}(A)$ e dunque tutti gli elementi non nulli di A sono invertibili: A è un campo.

* * *

Esercizio 3.3.2. Dimostrare che se A è un *UFD* e se S è una parte moltiplicativa di A, con $0 \notin S$, anche l'anello delle frazioni A_S è un *UFD*.

Soluzione. Cominciamo col provare la seguente affermazione:

$(*)$ a irriducibile in $A \implies \frac{a}{1}$ irriducibile in A_S.

Sia $\frac{a}{1} = \frac{x}{s}.\frac{y}{t}$. Allora $ast = xy$. Poiché A è un *UFD*, a è anche primo. Poiché $a \mid xy$, allora, ad esempio, $a \mid x$, cioè $x = ar$, $\exists r \in A$. Pertanto $\frac{a}{1} = \frac{a}{1}\cdot\frac{r}{s}\cdot\frac{y}{t}$. Semplificando, $1 = \frac{1}{1} = \frac{r}{s}.\frac{y}{t}$ e dunque $\frac{y}{t} \in \mathcal{U}(A_S)$. Dunque $\frac{a}{1}$ è irriducibile in A_S.

Ora proviamo che ogni $\frac{x}{s} \in A_S^{\cdot} - \mathcal{U}(A_S)$ è prodotto di un numero finito di elementi irriducibili in A_S. Osserviamo che $x \in A^{\cdot} - \mathcal{U}(A)$ [altrimenti, se $x \in \mathcal{U}(A)$ e $xy = 1$, allora $\frac{x}{s}.\frac{sy}{1} = \frac{xys}{s} = \frac{s}{s} = 1$]. Poiché A è un *UFD*, sia $x = a_1 \dots a_t$ una fattorizzazione irriducibile in A. Allora (in base a $(*)$):

$$\frac{x}{s} = (\tfrac{1}{s}\cdot\tfrac{a_1}{1})\cdot\tfrac{a_2}{1}\cdot\dots\cdot\tfrac{a_t}{1}$$

è una fattorizzazione in A_S con fattori irriducibili di A_S [si noti che $\frac{1}{s}$ è invertibile e dunque $(\frac{1}{s}\cdot\frac{a_1}{1})$ è irriducibile].

Resta da provare che due fattorizzazioni irriducibili coincidono a meno dell'ordine dei fattori e di fattori invertibili in A_S. Siano

$$\frac{a_1}{s_1}\cdot\frac{a_2}{s_2}\cdot\dots\cdot\frac{a_r}{s_r} = \frac{b_1}{t_1}\cdot\frac{b_2}{t_2}\cdot\dots\cdot\frac{b_n}{t_n}$$

due fattorizzazioni irriducibili di uno stesso elemento. Allora

$$u\,a_1 \dots a_r = v\,b_1 \dots b_n\,, \ \text{ con } \ u, v \in S.$$

Ogni a_i non può essere associato ad un fattore irriducibile v_i di v. Infatti, essendo $\frac{v_i}{1}$ invertibile in A_S, anche $\frac{a_i}{1}$ sarebbe invertibile, contro $(*)$]. Dunque a_i è associato ad uno dei b_j [e viceversa]. Pertanto le due fattorizzazioni coincidono a meno dell'ordine dei fattori e di elementi invertibili.

* * *

Esercizio 3.3.3. (*i*) Posto $I = (X^2 + Y^2) \subset \boldsymbol{Z}[X, Y]$, verificare che I è primo.

(*ii*) Determinare un ideale massimale di $\boldsymbol{Z}[X, Y]$ contenente I.

(*iii*) Rispondere alle precedenti domande assumendo $I \subset \boldsymbol{R}[X, Y]$.

Soluzione. (*i*) Poiché $\boldsymbol{Z}[X, Y]$ è un *UFD*, basta verificare che $f = X^2 + Y^2$ è un polinomio irriducibile in $\boldsymbol{Z}[X, Y]$.

Per assurdo, sia $f = gh$ una fattorizzazione non banale in $\boldsymbol{Z}[X, Y]$. Si può assumere $\partial f = \partial g = 1$ [f non ha fattori non invertibili in $\boldsymbol{Z}$]. La stessa fattorizzazione sussiste anche in $\boldsymbol{C}[X, Y]$, dove però vale anche la fattorizzazione: $f = (x - iY)(X + iY)$. Allora, essendo $\boldsymbol{C}[X, Y]$ un *UFD*, le due fattorizzazioni coincidono a meno di un coefficiente moltiplicativo $c \in \boldsymbol{C}^{\cdot}$. Ad esempio, sia $c(X - iY) = f$. Allora $c, -ci \in \boldsymbol{Z}$ e dunque $i \in \boldsymbol{Q}$: assurdo.

(*ii*) Risulta:

$$I \subset (X,\, Y) \subset (X,\, Y,\, 2).$$

Si ha:

$$\boldsymbol{Z}[X, Y]\big/_{(X,\,Y,\,2)} \cong \frac{\boldsymbol{Z}[X,Y]\big/_{(2)}}{(X,\,Y,\,2)\big/_{(2)}} \cong \boldsymbol{Z}_2[X, Y]\big/_{(X,\,Y)} \cong \boldsymbol{Z}_2 \ \text{ (campo)}.$$

Dunque $(X,\, Y,\, 2)$ è un ideale massimale contenente I. Altri ideali massimali sono ad esempio $(X,\, Y,\, p)$, $\forall\, p$ primo.

(*iii*) Con la stessa dimostrazione si prova che $I = (X^2 + Y^2)$ è primo in $\boldsymbol{R}[X, Y]$. Un massimale contenente I è ad esempio $(X,\, Y)$. Infatti $\boldsymbol{R}[X, Y]\big/_{(X,\,Y)} \cong \boldsymbol{R}$.

* * *

Esercizio 3.3.4. (*i*) Verificare che in $\boldsymbol{Z}[\sqrt{2}\,]$ i due elementi $z = 1 - \sqrt{2}$, $w = 7 + 5\sqrt{2}$ sono invertibili e calcolarne l'inverso.

(*ii*) Verificare che $\mathcal{U}(\boldsymbol{Z}[\sqrt{2}\,])$ è un gruppo infinito non ciclico.

(*iii*) Verificare che $1 + 2\sqrt{2}$ è un elemento primo di $\boldsymbol{Z}[\sqrt{2}\,]$.

(*iv*) Verificare che l'elemento 2 non è irriducibile in $\boldsymbol{Z}[\sqrt{2}\,]$.

Soluzione. (*i*) Risulta: $\mathcal{N}(z) = \mathcal{N}(w) = -1$. Ne segue che z, w sono invertibili ed hanno rispettivamente inverso:

$$z^{-1} = -\overline{z} = -1 - \sqrt{2}\,, \quad w^{-1} = -\overline{w} = -7 + 5\sqrt{2}\,.$$

(*ii*) Le potenze di z hanno norma ± 1 e dunque sono invertibili. Sono a due a due distinte [si osserva infatti che la "parte intera" di z^h cresce con h]. Dunque $\mathcal{U}(\boldsymbol{Z}[\sqrt{2}\,])$ è un gruppo infinito.

Assumendo per assurdo che tale gruppo sia ciclico, con generatore α, deve essere $\mathcal{N}(\alpha) = -1$ [altrimenti $z,\, w \notin \langle\alpha\rangle$]. Poiché $\overline{\alpha} \in \langle\alpha\rangle$, allora $\overline{\alpha} = \alpha^h$, $\exists\, h \geq 0$. Ne segue che $-1 = \alpha\,\overline{\alpha} = \alpha^{h+1}$ e quindi $\alpha^{2h+2} = 1$. Allora $\langle\alpha\rangle = \mathcal{U}(\boldsymbol{Z}[\sqrt{2}\,])$ sarebbe finito, contro quanto precedentemente dimostrato.

(*iii*) Si tratta di verificare che $I := (1 + 2\sqrt{2}\,)$ è un ideale primo in $\boldsymbol{Z}[\sqrt{2}\,]$. Poiché z è invertibile e $(1 + 2\sqrt{2}\,)z = (1 + 2\sqrt{2}\,)(1 - \sqrt{2}\,) = -3 + \sqrt{2}$, allora $I = (-3 + \sqrt{2})$. Risulta:

$$\boldsymbol{Z}[\sqrt{2}\,]\big/_I = \boldsymbol{Z}[\sqrt{2}\,]\big/_{(-3+\sqrt{2})} \cong \frac{\boldsymbol{Z}[X]\big/_{(X^2-2)}}{(X-3,\,X^2-2)\big/_{(X^2-2)}} \cong \boldsymbol{Z}[X]\big/_{(X-3,\,X^2-2)} \cong$$

$$\cong \frac{\boldsymbol{Z}[X]\big/_{(X-3)}}{(X^2-2,\,X-3)\big/_{(X-3)}} \cong \boldsymbol{Z}\big/_{(3^2-2)} = \boldsymbol{Z}_7 \ \text{ (campo)}.$$

Dunque I è massimale e perciò primo.

(*iv*) In $\boldsymbol{Z}[\sqrt{2}]$ si ha: $2 = \sqrt{2}\,\sqrt{2}$. $\sqrt{2}$ non è invertibile [se lo fosse, avrebbe norma ± 1, mentre $\mathcal{N}(\sqrt{2}) = \sqrt{2}\,(-\sqrt{2}) = -2$]. Dunque 2 non è irriducibile. Invece $\sqrt{2}$ ha norma prima (negativa) e pertanto è irriducibile. Dunque $2 = \sqrt{2}\,\sqrt{2}$ è una fattorizzazione irriducibile di 2.

* * *

Esercizio 3.3.5. In $\boldsymbol{Z}[\sqrt{2}]$ fattorizzare gli interi primi 2, 3, 5, 7 come prodotto di elementi irriducibili di $\boldsymbol{Z}[\sqrt{2}]$.

Soluzione. Posto $p = 2, 3, 5, 7$, si ha:

$$\boldsymbol{Z}[\sqrt{2}]/_{(p)} \cong \boldsymbol{Z}[X]/_{(p,\, X^2-2)} \cong \boldsymbol{Z}_p[X]/_{(X^2-\overline{2})}.$$

Per $p = 3, 5$, il polinomio $X^2 - \overline{2} \in \boldsymbol{Z}_p[X]$ è irriducibile [infatti si verifica subito che $X^2 - \overline{2}$ non ha zeri in $\boldsymbol{Z}_p$]. Ne segue che (p) è massimale e perciò primo. Dunque 3, 5 sono irriducibili in $\boldsymbol{Z}[\sqrt{2}]$.

Sia $p = 2$. In tal caso $\boldsymbol{Z}_2[X]/_{(X^2-\overline{2})} = \boldsymbol{Z}_2[X]/_{(X^2)}$ è non integro. Dunque 2 non è primo in $\boldsymbol{Z}[\sqrt{2}]$. In tale anello, 2 si fattorizza nella forma $2 = \sqrt{2}\,\sqrt{2}$, con $\mathcal{N}(\sqrt{2}) = \sqrt{2}\,(-\sqrt{2}) = -2$ primo (negativo). Ne segue che $\sqrt{2}$ è irriducibile e quindi una fattorizzazione richiesta è $2 = \sqrt{2}\,\sqrt{2}$.

Sia $p = 7$. In tal caso $\boldsymbol{Z}_7[X]/_{(X^2-\overline{2})} = \boldsymbol{Z}_7[X]/_{(X-\overline{3})(X-\overline{4})}$ è non integro e quindi 7 non è primo in $\boldsymbol{Z}[\sqrt{2}]$. Se $z \,|\, 7$ allora $\mathcal{N}(z) \,|\, \mathcal{N}(7) = 49 = 7\cdot 7$. Cerchiamo gli eventuali $z \in \boldsymbol{Z}[\sqrt{2}]$ tali che $\mathcal{N}(z) = 7$. Se $z = a + b\sqrt{2}$, allora $7 = \mathcal{N}(z) = a^2 - 2b^2$.
L'equazione $a^2 - 2b^2 = 7$ è risolta in $\boldsymbol{Z} \times \boldsymbol{Z}$ da $a = 3$, $b = 1$ (a meno del segno). Si verifica subito che $(3 + \sqrt{2})(3 - \sqrt{2}) = 7$. Inoltre $\mathcal{N}(3 + \sqrt{2}) = 7$ è primo e dunque $3 + \sqrt{2}$ è irriducibile. Analogamente, $3 - \sqrt{2}$ è irriducibile. Una fattorizzazione di 7 cercata è quindi

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}).$$

Nota. $3 + \sqrt{2}$ è anche primo. Infatti:

$$\boldsymbol{Z}[\sqrt{2}]/_{(3+\sqrt{2})} \cong \boldsymbol{Z}[X]/_{(X^2-2,\, X+3)} \cong \boldsymbol{Z}[X]/_{(3^2-2)} \cong \boldsymbol{Z}_7 \quad \text{(campo)}.$$

Lo stesso è vero anche per $3 - \sqrt{2}$.

* * *

Esercizio 3.3.6. Sono assegnati in $\boldsymbol{Z}[\sqrt{-5}]$ i due elementi

$$z_1 = 9, \quad z_2 = 3(2 + \sqrt{-5}).$$

(*i*) Determinare i divisori comuni di z_1, z_2.

(*ii*) Verificare se tali divisori sono elementi primi.

(*iii*) Verificare che non esiste $MCD(z_1, z_2)$.

Soluzione. (*i*) Se $z \,\Big|\, \begin{matrix} z_1 \\ z_2 \end{matrix}$, allora $\mathcal{N}(z) \,\Big|\, \begin{matrix} \mathcal{N}(z_1) \\ \mathcal{N}(z_2) \end{matrix}$. Poiché $\mathcal{N}(z_1) = \mathcal{N}(z_2) = 81$, allora $\mathcal{N}(z) \,|\, 81$. Se $\mathcal{N}(z) = 81$ e $z \,|\, z_1$, allora $z = \pm z_1$ e dunque $z \not| z_2$. I divisori comuni propri di z_1, z_2 possono quindi avere norma 3, 9, 27. Ma in $\boldsymbol{Z}[\sqrt{-5}]$ non esistono elementi di norma 3 [infatti l'equazione $a^2 + 5b^2 = 3$ non ha soluzioni intere]. Ne segue che $\mathcal{N}(z) \neq 3$ ed anche che $\mathcal{N}(z) \neq 27$ [se infatti $z_1 = zw$ e $\mathcal{N}(z) = 27$, allora $\mathcal{N}(w) = 3$, e ciò è escluso]. Quindi i possibili divisori z di z_1, z_2 hanno norma 9. Posto $z = a + b\sqrt{-5}$, si ha:

$$\mathcal{N}(z) = 9 \iff a^2 + 5b^2 = 9 \iff a^2 = 4,\ b^2 = 1 \ \text{ oppure } \ a^2 = 9,\ b^2 = 0 \iff$$
$$\iff \begin{cases} a = \pm 2 \\ b = \pm 1 \end{cases} \text{ oppure } \begin{cases} a = \pm 3 \\ b = 0 \end{cases} \iff z = \pm(2 + \sqrt{-5}),\ \pm(2 - \sqrt{-5}),\ \pm 3.$$

Si verifica subito che i tre elementi $2 + \sqrt{-5}$, $2 - \sqrt{-5}$, 3 sono divisori di z_1, mentre i due elementi $2 + \sqrt{-5}$, 3 sono divisori di z_2. Dunque i divisori comuni propri di z_1, z_2 sono:

$3,\ 2+\sqrt{-5}$ [ed i loro associati, cioè i loro opposti].

Nota. Si tratta di elementi irriducibili in $\boldsymbol{Z}[\sqrt{-5}]$ [infatti hanno norma 9 e in $\boldsymbol{Z}[\sqrt{-5}]$ non esistono elementi di norma 3].

(*ii*) $3,\ 2+\sqrt{-5}$ non sono elementi primi. Per verificarlo, calcoliamo i quozienti:

$$\boldsymbol{Z}[\sqrt{-5}]\big/_{(3)} \cong \boldsymbol{Z}[X]\big/_{(X^2+5,\,3)} \cong \boldsymbol{Z}_3[X]\big/_{(X^2+\overline{2})} \cong \boldsymbol{Z}_3[X]\big/_{(X+\overline{1})(X+\overline{2})} \quad \text{(anello non integro);}$$

$$\boldsymbol{Z}[\sqrt{-5}]\big/_{(2+\sqrt{-5})} \cong \boldsymbol{Z}[X]\big/_{(X^2+5,\,X+2)} \cong \frac{\boldsymbol{Z}[X]\big/_{(X+2)}}{(X^2+5,\,X+2)\big/_{(X+2)}} \cong \boldsymbol{Z}\big/_{(4+5)} = \boldsymbol{Z}_9 \quad \text{(anello non integro).}$$

(*iii*) Per assurdo, $\exists\, d := MCD(z_1,\, z_2)$. In base ad (*i*), $d \in \{\pm 1,\, \pm 3,\, \pm(2+\sqrt{-5})\}$ e (d) è il minimo tra gli ideali (3), $(2+\sqrt{-5}\,)$. Ma tali ideali non sono contenuti l'uno nell'altro e dunque nessuno dei comuni divisori di $z_1,\, z_2$ può essere il massimo comun divisore.

* * *

Esercizio 3.3.7. Sia d un intero ≤ -3.

(*i*) Verificare che 2 non è primo in $\boldsymbol{Z}[\sqrt{d}\,]$.

(*ii*) Verificare che 2 è irriducibile in $\boldsymbol{Z}[\sqrt{d}\,]$.

(*iii*) Confrontare (*i*) e (*ii*) con la Prop. **3.3**.

Soluzione. (*i*) Si ha:

$$\boldsymbol{Z}[\sqrt{d}]\big/_{(2)} \cong \boldsymbol{Z}[X]\big/_{(2,\,X^2-d)} \cong \boldsymbol{Z}_2[X]\big/_{(X^2-\overline{d})}.$$

Il polinomio $X^2-\overline{d} \in \boldsymbol{Z}_2[X]$ coincide con X^2 oppure con $X^2+\overline{1}$. In ogni caso è riducibile e pertanto (2) non è primo (in $\boldsymbol{Z}[\sqrt{d}]$).

(*ii*) Sia $2 = z_1 z_2 \in \boldsymbol{Z}[\sqrt{d}]$, con $z_1 = a_1 + b_1\sqrt{d},\ z_2 = a_2 + b_2\sqrt{d}$. Si tratta di verificare che $\mathcal{N}(z_1) = 1$ oppure $\mathcal{N}(z_2) = 1$. Si ha:

$$4 = \mathcal{N}(2) = \mathcal{N}(z_1)\mathcal{N}(z_2) = (a_1^2 + |d|\, b_1^2)(a_2^2 + |d|\, b_2^2).$$

Se fosse $b_1 b_2 \neq 0$, allora (essendo $d < -2$) $|d|^2 b_1^2 b_2^2 > 4$ e quindi la precedente uguaglianza non sarebbe verificata. Dunque $b_1 b_2 = 0$.

Ad esempio, sia $b_1 = 0$ (e quindi $z_1 = a_1$). Poiché $\mathcal{N}(z_1) \,\big|\, \mathcal{N}(2)$, allora $a_1^2 \,\big|\, 4$ e quindi $a_1 = \pm 1,\, \pm 2$. Se $a_1 = \pm 1$, allora $\mathcal{N}(z_1) = 1$, cioè $z_1 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}])$. Se invece $a_1 = \pm 2$, allora $4 = 4\mathcal{N}(z_2)$ e quindi $\mathcal{N}(z_2) = 1$, cioè $z_2 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{d}])$.

La fattorizzazione $2 = z_1 z_2$ è quindi banale e perciò 2 è irriducibile.

(*iii*) La Prop. **3.3** afferma che $\boldsymbol{Z}[\sqrt{-5}]$ non è un *UFD*. Da (*i*) e (*ii*) segue che, più generalmente, ogni $\boldsymbol{Z}[\sqrt{d}]$, con $d < -2$, non è un *UFD*. Infatti 2 è irriducibile ma non primo.

* * *

Esercizio 3.3.8. In $\boldsymbol{Z}[\sqrt{6}\,]$ fattorizzare $z = 4 + \sqrt{6}$ come prodotto di elementi irriducibili.

Soluzione. Assumiamo noto il fatto che $\boldsymbol{Z}[\sqrt{6}\,]$ è un *ED*. Si ha:

$$\boldsymbol{Z}[\sqrt{6}\,]\big/_{(4+\sqrt{6}\,)} \cong \boldsymbol{Z}[X]\big/_{(X^2-6,\,4+X)} \cong \frac{\boldsymbol{Z}[X]\big/_{(4+X)}}{(X^2-6,\,4+X)\big/_{(4+X)}} \cong \boldsymbol{Z}\big/_{((-4)^2-6,\,0)} \cong \boldsymbol{Z}_{10} \quad \text{(non integro).}$$

Dunque $z = 4 + \sqrt{6}$ non è primo e pertanto non è irriducibile.

Si ha: $\mathcal{N}(z) = 16-6 = 10$. Se quindi $z = z_1\, z_2$, allora $10 = \mathcal{N}(z_1)\mathcal{N}(z_2)$. Poiché deve esistere una fattorizzazione non banale, devono esistere $z_1,\, z_2 \in \boldsymbol{Z}[\sqrt{6}\,]$ tali che $(\mathcal{N}(z_1), \mathcal{N}(z_2)) = (2, 5)$, ovvero $(\mathcal{N}(z_1), \mathcal{N}(z_2)) = (-2, -5)$. Inoltre gli elementi $z_1,\, z_2$, essendo a norma prima, sono irriducibili e forniscono la fattorizzazione cercata.

Sia $z_1 = a+b\sqrt{6}$. z_1 ha norma $\pm 2 \iff (a,b)$ è una soluzione intera dell'equazione $X^2-6Y^2 = \pm 2$. Si vede con facilità che esistono soluzioni intere di $X^2-6Y^2 = -2$, ad esempio $(\pm 2, \pm 1)$. Proviamo a porre $z_1 = 2+\sqrt{6}$ e verifichiamo se $z_1 \,|\, z$, ovvero se $\frac{z}{z_1} \in \boldsymbol{Z}[\sqrt{6}\,]$. Risulta:

$$\frac{z}{z_1} = \frac{z\,\overline{z_1}}{z_1\,\overline{z_1}} = \frac{(4+\sqrt{6})(2-\sqrt{6})}{-2} = -1+\sqrt{6}.$$

Si ponga $z_2 := -1+\sqrt{6}$ (di norma -5). Allora la fattorizzazione cercata è

$$z = 4+\sqrt{6} = (2+\sqrt{6})(-1+\sqrt{6}).$$

Nota. Si noti che tale fattorizzazione essenzialmente unica [perché $\boldsymbol{Z}[\sqrt{6}\,]$ è un *UFD*]. Se quindi avessimo scelto un'altra soluzione dell'equazione $X^2-6Y^2 = -2$, ad esempio $(\pm 22, \pm 9)$, avremmo ottenuto ad esempio la fattorizzazione

$$z = 4+\sqrt{6} = (22+9\sqrt{6})(-17+7\sqrt{6}).$$

Ma si tratta della stessa fattorizzione. Infatti $22+9\sqrt{6} = (2+\sqrt{6})\,u$ e $-1+\sqrt{6} = (-17+7\sqrt{6})\,u$, con $u = 5+2\sqrt{6}$ invertibile in $\boldsymbol{Z}[\sqrt{6}\,]$.

* * *

Esercizio 3.3.9. Fattorizzare in $\boldsymbol{Z}[\sqrt{-2}\,]$ i tre elementi 2, 3, $z = 2+\sqrt{-2}$, come prodotto di fattori iriducibili.

Soluzione. Osserviamo preliminarmente che nessuno dei tre elementi è primo. Infatti:

$$\boldsymbol{Z}[\sqrt{-2}\,]\big/_{(2)} \cong \boldsymbol{Z}_2[X]\big/_{(X^2+\overline{2})} = \boldsymbol{Z}_2[X]\big/_{(X^2)},$$
$$\boldsymbol{Z}[\sqrt{-2}\,]\big/_{(3)} \cong \boldsymbol{Z}_3[X]\big/_{(X^2+\overline{2})} = \boldsymbol{Z}_3[X]\big/_{(X+\overline{1})(X+\overline{2})},$$
$$\boldsymbol{Z}[\sqrt{-2}\,]\big/_{(2+\sqrt{-2})} \cong \frac{\boldsymbol{Z}[X]\big/_{(X^2+2)}}{(X+2,\,X^2+2)\big/_{(X^2+2)}} \cong \frac{\boldsymbol{Z}[X]\big/_{(X+2)}}{(X+2,\,X^2+2)\big/_{(X+2)}} \cong \boldsymbol{Z}\big/_{((-2)^2+2)} = \boldsymbol{Z}_6.$$

Questi tre anelli sono non integri e quindi i tre elementi assegnati non sono primi. [Assumendo di sapere poi che $\boldsymbol{Z}[\sqrt{-2}\,]$ è un *UFD*, i tre elementi non sono irriducibili].

Osserviamo che in $\boldsymbol{Z}[\sqrt{-2}\,]$ risulta:

$$2 = (\sqrt{-2})(-\sqrt{-2}).$$

Tale fattorizzazione ha due fattori di norma 2 e quindi irriducibili. Pertanto è una fattorizzazione cercata.

Per fattorizzare 3 poniamo: $3 = z_1 z_2$, con $z_1 = a_1 + b_1\sqrt{-2}$, $z_2 = a_2 + b_2\sqrt{-2}$. Poiché $9 = \mathcal{N}(3) = \mathcal{N}(z_1)\mathcal{N}(z_2)$, per ottenere una fattorizzazione non banale di 3 cerchiamo elementi z_1, z_2 di norma 3. Deve risultare $a_1^2 = b_1^2 = a_2^2 = b_2^2 = 1$. Posto ad esempio $z_1 = 1+\sqrt{-2}$, $z_2 = 1-\sqrt{-2}$, si ottiene una fattorizzazione richiesta:

$$3 = (1+\sqrt{-2})(1-\sqrt{-2}).$$

Per fattorizzare $z = 2+\sqrt{-2}$, poniamo ancora: $z = z_1 z_2$, con $z_1 = a_1+b_1\sqrt{-2}$, $z_2 = a_2+b_2\sqrt{-2}$. Poiché $6 = \mathcal{N}(z) = \mathcal{N}(z_1)\mathcal{N}(z_2)$, dobbiamo determinare z_1, z_2 aventi norma rispettivamente 2, 3. Si ottiene subito $a_1 = 0$, $b_1 = \pm 1$ e $a_2 = \pm 1$, $b_2 = \pm 1$. Posto ad esempio $z_1 = \sqrt{-2}$, $z_2 = 1-\sqrt{-2}$, si ottiene una fattorizzazione richiesta:

$$z = 2+\sqrt{-2} = (\sqrt{-2})(1-\sqrt{-2}).$$

* * *

Esercizio 3.3.10. Sia A un dominio e siano $a, b, c \in A$.

(*i*) Verificare che se $(a,b) = (c)$, allora $c = MCD(a,b)$.

(*ii*) Se esiste $MCD(a,b) =: d$, è vero che $(a,b) = (d)$?

Suggerimento. Considerare in $\boldsymbol{Z}[\sqrt{-3}\,]$ gli elementi 2, $1+\sqrt{-3}$.

Soluzione. (*i*) Per ipotesi:

$$a = cx,\ b = cy,\ c = ar + bs,\ \exists\, x, y, r, s \in A.$$

Si tratta di verificare che:

$c \Big| \begin{matrix} a \\ b \end{matrix}$ [infatti $a = cx,\ b = cy$];

$c' \Big| \begin{matrix} a \\ b \end{matrix} \implies c' \,|\, c$ [infatti, se $\begin{cases} a = c'x' \\ b = c'y', \end{cases}$ allora $c = c'x'r + c'y's = c'(x'r + y's)$ e dunque $c' \,|\, c$].

(*ii*) Proveremo che $MCD(2, 1+\sqrt{-3}) = 1$, ma che l'ideale $I := (2,\ 1+\sqrt{-3})$ (in $\boldsymbol{Z}[\sqrt{-3}]$) è $\neq (1)$.

Per calcolare $MCD(2, 1+\sqrt{-3}) = 1$, determiniamo i divisori comuni di $2,\ 1+\sqrt{-3}$ (in $\boldsymbol{Z}[\sqrt{-3}]$). Se $z = a + b\sqrt{-3}$ è un divisore comune, allora $\mathcal{N}(z) \,|\, 4$. Ma $\mathcal{N}(z) \neq 2$ [infatti l'equazione $X^2 + 3Y^2 = 2$ non ha soluzioni intere]. Dunque $2,\ 1+\sqrt{-3}$ sono irriducibili ed hanno quindi soltanto i divisori banali. Pertanto:

$$2 \text{ ha divisori: } \pm 1,\ \pm 2; \quad 1+\sqrt{-3} \text{ ha divisori: } \pm 1,\ \pm(1+\sqrt{-3}).$$

Ne segue che gli unici divisori comuni sono ± 1. Pertanto (a meno del segno) $MCD(2, 1+\sqrt{-3}) = 1$.

Ora dimostriamo che $I = (2,\ 1+\sqrt{-3}) \neq (1)$. Basta provare che $\boldsymbol{Z}[\sqrt{-3}]/_I \neq 0$. Infatti:

$$\boldsymbol{Z}[\sqrt{-3}]/_I \cong \boldsymbol{Z}[X]/_{(2,\ 1+X,\ X^2+3)} \cong \boldsymbol{Z}_2[X]/_{(\overline{0},\ \overline{1}+X,\ X^2+\overline{1})} = \boldsymbol{Z}_2[X]/_{(X+\overline{1})} \cong \boldsymbol{Z}_2$$

[ed abbiamo anche provato che I è massimale in $\boldsymbol{Z}[\sqrt{-3}]$].

* * *

Esercizio 3.3.11. Dimostrare il Lemma **3.2**.

Soluzione. Sia $d - 1 = 4s,\ \exists\, s \in \boldsymbol{Z}$. Risulta:

$$\omega_d{}^2 = \tfrac{1+d}{4} + \tfrac{\sqrt{d}}{2} = \tfrac{1+d}{4} \pm \tfrac{1}{2} + \tfrac{\sqrt{d}}{2} = \tfrac{d-1}{4} + \omega_d = \omega_d + s.$$

Dunque ω_d è zero del polinomio monico

$$f = X^2 - X - s \in \boldsymbol{Z}[X].$$

Poiché d non è un quadrato perfetto, $\omega_d \notin \boldsymbol{Q}$ e dunque f è irriducibile su $\boldsymbol{Z}$ (e su $\boldsymbol{Q}$).

Tramite l'omomorfismo $\varphi : \boldsymbol{Z}[X] \to \boldsymbol{C}$, tale che $\varphi(g) = g(\omega_d),\ \forall\, g \in \boldsymbol{Z}[X]$, si ottiene che

$$\boldsymbol{Z}[X]/_{(f)} \cong Im\varphi = \{a + b\,\omega_d,\ \forall\, a, b \in \boldsymbol{Z}\} =: \boldsymbol{Z}[\omega_d].$$

Essendo $\boldsymbol{Z}[\omega_d]$ un sottoanello di $\boldsymbol{C}$, è un dominio d'integrità. Inoltre $\boldsymbol{Z}[\sqrt{d}] \subseteq \boldsymbol{Z}[\omega_d]$ [infatti $\sqrt{d} = 2\omega_d - 1$] e $\boldsymbol{Z}[\omega_d] \subseteq \boldsymbol{Q}(\sqrt{d})$ [infatti $\omega_d = \frac{1}{2} + \frac{1}{2}\sqrt{d}$]. Dunque $\boldsymbol{Q}(\boldsymbol{Z}[\omega_d]) = \boldsymbol{Q}(\sqrt{d})$.

* * *

Esercizio 3.3.12. Sia A un ED e v una sua valutazione euclidea. Scelti $a, b \in A^{\cdot}$, dimostrare che:

(*i*) $v(ab) = v(a) \iff b \in \mathcal{U}(A)$.

(*ii*) $v(ab) = max\{v(a), v(b)\} \iff a \in \mathcal{U}(A)$ oppure $b \in \mathcal{U}(A)$.

Soluzione. (*i*) ($\Longleftarrow$). Sia $b \in \mathcal{U}(A)$. Dunque $bc = 1,\ \exists\, c \in A$. Allora

$$v(ab) \geq v(a) = v(a1) = v(abc) \geq v(ab).$$

Ne segue che $v(ab) = v(a)$.

($\Longrightarrow$). Per ipotesi $v(a) = v(ab)$. Si esegua in A la divisione con resto di a per ab. Allora:

$$a = ab\,q + r, \text{ con } r = 0 \text{ oppure } v(r) < v(ab).$$

Se $r = 0$, allora $a = abq$, da cui $1 = bq$ e quindi $b \in \mathcal{U}(A)$. Se fosse invece $r \neq 0$, allora $v(r) < v(ab) = v(a)$. Ma $r = a - abq = a(1 - bq)$ e quindi $v(r) \geq v(a)$: assurdo.

(*ii*) È conseguenza immediata di (*i*):

$$v(ab) = max\{v(a), v(b)\} \iff v(ab) = v(a) \vee v(ab) = v(b) \iff b \in \mathcal{U}(A) \vee a \in \mathcal{U}(A).$$

* * *

Esercizio 3.3.13. È noto che $\boldsymbol{Z}[\sqrt{2}]$ è un *ED* (rispetto al valore assoluto della norma). Scelti $z = 10 + 3\sqrt{2}$, $w = 1 + 2\sqrt{2} \in \boldsymbol{Z}[\sqrt{2}]$:

(*i*) Calcolare quoziente e resto della divisione euclidea di z per w. [*Suggerimento.* Procedere come visto in $\boldsymbol{Z}[i]$, cfr. [AA] pag. 126].

(*ii*) Con l'algoritmo euclideo delle divisioni successive, verificare che $MCD(z, w) = 1$ e determinare un'identità di Bézout relativa a z, w.

Soluzione. (*i*) La funzione di valutazione euclidea è

$$v : \boldsymbol{Z}[\sqrt{2}]^{\cdot} \to \boldsymbol{N} \text{ tale che } v(a + b\sqrt{2}) = |\mathcal{N}(a + b\sqrt{2})| = |a^2 - 2b^2|, \ \ \forall\, a + b\sqrt{2} \in \boldsymbol{Z}[\sqrt{2}]^{\cdot}.$$

Si ha:

$$\tfrac{z}{w} = \tfrac{z\,\overline{w}}{w\,\overline{w}} = \tfrac{-2-17\sqrt{2}}{-7} = \tfrac{2}{7} + \tfrac{17}{7}\sqrt{2}.$$

L'intero più vicino a $\frac{2}{7}$ è 0; l'intero più vicino a $\frac{17}{7}$ è 2. Si ponga $q = 0+2\sqrt{2} = 2\sqrt{2}$ e $r := z - qw$. Risulta allora $r = 2+\sqrt{2}$. Si ha: $v(r) = |4-2| = 2 < v(w) = |-7| = 7$ e, per costruzione $z = wq+r$. q, r sono il resto ed il quoziente cercati.

(*ii*) Da (*i*), $z = wq + r$, con $q = 2\sqrt{2}$, $r = 2 + \sqrt{2}$.

Si calcoli ora $w = rq_1 + r_1$, con $v(r_1) < v(r)$. Si ha: $\frac{w}{r} = -1 + \frac{3}{2}\sqrt{2}$ e si ponga $q_1 = -1 + \sqrt{2}$. Allora $r_1 := w - rq_1 = 1 + \sqrt{2}$. Si ha $v(r_1) = |1 - 2| = 1$ e dunque $r_1 \in \mathcal{U}(\boldsymbol{Z}[\sqrt{2}])$. Il procedimento delle divisioni successive termina e $MCD(z, w) = r_1 \sim 1$.

Da $z = wq + r$ e $w = rq_1 + r_1$, risulta:

$$r_1 = -q_1\, z + w(1 + q\, q_1) = (1 - \sqrt{2})z + (5 - 2\sqrt{2})w.$$

Moltiplicando ambo i membri per $r_1^{-1} = -\overline{r_1}$, si ottiene l'identità di Bézout:

$$1 = (-3 + 2\sqrt{2})\, z + (-9 + 7\sqrt{2})\, w.$$

* * *

Esercizio 3.4.1. Sia K un campo di caratteristica $p > 0$. Verificare che l'applicazione

$$\varphi : K \to K \text{ tale che } \varphi(a) = a^p, \ \ \forall\, a \in K,$$

è un omomorfismo iniettivo di anelli. Se K è finito, verificare che φ è un automorfismo di K. Tale automorfismo è detto *automorfismo di Frobenius di* K.

Soluzione. Ovviamente $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$, $\forall\, a, b \in K$. Per provare che φ è un omomorfismo, va verificato che $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall\, a, b \in K$ Risulta:

$$(a + b)^p = \sum_{t=0}^{p} \tbinom{p}{t} a^{p-t} b^t = a^p + p\, a^{p-1} b + \tbinom{p}{2} a^{p-2} b^2 + \ \ldots\ + p\, a\, b^{p-1} + b^p.$$

Siccome $car(K) = p$, tutti i termini intermedi della precedente somma sono nulli, in quanto multipli di p [e $p = 0$ in K]. Quindi

$$\varphi(a + b) = (a + b)^p = a^p + b^p = \varphi(a) + \varphi(b).$$

Poiché $\varphi(1) = 1$, $Ker\varphi \neq K$ e dunque $Ker\varphi = \{0\}$, cioè φ è iniettivo.

Sia infine $|K| < \infty$. È noto che ogni applicazione iniettiva di un insieme finito in sé è anche suriettiva. Dunque φ è un automorfismo di K.

* * *

Esercizio 3.4.2. Siano A, B anelli commutativi unitari, entrambi di caratteristica positiva. Determinare la caratteristica del prodotto diretto $A \times B$.

Soluzione. Sia $car(A) = c > 0$, $car(B) = d > 0$. Sia $h := mcm(c, d)$. Per definizione di minimo comune multiplo, $\begin{matrix} c \\ d \end{matrix} \Big| h$ e $\big[\begin{matrix} c \\ d \end{matrix} \Big| h' \implies h \,|\, h' \big]$. Sia $h = cr = ds$. Si ha:

$$h(1_A, 1_B) = (h1_A, h1_B) = (cr1_A, ds1_B) = (0_A, 0_B)$$

[infatti $cr1_A = c1_A \cdot r1_A = 0_A$ e $ds1_B = d1_B \cdot s1_B = 0_B$]. Abbiamo così provato che $car(A\times B) > 0$. Posto $\ell := car(A\times B)$, allora $\ell \,\big|\, h$.

Viceversa, $(0_A, 0_B) = \ell(1_A, 1_B) = (\ell 1_A, \ell 1_B)$. Dunque $\ell \in (c)$ e $\ell \in (d)$, cioè $\begin{matrix} c \\ d \end{matrix}\Big| \ell$. Allora $h \,\big|\, \ell$. Abbiamo così provato che

$$car(A\times B) = mcm\big(car(A), car(B)\big), \text{ se } car(A), car(B) > 0.$$

* * *

Esercizio 3.4.3. Sia $\varphi : A \to B$ un omomorfismo unitario di anelli commutativi unitari. Verificare che $car(B) \,\big|\, car(A)$.

Soluzione. Se $car(A) = 0$, la tesi è ovvia. Sia allora $c = car(A) > 0$ e sia $c' = car(B)$. Denotiamo inoltre con $f' : \boldsymbol{Z} \to B$ l'omomorfismo tale che $f'(n) = n\,1_B$, $\forall\, n \in \boldsymbol{Z}$. Allora $Kerf' = (c')$. Si ha:

$$0 = \varphi(0) = \varphi(c1_A) = c\varphi(1_A) = c\,1_B.$$

Dunque $c \in Kerf' = (c')$. Allora $c' \,\big|\, c$, come richiesto.

* * *

Esercizio 3.4.4. Sia A un anello commutativo unitario.

(*i*) Indicato con A_{S_0} l'anello totale delle frazioni di A, verificare che $car(A_{S_0}) = car(A)$.

(*ii*) Determinare un esempio di parte moltiplicativa S di A tale che $car(A_S) \neq car(A)$.

Soluzione. (*i*) Sia $f : A \to A_{S_0}$ l'omomorfismo canonico [tale che $f(a) = \frac{a}{1}$, $\forall\, a \in A$]. È noto che f è un omomorfismo iniettivo (cfr. Eserc. **3.2.7**) ed unitario. In base a Prop. **4.1**(*i*), $car(A) = car(A_{S_0})$.

(*ii*) Si consideri in $\boldsymbol{Z}_{12}$ la parte moltiplicativa $S = \overline{1} + \overline{3}\,\boldsymbol{Z}_{12} = \{\overline{1}, \overline{4}, \overline{7}, \overline{11}\}$. Dall'Eserc. **3.2.3**(*ii*) è noto che $(\boldsymbol{Z}_{12})_S \cong \boldsymbol{Z}_3$. Dunque $car(\boldsymbol{Z}_{12}) = 12$, mentre $car\big((\boldsymbol{Z}_{12})_S\big) = 3$.

Un altro esempio (banale) si ottiene scegliendo un anello c.u. $A \neq \boldsymbol{0}$ ed una sua parte moltiplicativa S con $0 \in S$. In tal caso $A_S = \boldsymbol{0}$ e quindi $1 = car(A_S) \neq car(A)$.

* * *

Esercizio 3.4.5. Ogni anello commutativo unitario A contiene, come sottoanello unitario, al più un solo anello $\boldsymbol{Z}_n$, $n \geq 2$.

Soluzione. Se $car(A) = 0$, A non possiede alcun sottoanello $\boldsymbol{Z}_n$ [altrimenti $n1_A = 0_A$ e quindi $n \in Kerf = (0)$].

Sia invece $car(A) = c > 0$ e sia $\boldsymbol{Z}_n \subseteq A$. Allora $\overline{n} = \overline{0}$, cioè $n1_A = 0_A$, per cui $d \in (c)$, cioè $d = cr$, $\exists\, r \geq 1$. Se fosse $r > 1$, allora $0 < c < n$ e quindi $\overline{c} \neq \overline{0}$ in $\boldsymbol{Z}_n$, cioè $\overline{c} \neq \overline{0}$ in A, ovvero $c1_A \neq 0_A$: assurdo. Pertanto $r = 1$ e $\boldsymbol{Z}_c$ è l'unico anello di tipo $\boldsymbol{Z}_n$ in A.

* * *

SOLUZIONI DEGLI ESERCIZI

DEL CAPITOLO 4

Esercizio 4.1.1. Si consideri in $\boldsymbol{R}$ l'insieme

$$L = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, \ \ \forall\, a, b, c \in \boldsymbol{Q}\}.$$

Verificare che L è un campo ed è un'estensione semplice di $\boldsymbol{Q}$.

Soluzione. Si verifica facilmente che $L - L \subseteq L$ e $L \cdot L \subseteq L$. Dunque L è un sottoanello di $\boldsymbol{R}$ e quindi è un dominio. Per dimostrare che L è un campo occorre verificare che ogni elemento $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in L^{\cdot}$ ammette inverso. A tal fine si potrebbe considerare un elemento "incognito" $x + y\sqrt[3]{2} + z\sqrt[3]{4} \in L$ ed imporre la condizione:

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = 1.$$

Sviluppando i calcoli si ottiene un sistema lineare di tre equazioni nelle incognite x, y, z. La soluzione di tale sistema fornisce (in funzione di a, b, c) i coefficienti x, y, z dell'inverso cercato. Va però verificata l'esistenza ed unicità della soluzione del sistema.

Conviene invece seguire un'altra strada. Poiché $X^3 - 2 \in \boldsymbol{Q}[X]$ è irriducibile, allora $\boldsymbol{Q}[X]/_{(X^3-2)}$ è un campo. Risulta:

$$\boldsymbol{Q}[X]/_{(X^3-2)} \cong \boldsymbol{Q}[x \mid x^3 = 2] = \{a + bx + cx^2, \ \ \forall\, a, b, c \in \boldsymbol{Q};\ x^3 = 2\}.$$

Per creare un isomorfismo tra L e $\boldsymbol{Q}[X]/_{(X^3-2)}$, si definisce

$$\varphi : \boldsymbol{Q}[X] \to \boldsymbol{R} \ \text{ tale che } \ \varphi(f) = f(\sqrt[3]{2}), \ \ \forall\, f \in \boldsymbol{Q}[X].$$

φ è un omomorfismo di anelli. Inoltre $Ker\varphi = (X^3 - 2)$ [infatti $Ker\varphi$ è un ideale principale e non contiene polinomi di grado < 3].

Infine $Im\,\varphi = L$. Infatti, $\forall\, k \in \boldsymbol{N}$, se $k = 3q + r$ $(0 \le r < 3)$, si ha: $(\sqrt[3]{2})^k = 2^q(\sqrt[3]{2})^r$. Dunque $(\sqrt[3]{2})^k \in L$. Pertanto $f(\sqrt[3]{2}) \in L$, $\forall\, f \in \boldsymbol{Q}[X]$, cioè $Im\,\varphi \subseteq L$ [mentre l'inclusione opposta è ovvia].

Abbiamo così provato che $L \cong \boldsymbol{Q}[X]/_{(X^3-2)}$. Dunque L è un campo.

Infine $L = \boldsymbol{Q}(\sqrt[3]{2})$ [in quanto ogni $\alpha \in L$ è generato a partire da $\boldsymbol{Q} \cup \{\sqrt[3]{2}\}$].

* * *

Esercizio 4.1.2. Dire se sono isomorfe le seguenti estensioni di campi

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2}), \qquad \boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{3}).$$

Soluzione. Se le due estensioni fossero isomorfe, esisterebbero due isomorfismi

$$f : \boldsymbol{Q} \to \boldsymbol{Q}, \quad F : \boldsymbol{Q}(\sqrt{2}) \to \boldsymbol{Q}(\sqrt{3})$$

che rendono commutativo il seguente diagramma di campi:

$$\begin{array}{ccc} \boldsymbol{Q} & \xrightarrow{\ f\ } & \boldsymbol{Q} \\ \downarrow & & \downarrow \\ \boldsymbol{Q}(\sqrt{2}) & \xrightarrow{\ F\ } & \boldsymbol{Q}(\sqrt{3}) \end{array}$$

Ora $f = \mathbf{1}_{\boldsymbol{Q}}$ [infatti $f(\frac{a}{b}) = \frac{f(a)}{f(b)} = \frac{af(1)}{bf(1)} = \frac{a}{b}$]. Ne segue che $F_{|_{\boldsymbol{Q}}} = \mathbf{1}_{\boldsymbol{Q}}$. Poniamo $F(\sqrt{2}) = a + b\sqrt{3}$, per opportuni $a, b \in \boldsymbol{Q}$. Allora:

$$2 = F(2) = F((\sqrt{2})^2) = (F(\sqrt{2}))^2 = (a + b\sqrt{3})^2.$$

Dunque $a + b\sqrt{3}$ è uno zero di $X^2 - 2$. Perciò $a + b\sqrt{3} = \pm\sqrt{2}$. Quadrando si otterrebbe $\sqrt{3} \in \boldsymbol{Q}$ (assurdo) oppure $a = b = 0$ e dunque F non sarebbe suriettiva (assurdo).

* * *

Esercizio 4.1.3. Si consideri in $\boldsymbol{R}$ il sottoinsieme $T = \{\sqrt{2^k},\ \forall\, k \in \boldsymbol{Z}\}$. Verificare che

$$\langle\, T\,\rangle = \boldsymbol{Q}(\sqrt{2}).$$

Soluzione. Si osserva subito che

$$\boldsymbol{Q}(\sqrt{2}) = \langle\, \boldsymbol{Q} \cup \{\sqrt{2}\}\,\rangle = \{q_1 + q_2\sqrt{2},\ \forall\, q_1, q_2 \in \boldsymbol{Q}\}.$$

Infatti ogni frazione $\frac{f(\sqrt{2})}{g(\sqrt{2})}$, con $f, g \in \boldsymbol{Q}[X]$, può essere prima trasformata in un'espressione del tipo $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ (con $a, b, c, d \in \boldsymbol{Q}$, $cd \neq 0$) e poi "razionalizzata" [moltiplicandola per $\frac{c-d\sqrt{2}}{c-d\sqrt{2}}$].

Poiché il sottocampo fondamentale $\boldsymbol{R}_f$ è $\boldsymbol{Q}$, allora

$$\langle\, T\,\rangle = \langle\, \boldsymbol{Q} \cup T\,\rangle = \boldsymbol{Q}(T) = \boldsymbol{Q}(T - \boldsymbol{Q}).$$

Si ha:

$$T = \{1, \sqrt{2}, 2, 2\sqrt{2}, 4, 4\sqrt{2}, 8, 8\sqrt{2}, ...\} \cup \{\tfrac{1}{2}\sqrt{2}, \tfrac{1}{2}, \tfrac{1}{4}\sqrt{2}, \tfrac{1}{4}, \tfrac{1}{8}\sqrt{2}, \tfrac{1}{8}, ...\}.$$

Ne segue che

$$T - \boldsymbol{Q} = \{2^h\sqrt{2},\ \forall\, h \in \boldsymbol{N}\} \cup \{\tfrac{1}{2^h}\sqrt{2},\ \forall\, h > 0\} = \{2^h\sqrt{2},\ \forall\, h \in \boldsymbol{Z}\}.$$

Ovviamente $\boldsymbol{Q}(\sqrt{2}) \subseteq \boldsymbol{Q}(T - \boldsymbol{Q})$, perché $\sqrt{2} \in T - \boldsymbol{Q}$. Viceversa ogni $2^h\sqrt{2} \in \boldsymbol{Q}(\sqrt{2})$ e quindi $\boldsymbol{Q}(T - \boldsymbol{Q}) \subseteq \boldsymbol{Q}(\sqrt{2})$. Possiamo concludere che $\boldsymbol{Q}(\sqrt{2}) = \langle\, T\,\rangle$.

* * *

Esercizio 4.1.4. Nel campo $\boldsymbol{C}(X)$ è assegnato il sottoinsieme $T = \{X^4, X^{-6}\}$. Determinare il sottocampo $\langle\, T\,\rangle$.

Soluzione. Si ha: $\langle\, T\,\rangle = \langle\, \boldsymbol{C}_f \cup T\,\rangle = \boldsymbol{Q}(T) = \boldsymbol{Q}(X^4, X^{-6})$.

Ovviamente $X^2 = (X^{-6})^{-1}(X^4)^{-1}$ e dunque $X^2 \in \langle\, T\,\rangle$. Pertanto $\boldsymbol{Q}(X^2) \subseteq \langle\, T\,\rangle$. Viceversa, il generico elemento di $\langle\, T\,\rangle$ è della forma $\frac{F}{G}$, con

$$F = \sum_{i,j} a_{i,\,j}\,(X^4)^i\,(X^{-6})^j, \quad G = \sum_{r,s} b_{r,\,s}\,(X^4)^r\,(X^{-6})^s$$

e $a_{i,\,j}, b_{r,\,s} \in Q$. Poichè

$$F = \sum_{i,j} a_{i,\,j}\,X^{4i-6j} = \sum_{i,j} a_{i,\,j}\,(X^2)^{2i-3j} \in K[X^2], \quad G = \sum_{r,s} b_{r,\,s}\,X^{4r-6s} = \sum_{r,s} b_{r,\,s}\,(X^2)^{2r-3s} \in K[X^2],$$

allora $\frac{F}{G} \in \boldsymbol{Q}(X^2)$ e quindi $\langle\, T\,\rangle \subseteq \boldsymbol{Q}(X^2)$.

* * *

Esercizio 4.1.5. Dimostrare che l'estensione $\boldsymbol{Q} \subset \boldsymbol{R}$ è non semplice.

[*Suggerimento*. Valutare la cardinalità di un'estensione semplice di $\boldsymbol{Q}$.]

Soluzione. Per assurdo, sia $\boldsymbol{R} = \boldsymbol{Q}(\alpha)$, con $\alpha \in \boldsymbol{R}$. Si ha: $\boldsymbol{Q}(\alpha) = \langle \boldsymbol{Q} \cup \{\alpha\}\rangle$. Quindi gli elementi di $\boldsymbol{Q}(\alpha)$ sono espressioni del tipo:

$$\tfrac{F(\alpha)}{G(\alpha)},\ \text{con}\ \ F, G \in \boldsymbol{Q}[X]\ \ \text{e}\ \ G(\alpha) \neq 0.$$

Ne segue che $|\boldsymbol{Q}(\alpha)| \leq |\boldsymbol{Q}(X)|$. Ricordiamo che $\boldsymbol{Q}(X) = \boldsymbol{Q}(\boldsymbol{Q}[X])$ (campo dei quozienti di $\boldsymbol{Q}[X]$). Inoltre:

- $\boldsymbol{Q}[X]$ è numerabile [infatti $|\boldsymbol{Q}[X]| \leq \sum_{i=1}^{\infty} |\boldsymbol{Q}| = |\boldsymbol{Q}|$, in base al teorema fondamentale del numerabile];

- per ogni dominio A, $|A| \leq |\boldsymbol{Q}(A)| \leq |A \times A|$, essendo $\boldsymbol{Q}(A) = A_{A^\cdot} = A \times A^\cdot/_\sim$. Ne segue che, se $|A| = |\boldsymbol{N}|$, allora $|\boldsymbol{Q}(A)| \leq |\boldsymbol{N} \times \boldsymbol{N}| = |\boldsymbol{N}|$ e quindi $|\boldsymbol{Q}(A)| = |\boldsymbol{N}|$.

In particolare allora $|\boldsymbol{Q}(X)| = |\boldsymbol{N}|$. Ne segue l'assurdo, visto che $|\boldsymbol{R}| > |\boldsymbol{N}|$.

* * *

Esercizio 4.1.6. Sia K un campo e si consideri l'estensione $K(X^2) \subset K(X)$. Verificare che $\{1, X\}$ è una base di $K(X)$ su $K(X^2)$.

Soluzione. Sia $\frac{F}{G} \in K(X)$ una funzione razionale. Scriviamo i due polinomi $F, G \in K[X]$ nella forma:

$$F = F_0 + X\,F_1,\ G = G_0 + X\,G_1,$$

con $F_0, F_1, G_0, G_1 \in K[X^2]$. Allora:

$$\frac{F}{G} = (F_0 + X\,F_1)\,\frac{1}{G_0+X\,G_1} = (F_0 + X\,F_1)\,\frac{G_0-X\,G_1}{(G_0+X\,G_1)(G_0-X\,G_1)} = \frac{F_0G_0+XF_1G_0-XF_0G_1-X^2F_1G_1}{G_0^{\,2}-X^2G_1^{\,2}} =$$

$$= \frac{F_0G_0-X^2F_1G_1}{G_0^{\,2}-X^2G_1^{\,2}} + X\,\frac{F_1G_0-F_0G_1}{G_0^{\,2}-X^2G_1^{\,2}} \in 1\cdot K(X^2) + X\cdot K(X^2).$$

Abbiamo così verificato che $\{1,\ X\}$ è un sistema di generatori di $K(X)$ come $K(X^2)$-spazio vettoriale.

Sia ora $\frac{F_0}{G_0} + X\,\frac{F_1}{G_1} = 0$, con $F_0, G_0, F_1, G_1 \in K[X^2]$ e $G_0, G_1 \neq 0$. Allora $X\,F_1G_0 = -F_0G_1$. Poiché i polinomi F_0, G_0, F_1, G_1 hanno grado pari, allora $X\,F_1G_0$ ha grado dispari, mentre $-F_0G_1$ lo ha pari. Ne segue che i due polinomi sono nulli e quindi $F_0 = F_1 = 0$. Abbiamo così verificato che $1,\ X$ sono linearmente indipendenti su $K(X^2)$.

* * *

Esercizio 4.2.1. Sia $z \in \boldsymbol{C} - \boldsymbol{R}$.

(*i*) Determinare il polinomio minimo di z su $\boldsymbol{R}$ [in funzione della norma e della traccia di z].

(*ii*) Esiste il polinomio minimo di z su $\boldsymbol{Q}$?

Soluzione. (*i*) Intendiamo per *traccia* di $z = x + iy \in \boldsymbol{C}$ il numero reale $Tr(z) := z + \overline{z} = 2x$. Si verifica immediatamente che $z^2 - Tr(z)\,z + \mathcal{N}(z) = 0$. Ne segue che z è zero del polinomio

$$f = X^2 - Tr(z)\,X + \mathcal{N}(z) \in \boldsymbol{R}[X].$$

Tale polinomio ha come zeri $z, \overline{z},$ non in $\boldsymbol{R}$. Dunque è irriducibile su $\boldsymbol{R}$. È poi monico e quindi f è il polinomio minimo di z su $\boldsymbol{R}$.

(*ii*) Il polinomio minimo di z su $\boldsymbol{Q}$ non esiste sempre, perché in generale z non è algebrico su $\boldsymbol{Q}$. Ad esempio, si consideri $z = i\,\pi \in \boldsymbol{C} - \boldsymbol{R}$. Se per assurdo z fosse algebrico su $\boldsymbol{Q}$, esisterebbe un polinomio non nullo $q = \sum_{t=0}^{n} a_t\,X^t \in \boldsymbol{Q}[X]$ tale che $q(i\,\pi) = 0$. Allora:

$$0 = \sum_{t=0}^{n} a_t\,(i\,\pi)^t = (a_0 - a_2\pi^2 + a_4\pi^4 + \ldots) + i(a_1\pi - a_3\pi^3 + a_5\pi^5 + \ldots).$$

Trattando separatamente parte reale e parte immaginaria, si ottengono due polinomi in $\boldsymbol{Q}[X]$ (non entrambi nulli) che ammettono π come zero. Ma π è trascendente su $\boldsymbol{Q}$: assurdo.

* * *

Esercizio 4.2.2. Siano p, q due primi distinti. Determinare il grado $[\boldsymbol{Q}(\sqrt{p},\ \sqrt{q}) : \boldsymbol{Q}]$ ed una base di $\boldsymbol{Q}(\sqrt{p},\ \sqrt{q})$ su $\boldsymbol{Q}$.

Soluzione. Risulta: $\boldsymbol{Q}(\sqrt{p},\ \sqrt{q}) = \boldsymbol{Q}(\sqrt{p})(\sqrt{q})$.

[Tale fatto è del tutto generale: per ogni campo K risulta che $K(\alpha,\ \beta) = K(\alpha)(\beta)$. Infatti $K(\alpha,\ \beta)$ è il più piccolo campo contenente $K, \alpha,\ \beta$. Siccome $\alpha, \beta \in K(\alpha)(\beta)$, allora $K(\alpha,\ \beta) \subseteq K(\alpha)(\beta)$. Viceversa, $K(\alpha) \subseteq K(\alpha,\ \beta)$, $\beta \in K(\alpha,\ \beta)$ e quindi $K(\alpha)(\beta) \subseteq K(\alpha,\ \beta)$.]

Si consideri la seguente catena di estensioni algebriche semplici:

$$\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{p}) \subseteq \boldsymbol{Q}(\sqrt{p},\ \sqrt{q}).$$

La prima ha grado 2 e $\sqrt{p}$ ha polinomio minimo $X^2 - p \in \boldsymbol{Q}[X]$. Anche la seconda ha grado 2. Per verificarlo, si osservi che $\sqrt{q}$ è zero del polinomio $X^2 - q \in \boldsymbol{Q}(\sqrt{p})[X]$. Tale polinomio è irriducibile su $\boldsymbol{Q}(\sqrt{p})$. Se infatti non lo fosse, esisterebbe $a + b\sqrt{p} \in \boldsymbol{Q}(\sqrt{p})$ tale che $(a + b\sqrt{p})^2 = q$. Ma allora $\sqrt{p} \in \boldsymbol{Q}$: assurdo. Si conclude che $[\boldsymbol{Q}(\sqrt{p},\ \sqrt{q}) : \boldsymbol{Q}] = 2\cdot 2 = 4$.

Per ottenere una base del $\boldsymbol{Q}$-spazio vettoriale $\boldsymbol{Q}(\sqrt{p},\ \sqrt{q})$, si scelgano le basi $\{1,\ \sqrt{p}\}$ di $\boldsymbol{Q}(\sqrt{p})$ su $\boldsymbol{Q}$ e $\{1,\ \sqrt{q}\}$ di $\boldsymbol{Q}(\sqrt{p})(\sqrt{q})$ su $\boldsymbol{Q}(\sqrt{p})$. Il loro "prodotto"

$$1,\ \sqrt{p},\ \sqrt{q},\ \sqrt{pq}$$

è una base di $\boldsymbol{Q}(\sqrt{p},\sqrt{q})$ su $\boldsymbol{Q}$.

* * *

Esercizio 4.2.3. Determinare il grado ed una base dell'estensione $\boldsymbol{Q}\subset\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$.

Soluzione. Si consideri la catena di estensioni:

$$\boldsymbol{Q}\subset\boldsymbol{Q}(\sqrt[3]{2})\subset\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2}).$$

Risulta subito che $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ è una base della prima estensione. Verifichiamo che $\sqrt{2}\notin\boldsymbol{Q}(\sqrt[3]{2})$. Altrimenti, se fosse $\sqrt{2}=a+b\sqrt[3]{2}+c\sqrt[3]{4}$ (con $a,b,c\in\boldsymbol{Q}$), allora quadrando:

$$2=a^2+b^2\sqrt[3]{4}+2c^2\sqrt[3]{2}+2ab\sqrt[3]{2}+2ac\sqrt[3]{4}+4bc.$$

Ne segue:

$$\{\ 2=a^2+4bc,\quad 0=2c^2+2ab,\quad 0=b^2+2ac.$$

Dalla seconda e terza uguaglianza, $2c^3=b^3$ e quindi, se $b,c\neq 0$, $(\frac{b}{c})^3=2$: assurdo [in $\boldsymbol{Q}$]. Ne segue che $\{1,\sqrt{2}\}$ è una base di $\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ su $\boldsymbol{Q}(\sqrt[3]{2})$ e si conclude che:

$$[\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2}):\boldsymbol{Q}]=[\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2}):\boldsymbol{Q}(\sqrt[3]{2})]\cdot[\boldsymbol{Q}(\sqrt[3]{2}):\boldsymbol{Q}]=2\cdot 3=6.$$

Infine una base di $\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ su $\boldsymbol{Q}$ è data dal prodotto delle due basi:

$$\{1,\sqrt[3]{2},\sqrt[3]{4},\ \sqrt{2},\sqrt{2}\sqrt[3]{2},\ \sqrt{2}\sqrt[3]{4}\}=\{1,\,2^{1/3},\,2^{2/3},\,2^{1/2},\,2^{1/2+1/3},\,2^{1/2+2/3}\}=$$
$$=\{1,\,2^{2/6},\,2^{4/6},\,2^{3/6},\,2^{5/6},\,2\cdot 2^{1/6}\}.$$

Quindi una base è anche $\{2^{k/6},\ 0\le k\le 5\}$.

* * *

Esercizio 4.2.4. Determinare il grado ed il polinomio minimo dell'estensione algebrica semplice $\boldsymbol{Q}\subset\boldsymbol{Q}(\sqrt{2}+\sqrt{3})$.

Soluzione. Risulta: $\boldsymbol{Q}\subseteq\boldsymbol{Q}(\sqrt{2}+\sqrt{3})\subseteq\boldsymbol{Q}(\sqrt{2},\sqrt{3})$. Poiché $[\boldsymbol{Q}(\sqrt{2},\sqrt{3}):\boldsymbol{Q}]=4$, allora $[\boldsymbol{Q}(\sqrt{2}+\sqrt{3}):\boldsymbol{Q}]\le 4$. Posto $\alpha=\sqrt{2}+\sqrt{3}$, esiste un polinomio $P\in\boldsymbol{Q}[X]$ tale che $\partial P\le 4$ e $P(\alpha)=0$.

Per calcolare P osserviamo: $\alpha^2=5+2\sqrt{6}$, $\alpha^4=49+20\sqrt{6}$. Dunque $\alpha^4-10\alpha^2=-1$. Pertanto

$$P=X^4-10X^2+1\in\boldsymbol{Q}[X]$$

ammette α come zero. Per provare che P è il polinomio minimo di α su $\boldsymbol{Q}$ [e quindi $[\boldsymbol{Q}(\alpha):\boldsymbol{Q}]=4$] basta verificare che P è irriducibile su $\boldsymbol{Q}$.

P non ha zeri razionali [infatti $P(\pm 1)\neq 0$]. Verifichiamo che P non è prodotto di due polinomi irriducibili di grado 2 in $\boldsymbol{Q}[X]$. Risolvendo l'equazione $Y^2-10Y+1=0$ si ottengono gli zeri $5\pm 2\sqrt{6}\in\boldsymbol{R}$. Allora in $\boldsymbol{R}[X]$ si ha:

$$P=(X^2-5+2\sqrt{6})(X^2-5-2\sqrt{6}).$$

Tale fattorizzazione è unica (in $\boldsymbol{R}[X]$) e i due fattori non sono associati a polinomi a coefficienti razionali. Se ne deduce che P è irriducibile su $\boldsymbol{Q}$, come richiesto.

* * *

Esercizio 4.2.5. Assegnato $\alpha=\sqrt{2+\sqrt{2}}\in\boldsymbol{R}$,

(*i*) determinare il polinomio minimo di α su $\boldsymbol{Q}$;

(*ii*) esprimere $\frac{1}{\sqrt{2}}$ come combinazione lineare (a coefficienti razionali) delle potenze di α.

(*iii*) determinare il polinomio minimo di α su $\boldsymbol{Q}(\frac{1}{\sqrt{2}})$.

Soluzione. (*i*) Si ha: $\alpha^2=2+\sqrt{2}$, $\alpha^4=6+4\sqrt{2}$. Allora $\alpha^4-4\alpha^2=6+4\sqrt{2}-8-4\sqrt{2}=-2$. Dunque il polinomio

$$f = X^4 - 4X^2 + 2 \in \boldsymbol{Q}[X]$$

ammette α come zero. Tale polinomio è monico ed irriducibile (dal criterio di Eisenstein). Quindi è il polinomio minimo di α su $\boldsymbol{Q}$.

(*ii*) $\boldsymbol{Q}(\alpha)$ ha base $\{1, \alpha, \alpha^2, \alpha^3\}$. Poiché $\frac{1}{\sqrt{2}} \in \boldsymbol{Q}(\alpha)$ [infatti $\sqrt{2} = \alpha^2 - 2 \in \boldsymbol{Q}(\alpha)$], allora

$$\tfrac{1}{\sqrt{2}} = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3, \text{ per opportuni } a_0, a_1, a_2, a_3 \in \boldsymbol{Q}.$$

Da $\alpha^2 = 2 + \sqrt{2}$ segue: $\frac{\alpha^2}{2} = 1 + \frac{\sqrt{2}}{2} = 1 + \frac{1}{\sqrt{2}}$ e quindi $\frac{1}{\sqrt{2}} = -1 + \frac{\alpha^2}{2}$ è la combinazione lineare richiesta.

(*iii*) Ovviamente $\boldsymbol{Q}(\frac{1}{\sqrt{2}}) = \boldsymbol{Q}(\sqrt{2})$. Sussiste la catena di inclusioni

$$\boldsymbol{Q} \supset \boldsymbol{Q}(\sqrt{2}) \supset \boldsymbol{Q}(\alpha).$$

Poiché $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = \partial f = 4$ e $[\boldsymbol{Q}(\sqrt{2}) : \boldsymbol{Q}] = 2$, allora $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}(\sqrt{2})] = 2$. Si osservi che α è zero del polinomio $g = X^2 - (2 + \sqrt{2}) \in \boldsymbol{Q}(\sqrt{2})[X]$. Poiché $\alpha \notin \boldsymbol{Q}(\sqrt{2})$, g è irriducibile su $\boldsymbol{Q}(\sqrt{2})$. Essendo g monico, g è il polinomio minimo di α su $\boldsymbol{Q}(\frac{1}{\sqrt{2}})$.

* * *

Esercizio 4.2.6. Sia $K := \boldsymbol{Z}_2(x) = \boldsymbol{Z}_2[X]/_{(p)}$, con $p = X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X]$ (estensione algebrica semplice di $\boldsymbol{Z}_2$). Sia $q = X^2 + xX + \overline{1} \in K[X]$.

(*i*) Verificare che q è irriducibile su K e determinare gli elementi del campo $K[y] := K[X]/_{(q)}$ (con $y := X + (q)$).

(*ii*) Calcolare il grado di $[K[y] : \boldsymbol{Z}_2]$ e studiare l'estensione algebrica semplice $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(y)$, determinando il polinomio minimo di y su $\boldsymbol{Z}_2$.

Soluzione. (*i*) Si ha:

$$K = \boldsymbol{Z}_2(x) = \{\overline{0}, \overline{1}, x, x + \overline{1};\ x^2 = x + \overline{1}\}.$$

Per verificare che q è irriducibile in $K[X]$ è sufficiente verificare che non ha zeri in K [infatti $q(\overline{0}) = q(\overline{1}) = q(x) = \overline{1}$, $q(x + \overline{1}) = x + \overline{1}$].

Gli elementi del campo $L := K[y] = \boldsymbol{Z}_2(x)[y] = \boldsymbol{Z}_2(x, y)$ sono del tipo $a + by$, con $a, b \in \boldsymbol{Z}_2(x)$, e dunque sono i seguenti sedici:

$$\begin{array}{cccc} \overline{0} & y & xy & (x+\overline{1})y \\ \overline{1} & \overline{1}+y & \overline{1}+xy & \overline{1}+(x+\overline{1})y \\ x & x+y & x+xy & x+(x+\overline{1})y \\ x+\overline{1} & x+\overline{1}+y & x+\overline{1}+xy & x+\overline{1}+(x+\overline{1})y. \end{array}$$

(*ii*) Si ha: $[L : \boldsymbol{Z}_2] = [K[y] : K] \cdot [K : \boldsymbol{Z}_2] = 2 \cdot 2 = 4$.

Vogliamo valutare $[\boldsymbol{Z}_2(y) : \boldsymbol{Z}_2]$. A priori, essendo $\boldsymbol{Z}_2(y)$ un campo intermedio tra Z_2 ed L, $[\boldsymbol{Z}_2(y) : \boldsymbol{Z}_2] = 2$ oppure $= 4$. Nel primo caso $|\boldsymbol{Z}_2(y)| = 4$; nel secondo $\boldsymbol{Z}_2(y) = K[y]$.

Osserviamo che $\overline{0}, \overline{1}, y, \overline{1} + y \in \boldsymbol{Z}_2(y)$. Ma anche $y^2 - \overline{1} = xy \in \boldsymbol{Z}_2(y)$. Dunque $|\boldsymbol{Z}_2(y)| \geq 5$ e pertanto $\boldsymbol{Z}_2(y) = K[y]$. Quindi il polinomio minimo f di y su $\boldsymbol{Z}_2$ ha grado 4.

Per calcolare f osserviamo che $\overline{1}, y, y^2, y^3$ è una base di $\boldsymbol{Z}_2(y)$ su $\boldsymbol{Z}_2$. Quindi devono esistere $a, b, c, d \in \boldsymbol{Z}_2$ tali che

$$y^4 = a + by + cy^2 + dy^3.$$

Si ha, con semplici calcoli: $y^2 = xy + \overline{1}$, $y^3 = x + xy$, $y^4 = x + y$. Allora

$$x + y = a + by + cxy + c + dx + dxy = (a + c) + dx + by + (c + d)xy.$$

Ne segue: $a + c = \overline{0}$, $d = \overline{1}$, $b = \overline{1}$, $c + d = \overline{0}$, da cui $b = d = \overline{1}$, $c = \overline{1}$, $d = \overline{1}$. Pertanto

$$y^4 = \overline{1} + y + y^2 + y^3.$$

Il polinomio minimo cercato è quindi

$$f = X^4 + X^3 + X^2 + X + \overline{1} \in \boldsymbol{Z}_2[X].$$

Nota. Abbiamo provato che $L = K[y]$ è un'estensione semplice di $\boldsymbol{Z}_2$, di grado 4.

* * *

Esercizio 4.2.7. Sia $K \subset L$ un'estensione finita di campi e sia $f \in K[X]$ un polinomio irriducibile. Verificare che, se f ha uno zero in L, $\partial f \,\big|\, [L:K]$.

Soluzione. Sia $n = [L:K]$ e sia α uno zero di f in $K[X]$. Poiché f è irriducibile, f (a meno di un fattore in $K^{\cdot}$) è il polinomio minimo di α su K. Dunque $[K(\alpha):K] = n$. Poiché

$$n = [L:K] = [L:K(\alpha)] \cdot [K(\alpha):K] = [L:K(\alpha)] \cdot \partial f,$$

allora $\partial f \,\big|\, n$, cioè $\partial f \,\big|\, [L:K]$.

* * *

Esercizio 4.2.8. Sia p un primo. Calcolare il polinomio ciclotomico $\Phi_{p^2} \in \boldsymbol{Z}[X]$ e verificare che è irriducibile.

[*Suggerimento*: applicare il criterio di Eisenstein a $\Phi_{p^2}(X+1)$].

Soluzione. Si ha:

$$\Phi_{p^2} = \tfrac{X^{p^2}-1}{\Phi_1 \Phi_p} = \tfrac{X^{p^2}-1}{X^p-1}.$$

Eseguendo la divisione con resto di $X^{p^2}-1$ per X^p-1, si ottiene:

$$\Phi_{p^2} = \sum_{k=0}^{p-1} X^{pk} = 1 + X^p + X^{2p} + \,...\, + X^{p(p-1)}.$$

Per dimostrarne l'irriducibilità, verifichiamo che è possibile applicare il criterio di Eisenstein a $\Phi_{p^2}(X+1)$. Si ha:

$$\Phi_{p^2}(X+1) = \sum_{k=0}^{p-1} (X+1)^{pk}.$$

L'addendo di grado massimo di tale polinomio è $X^{p(p-1)}$ ed il termine noto è $p\ (= 1 + \,...\, + 1)$. Per applicare il criterio di Eisenstein (relativamente a p) basta verificare che i coefficienti intermedi del polinomio sono multipli di p. Poniamo:

$$\Phi_{p^2}(X+1) - X^{p(p-1)} = \sum_{j=0}^{p^2-p-1} \alpha_j X^j.$$

Dobbiamo verificare che $p \,\big|\, \alpha_j$, $\forall\, j = 1, \,...\, , p^2-p-1$. Si ha:

$$\Phi_{p^2}(X+1) = \tfrac{(X+1)^{p^2}-1}{(X+1)^p-1} = \tfrac{X^{p^2}+p\,f_1}{X^p+p\,f_2}, \text{ per opportuni } f_1,\, f_2 \in \boldsymbol{Z}[X].$$

Allora:

$$X^{p^2} + p\,f_1 = \big(X^p + p\,f_2\big)\,\Phi_{p^2}(X+1) = \big(X^p + p\,f_2\big)\,\big(X^{p(p-1)} + \sum_{j=0}^{p^2-p-1} \alpha_j X^j\big) =$$

$$= X^{p^2} + p\,f_2 X^{p(p-1)} + \textstyle\sum \alpha_j X^{j+p} + p\,f_2\big(\sum \alpha_j X^j\big).$$

Cancellando il fattore X^{p^2} e raccogliendo p a fattore, si ottiene

$$\sum_{j=0}^{p^2-p-1} \alpha_j X^{j+p} = p\,f_3, \text{ per un opportuno } f_3 \in \boldsymbol{Z}[X].$$

Dunque $p \,\big|\, \alpha_j$, $\forall\, j = 1, \,...\, , p^2-p-1$, come richiesto.

Nota. Il procedimento può essere esteso per provare che Φ_{p^n} è irriducibile su $\boldsymbol{Z}$, $\forall\, n \geq 1$.

* * *

Esercizio 4.2.9. Determinare $[\boldsymbol{Q}(\zeta_3,\, \zeta_4) : \boldsymbol{Q}]$, con $\zeta_3 = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$, $\zeta_4 = \cos\frac{2\pi}{4} + i \sin\frac{2\pi}{4}$.

Soluzione. Si ha: $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ ha polinomio minimo su $\boldsymbol{Q}$: $\Phi_3 = X^2 + X + 1$, mentre $\zeta_4 = i$ ha polinomio minimo su $\boldsymbol{Q}$: $\Phi_2 = X^2 + 1$. Risulta:

$$[\boldsymbol{Q}(\zeta_3,\, \zeta_4) : \boldsymbol{Q}] = [\boldsymbol{Q}(\zeta_3,\, \zeta_4) : \boldsymbol{Q}(\zeta_4)] \cdot [\boldsymbol{Q}(\zeta_4) : \boldsymbol{Q}] = 2 \cdot [\boldsymbol{Q}(\zeta_3,\, i) : \boldsymbol{Q}(i)].$$

L'estensione semplice $\boldsymbol{Q}(i) \subset \boldsymbol{Q}(\zeta_3, i)$ ha grado ≤ 2 [infatti $\Phi_3 \in \boldsymbol{Q}(i)[X]$ e $\Phi_3(\zeta_3) = 0$]. Se per assurdo il grado fosse 1, Φ_3 sarebbe riducibile su $\boldsymbol{Q}(i)$ e quindi $\zeta_3 \in \boldsymbol{Q}(i)$, cioè $-1 + i\sqrt{3} = 2a + 2bi$, $\exists\, a, b \in \boldsymbol{Q}$. Quindi $\sqrt{3} \in \boldsymbol{Q}$: assurdo.

Si è provato che $[\boldsymbol{Q}(\zeta_3, \zeta_4) : \boldsymbol{Q}] = 4$.

* * *

Esercizio 4.2.10. Sia K_4 [risp. K_5] l'estensione di $\boldsymbol{Z}_3$ generata dalle radici quarte [risp. quinte] dell'unità (su $\boldsymbol{Z}_3$). Calcolare $[K_4 : \boldsymbol{Z}_3]$ e $[K_5 : \boldsymbol{Z}_3]$.

Soluzione. Le radici quarte e quinte dell'unità (su $\boldsymbol{Z}_3$) sono rispettivamente le soluzioni delle equazioni $X^4 - \overline{1} \in \boldsymbol{Z}_3[X]$, $X^5 - \overline{1} \in \boldsymbol{Z}_3[X]$.

Si ha: $X^4 - \overline{1} = (X^2 - \overline{1})(X^2 + \overline{1}) = (X - \overline{1})(X + \overline{1})(X^2 + \overline{1}) \in \boldsymbol{Z}_3[X]$. Due radici quarte dell'unità sono quindi $\overline{1}$ e $-\overline{1} = \overline{2}$. Inoltre $X^2 + \overline{1} \in \boldsymbol{Z}_3[X]$ è irriducibile [infatti non ha zeri in $\boldsymbol{Z}_3$]. Allora K_4 è generato su $\boldsymbol{Z}_3$ dai due zeri di $X^2 + \overline{1}$. Se x è uno dei due zeri, l'altro è $-x = \overline{2}x$ [infatti $X^2 + \overline{1} = (X - x)(X + x)$]. Pertanto:

$$K_4 = \boldsymbol{Z}_3(x, -x) = \boldsymbol{Z}_3(x) = \{a + bx,\ \forall\, a, b \in \boldsymbol{Z}_3;\ x^2 = 2\} \cong \boldsymbol{Z}_3[X]/_{(X^2+\overline{1})}.$$

Ovviamente $[K_4 : \boldsymbol{Z}_3] = [\boldsymbol{Z}_3(x) : \boldsymbol{Z}_3] = 2$.

Veniamo al campo K_5. Si ha:

$$X^5 - \overline{1} = (X - \overline{1})(X^4 + X^3 + X^2 + X + \overline{1}) \in \boldsymbol{Z}_3[X].$$

Cominciamo col verificare che il polinomio $f = X^4 + X^3 + X^2 + X + \overline{1}$ è irriducibile su $\boldsymbol{Z}_3$. Certamente f non ha zeri in $\boldsymbol{Z}_3$ [infatti $f(\overline{1}), f(\overline{2}) \neq \overline{0}$]. Per assurdo, f ammetta una fattorizzazione con due polinomi di grado 2, cioè

$$f = (X^2 + aX + b)(X^2 + cX + d).$$

Poiché $bd = \overline{1}$, allora $b = d = \overline{1}$ oppure $b = d = \overline{2}$. Nel primo caso, confrontando i coefficienti di ugual grado, si ottiene il sistema

$$\{\ a + c = \overline{1},\ ac + \overline{2} = \overline{1},\ a + c = \overline{1}\ ,$$

da cui $a(a - \overline{1}) = \overline{1}$, che non ha soluzioni in $\boldsymbol{Z}_3$. Nel secondo caso (cioè $b = d = \overline{2}$) si ottiene il sistema

$$\{\ a + c = \overline{1},\ ac + \overline{1} = \overline{1},\ \overline{2}a + \overline{2}c = \overline{1}\ ,$$

da cui $\overline{2} = \overline{1}$: assurdo. Si conclude che f è irriducibile. Ne segue che $\boldsymbol{Z}_3(x) \cong \boldsymbol{Z}_3[X]/_{(f)}$ è un'estensione di grado 4 su $\boldsymbol{Z}_3$, con base $\overline{1}, x, x^2, x^3$.

Si osserva subito che $x^2, x^3, x^4 (= -\overline{1} - x - x^2 - x^3)$ sono zeri di f [infatti sono zeri di $X^5 - \overline{1}$ e sono distinti dagli altri due zeri $\overline{1}, x$ di $X^5 - \overline{1}$]. Si conclude che

$$K_5 = \boldsymbol{Z}_3(x, x^2, x^3, x^4) = \boldsymbol{Z}_3(x).$$

Ovviamente $[K_5 : \boldsymbol{Z}_3] = \partial f = 4$.

* * *

Esercizio 4.2.11. Determinare un isomorfismo tra i due campi

$$K_1 = \boldsymbol{Z}_3[X]/_{(X^2+\overline{1})}, \quad K_2 = \boldsymbol{Z}_3[X]/_{(X^2+X+\overline{2})}\,.$$

Soluzione. Che K_1, K_2 siano campi dipende dal fatto che i due polinomi $f = X^2 + \overline{1}$, $g = X^2 + X + \overline{2} \in \boldsymbol{Z}_3[X]$ sono irriducibili su $\boldsymbol{Z}_3$ [infatti non hanno zeri in $\boldsymbol{Z}_3$, come subito si verifica].

Si tratta di due campi finiti di cardinalità 9, che possiamo rappresentare come estensioni algebriche semplici di $\boldsymbol{Z}_3$. Si ha:

$$K_1 = \boldsymbol{Z}_3(\alpha),\ \text{con}\ \alpha^2 + \overline{1} = \overline{0},\ \text{cioè}\ \alpha^2 = \overline{2}; \quad K_2 = \boldsymbol{Z}_3(\beta),\ \text{con}\ \beta^2 + \beta + \overline{2} = \overline{0},\ \text{cioè}\ \beta^2 = \overline{1} + \overline{2}\beta.$$

Si noti che (in base al Coroll. **2.1** di Cap. **5**) due campi finiti della stessa cardinalità sono isomorfi e dunque un isomorfismo tra K_1 e K_2 deve esistere. Lo otterremo cercando l'immagine di α in $\boldsymbol{Z}(\beta)$.

Sia $\varphi : \boldsymbol{Z}_3(\alpha) \to \boldsymbol{Z}_3(\beta)$ un isomorfismo (e quindi uno $\boldsymbol{Z}_3$-isomorfismo). Poniamo:

$$\varphi(\alpha) = a + b\beta, \text{ con } a, b \in \boldsymbol{Z}_3.$$

Si ha: $\varphi(\alpha)^2 = \varphi(\alpha^2) = \varphi(\overline{2}) = \overline{2}$ e quindi

$$\overline{2} = (a + b\beta)^2 = a^2 + \overline{2}ab\beta + b^2(\overline{1} + \overline{2}\beta) = a^2 + b^2 + \overline{2}b\beta(a + b).$$

Ne segue:

$$\overline{2}b\beta(a + b) = \overline{2}(\overline{1} + a^2 + b^2).$$

Poiché $\beta \notin \boldsymbol{Z}_3$, tale relazione è verificata $\iff b(a + b) = \overline{0}$ e $\overline{1} + a^2 + b^2 = \overline{0}$.

Se $b = \overline{0}$, allora $a^2 + \overline{1} = \overline{0}$ e ciò è assurdo, essendo $f(a) \neq \overline{0}$, $\forall\, a \in \boldsymbol{Z}_3$. Se $a + b = \overline{0}$, allora $\overline{1} + a^2 + (-a)^2 = \overline{0}$, cioè $a^2 = \overline{1}$ e quindi $a = \overline{1}, \overline{2}$. Ne segue che le possibili coppie (a, b) cercate sono: $(\overline{1}, \overline{2})$, $(\overline{2}, \overline{1})$.

Scegliamo la prima. Allora $\varphi(\alpha) = \overline{1} + \overline{2}\beta$. Quindi:

$$\varphi: \begin{array}{lll} \overline{0} \to \overline{0}, & \alpha \to \overline{1} + \overline{2}\beta, & \overline{2}\alpha \to \overline{2} + \beta \\ \overline{1} \to \overline{1}, & \overline{1} + \alpha \to \overline{2} + \overline{2}\beta, & \overline{1} + \overline{2}\alpha \to \beta \\ \overline{2} \to \overline{2}, & \overline{2} + \alpha \to \overline{2}\beta, & \overline{2} + \overline{2}\alpha \to \overline{1} + \beta. \end{array}$$

Dunque φ è biiettiva. Resta da verificare che è un omomorfismo. Si ha, $\forall\, a_1, a_2, b_1, b_2 \in \boldsymbol{Z}_3$:

$$\begin{aligned} \varphi\big((a_1 + b_1\alpha) + (a_2 + b_2\alpha)\big) &= \varphi(a_1 + a_2 + (b_1 + b_2)\alpha) = a_1 + a_2 + (b_1 + b_2)(\overline{1} + \overline{2}\beta) = \\ &= a_1 + b_1(\overline{1} + \overline{2}\beta) + a_2 + b_2(\overline{1} + \overline{2}\beta) = \\ &= \varphi\big((a_1 + b_1\alpha)\big) + \varphi\big((a_2 + b_2\alpha)\big); \\ \varphi\big((a_1 + b_1\alpha)\cdot(a_2 + b_2\alpha)\big) &= a_1a_2 + \overline{2}b_1b_2 + (b_1a_2 + a_1b_2)(\overline{1} + \overline{2}\beta); \\ \varphi\big((a_1 + b_1\alpha)\big)\cdot\varphi\big((a_2 + b_2\alpha)\big) &= \big((a_1 + b_1(\overline{1} + \overline{2}\beta))\big)\big((a_2 + b_2(\overline{1} + \overline{2}\beta))\big) = \\ &= a_1a_2 + b_1b_2(\overline{1} + \beta^2 + \beta) + (a_1b_2 + a_2b_1)(\overline{1} + \overline{2}\beta) = \\ &= a_1a_2 + \overline{2}b_1b_2 + (b_1a_2 + a_1b_2)(\overline{1} + \overline{2}\beta). \end{aligned}$$

* * *

Esercizio 4.3.1. Sia K un campo. È assegnata l'estensione di campi

$$K(X^2, XY) \subset K(X, Y).$$

Verificare che tale estensione è algebrica semplice e determinarne il grado.

Soluzione. Sia $L = K(X^2, XY)$ e $M = K(X, Y)$. Si consideri la catena di estensioni semplici:

$$L \subseteq L(X) \subseteq L(X, Y) = M.$$

L'estensione $L \subseteq L(X)$ è algebrica semplice. Infatti X è zero del polinomio $T^2 - X^2 \in L[T]$. Tale polinomio è monico ed irriducibile su L [infatti in M ha zeri $\pm X$ e $X \notin L$]. Dunque $[L(X) : L] = 2$. Si ha poi: $Y = \frac{XY}{X}$ (in $L(X)$). Dunque $M = L(X)(Y) = L(X)$. Pertanto $L \subset M$ è algebrica semplice di grado 2. È generata da X, con polinomio minimo $T^2 - X^2 \in L[T]$.

* * *

Esercizio 4.3.2. Sia K un campo. Verificare che l'estensione di campi

$$K(X^2Y, XY^2) \subseteq K(X, Y)$$

è algebrica semplice, di grado 3.

Soluzione. Si ponga: $L = K(X^2Y, XY^2)$, $M = K(X, Y)$. Dimostriamo preliminarmente che $X \notin L$ (e dunque $L \subset M$).

Per assurdo, sia $X = \frac{F}{G}$, con $F = F(X^2Y, XY^2)$, $G = G(X^2Y, XY^2) \in K[X^2Y, XY^2] \subset K[X, Y]$. Ovviamente F, G hanno in $K[X, Y]$ grado $\equiv 0\ (mod\ 3)$. Se quindi fosse $X = \frac{F}{G}$, allora $F = XG$ e $\partial F = \partial(XG) = 1 + \partial G \equiv 1\ (mod\ 3)$: assurdo.

Osserviamo che $\frac{X}{Y} = \frac{X^2Y}{XY^2} \in L$ e quindi anche $\frac{X}{Y}X^2Y = X^3 \in L$. Posto $h := T^3 - X^3 \in L[T]$, tale polinomio ammette X come zero. Dunque X è algebrico su L.

Si ha poi: $Y = X\frac{Y}{X}$. Anche $\frac{Y}{X} \in L$ [in quanto $\frac{Y}{X} = \frac{XY^2}{X^2Y}$] e quindi $Y = X\frac{Y}{X} \in L(X)$. Ne segue che $M = L(X)(Y) = L(X)$.

L'estensione $L \subset M$ è dunque algebrica semplice. Per dimostrare che ha grado 3 basta verificare che h è irriducibile in $L[T]$.

Si noti che gli zeri di h sono X, αX, $\alpha^2 X$, con α radice primitiva terza dell'unità (in un'estensione di K). Se in $L[T]$, h fosse riducibile, uno dei suoi tre zeri apparterrebbe ad L. Ma $X \notin L$ e dunque anche αX, $\alpha^2 X \notin L$ [se ad esempio $\alpha X \in L$, allora $\frac{1}{X}\alpha X = \alpha \in M$ e quindi $\alpha \in K$ (essendo $M = K(X, Y)$); allora $X = \frac{1}{\alpha}\,\alpha X \in L$: assurdo].

* * *

Esercizio 4.3.3. È assegnata l'estensione algebrica semplice $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{1+\sqrt{3}})$.

(*i*) Determinarne grado, base e polinomio minimo.

(*ii*) Esprimere $\frac{1}{\sqrt{3}\sqrt{1+\sqrt{3}}}$ in tale base.

Soluzione. (*i*) $\sqrt{1+\sqrt{3}}$ è zero del polinomio $X^2 - (1+\sqrt{3}) \in \boldsymbol{Q}(\sqrt{3})[X]$. Tale polinomio è irriducibile su $\boldsymbol{Q}(\sqrt{3})$ [altrimenti $\exists\, a, b \in \boldsymbol{Q}$ tali che $(a+b\sqrt{3})^2 = 1+\sqrt{3}$; in tal caso $a^2+3b^2-1 = (1-2ab)\sqrt{3}$ e dunque necessariamente $2ab = 1 = a^2+3b^2$. Ne seguirebbe $b = 0$, $ab = \frac{1}{2}$: assurdo].

Consideriamo la catena di estensioni:

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{3}) \subset \boldsymbol{Q}(\sqrt{1+\sqrt{3}}).$$

Risulta:

$$[\boldsymbol{Q}(\sqrt{1+\sqrt{3}}) : \boldsymbol{Q}] = [\boldsymbol{Q}(\sqrt{1+\sqrt{3}}) : \boldsymbol{Q}(\sqrt{3})]\cdot[\boldsymbol{Q}(\sqrt{3}) : \boldsymbol{Q}] = 2\cdot 2 = 4.$$

Una base di $\boldsymbol{Q}(\sqrt{1+\sqrt{3}})$ su $\boldsymbol{Q}$ si ottiene moltiplicando le due basi $\{1, \sqrt{1+\sqrt{3}}\}$, $\{1, \sqrt{3}\}$. Si ottiene la base:

$$\{1,\ \sqrt{3},\ \sqrt{1+\sqrt{3}},\ \sqrt{3}\sqrt{1+\sqrt{3}}\}.$$

Il polinomio minimo di $\sqrt{1+\sqrt{3}}$ su $\boldsymbol{Q}$ ha grado 4. Per ottenerlo poniamo $\alpha = \sqrt{1+\sqrt{3}}$ ed osserviamo che $\alpha^2 - 1 = \sqrt{3}$, da cui, quadrando, segue che $\alpha^4 - 2\alpha^2 - 2 = 0$. Dunque α è zero del polinomio $f = X^4 - 2X^2 - 2$ (necessariamente irriducibile su $\boldsymbol{Q}$).

Alternativamente, possiamo verificare che il polinomio minimo $g(Y) \in \boldsymbol{Q}[Y]$ di $1+\sqrt{3}$ è $g = Y^2 - 2Y - 2$. Sostituendo Y con X^2 otterremo un polinomio di grado 4 che ammette α come zero; si tratta dello stesso polinomo f già ottenuto.

(*ii*) Sia

$$\frac{1}{\sqrt{3}\sqrt{1+\sqrt{3}}} = a + b\sqrt{3} + c\sqrt{1+\sqrt{3}} + d\sqrt{3}\sqrt{1+\sqrt{3}},$$

per opportuni $a, b, c, d \in \boldsymbol{Q}$ da determinare. Si ha:

$$a\sqrt{3}\sqrt{1+\sqrt{3}} + 3b\sqrt{1+\sqrt{3}} + c\sqrt{3}(1+\sqrt{3}) + 3d(1+\sqrt{3}) - 1 = 0,$$

da cui:

$$a\sqrt{3}\sqrt{1+\sqrt{3}} + 3b\sqrt{1+\sqrt{3}} + (3d+c)\sqrt{3} + 3c + 3d - 1 = 0.$$

Ne segue: $a = 3b = 3d + c = 0$, $3c + 3d = 1$, cioè $a = b = 0$, $c = \frac{1}{2}$, $d = -\frac{1}{6}$. Pertanto

$$\frac{1}{\sqrt{3}\sqrt{1+\sqrt{3}}} = \tfrac{1}{2}\sqrt{1+\sqrt{3}} - \tfrac{1}{6}\sqrt{3}\sqrt{1+\sqrt{3}}.$$

* * *

Esercizio 4.3.4. È assegnata l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.

(*i*) Determinarne il grado.

(*ii*) Determinare tutti i possibili elementi primitivi della forma $\sqrt[3]{2} + c\sqrt[3]{3}$, al variare di $c \in \boldsymbol{Q}$.

Soluzione. (*i*) Risulta:

$$[Q\sqrt[3]{2},\ \sqrt[3]{3}) : \boldsymbol{Q}] = [Q\sqrt[3]{2},\ \sqrt[3]{3}) : \boldsymbol{Q}(\sqrt[3]{3})]\cdot[\boldsymbol{Q}(\sqrt[3]{3}) : \boldsymbol{Q}].$$

Si tratta di due estensioni semplici. La seconda ha polinomio minimo $X^3 - 3$ e quindi grado 3. Anche la prima ha grado 3, se verifichiamo che $X^3 - 2$ è irriducibile su $\boldsymbol{Q}(\sqrt[3]{3})$.

Infatti X^3-2 ha tre zeri in $\boldsymbol{C}$: $\sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3,\ \sqrt[3]{2}\,\zeta_3^{\,2}$, con $\zeta_3=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ (radice primitiva terza dell'unità). L'unico zero reale di tale polinomio è $\sqrt[3]{2}$: verifichiamo che $\notin \boldsymbol{Q}(\sqrt[3]{3})$. Altrimenti, si avrebbe $\sqrt[3]{2}=a+b\sqrt[3]{3}+c\sqrt[3]{9}$ (con $a,b,c\in\boldsymbol{Q}$). Elevando al cubo, si otterrebbe un polinomio in $\boldsymbol{Q}[X]$ di grado 2 che ammette $\sqrt[3]{3}$ come zero: assurdo.

Si conclude che $[Q\sqrt[3]{2},\ \sqrt[3]{3}):\boldsymbol{Q}]=3\cdot 3=9$.

(*ii*) Abbiamo già osservato che $\sqrt[3]{2}$ ha polinomio minimo $X^3-2\in\boldsymbol{Q}[X]$ ed ha zeri $\alpha=\alpha_1=\sqrt[3]{2},\ \alpha_2=\sqrt[3]{2}\,\zeta_3,\ \alpha_3=\sqrt[3]{2}\,\zeta_3^{\,2}$. Analogamente $\sqrt[3]{3}$ ha polinomio minimo $X^3-3\in\boldsymbol{Q}[X]$ ed ha zeri $\beta=\beta_1=\sqrt[3]{3},\ \beta_2=\sqrt[3]{3}\,\zeta_3,\ \beta_3=\sqrt[3]{3}\,\zeta_3^{\,2}$. Dal teorema dell'elemento primitivo, $c\in\boldsymbol{Q}$ deve essere distinto dai sei elementi $\frac{\alpha_i-\alpha}{\beta-\beta_j}\in\boldsymbol{C}$ (con $i=1,2,3,\ j=2,3$). Tali elementi sono:

$$\frac{\sqrt[3]{2}\,\zeta_3^{\,k}-\sqrt[3]{2}}{\sqrt[3]{3}-\sqrt[3]{3}\,\zeta_3^{\,h}}=\sqrt[3]{\tfrac{2}{3}}\,\frac{\zeta_3^{\,k}-1}{1-\zeta_3^{\,h}}\quad\text{con}\quad k=0,1,2,\ h=1,2.$$

Posto $z_{hk}=\frac{\zeta_3^{\,k}-1}{1-\zeta_3^{\,h}}$, si verifica che

$$z_{10}=z_{20}=0,\quad z_{11}=z_{22}=-1,\quad z_{21}=z_{12}=\zeta_3.$$

Pertanto $c\in\boldsymbol{Q}$ deve essere diverso da $0,\ -\sqrt[3]{\frac{2}{3}},\ \zeta_3\sqrt[3]{\frac{2}{3}}$. Quindi c può essere scelto arbitrariamente in $\boldsymbol{Q}^{\cdot}=\boldsymbol{Q}-\{0\}$.

* * *

Esercizio 4.3.5. Si denoti con $\mathbf{A}$ la chiusura algebrica $\boldsymbol{C}_{alg,\boldsymbol{Q}}$ dell'estensione $\boldsymbol{Q}\subseteq\boldsymbol{C}$. [$\mathbf{A}$ è detto *campo dei numeri algebrici*].

(*i*) Utilizzando il *TFA* (teorema fondamentale dell'algebra) verificare che ogni polinomio non costante $p\in\mathbf{A}[X]$ ammette uno zero in $\mathbf{A}$.

(*ii*) Dimostrare che $\mathbf{A}$ non ha estensioni algebriche proprie.

Soluzione. (*i*) Poiché $\mathbf{A}\subseteq\boldsymbol{C}$, allora $p\in\mathbf{A}[X]\subseteq\boldsymbol{C}[X]$. Dal *TFA* p ammette uno zero $z\in\boldsymbol{C}$. Si tratta di verificare che z è algebrico su $\boldsymbol{Q}$, cioè $z\in\mathbf{A}$.

Se $p=\sum_{i=0}^{n}a_iX^i$, basta provare che l'estensione $\boldsymbol{Q}\subseteq\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n,\,z)$ è algebrica.

Infatti, essendo $\boldsymbol{Q}\subseteq\mathbf{A}$ algebrica e $\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n)\subseteq\mathbf{A}$, allora $\boldsymbol{Q}\subseteq\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n)$ è algebrica; essendo inoltre finitamente generata, è finita. Inoltre $\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n)\subseteq\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n,\,z)$ è algebrica semplice [infatti z è zero di $p\in\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n)[X]$] e quindi è anch'essa finita. Allora $\boldsymbol{Q}\subseteq\boldsymbol{Q}(a_0,\,a_1,\,\dots,a_n,\,z)$ è finita e quindi anche algebrica, come richiesto.

(*ii*) Sia $\mathbf{A}\subseteq L$ un'estensione algebrica. Sia $\alpha\in L$ e sia m_α il suo polinomio minimo su $\mathbf{A}$. Poiché m_α è irriducibile e [in base a (*i*)] ammette uno zero in $\mathbf{A}$, allora $\partial m_\alpha=1$, cioè $\alpha\in L$. Dunque $\mathbf{A}=L$.

* * *

Esercizio 4.3.6. Siano $n,\,m$ due naturali relativamente primi. Verificare che

$$[\boldsymbol{Q}(\zeta_n,\,\zeta_m):\boldsymbol{Q}]=\varphi(nm).$$

Cosa avviene se $n,\,m$ non sono coprimi?

Soluzione. Siano $n,\,m$ coprimi. È noto che $[\boldsymbol{Q}(\zeta_{nm}):\boldsymbol{Q}]=\partial\Phi_{nm}=\varphi(nm)$. Basta quindi verificare che $\boldsymbol{Q}(\zeta_n,\,\zeta_m)=\boldsymbol{Q}(\zeta_{nm})$.

Poiché $\zeta_n=\zeta_{nm}^{\,m}$ e $\zeta_m=\zeta_{nm}^{\,n}$ allora $\zeta_n,\,\zeta_m\in\boldsymbol{Q}(\zeta_{nm})$ e dunque $\boldsymbol{Q}(\zeta_n,\,\zeta_m)\subseteq\boldsymbol{Q}(\zeta_{nm})$.

Viceversa, essendo $n,\,m$ coprimi, esistono $a,\,b\in\boldsymbol{Z}$ tali che $1=an+bm$. Allora

$$\zeta_{nm}=\zeta_{nm}^{\,1}=\zeta_{nm}^{\,an}\cdot\zeta_{nm}^{\,bm}=(\zeta_{nm}^{\,n})^a\cdot(\zeta_{nm}^{\,m})^b=\zeta_n^{\,a}\cdot\zeta_m^{\,b}\in\boldsymbol{Q}(\zeta_n,\,\zeta_m).$$

Quindi $\boldsymbol{Q}(\zeta_{nm})\subseteq\boldsymbol{Q}(\zeta_n,\,\zeta_m)$.

Rispondiamo ora all'ultima domanda, verificando che

$$\boldsymbol{Q}(\zeta_n, \zeta_m) = \boldsymbol{Q}(\zeta_h), \text{ se } h = mcm(n,m).$$

Se $h = nu = mv$, con $u, v \in \boldsymbol{Z}$, allora $\zeta_n = \zeta_{nu}^{u} = \sqrt[u]{\zeta_h}$, $\zeta_m = \zeta_{mv}^{v} = \sqrt[v]{\zeta_h}$. Dunque $\zeta_n, \zeta_m \in \boldsymbol{Q}(\zeta_h)$, cioè $\boldsymbol{Q}(\zeta_n, \zeta_m) \subseteq \boldsymbol{Q}(\zeta_h)$.

Viceversa si osserva subito, dalla definizione di minimo comune multiplo, che u, v sono coprimi. Dunque $1 = au + bv$, $\exists\, a, b \in \boldsymbol{Z}$. Pertanto

$$\zeta_h = \zeta_h^{au} \cdot \zeta_h^{bv} = (\zeta_{nu}^{u})^a \cdot (\zeta_{mv}^{v})^b = \zeta_n^a \cdot \zeta_m^b \in \boldsymbol{Q}(\zeta_n, \zeta_m).$$

Quindi $\boldsymbol{Q}(\zeta_h) \subseteq \boldsymbol{Q}(\zeta_n, \zeta_m)$.

* * *

Esercizio 4.4.1. Sia $\boldsymbol{\mathcal{P}}_0 = \{O, U\} \subset \boldsymbol{E}^2$ e sia $\boldsymbol{Q}_c$ il sottocampo di $\boldsymbol{R}$ generato dalle coordinate dei punti costruibili con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$. Verificare che $\boldsymbol{Q} \subset \boldsymbol{Q}_c$ è un'estensione algebrica infinita, con $\boldsymbol{Q}_c$ contenuto propriamente in $\boldsymbol{R}_{alg,\boldsymbol{Q}}$ (chiusura algebrica di $\boldsymbol{Q}$ in $\boldsymbol{R}$).

Soluzione. Sia $x \in \boldsymbol{Q}_c$. Allora $(x, 0)$ è costruibile con $R\&C$ a partire da $\{O, U\}$. In base al Teor. **4.1**, esistono $\alpha_1, \dots, \alpha_n \in \boldsymbol{R}$ tali che $\alpha_1^2 \in \boldsymbol{Q}$, $\alpha_2^2 \in \boldsymbol{Q}(\alpha_1)$, $\dots$, $\alpha_n^2 \in \boldsymbol{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ e $x \in \boldsymbol{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$. L'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ è finita [in quanto coincide con una catena di estensioni algebriche semplici (di gradi ≤ 2)]. Dunque è algebrica e pertanto x è algebrico su $\boldsymbol{Q}$.

Per dimostrare che $\boldsymbol{Q} \subset \boldsymbol{Q}_c$ è un'estensione infinita, basta osservare che, per ogni $k \geq 1$, $\sqrt[2^k]{2}$ è costruibile con $R\&C$ a partire da $\{O, U\}$. Dunque $\boldsymbol{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots, \sqrt[2^k]{2}, \dots) \subseteq \boldsymbol{Q}_c$. Poiché

$$\boldsymbol{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots, \sqrt[2^k]{2}) = \boldsymbol{Q}(\sqrt[2^k]{2}) \text{ e } [\boldsymbol{Q}(\sqrt[2^k]{2}) : \boldsymbol{Q}] = 2^k,$$

allora $[\boldsymbol{Q}_c : \boldsymbol{Q}] \geq 2^k$, $\forall\, k \geq 1$. Dunque $[\boldsymbol{Q}_c : \boldsymbol{Q}] = \infty$.

Infine, ad esempio $\sqrt[3]{2} \notin \boldsymbol{Q}_c$, ma $\sqrt[3]{2} \in \boldsymbol{R}_{alg,\boldsymbol{Q}}$. Quindi $\boldsymbol{Q}_c \subset \boldsymbol{R}_{alg,\boldsymbol{Q}}$.

* * *

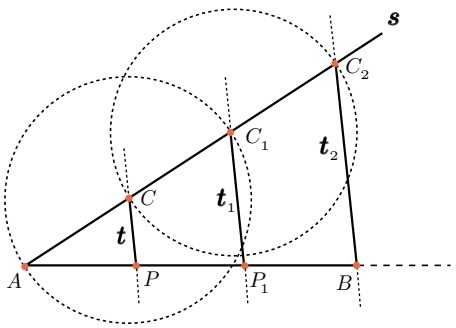
Esercizio 4.4.2. Utilizzando $R\&C$ dividere in tre parti uguali un assegnato segmento di $\boldsymbol{E}^2$.

Soluzione. Supponiamo assegnato in $\boldsymbol{E}^2$ l'insieme $\boldsymbol{\mathcal{P}}_0 = \{A, B, C\}$, con $C \notin \boldsymbol{R}(A, B)$. Vogliamo dividerere in tre parti uguali il segmento di estremi A, B.

Si tracci la retta $\boldsymbol{s} = \boldsymbol{R}(A, C)$ e si costruiscano su $\boldsymbol{s}$ i due seguenti punti

$$C_1 = \boldsymbol{s} \cap [\boldsymbol{C}(C, \overline{AC}) - \{A\}]; \quad C_2 = \boldsymbol{s} \cap [\boldsymbol{C}(C_1, \overline{AC}) - \{C\}].$$

Per costruzione, $\overline{AC} = \overline{CC_1} = \overline{C_1C_2}$.



Si costruisca ora la retta $\boldsymbol{t}_2 := \boldsymbol{R}(B, C_2)$ e, successivamente, le due rette $\boldsymbol{t}_1$, $\boldsymbol{t}$ ad essa parallele, condotte rispettivamente per i punti C_1, C. Intersecando tali rette con $\boldsymbol{R}(A, B)$, si ottengono i punti $P_1 = \boldsymbol{t}_1 \cap \boldsymbol{R}(A, B)$, $P = \boldsymbol{t} \cap \boldsymbol{R}(A, B)$. In base al teorema di Talete,

$$\frac{\overline{AC}}{\overline{AP}} = \frac{\overline{CC_1}}{\overline{PP_1}} = \frac{\overline{C_1C_2}}{\overline{P_1B}}.$$

Poiché i tre numeratori coincidono, lo stesso è vero per i tre denominatori. Quindi i due punti P, P_1 trisecano (in parti uguali) il segmento AB.

* * *

Esercizio 4.4.3. Verificare che l'angolo di 120^0 non è trisecabile con *R&C*. Dedurne che il poligono regolare 9-latero non può essere costruito con *R&C*.

Soluzione. Sia $\vartheta = \frac{2\pi}{3}$. Poiché $\cos\vartheta = -\frac{1}{2} \in \boldsymbol{Q}$, si può assumere $\boldsymbol{\mathcal{P}}_0 = \{O, U\}$ e dunque $K_0 = \boldsymbol{Q}$.

$\cos\frac{\vartheta}{3} = \cos\frac{2\pi}{9}$ è zero del polinomio

$$f = 4X^3 - 3X + \tfrac{1}{2} \in \boldsymbol{Q}[X].$$

Posto $g := 2f = 8X^3 - 6X + 1 \in \boldsymbol{Z}[X]$, si può facilmente verificare che g non ha zeri in $\boldsymbol{Q}$ [se infatti $\frac{r}{s} \in \boldsymbol{Q}$ è uno zero di g, con $MCD(r,s) = 1$, deve risultare $r \,|\, 1$, $s \,|\, 8$. Dunque $r = \pm 1$, $s = \pm 1, \pm 2, \pm 4, \pm 8$ e pertanto $\frac{r}{s} \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}\}$. Ma si verifica, con un po' di calcoli, che nessuno di tali otto elementi è uno zero di g].

Poiché g è irriducibile su $\boldsymbol{Z}$, f lo è su $\boldsymbol{Q}$ e quindi $(\cos\frac{2\pi}{9}, 0)$ non è costruibile con *R&C*.

Il punto $(\cos\frac{2\pi}{9}, \sin\frac{2\pi}{9})$ (vertice del poligono regolare unitario $\boldsymbol{\mathcal{P}}_9$) non è quindi costruibile con *R&C*, cioè $\boldsymbol{\mathcal{P}}_9$ non è costruibile con *R&C* (come ben noto).

* * *

Esercizio 4.4.4. Verificare se l'angolo di 45^0 è trisecabile con *R&C*.

Soluzione. Si ponga $\boldsymbol{\mathcal{P}}_0 = \{O, U, (\cos\frac{\pi}{4}, 0)\}$. Poiché $\cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$, allora $K_0 = \boldsymbol{Q}(\sqrt{2})$.

Risulta: $\cos\frac{\pi}{12}$ è zero del polinomio $4X^3 - 3X - \frac{1}{\sqrt{2}} \in \boldsymbol{Q}(\sqrt{2})[X]$. Verifichiamo se tale polinomio è irriducibile su $\boldsymbol{Q}(\sqrt{2})$. Sia $f = 8X^3 - 6X - \sqrt{2} \in \boldsymbol{Q}(\sqrt{2})[X]$. Risulta:

$$f \text{ è riducibile su } \boldsymbol{Q}(\sqrt{2}) \iff \exists\, a + b\sqrt{2} \in \boldsymbol{Q}(\sqrt{2}) \text{ tale che } f(a + b\sqrt{2}) = 0.$$

Si ha:

$$f(a + b\sqrt{2}) = 0 \iff -6a + 8a^3 + 48ab^2 + \sqrt{2}(-1 - 6b + 24a^2b + 16b^3) = 0$$
$$\iff \begin{cases} -6a + 8a^3 + 48ab^2 = 0 \\ -1 - 6b + 24a^2b + 16b^3 = 0. \end{cases}$$

Tale sistema ammette soluzione $a = 0$, $b = -\frac{1}{2}$. Dunque $f(-\frac{1}{\sqrt{2}}) = 0$. Allora f è riducibile su $\boldsymbol{Q}(\sqrt{2})$ e si fattorizza nella forma:

$$f = 2(X + \tfrac{1}{\sqrt{2}})(4X^2 - 2\sqrt{2}\,X - 1).$$

Pertanto l'angolo di 45^0 è trisecabile con *R&C*.

Nota. La precedente fattorizzazione fornisce una semplice espressione radicale per $\cos\frac{\pi}{12}$. Infatti $\cos\frac{\pi}{12}$ è uno zero di $4X^2 - 2\sqrt{2}\,X - 1$. Tale polinomio ha zeri $\frac{\sqrt{2}\pm\sqrt{6}}{4}$. Poiché $\cos\frac{\pi}{12} > 0$, allora $\cos\frac{\pi}{12} = \frac{\sqrt{2}+\sqrt{6}}{4} = \frac{1+\sqrt{3}}{2\sqrt{2}}$.

* * *

Esercizio 4.4.5. Verificare che l'angolo retto è *pentasecabile* con *R&C* e determinare un'espressione algebrica per il coseno dell'angolo di 18^0.

Suggerimento. Utilizzare l'identità trigonometrica $\cos 5\vartheta = 16\cos^5\vartheta - 20\cos^3\vartheta + 5\cos\vartheta$.

Soluzione. Il problema della "pentasecabilità" di un angolo di ampiezza ϑ (radianti) si traduce nella costruibilità con *R&C* del punto $(\cos\frac{\vartheta}{5}, 0)$.

Dall'identità trigonometrica suggerita segue che

$$\cos\vartheta = 16\cos^5\tfrac{\vartheta}{5} - 20\cos^3\tfrac{\vartheta}{5} + 5\cos\tfrac{\vartheta}{5}.$$

Dunque $\cos\frac{\vartheta}{5}$ è uno zero del polinomio

$$f = 16X^5 - 20X^3 + 5X - \cos\vartheta \in \boldsymbol{Q}(\cos\vartheta)[X].$$

Nel caso in esame, $\cos\vartheta = \cos\frac{\pi}{2} = 0$ e dunque $f = X(16X^4 - 20X^2 + 5)$.

Il polinomio biquadratico $g = 16X^4 - 20X^2 + 5 \in \boldsymbol{Q}[X]$ ha quattro zeri reali $\pm\sqrt{\frac{5\pm\sqrt{5}}{8}}$ e si fattorizza in $\boldsymbol{R}[X]$ nella forma

$$g = 16(X^2 - \tfrac{5}{8} + \tfrac{\sqrt{5}}{8})(X^2 - \tfrac{5}{8} - \tfrac{\sqrt{5}}{8}).$$

I due fattori quadratici non appartengono a $\boldsymbol{Q}[X]$ e dunque g è irriducibile su $\boldsymbol{Q}$.

Dei quattro zeri di g, $\cos\frac{\pi}{10}$ coincide con $\sqrt{\frac{5+\sqrt{5}}{8}}$ [in quanto $\cos\frac{\pi}{10} > 0$ e prossimo ad 1]. Posto $\alpha = \sqrt{\frac{5+\sqrt{5}}{8}}$, risulta subito che $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 4$. Inoltre esiste la catena di estensioni

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha^2) \subset \boldsymbol{Q}(\alpha),$$

entrambe di grado 2 [α^2 ha polinomio minimo $X^2 - \frac{5}{4}X + \frac{5}{16}$ su $\boldsymbol{Q}$, mentre α ha polinomio minimo $X^2 - \alpha^2$ su $\boldsymbol{Q}(\alpha^2)$]. Dalla Prop. **4.3** segue che $\alpha = \cos\frac{\pi}{10}$ è costruibile con *R&C*.

* * *

Esercizio 4.4.6. Spiegare, senza eseguire costruzioni grafiche, perché, assegnato un angolo di ampiezza ϑ (radianti), è possibile con *R&C* costruire un angolo di ampiezza $n\vartheta$, $\forall\, n \geq 1$.

Soluzione. Supponiamo assegnato l'insieme $\boldsymbol{\mathcal{P}}_0 = \{O, U, (\cos\vartheta, 0)\} \subset \boldsymbol{E}^2$ e consideriamo in $\boldsymbol{R}$ il corrispondente sottocampo $K_0 = \boldsymbol{Q}(\cos\vartheta)$.

Si ha: $\sin^2\vartheta = 1 - \cos^2\vartheta \in K_0$ e dunque $\sin\vartheta$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$. Utilizzando ripetutamente le formule di addizione del seno e del coseno, si può esprimere $\cos(n\vartheta)$ nella forma $f_n(\cos\vartheta, \sin\vartheta)$, con $f_n \in \boldsymbol{Q}[X, Y]$. Ne segue che $\cos(n\vartheta)$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0 \cup \{(\sin\vartheta, 0)\}$ e quindi a partire da $\boldsymbol{\mathcal{P}}_0$.

* * *

Esercizio 4.4.7. Determinare tutti i naturali n, con $3 \leq n \leq 100$, per cui il poligono regolare $\boldsymbol{\mathcal{P}}_n$ è costruibile con *R&C*.

Soluzione. In base al teorema di Gauss, è sufficiente determinare i naturali n, con $3 \leq n \leq 100$, della forma:

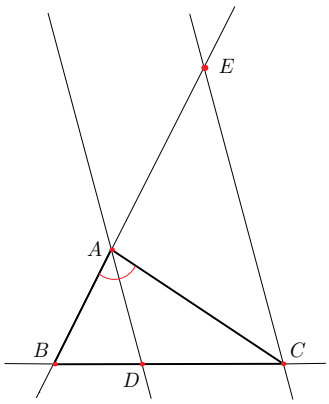
$n = 2^r p_1 \dots p_s$, con $r, s \geq 0$ e $p_1, \dots, p_s$ primi distinti di Fermat (cioè tali che $p_i = 2^{2^{k_i}} + 1$).

I primi di Fermat ≤ 100 sono: $p_1 = 3$, $p_2 = 5$, $p_3 = 17$ ed i loro prodotti ≤ 100 sono: $p_1p_2 = 15$, $p_1p_3 = 51$, $p_2p_3 = 85$. Le potenze di 2 inferiori a 100 sono: 1, 2, 4, 8, 16, 32, 64. Moltiplicando tra loro tali numeri e sopprimendo quelli > 100, si ottengono i 24 naturali di questa tavola moltiplicativa

·	1	2	4	8	16	32	64
1	/	/	4	8	16	32	64
3	3	6	12	24	48	96	/
5	5	10	20	40	80	/	
17	17	34	68	/			
15	15	30	60	/			
51	51	/					
85	85	/					

* * *

Esercizio 4.4.8. Dimostrare il teorema delle bisettrici, utilizzando il teorema di Talete (come suggerito dalla figura che segue)



Soluzione. Assegnato il triangolo ABC, sia AD la bisettrice del vertice A [dunque $D \in BC$]. Dal vertice C si traccia la parallela ad AD, sino ad incontrare in E la retta $\boldsymbol{R}(A,B)$. Le due rette $\boldsymbol{R}(A,D)$, $\boldsymbol{R}(E,C)$ sono parallele [intersecate dalle rette $\boldsymbol{R}(B,E)$, $\boldsymbol{R}(B,C)$]. Si applica ad esse il teorema di Talete:

$$(*) \qquad \frac{\overline{BD}}{\overline{DC}} = \frac{\overline{BA}}{\overline{AE}}.$$

Il triangolo AEC è isoscele [infatti $D\hat{A}C = A\hat{C}E$ (sono alterni interni) e $B\hat{A}D = A\hat{E}C$ (sono corrispondenti); inoltre $D\hat{A}C = B\hat{A}D$. Dunque $A\hat{C}E = A\hat{E}C$]. Allora $\overline{AC} = \overline{AE}$. Da $(*)$ segue che

$$\frac{\overline{BD}}{\overline{DC}} = \frac{\overline{AB}}{\overline{AC}} \quad (\textit{Teorema delle bisettrici}).$$

* * *

SOLUZIONI DEGLI ESERCIZI

DEL CAPITOLO 5

Esercizio 5.2.1. Verificare che il campo di spezzamento E di $f = X^4+1 \in \boldsymbol{Q}[X]$ è $E = \boldsymbol{Q}(i, \sqrt{2})$.

Soluzione. f è il polinomio ciclotomico Φ_8. Infatti

$$\Phi_8 = \tfrac{X^8-1}{\Phi_1\Phi_2\Phi_4} = \tfrac{X^8-1}{(X-1)(X+1)(X^2+1)} = \tfrac{X^8-1}{X^4-1} = X^4+1 = f.$$

Allora $f = (X-\zeta_8)(X-\zeta_8^3)(X-\zeta_8^5)(X-\zeta_8^7)$ e quindi $E = \boldsymbol{Q}(\zeta_8)$. Inoltre $[\boldsymbol{Q}(\zeta_8):\boldsymbol{Q}] = \partial\Phi_8 = 4$. Risulta:

$$\zeta_8 = \cos\tfrac{2\pi}{8} + i\sin\tfrac{2\pi}{8} = \tfrac{1}{\sqrt{2}}(1+i).$$

Dunque $\boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}(\frac{1+i}{\sqrt{2}})$.

Si osservi che $i = \zeta_8^2$, $\sqrt{2} = \zeta_8 - \zeta_8^3$ (come subito si verifica). Dunque $i, \sqrt{2} \in \boldsymbol{Q}(\zeta_8)$ e pertanto $\boldsymbol{Q}(i, \sqrt{2}) \subseteq \boldsymbol{Q}(\zeta_8)$. Poiché $[\boldsymbol{Q}(i, \sqrt{2}) : \boldsymbol{Q}] = 4$, allora $\boldsymbol{Q}(\zeta_8) = \boldsymbol{Q}(i, \sqrt{2})$, cioè $E = \boldsymbol{Q}(i, \sqrt{2})$.

* * *

Esercizio 5.2.2. Determinare il campo di spezzamento E di $f = X^6 - 8 \in \boldsymbol{Q}[X]$. Calcolare il grado $[E : \boldsymbol{Q}]$.

Soluzione. Poiché ovviamente $\sqrt{2}$ è uno zero di f, i sei zeri di f sono: $\sqrt{2}\,\zeta_6^k$, $\forall\, k = 0, \dots, 5$. Allora:

$$E = \boldsymbol{Q}(\sqrt{2}, \sqrt{2}\,\zeta_6, \dots, \sqrt{2}\,\zeta_6^5) = \boldsymbol{Q}(\sqrt{2}, \zeta_6).$$

Si ha: $\zeta_6 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ e dunque $\boldsymbol{Q}(\zeta_6) = \boldsymbol{Q}(i\sqrt{3})$. Allora $E = \boldsymbol{Q}(\sqrt{2}, i\sqrt{3})$. Si ha:

$$[E : \boldsymbol{Q}] = [E : \boldsymbol{Q}(i\sqrt{3})]\cdot[\boldsymbol{Q}(i\sqrt{3}) : \boldsymbol{Q}] = 2\cdot 2 = 4.$$

* * *

Esercizio 5.2.3. Determinare il campo di spezzamento del polinomio $f = X^3+X^2+X+\overline{2} \in \boldsymbol{Z}_3[X]$ e fattorizzare f in tale campo.

Soluzione. f è irriducibile su $\boldsymbol{Z}_3$, in quanto $f(\overline{0}), f(\overline{1}), f(\overline{2}) \neq \overline{0}$. Si ponga

$$\boldsymbol{Z}_3(x) := \boldsymbol{Z}_3[X]/_{(f)} = \{a + bx + cx^2,\ \forall\, a, b, c \in \boldsymbol{Z}_3;\ x^3 = \overline{2}x^2 + \overline{2}x + \overline{1}\}.$$

Si tratta di un campo con 27 elementi, estensione algebrica semplice di grado 3 su $\boldsymbol{Z}_3$. In $\boldsymbol{Z}_3(x)$ f si fattorizza nella forma

$$f = (X-x)g, \text{ con } g := X^2 + (\overline{1}+x)X + (\overline{1}+x+x^2).$$

Per determinare gli zeri di g [eventualmente in un'estensione di $\boldsymbol{Z}_3(x)$], utilizziamo la ben nota formula risolutiva per radicali dei polinomi di grado 2 [sempre valida in caratteristica $\neq 2$]. Si ottengono gli zeri

$$\tfrac{1}{2}[-(\overline{1}+x) \pm \sqrt{(\overline{1}+x)^2 - \overline{4}(\overline{1}+x+x^2)}] = \overline{2}(-\overline{1} - x \pm \sqrt{x}) = \overline{1} + x \pm \overline{2}\sqrt{x}.$$

Per decidere se tali zeri sono in $\boldsymbol{Z}_3(x)$, basta verificare se $\sqrt{x} \in \boldsymbol{Z}_3(x)$, ovvero se il polinomio $X^2 - x$ ammette zeri in $\boldsymbol{Z}_3(x)$.

Si può verificare che ad esempio, posto $y = x + \overline{2}x^2$, si ha $y^2 = x$ [per ottenere un tale elemento y si risolva l'equazione $(a + bx + cx^2)^2 = x$, nelle incognite a, b, c a valori in $\boldsymbol{Z}_3$]. Ne segue che g si spezza su $\boldsymbol{Z}_3(x)$ e quindi che lo stesso è vero per f. I due zeri di g sono quindi:

$$\overline{1} + x \pm \overline{2}(x + \overline{2}x^2), \text{ cioè } x^2 + \overline{1},\ \overline{2}x^2 + \overline{2}x + \overline{1}.$$

Si conclude che $\Sigma_{f,\boldsymbol{Z}_3} = \boldsymbol{Z}_3(x)$ e la fattorizzazione di f su tale campo è la seguente:

$$f = (X - x)(X - (x^2 + \overline{1}))(X - (\overline{2}x^2 + \overline{2}x + \overline{1})).$$

* * *

Esercizio 5.2.4. Determinare il campo di spezzamento E di $f = X^3 + \overline{5} \in \boldsymbol{Z}_7[X]$. Fattorizzare f in $E[X]$ e calcolare $[E : \boldsymbol{Z}_7]$.

Soluzione. Risulta: $f(k) \neq \overline{0},\ \forall\, k \in \boldsymbol{Z}_7$. Dunque $f = X^3 + \overline{5}$ è irriducibile in $\boldsymbol{Z}_7[X]$. Si ponga:

$$\boldsymbol{Z}_7[X]/_{(f)} = \boldsymbol{Z}_7[x \,|\, x^3 + \overline{5} = \overline{0}\,] = \boldsymbol{Z}_7[x \,|\, x^3 = \overline{2}\,] = \{a + bx + cx^2,\ \forall\, a, b, c \in \boldsymbol{Z}_7;\ x^3 = \overline{2}\}$$

e si denoti tale campo con $\boldsymbol{Z}_7(x)$. Fattorizziamo f in $\boldsymbol{Z}_7(x)[X]$. Eseguendo la divisione con resto di f per $X - x$, si ottiene:

$$f = (X - x)(X^2 + xX + x^2).$$

Posto $g = X^2 + xX + x^2 \in \boldsymbol{Z}_7(x)[X]$, vogliamo verificare se g è irriducibile su $\boldsymbol{Z}_7(x)$. Gli zeri di g (in un'estensione di $\boldsymbol{Z}_7(x)$) sono

$$\tfrac{-x \pm \sqrt{x^2 - \overline{4}x^2}}{\overline{2}} = \tfrac{-x \pm \sqrt{\overline{4}x^2}}{\overline{2}}.$$

Tali zeri appartengono a $\boldsymbol{Z}_7(x) \iff \sqrt{\overline{4}x^2} \in \boldsymbol{Z}_7(x) \iff \exists\, y \in \boldsymbol{Z}_7(x)$ tale che $y^2 = \overline{4}\,x^2$. Basta porre $y = \overline{2}\,x$ e si conclude che g è riducibile su $\boldsymbol{Z}_7(x)$ ed ha zeri

$$\tfrac{-x \pm \overline{2}\,x}{\overline{2}} = \overline{4}\,(-x \pm \overline{2}\,x) = \begin{cases} \overline{4}\,x \\ \overline{2}\,x. \end{cases}$$

Pertanto $g = (X - \overline{2}\,x)(X - \overline{4}\,x)$ e quindi $f = (X - x)(X - \overline{2}\,x)(X - \overline{4}\,x)$ in $\boldsymbol{Z}_7(x)[X]$. Si conclude che $E = \boldsymbol{Z}_7(x)$ e $[E : \boldsymbol{Z}_7] = \partial f = 3$.

* * *

Esercizio 5.2.5. Sia $f = X\,T^5 - X^2T^3 - \frac{1}{X^2}T^2 + \frac{1}{X} \in \boldsymbol{Z}_3(X)[T]$. Fattorizzare f e determinare il campo di spezzamento $\Sigma_{f, \boldsymbol{Z}_3(X)}$.

Soluzione. Risulta:

$$f = X\,T^5 - \tfrac{1}{X^2}T^2 - (X^2T^3 - \tfrac{1}{X}) = T^2(X\,T^3 - \tfrac{1}{X^2}) - X(X\,T^3 - \tfrac{1}{X^2}) = (T^2 - X)(X\,T^3 - \tfrac{1}{X^2}) =$$
$$= X(T^2 - X)(T^3 - \tfrac{1}{X^3}) = X(T^2 - X)(T - \tfrac{1}{X})^3$$

[l'ultima uguaglianza segue dal fatto che $car(\boldsymbol{Z}_3(X)) = 3$].

Dunque f ha lo zero triplo $\frac{1}{X}$ in $\boldsymbol{Z}_3(X)$ ed ha i due zeri $\pm\sqrt{X}$ di $T^2 - X$ nell'estensione algebrica semplice $\boldsymbol{Z}_3(X)[T]/_{(T^2 - X)} \cong \boldsymbol{Z}_3(X)(\sqrt{X})$. Il campo di spezzamento cercato è quindi

$$\Sigma_{f, \boldsymbol{Z}_3(X)} = \boldsymbol{Z}_3(X)(\sqrt{X}).$$

Un generico elemento di tale campo è del tipo $\frac{F(\sqrt{X})}{G(\sqrt{X})}$, con $F, G \in \boldsymbol{Z}_3(X)[T]$. Se ad esempio $F = \sum \frac{f_i(X)}{g_i(X)}T^i$, allora $F(\sqrt{X}) = \sum \frac{f_i(\sqrt{X}^2)}{g_i(\sqrt{X}^2)}\sqrt{X}^i = \frac{f_1(\sqrt{X})}{f_2(\sqrt{X})}$, con $f_1, f_2 \in \boldsymbol{Z}_3[T]$. Ne segue che $\frac{F(\sqrt{X})}{G(\sqrt{X})} = \frac{f(\sqrt{X})}{g(\sqrt{X})}$, per opportuni $f, g \in \boldsymbol{Z}_3[T]$, e pertanto $\Sigma_{f, \boldsymbol{Z}_3(X)} = \boldsymbol{Z}_3(\sqrt{X})$.

* * *

Esercizio 5.2.6. Determinare il campo di spezzamento del polinomio $f = X^8 + X^2 + \overline{1} \in \boldsymbol{Z}_2[X]$.

Soluzione. Si osserva subito che $f = X^8 + X^2 + \overline{1} = (X^4 + X + \overline{1})^2$. Poniamo $g = X^4 + X + \overline{1} \in \boldsymbol{Z}_2[X]$ e verifichiamo se g è irriducibile su $\boldsymbol{Z}_2$.

Poiché $g(\overline{0}), g(\overline{1}) \neq \overline{0}$, se g fosse riducibile, risulterebbe

$$g = (X^2 + aX + \overline{1})(X^2 + bX + \overline{1}),\ \text{con}\ a, b \in \boldsymbol{Z}_2.$$

Risolvendo il corrispondente sistema (nelle incognite a, b a valori in $\boldsymbol{Z}_2$), si ottiene $a+b=\overline{0}$ e $a+b=\overline{1}$, da cui un assurdo. Ne segue che g è irriducibile su $\boldsymbol{Z}_2$.

Il campo $\boldsymbol{Z}_2(\alpha)=\boldsymbol{Z}_2[X]\big/_{(g)}$ ha 16 elementi, e precisamente

$$\begin{array}{cccccccc}\overline{0} & \alpha & \alpha+\alpha^2 & \alpha+\alpha^3 & \alpha+\alpha^2+\alpha^3 & \alpha^2 & \alpha^2+\alpha^3 & \alpha^3\\ \overline{1} & \overline{1}+\alpha & \overline{1}+\alpha+\alpha^2 & \overline{1}+\alpha+\alpha^3 & \overline{1}+\alpha+\alpha^2+\alpha^3 & \overline{1}+\alpha^2 & \overline{1}+\alpha^2+\alpha^3 & \overline{1}+\alpha^3.\end{array}$$

In $\boldsymbol{Z}_2(\alpha)[X]$, g si fattorizza nella forma:

$$g=(X+\alpha)h,\ \text{ con }\ h=X^3+\alpha X^2+\alpha^2X+\alpha^3+\overline{1}.$$

Si tratta ora di determinare eventuali zeri di h in $\boldsymbol{Z}_2(\alpha)$. Basta calcolare h sugli elementi di $\boldsymbol{Z}_2(\alpha)$. Si verifica ad esempio che $h(\overline{1}+\alpha)=\overline{0}$. Ne segue che $(X+\overline{1}+\alpha)\,\big|\,h$. Eseguendo la divisione, si ottiene

$$h=(X+\overline{1}+\alpha)\ell,\ \text{ con }\ \ell=X^2+X+(\overline{1}+\alpha+\alpha^2)\in\boldsymbol{Z}_2(\alpha)[X].$$

Infine si verifica che $\ell(\alpha^2)=0$. Dunque $(X+\alpha^2)\,\big|\,\ell$ e si ha

$$\ell=(X+\alpha^2)(X+\overline{1}+\alpha^2).$$

Riassumendo,

$$g=(X+\alpha)(X+\overline{1}+\alpha)(X+\alpha^2)(X+\overline{1}+\alpha^2).$$

Pertanto f ha quattro zeri doppi: $\alpha,\ \overline{1}+\alpha,\ \alpha^2,\ \overline{1}+\alpha^2$. il campo di spezzamento di f su $\boldsymbol{Z}_2$ è

$$\Sigma_{f,\boldsymbol{Z}_2}=\boldsymbol{Z}_2(\alpha)$$

ed ha grado 4 su $\boldsymbol{Z}_2$.

* * *

Esercizio 5.2.7. Determinare la chiusura normale N dell'estensione $\boldsymbol{Q}\subset\boldsymbol{Q}(\sqrt{3},\sqrt[3]{2})$ e calcolare il grado di $\boldsymbol{Q}\subset N$.

Soluzione. $\sqrt[3]{2}$ ha polinomio minimo $f=X^3-2$ su $\boldsymbol{Q}$, mentre $\sqrt{3}$ ha polinomio minimo $g=X^2-3$ su $\boldsymbol{Q}$. Gli zeri del polinomio fg sono $\pm\sqrt{3},\ \sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3,\ \sqrt[3]{2}\,\zeta_3^2$, con $\zeta_3=\frac{-1+i\sqrt{3}}{2}$ (radice primitiva terza dell'unità). Allora

$$N=\Sigma_{fg,\boldsymbol{Q}}=\boldsymbol{Q}(\pm\sqrt{3},\ \sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3,\ \sqrt[3]{2}\,\zeta_3^2)=\boldsymbol{Q}(\sqrt{3},\ \sqrt[3]{2},\ \zeta_3)=\boldsymbol{Q}(\sqrt{3},\ \sqrt[3]{2},\ i).$$

Ovviamente $[N:\boldsymbol{Q}(\sqrt{3},\sqrt[3]{2})]=2$ e $[\boldsymbol{Q}(\sqrt[3]{2}):\boldsymbol{Q}]=3$. Resta da calcolare $[\boldsymbol{Q}(\sqrt{3},\sqrt[3]{2}):\boldsymbol{Q}(\sqrt[3]{2})]$.

Ovviamente $\sqrt{3}$ è zero di $g\in\boldsymbol{Q}(\sqrt[3]{2})[X]$. Se verifichiamo che tale polinomio è irriducibile, allora il grado cercato è 2. Se per assurdo g fosse riducibile, $\sqrt{3}\in\boldsymbol{Q}(\sqrt[3]{2})$, cioè

$$\sqrt{3}=a+b\sqrt[3]{2}+c\sqrt[3]{4},\ \exists\, a,b,c\in\boldsymbol{Q}.$$

Quadrando, $3=a^2+4bc+(2c^2+2ab)\sqrt[3]{2}+(b^2+2ac)\sqrt[3]{4}$ e quindi, tenuto conto del fatto che $1,\ \sqrt[3]{2},\ \sqrt[3]{4}$ sono $\boldsymbol{Q}$-linearmente indipendenti,

$$3-a^2-4bc=0,\ 2c^2+2ab=0,\ b^2+2ac=0.$$

Dalle ultime due equazioni (moltiplicate risp. per c, b) segue $b^3=2c^3$ e quindi $\frac{b^3}{c^3}=2$ [assurdo] oppure $b=c=0$; in quest'ultimo caso, dalla prima equazione, $a^2=3$ [assurdo].

Riassumendo, $[N:\boldsymbol{Q}]=3\cdot2\cdot2=12$.

* * *

Esercizio 5.2.8. Determinare (se esiste) la chiusura normale dell'estensione $\boldsymbol{Q}\subset\boldsymbol{R}$.

Soluzione. L'estensione $\boldsymbol{Q}\subset\boldsymbol{C}$ è certamente normale (in base al Teorema Fondamentale dell'Algebra). Per dimostrare che $\boldsymbol{C}$ è la chiusura normale dell'estensione $\boldsymbol{Q}\subset\boldsymbol{R}$, occorre verificare la condizione (*ii*) della Def. **2.4**:

per ogni campo N', tale che $\boldsymbol{R}\subseteq N'\subseteq\boldsymbol{C}$ e $\boldsymbol{Q}\subset N'$ è normale, risulta: $N'=\boldsymbol{C}$.

Si consideri infatti il polinomio $f=X^3-2\in\boldsymbol{Q}[X]$. f ha in N' lo zero $\sqrt[3]{2}$ [infatti $\sqrt[3]{2}\in\boldsymbol{R}\subseteq N'$]. Dunque ogni zero di f è in N'. Pertanto $\sqrt[3]{2}\,\zeta_3\in N'$ e quindi anche $\zeta_3\in N'$. Allora $\boldsymbol{R}\neq N'$ e quindi $N'=\boldsymbol{C}$ [essendo $[\boldsymbol{C}:\boldsymbol{R}]=2$].

* * *

Esercizio 5.2.9. Dire perché l'estensione $\boldsymbol{Q}(X) \subset \boldsymbol{Q}(\sqrt[3]{X})$ è non normale e determinarne la chiusura normale.

Soluzione. Si consideri il polinomio $f = T^3 - X \in \boldsymbol{Q}(X)[T]$. Tale polinomio è irriducibile. Infatti i suoi tre zeri sono $\sqrt[3]{X}, \sqrt[3]{X}\,\zeta_3, \sqrt[3]{X}\,\zeta_3^2$, con ζ_3 radice primitiva terza dell'unità.

L'estensione $\boldsymbol{Q}(X) \subset \boldsymbol{Q}(\sqrt[3]{X})$ è non normale perché $\sqrt[3]{X} \in \boldsymbol{Q}(\sqrt[3]{X})$, mentre $\sqrt[3]{X}\,\zeta_3 \notin \boldsymbol{Q}(\sqrt[3]{X})$ [in quanto $\zeta_3 \in \boldsymbol{C} - \boldsymbol{R}$].

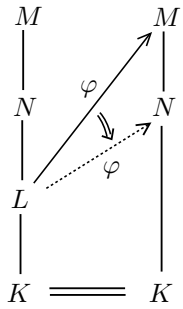
La chiusura normale N dell'estensione $\boldsymbol{Q}(X) \subset \boldsymbol{Q}(\sqrt[3]{X})$ coincide con il campo di spezzamento $\Sigma_{f,\boldsymbol{Q}(X)}$. Si ottiene subito

$$N = \Sigma_{f,\boldsymbol{Q}(X)} = \boldsymbol{Q}(\sqrt[3]{X},\ \zeta_3) = \boldsymbol{Q}(i\sqrt{3})(\sqrt[3]{X}).$$

* * *

Esercizio 5.2.10. Sia $K \subseteq L$ un'estensione finita e sia N la sua chiusura normale. Sia M un'estensione di N e sia $\varphi : L \to M$ un K-omomorfismo. Verificare che $Im\,\varphi \subseteq N$.

Soluzione. Sia $\alpha \in L$ e sia $m \in K[X]$ il suo polinomio minimo. Si ha: $m(\varphi(\alpha)) = \varphi(m(\alpha)) = \varphi(0) = 0$. Dunque $\varphi(\alpha)$ è uno zero di m. Ovviamente m ha uno zero in N (si tratta di α) e $K \subseteq N$ è normale; Allora m ha tutti gli zeri in N. In particolare $\varphi(\alpha) \in N$. Quindi $Im\,\varphi \subseteq N$.



* * *

Esercizio 5.3.1. Sia $K \subseteq L$ un'estensione algebrica e separabile e sia M un campo intermedio (tra K ed L). Verificare che le estensioni $K \subseteq M$ e $M \subseteq L$ sono separabili.

Soluzione. Verifichiamo che $K \subseteq M$ è separabile. Ogni $\alpha \in M$ è anche elemento di L. Il suo polinomio minimo su K è separabile. Dunque α è separabile su K.

Verifichiamo che $M \subseteq L$ è separabile. Sia $\alpha \in L$ e siano m_K, m_M rispettivamente i polinomi minimi di α su K e su M. Si tratta di verificare che m_M ha tutti zeri semplici. Ovviamente $m_M \,|\, m_K$ (in $M[X]$). Ne segue che gli zeri di m_M sono anche zeri di m_K. Ma m_K ha tutti zeri semplici. Quindi anche m_M ha tutti zeri semplici.

* * *

Esercizio 5.3.2. Sia n un naturale positivo e sia d un suo divisore positivo. Per ogni primo p, verificare che ogni campo di cardinalità p^n contiene un unico campo di cardinalità p^d.

Soluzione. Siano K, L campi finiti di caratteristica p, aventi rispettivamente cardinalità $|K| = p^d$, $|L| = p^n$. Dal Teor. **3.3** è noto che $K \cong \Sigma_{f,\boldsymbol{Z}_p}$ ed $L \cong \Sigma_{g,\boldsymbol{Z}_p}$, con $f = X^{p^d} - X$, $g = X^{p^n} - X \in \boldsymbol{Z}_p[X]$.

Per provare l'inclusione (a meno di isomorfismi) di K in L, basta verificare che ogni zero x di f (e quindi $x \in K$) è anche zero di g, cioè che: $f(x) = \overline{0} \implies g(x) = \overline{0}$. Poiché $d \,|\, n$, allora

$$x^{p^n} = (x^{p^d})^{p^d \cdot \ldots \cdot p^d} = (x)^{p^d \cdot \ldots \cdot p^d} = (x^{p^d})^{p^d \cdot \ldots \cdot p^d} = \ldots = x^{p^d} = x,$$

cioè $g(x) = \overline{0}$, come richiesto.

Se poi K' è un altro sottocampo di L di cardinalità p^d, i suoi p^d elementi, verificando l'equazione $X^{p^d} = X$, devono coincidere con quelli di K. Da ciò segue l'unicità di K (come sottocampo di L).

* * *

Esercizio 5.3.3. Verificare se un campo L di cardinalità 8 può ammettere un sottocampo K di cardinalità 4.

Soluzione. Due dimostrazioni.

(*1*) Per assurdo, esistano due campi K, L tali che $K \subset L$ e $|K| = 4$, $|L| = 8$. K ed L ammettono come sottocampo $\boldsymbol{Z}_2$. Inoltre sono estensioni algebriche semplici di $\boldsymbol{Z}_2$, di gradi rispettivamente 2, 3. Infatti, dall'unicità a meno di isomorfismi di tali campi, si può assumere

$$K =: \boldsymbol{Z}_2(\alpha) = \boldsymbol{Z}_2[X]\big/_{(X^2+X+\overline{1})}; \quad L =: \boldsymbol{Z}_2(\beta) = \boldsymbol{Z}_2[X]\big/_{(X^3+X+\overline{1})}.$$

Ne segue: $3 = [L : \boldsymbol{Z}_2] = [L : K]\cdot[K : \boldsymbol{Z}_2] = [L : K]\cdot 2$, cioè $2 \,|\, 3$: assurdo.

(*2*) Assumiamo $K = \boldsymbol{Z}_2(\alpha)$ ed $L = \boldsymbol{Z}_2(\beta)$, come sopra. Per assurdo, esista uno $\boldsymbol{Z}_2$-omomorfismo $\psi : K \to L$ [per cui $\psi(K)$ è un sottocampo di L]. Osserviamo che il polinomio $f = X^2 + X + \overline{1}$ ammette in K lo zero α. Allora $\psi(\alpha)$ è uno zero di f in $L[X]$ [infatti $f(\psi(\alpha)) = \psi'(f(\alpha)) = \psi'(\overline{0}) = \overline{0}$, con $\psi' : K[X] \to L[X]$ $\boldsymbol{Z}_2$-omomorfismo indotto da ψ]. Ne segue che $\psi(\alpha)^2 + \psi(\alpha) + \overline{1} = \overline{0}$, cioè, posto $\psi(\alpha) = a + b\beta + c\beta^2$, con $a, b, c \in \boldsymbol{Z}_2$:

$$\overline{0} = (a + b\beta + c\beta^2)^2 + (a + b\beta + c\beta^2) + \overline{1} = (a^2 + a + \overline{1}) + \beta(b + c^2) + \beta^2(b^2 + c^2 + c),$$

da cui: $a^2 + a + \overline{1} = b + c^2 = b^2 + c^2 + c = \overline{0}$. In particolare, $a^2 + a + \overline{1} = \overline{0}$, cioè $f(a) = \overline{0}$: assurdo [essendo f irriducibile su $\boldsymbol{Z}_2$].

* * *

Esercizio 5.4.1. Dimostrare il Lemma **4.1** nei casi $n = 3$ e $n = 4$.

Soluzione. Sia $n = 3$. In tal caso $\boldsymbol{A}_3 = \langle (1\,2\,3) \rangle \cong \boldsymbol{C}_3$. $\boldsymbol{A}_3$ non ha sottogruppi propri e dunque l'asserto è ovviamente verificato.

Sia $n = 4$. $\boldsymbol{A}_4$ possiede otto 3-cicli:

$$(1\,2\,3),\ (1\,2\,4),\ (1\,3\,4),\ (2\,3\,4),$$
$$(1\,3\,2),\ (1\,4\,2),\ (1\,4\,3),\ (2\,4\,3).$$

Sia $H \trianglelefteq \boldsymbol{A}_4$ e, ad esempio, $(1\,2\,3) \in H$. Allora, per ogni 3-ciclo γ, $\gamma^{-1}(1\,2\,3)\,\gamma \in H$. Calcoliamo tali coniugati. Ad esempio:

$$\text{se } \gamma = (1\,3\,4), \quad \gamma^{-1}(1\,2\,3)\,\gamma = (2\,4\,3) \in H;$$
$$\text{se } \gamma = (1\,4\,3), \quad \gamma^{-1}(1\,2\,3)\,\gamma = (1\,4\,2) \in H;$$
$$\text{se } \gamma = (1\,4\,2), \quad \gamma^{-1}(1\,2\,3)\,\gamma = (1\,3\,4) \in H.$$

Ciò è sufficiente ad affermare che tutti gli otto 3-cicli di $\boldsymbol{A}_4$ appartengono ad H.

Assumendo invece che $H \ni (1\,2\,4)$ oppure $(1\,3\,4)$ o $(2\,3\,4)$, si perviene alla stessa conclusione.

Nota. Conoscendo il reticolo dei sottogruppi di $\boldsymbol{A}_4$, è facile concludere subito che nessun sottogruppo proprio normale di $\boldsymbol{A}_4$ possiede 3-cicli.

* * *

Esercizio 5.4.2. Dimostrare che, $\forall\, n \geq 2$ risulta: $\boldsymbol{S}_n = \langle (1\,2),\ (1\,2\,3\,\ldots\,n) \rangle$.

Suggerimento. Si ponga $n \geq 3$, $\gamma = (1\,2)$, $\sigma = (1\,2\,3\,\ldots\,n)$ e $H = \langle \gamma, \sigma \rangle$. Ricordato che ogni permutazione di $\boldsymbol{S}_n$ è prodotto di 2-cicli, verificare:

(a) $H \ni (t,\ t{+}1),\ \forall\, t = 1, \dots, n-1$;

(b) $H \ni (1\ t),\ \forall\, t = 2, \dots, n$;

(c) ogni $(h\ k)$ è prodotto di 2-cicli di tipo $(1\ t)$.

Soluzione. Per $n = 2$ la tesi è ovvia. Sia $n \geq 3$. Per quanto detto nel suggerimento, va dimostrato che H contiene tutti i 2-cicli.

(a) Risulta:

$$\sigma^{-1}\gamma\,\sigma = (1\,n\dots 3\,2)(1\,2)(1\,2\dots n) = (2\,3) \quad \text{e}$$
$$\sigma^{-1}(2\,3)\,\sigma = (1\,n\dots 3\,2)(2\,3)(1\,2\dots n) = (3\,4).$$

Analogamente, per $1 \leq t \leq n-2$:

$$\sigma^{-1}(t,\ t{+}1)\,\sigma = (1\,n\dots 3\,2)(t,\ t{+}1)(1\,2\dots n) = (t{+}1,\ t{+}2).$$

È così provato che $H \supseteq \{(1\,2),\ (2\,3),\ (3\,4),\ \dots,\ (n{-}1\ n)\}$.

(b) Si ha: $(1\,3) = (1\,2)(2\,3)(1\,2)$. Poiché [da ($a$)] $(1\,2),\ (2\,3) \in H$, anche $(1\,3) \in H$. Risulta poi: $(1\,4) = (1\,3)(3\,4)(1\,3)$ e, analogamente,

$$(1\,k) = (1,\ k-1)(k-1,\ k)(1,\ k-1),\quad \forall\, k = 2, \dots, n.$$

In questo modo si è provato che $H \supseteq \{(1\,2),\ (1\,3),\ \dots,\ (1\,n)\}$.

(c) Risulta subito che, $\forall$ 2-ciclo $(h\ k)$:

$$(h\ k) = (1\ h)(1\ k)(1\ h).$$

Dunque $(h\ k) \in H$.

* * *

Esercizio 5.4.3. Dimostrare le affermazioni (i) e (ii) enunciate in Osserv **4.1**.

Soluzione. (i) Essendo G risolubile, esiste una catena di risolubilità

$$\{1\} = G_0 < G_1 < G_2 < \dots < G_n = G.$$

Poiché $H \trianglelefteq G$, si ottiene subito la catena di sottogruppi

$$H = G_0H \leq G_1H \leq G_2H \leq \dots \leq G_nH = G.$$

Possiamo facilmente verificare che $G_{i-1}H \trianglelefteq G_iH$ $(\forall\, i = 1, \dots, n)$. Ciò segue dal seguente semplice fatto:

siano $G', G'' \leq G$ e sia $H \trianglelefteq G$. Se $G' \trianglelefteq G''$, anche $G'H \trianglelefteq G''H$.

[Infatti, $\forall\, gh \in G''H$, essendo $HG' = G'H$, si ha:

$$ghG'H = ghHG' = gHG' = gG'H; \quad G'Hgh = G'gHh = G'gH = gG'H].$$

Poiché $H \trianglelefteq G$, allora $H \trianglelefteq G_iH$ $(\forall\, i = 0, \dots, n)$ e dunque è definita la catena

(*****) $$H/_H \leq G_1H/_H \leq G_2H/_H \leq \dots \leq G_{n-1}H/_H \leq G/_H.$$

Vogliamo verificare che (*****) è una catena di risolubilità di $G/_H$ e cioè che, $\forall\, i = 1, \dots, n$.:

(a) $G_{i-1}H/_H \trianglelefteq G_iH/_H$; ($b$) $\dfrac{G_iH/_H}{G_{i-1}H/_H}$ è abeliano.

Per verificare (a) osserviamo che $G_{i-1}H \trianglelefteq G_iH$ ed applichiamo il terzo teorema di isomorfismo ai due sottogruppi normali $H,\ G_{i-1}H$ di G_iH. Si ottiene

$$G_iH/_{G_{i-1}H} \cong \frac{G_iH/_H}{G_{i-1}H/_H},\ \text{da cui}\ G_{i-1}H/_H \trianglelefteq G_iH/_H.$$

Resta da verificare (b). Si ha [in base al secondo teorema di isomorfismo applicato ai sottogruppi $G_i,\ G_{i-1}H$ di G_iH]:

$$\frac{G_iH/_H}{G_{i-1}H/_H} \cong G_iH/_{G_{i-1}H} = G_i(G_{i-1}H)/_{G_{i-1}H} \cong G_i/_{G_i\cap(G_{i-1}H)} \cong \frac{G_i/_{G_{i-1}}}{G_i\cap(G_{i-1}H)/_{G_{i-1}}}.$$

L'ultimo gruppo è un quoziente del gruppo abeliano $G_i/_{G_{i-1}}$ e quindi è abeliano.

(*ii*) Sia $H \trianglelefteq G$ e siano H, $G/_H$ risolubili, con catene di risolubilità rispettivamente:

$$\{1\} = H_0 < H_1 < \ldots < H_{m-1} < H \quad \text{e} \quad H/_H < G_1/_H < \ldots < G_{n-1}/_H < G/_H.$$

Consideriamo la catena di sottogruppi

$$(**) \qquad \{1\} = H_0 < H_1 < \ldots < H_{m-1} < H < G_1 < \ldots < G_{m-1} < G.$$

Dal teorema di corrispondenza, $G_{i-1} \trianglelefteq G_i$, $(\forall\, i = 0, \ldots, n)$. Inoltre i quozienti di (**) sono tutti abeliani, in quanto coincidono con i quozienti delle due catene di risolubilità. Si conclude che (**) è una catena di risolubilità di G.

* * *

Esercizio 5.5.1. Se $K \subseteq L$ è un'estensione finita, verificare che $G(L|K)$ è un gruppo finito.

Soluzione. Per ipotesi, $L = K(\alpha_1, \ldots, \alpha_t)$, con $\alpha_1, \ldots, \alpha_t$ algebrici su K. Siano $m_1, \ldots, m_t$ i rispettivi polinomi minimi su K. Assumiamo che, $\forall\, i = 1, \ldots, t$, m_i posseggga in L gli zeri, a due a due distinti, $\alpha_i = \alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{is_i}$. Se $m_i = \sum c_j X^j$, si ha, $\forall\, \varphi \in G(L|K)$:

$$m_i(\varphi(\alpha_i)) = \sum c_j \varphi(\alpha_i)^j = \sum \varphi(c_j \alpha_i^j) = \varphi(\sum c_j \alpha_i^j) = \varphi(0) = 0$$

e dunque $\varphi(\alpha_i) \in \{\alpha_i, \alpha_{i2}, \ldots, \alpha_{is_i}\}$. Poiché φ è completamente individuato dalle immagini $\varphi(\alpha_1), \ldots, \varphi(\alpha_t)$ [infatti, $\forall\, x \in L$, se $x = p(\alpha_1, \ldots, \alpha_t) \in K[\alpha_1, \ldots, \alpha_t]$, $\varphi(x) = p(\varphi(\alpha_1), \ldots, \varphi(\alpha_t))$], si conclude che $|G(L|K)| \leq s_1 \cdot \ldots \cdot s_t < \infty$.

* * *

Esercizio 5.5.2. Sia $\zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, $n \geq 1$. Verificare che $G(\boldsymbol{Q}(\zeta_n)\,|\,\boldsymbol{Q})$ è abeliano e ha ordine $\varphi(n)$.

Soluzione. Il polinomio minimo di ζ_n è l'n-simo polinomio ciclotomico $\Phi_n \in \boldsymbol{Z}[X]$, i cui $\varphi(n)$ zeri sono le radici primitive n-sime dell'unità ζ_n^k, con $1 \leq k \leq n$, $MCD(k, n) = 1$. È noto che Φ_n è monico e irriducibile (cfr. Teor. **2.1** di Cap. **4**).

Sia $\varphi \in G = G(\boldsymbol{Q}(\zeta_n)\,|\,\boldsymbol{Q})$. φ è completamente individuato da $\varphi(\zeta_n)$. Inoltre, poiché

$$\Phi_n\big(\varphi(\zeta_n)\big) = \varphi\big(\Phi_n(\zeta_n)\big) = \varphi(0) = 0,$$

allora $\varphi(\zeta_n)$ è una radice primitiva n-sima dell'unità, cioè $\varphi(\zeta_n) = \zeta_n^k$, per un opportuno k tale che $1 \leq k \leq n$, $MCD(k, n) = 1$. Ne segue che esistono esattamente $\varphi(n)$ $\boldsymbol{Q}$-automorfismi di $\boldsymbol{Q}(\zeta_n)$, cioè $|G| = \varphi(n)$.

Verifichiamo che tali automorfismi commutano. Siano infatti $\varphi, \psi \in G$, con $\varphi(\zeta_n) = \zeta_n^k$, $\psi(\zeta_n) = \zeta_n^h$. Allora

$$\varphi \circ \psi(\zeta_n) = \varphi(\zeta_n^h) = \varphi(\zeta_n)^h = \zeta_n^{hk} = \psi(\zeta_n^k) = \psi(\varphi(\zeta_n)) = \psi \circ \varphi(\zeta_n).$$

Dunque $\varphi \circ \psi = \psi \circ \varphi$, cioè G è abeliano.

Nota. Per ogni k tale che $1 \leq k < n$ e $MCD(k, n) = 1$, sia $\varphi_k \in G(\boldsymbol{Q}(\zeta_n)\,|\,\boldsymbol{Q})$ tale che $\varphi_k(\zeta_n) = \zeta_n^k$. Si verifica con facilità che l'applicazione

$$F : G(\boldsymbol{Q}(\zeta_n)\,|\,\boldsymbol{Q}) \to (\mathcal{U}(\boldsymbol{Z}_n), \cdot) \text{ tale che } F(\varphi_k) = \overline{k}, \ \forall\, \varphi_k \in G(\boldsymbol{Q}(\zeta_n)\,|\,\boldsymbol{Q}),$$

è un isomorfismo (di gruppi). Infatti $F(\varphi_h \circ \varphi_k) = F(\varphi_{hk}) = \overline{hk} = \overline{h} \cdot \overline{k} = F(\varphi_h) \cdot F(\varphi_k)$.

* * *

Esercizio 5.5.3. Posto $f = X^3 - 2 \in \boldsymbol{Q}[X]$, calcolare $G(\Sigma_{f,\,Q}\,|\,\boldsymbol{Q})$ e determinare i campi intermedi dell'estensione $\boldsymbol{Q} \subset \Sigma_{f,\,Q}$.

Soluzione. In $\Sigma_{f,\,Q}$ il polinomio f ha zeri $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$, con $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$. Allora

$$\Sigma_{f,\,Q} = \boldsymbol{Q}(\sqrt[3]{2},\ \zeta_3).$$

Risulta: $[\Sigma_{f,Q} : \boldsymbol{Q}] = 6$. Infatti ζ_3 ha polinomio minimo $\Phi_3 = X^2 + X + 1$ su $\boldsymbol{Q}(\sqrt[3]{2})[X]$. Dal *TFTG*, $|G(\Sigma_{f,Q}\,|\,\boldsymbol{Q})| = 6$. Inoltre $G(\Sigma_{f,Q}\,|\,\boldsymbol{Q})$ è un sottogruppo di $\boldsymbol{S}_3$ [infatti, $\forall\,\varphi \in G(\Sigma_{f,Q}\,|\,\boldsymbol{Q})$, risulta: $\varphi(\zeta_3) = \frac{\varphi(\sqrt[3]{2}\,\zeta_3)}{\varphi(\sqrt[3]{2})}$]. Dunque

$$G(\Sigma_{f,Q}\,|\,\boldsymbol{Q}) = \boldsymbol{S}_3.$$

I $\boldsymbol{Q}$-automorfismi di tale gruppo di Galois corrispondono biunivocamente alle sei permutazioni degli zeri di f. Posto $\alpha = \sqrt[3]{2}$, tali $\boldsymbol{Q}$-automorfismi sono:

$$(1) \equiv \mathbf{1}: \begin{matrix}\alpha \to \alpha\\ \alpha\zeta_3 \to \alpha\zeta_3\\ \alpha\zeta_3^2 \to \alpha\zeta_3^2,\end{matrix} \qquad (2\,3) \equiv \varphi_2: \begin{matrix}\alpha \to \alpha\\ \alpha\zeta_3 \to \alpha\zeta_3^2\\ \alpha\zeta_3^2 \to \alpha\zeta_3,\end{matrix} \qquad (1\,2) \equiv \varphi_3: \begin{matrix}\alpha \to \alpha\zeta_3\\ \alpha\zeta_3 \to \alpha\\ \alpha\zeta_3^2 \to \alpha\zeta_3^2,\end{matrix}$$

$$(1\,3) \equiv \varphi_4: \begin{matrix}\alpha \to \alpha\zeta_3^2\\ \alpha\zeta_3 \to \alpha\zeta_3\\ \alpha\zeta_3^2 \to \alpha,\end{matrix} \qquad (1\,2\,3) \equiv \varphi_5: \begin{matrix}\alpha \to \alpha\zeta_3\\ \alpha\zeta_3 \to \alpha\zeta_3^2\\ \alpha\zeta_3^2 \to \alpha,\end{matrix} \qquad (1\,3\,2) \equiv \varphi_6: \begin{matrix}\alpha \to \alpha\zeta_3^2\\ \alpha\zeta_3 \to \alpha\\ \alpha\zeta_3^2 \to \alpha\zeta_3.\end{matrix}$$

Determiniamo ora i campi intermedi dell'estensione $\boldsymbol{Q} \subset \Sigma_{f,Q}$. Poichè $G(\Sigma_{f,Q}\,|\,\boldsymbol{Q}) \cong \boldsymbol{S}_3$, esistono quattro campi intermedi:

$$\langle(1\,2\,3)\rangle^\flat,\ \langle(1\,2)\rangle^\flat,\ \langle(1\,3)\rangle^\flat,\ \langle(2\,3)\rangle^\flat.$$

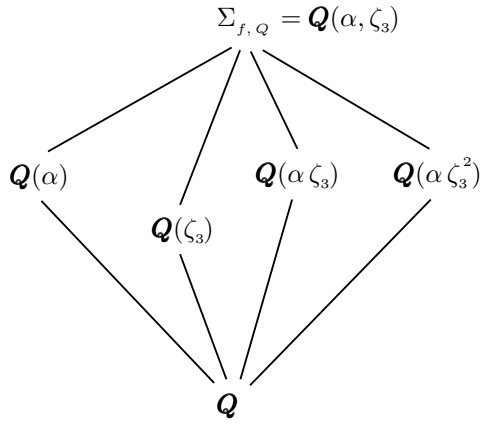
Inoltre $[\langle(1\,2\,3)\rangle^\flat : \boldsymbol{Q}] = \frac{6}{|\langle(1\,2\,3)\rangle|} = 2$, mentre $[\langle(1\,2)\rangle^\flat : \boldsymbol{Q}] = \frac{6}{|\langle(1\,2)\rangle|} = 3$ e, analogamente, $[\langle(2\,3)\rangle^\flat : \boldsymbol{Q}] = [\langle(1\,3)\rangle^\flat : \boldsymbol{Q}] = 3$.

Risulta: $\langle(1\,2\,3)\rangle^\flat \ni \zeta_3$ [infatti $\varphi_5(\zeta_3) = \varphi_5\big(\frac{\alpha\,\zeta_3}{\alpha}\big) = \frac{\alpha\,\zeta_3^2}{\alpha\,\zeta^3} = \zeta_3$]. Dunque $\langle(1\,2\,3)\rangle^\flat = \boldsymbol{Q}(\zeta_3)$.

Analogamente, $\langle(1\,2)\rangle^\flat \ni \alpha\,\zeta_3^2$, $\langle(1\,3)\rangle^\flat \ni \alpha\,\zeta_3$, $\langle(2\,3)\rangle^\flat \ni \alpha$ e dunque

$$\langle(1\,2)\rangle^\flat = \boldsymbol{Q}(\alpha\,\zeta_3^2), \quad \langle(1\,3)\rangle^\flat = \boldsymbol{Q}(\alpha\,\zeta_3), \quad \langle(2\,3)\rangle^\flat = \boldsymbol{Q}(\alpha).$$

Il reticolo dei campi intermedi dell'estensione è quindi il seguente.



* * *

Esercizio 5.5.4. Sia N la chiusura normale dell'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{1+\sqrt{2}})$.

(*i*) Determinare il gruppo di Galois $G(N\,|\,\boldsymbol{Q})$.

(*ii*) Verificare che l'unico campo intermedio tra $\boldsymbol{Q}$ e $\boldsymbol{Q}(\sqrt{1+\sqrt{2}})$ è il campo $\boldsymbol{Q}(\sqrt{2})$.

Soluzione. (*i*) Sia $m \in \boldsymbol{Q}[X]$ il polinomio minimo di $\alpha = \sqrt{1+\sqrt{2}}$ su $\boldsymbol{Q}$. Dall'Esempio **5.3** è noto che $m = X^4 - 2X^2 - 1 \in \boldsymbol{Q}[X]$. La chiusura normale N di $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$ deve contenere $\Sigma_{m,Q}$ e dunque coincide con tale campo di spezzamento. I quattro zeri di m [in N] sono

$$\alpha,\ -\alpha,\ \beta := i\,\sqrt{\sqrt{2}-1},\ \overline{\beta} = -\beta.$$

Allora $N = \boldsymbol{Q}(\alpha, -\alpha, \beta, -\beta) = \boldsymbol{Q}(\alpha, \beta)$. Calcoliamo $[N : \boldsymbol{Q}]$. Risulta:

$$[N : \boldsymbol{Q}] = [\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}] = [\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}(\alpha)]\cdot[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}].$$

Ovviamente $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 4$. Inoltre $\beta^2 = -(\alpha^2 - 2)$ e dunque β è uno zero del polinomio $f = X^2 + (\alpha^2 - 2) \in \boldsymbol{Q}(\alpha)[X]$. Tale polinomio è irriducibile [i suoi zeri sono complessi non reali] e dunque f è il polinomio minimo di β su $\boldsymbol{Q}(\alpha)$. Pertanto $[N : \boldsymbol{Q}] = 2\cdot 4 = 8$.

Dal *TFTG*,

$$|G(N\,|\,\boldsymbol{Q})| = 8.$$

Per descrivere ogni $\boldsymbol{Q}$-automorfismo di $\varphi \in G(N\,|\,\boldsymbol{Q})$, osserviamo che è sufficiente indicare le immagini di α, β [infatti $\varphi(-\alpha) = -\varphi(\alpha)$, $\varphi(-\beta) = -\varphi(\beta)$]. Inoltre, da $\beta^2 = 2 - \alpha^2$, segue che:

$$\varphi(\alpha) = \pm\alpha \implies \varphi(\beta)^2 = 2 - \alpha^2 = \beta^2 \implies \varphi(\beta) = \pm\beta,$$
$$\varphi(\alpha) = \pm\beta \implies \varphi(\beta)^2 = 2 - \beta^2 = \alpha^2 \implies \varphi(\beta) = \pm\alpha.$$

Infine osserviamo che $G(N\,|\,\boldsymbol{Q})$ è un sottogruppo di $\boldsymbol{S}_4$ e quindi i $\boldsymbol{Q}$-automorfismi di $G(N\,|\,\boldsymbol{Q})$ possono essere identificati a permutazioni di $\boldsymbol{S}_4$. Facendo corrispondere gli zeri α, $-\alpha$, β, $-\beta$ rispettivamente a 1, 2, 3, 4, si ottiene:

$$\varphi_1 \equiv \mathbf{1}_N : \begin{matrix}\alpha \to \alpha\\ \beta \to \beta,\end{matrix} \quad \varphi_1 \equiv (1); \qquad \varphi_2 : \begin{matrix}\alpha \to \alpha\\ \beta \to -\beta,\end{matrix} \quad \varphi_2 \equiv (3\,4);$$
$$\varphi_3 : \begin{matrix}\alpha \to -\alpha\\ \beta \to \beta,\end{matrix} \quad \varphi_3 \equiv (1\,2); \qquad \varphi_4 : \begin{matrix}\alpha \to -\alpha\\ \beta \to -\beta,\end{matrix} \quad \varphi_4 \equiv (1\,2)(3\,4);$$
$$\varphi_5 : \begin{matrix}\alpha \to \beta\\ \beta \to \alpha,\end{matrix} \quad \varphi_5 \equiv (1\,3)(2\,4); \quad \varphi_6 : \begin{matrix}\alpha \to \beta\\ \beta \to -\alpha,\end{matrix} \quad \varphi_6 \equiv (1\,3\,2\,4);$$
$$\varphi_7 : \begin{matrix}\alpha \to -\beta\\ \beta \to \alpha,\end{matrix} \quad \varphi_7 \equiv (1\,4\,2\,3); \quad \varphi_8 : \begin{matrix}\alpha \to -\beta\\ \beta \to -\alpha,\end{matrix} \quad \varphi_8 \equiv (1\,4)(2\,3).$$

$G(N\,|\,\boldsymbol{Q}) = \{\varphi_1, \dots, \varphi_8\}$ ha cinque elementi di periodo 2 e due elementi di periodo 4. Conoscendo la struttura dei gruppi di ordine 8, si conclude che

$$G(N\,|\,\boldsymbol{Q}) \cong \boldsymbol{D}_4 \ \text{(gruppo diedrale del quadrato)}.$$

(*ii*) Tenuto conto che i campi intermedi tra $\boldsymbol{Q}$ ed N sono in corrispondenza biunivoca con i sottogruppi di $G(N|\boldsymbol{Q})$, si tratta di verificare che tra i gruppi $\boldsymbol{Q}^\sharp$ e $\boldsymbol{Q}(\alpha)^\sharp$ c'è un solo sottogruppo intermedio. Si ha (in base alle definizioni dei φ_i):

$$\boldsymbol{Q}^\sharp = G(N|\boldsymbol{Q}) \cong \boldsymbol{D}_4 \ \text{ e } \ \boldsymbol{Q}(\alpha)^\sharp = G(N|\boldsymbol{Q}(\alpha)) = \langle\varphi_2\rangle.$$

Si noti che ad esempio $\boldsymbol{D}_4 = \langle\varphi_6, \varphi_3\rangle$ [infatti φ_6 è un 4-ciclo e φ_3 è un 2-ciclo]; inoltre $\varphi_6^{\,2} = \varphi_4$ e $\varphi_2 = \varphi_3 \circ \varphi_4$. Tenuto conto del reticolo dei sottogruppi di $\boldsymbol{D}_4$, si osserva che l'unico sottogruppo intermedio tra $\langle\varphi_2\rangle$ e $\boldsymbol{D}_4$ è il gruppo di Klein $\langle\varphi_2, \varphi_4\rangle = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$. Conseguentemente, l'unico campo intermedio tra $\boldsymbol{Q}$ e $\boldsymbol{Q}(\alpha)$ è $\langle\varphi_2, \varphi_4\rangle^\flat$. Si verifica subito che

$$\langle\varphi_2, \varphi_4\rangle^\flat = \boldsymbol{Q}(\alpha^2) \ [= \boldsymbol{Q}(\sqrt{2})]$$

[infatti risulta $\varphi_2(\alpha^2) = \alpha^2 = \varphi_4(\alpha^2)$].

* * *

Esercizio 5.5.5. Sia $\zeta_5 = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$. Dimostrare che l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\zeta_5)$ contiene un unico campo intermedio K. Determinare il polinomio minimo di ζ_5 su K.

Soluzione. ζ_5 ha polinomio minimo $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, i cui zeri sono $\zeta_5, \zeta_5^{\,2}, \zeta_5^{\,3}, \zeta_5^{\,4}$. Il polinomio Φ_5 si fattorizza linearmente in $\boldsymbol{Q}(\zeta_5)$:

$$\Phi_5 = (X - \zeta_5)(X - \zeta_5^{\,2})(X - \zeta_5^{\,3})(X - \zeta_5^{\,4}).$$

Risulta: $[\boldsymbol{Q}(\zeta_5) : \boldsymbol{Q}] = 4$ e $\boldsymbol{Q}(\zeta_5) = \Sigma_{\Phi_5,\boldsymbol{Q}}$ (campo di spezzamento di Φ_5 su $\boldsymbol{Q}$). Poiché l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\zeta_5)$ è finita, normale e separabile, allora $\big|G(\boldsymbol{Q}(\zeta_5)\,|\,\boldsymbol{Q})\big| = 4$.

I quattro $\boldsymbol{Q}$-automorfismi di tale gruppo sono univocamente determinati dall'immagine di ζ_5. Poniamo: $\varphi(\zeta_5) = \zeta_5^{\,2}$. Allora $\varphi^2(\zeta_5) = \zeta_5^{\,4}$. Pertanto $\circ(\varphi) = 4$. Dunque $G(\boldsymbol{Q}(\zeta_5)\,|\,\boldsymbol{Q}) \cong \boldsymbol{C}_4$ e tale gruppo è generato da φ [tale che $\varphi(\zeta_5) = \zeta_5^{\,2}$].

In quanto ciclico di ordine 4, $G(\boldsymbol{Q}(\zeta_5)\,|\,\boldsymbol{Q})$ ha un solo sottogruppo proprio: $\langle\,\varphi^2\rangle$ [con $\varphi^2(\zeta_5) = \zeta_5^{\,4}$; si noti che in $\boldsymbol{Q}(\zeta_5)$ si ha: $\zeta_5^{\,4} = -1 - \zeta_5 - \zeta_5^{\,2} - \zeta_5^{\,3}$].

Dal *TFTG*, il campo K cercato è

$$\langle\,\varphi^2\rangle^\flat = \boldsymbol{Q}(\zeta_5)^{\langle\,\varphi^2\rangle} = \{x \in \boldsymbol{Q}(\zeta_5) \mid \varphi^2(x) = x\}.$$

Sia $x = a + b\,\zeta_5 + c\,\zeta_5^{\,2} + d\,\zeta_5^{\,3}$, con $a, b, c, d \in \boldsymbol{Q}$. Allora

$$\varphi^2(x) = a + b\,\zeta_5^{\,4} + c\zeta_5^{\,3} + d\,\zeta_5^{\,2} =$$

$$= a - b - b\,\zeta_5 - b\,\zeta_5^2 - b\,\zeta_5^3 + c\,\zeta_5^3 + d\,\zeta_5^2 =$$
$$= (a-b) - b\,\zeta_5 + (d-b)\,\zeta_5^2 + (c-b)\,\zeta_5^3.$$

Pertanto $x = \varphi^2(x) \iff \begin{cases} a = a-b, & b = -b, \\ c = d-b, & d = c-b \end{cases} \iff \begin{cases} b = 0, & a = a, \\ c = d, & d = c. \end{cases}$

Quindi

$$\langle \varphi^2 \rangle^{\flat} = \{a + c\,\zeta_5^2 + c\,\zeta_5^3,\ \forall\, a, c \in \boldsymbol{Q}\} = \{a + c(\zeta_5^2 + \zeta_5^3),\ \forall\, a, c \in \boldsymbol{Q}\} = \boldsymbol{Q}(\zeta_5^2 + \zeta_5^3) =: K.$$

Ovviamente $[K : \boldsymbol{Q}] = 2$ [infatti $(\zeta_5^2 + \zeta_5^3)^2 = 1 - (\zeta_5^2 + \zeta_5^3)$ e dunque il polinomio minimo di $\zeta_5^2 + \zeta_5^3$ su $\boldsymbol{Q}$ è $g = X^2 + X - 1$.]

Il polinomio minimo richiesto è quello di ζ_5 su $K[X]$. Deve essere di grado 2 e dunque del tipo

$$f = X^2 = (a + b(\zeta_5^2 + \zeta_5^3))X + (c + d(\zeta_5^2 + \zeta_5^3)).$$

Poiché $f(\zeta_5) = 0$, allora

$$0 = f(\zeta_5) = \zeta_5^2 + a\,\zeta_5 + b\,\zeta_5^3 + b\,\zeta_5^4 + c + d\,\zeta_5^2 + d\,\zeta_5^3 = c - b + (a-b)\zeta_5 + (1 - b + d)\zeta_5^2 + d\,\zeta_5^3$$

e quindi $d = 0$, $a = b = c = 1$. Si conclude che

$$f = X^2 + (1 + \zeta_5^2 + \zeta_5^3)X + 1$$

è il polinomio minimo cercato.

* * *

Esercizio 5.5.6. Sia $f = X^3 + X + \overline{1} \in \boldsymbol{Z}_2[X]$.

(*i*) Determinare il campo di spezzamento $\Sigma = \Sigma_{f, \boldsymbol{Z}_2}$.

(*ii*) Calcolare il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_2)$, esplicitandone tutti gli $\boldsymbol{Z}_2$-automorfismi.

Soluzione. (*i*) f è irriducibile su $\boldsymbol{Z}_2$ [infatti $f(\overline{0}) \neq \overline{0}$ e $f(\overline{1}) \neq \overline{0}$]. Allora:

$$\boldsymbol{Z}_2[X]\big/_{(f)} = \boldsymbol{Z}_2(x) = \{a + bx + cx^2,\ \forall\, a, b, c \in \boldsymbol{Z}_2;\ x^3 = x + \overline{1}\}$$

è un campo di cardinalità 8. In tale campo f si fattorizza tramite $X + x$. Eseguendo la divisione con resto:

$$X^3 + X + \overline{1} = (X + x)(X^2 + xX + (x^2 + \overline{1})).$$

Poniamo $g := X^2 + xX + (x^2 + \overline{1}) \in \boldsymbol{Z}_2(x)[X]$. Vogliamo verificare se g è riducibile o irriducibile su $\boldsymbol{Z}_2(x)$. Ciò significa verificare se tra gli otto elementi di $\boldsymbol{Z}_2(x)$ esiste uno zero di g. Si ha:

$$g(x^2) = x^4 + x^3 + x^2 + \overline{1} = x^2 + x + x + \overline{1} + x^2 + \overline{1} = \overline{0}.$$

Dunque $X + x^2 \,\big|\, g$. Eseguendo la divisione con resto:

$$g = X^2 + xX + x^2 + \overline{1} = (X + x^2)(X + x^2 + x).$$

Pertanto $f = (X + x)(X + x^2)(X + x^2 + x) \in \boldsymbol{Z}_2(x)[X]$. Si conclude che $\Sigma = \Sigma_{f, \boldsymbol{Z}_2} = \boldsymbol{Z}_2(x)$.

(*ii*) Il polinomio f è separabile [infatti $f \notin \boldsymbol{Z}_2[X^2]$] e dunque l'estensione $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(x)$ è finita normale e separabile. Pertanto

$$|G(\Sigma \,|\, \boldsymbol{Z}_2)| = [\Sigma : \boldsymbol{Z}_2] = 3 \ \text{ e quindi } \ G(\Sigma \,|\, \boldsymbol{Z}_2) \cong \boldsymbol{C}_3.$$

Calcoliamo i tre $\boldsymbol{Z}_2$-automorfismi di Σ. Ogni siffatto $\boldsymbol{Z}_2$-automorfismo è individuato dalla sua azione su x. Si ponga:

$$\mathbf{1} : x \to x, \quad \varphi : x \to x^2, \quad \psi : x \to x^2 + x.$$

Allora

$$\begin{cases} \varphi(x^2) = x^4 = x^2 + x \\ \varphi(x^2 + x) = x^2 + x + x^2 = x, \end{cases} \qquad \begin{cases} \psi(x^2) = x^4 + x^2 = x^2 + x + x^2 = x \\ \psi(x^2 + x) = x + x^2 + x = x^2. \end{cases}$$

Pertanto

$$\mathbf{1} \equiv (1),\ \varphi \equiv (1\,2\,3),\ \psi \equiv (1\,3\,2) \in \boldsymbol{C}_3\ (\leq \boldsymbol{S}_3)$$

[avendo ordinato i tre zeri di f in ordine crescente nella forma $x,\ x^2,\ x^2 + x$].

* * *

Esercizio 5.5.7. Sia $f = X^3 + \overline{2}X + \overline{1} \in \boldsymbol{Z}_3[X]$. Determinare il campo di spezzamento $\Sigma = \Sigma_{f,\boldsymbol{Z}_3}$ e dedurne il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_3)$.

Soluzione. Risulta: $\overline{1} = f(\overline{0}) = f(\overline{1}) = f(\overline{2}) \neq \overline{0}$. Dunque f è irriducibile su $\boldsymbol{Z}_3$ e f ha zero $x := X + (f)$ in $\boldsymbol{Z}_3[X]/_{(f)} = \boldsymbol{Z}_3(x)$.

Il campo $K := \boldsymbol{Z}_3(x)$ ha cardinalità 27 ed in esso vale la relazione $x^3 = x + \overline{1}$. Dividendo f per $X - x$, si ottiene

$$f = (X - x)\, g, \text{ con } g = X^2 + xX + (x^2 + \overline{2}) \in \boldsymbol{Z}_3(x).$$

Ci chiediamo se g è irriducibile su $\boldsymbol{Z}_3(x)$. Per calcolare gli eventuali zeri di g, possiamo usare la formula risolutiva per polinomi di secondo grado:

$$\tfrac{-x \pm \sqrt{x^2 - \overline{4}\,(x^2+\overline{2})}}{\overline{2}} = \overline{2}\big(-x \pm \sqrt{x^2 - (x^2+\overline{2})}\big) = \overline{2}\big(-x \pm \sqrt{-\overline{2}}\big) = \overline{2}\big(-x \pm \sqrt{\overline{1}}\big) = \overline{2}(-x \pm \overline{1}).$$

Pertanto g ammette i due zeri

$$\overline{2}(-x + \overline{1}) = x + \overline{2}, \quad \overline{2}(-x - \overline{1}) = x + \overline{1}$$

e quindi $f = (X - x)(X - (x + \overline{2}))(X - (x + \overline{1}))$. Allora

$$\Sigma = \boldsymbol{Z}_3(x) \text{ e } [\Sigma : \boldsymbol{Z}_3] = 3.$$

Essendo f separabile, l'estensione $\boldsymbol{Z}_3 \subset \boldsymbol{Z}_3(x)$ è finita, normale, separabile. Quindi $|G(\Sigma \,|\, \boldsymbol{Z}_3)| = 3$ e pertanto $G(\Sigma \,|\, \boldsymbol{Z}_3) \cong \boldsymbol{C}_3$ (gruppo ciclico).

I tre $\boldsymbol{Z}_3$-automorfismi di $G(\Sigma \,|\, \boldsymbol{Z}_3)$ sono individuati dalla loro azione su x. Sono

$$\mathbf{1} : x \to x, \quad \varphi : x \to x + \overline{2}, \quad \psi : x \to x + \overline{1}.$$

Si ha:

$$\begin{cases} \varphi(x + \overline{2}) = x + \overline{2} + \overline{2} = x + \overline{1} \\ \varphi(x + \overline{1}) = x + \overline{2} + \overline{1} = x, \end{cases} \qquad \begin{cases} \psi(x + \overline{2}) = x + \overline{2} + \overline{1} = x \\ \psi(x + \overline{1}) = x + \overline{1} + \overline{1} = x + \overline{2}. \end{cases}$$

* * *

Esercizio 5.5.8. Si consideri l'estensione di campi $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(*i*) Determinare il grado di tale estensione e dire se è normale.

(*ii*) Determinare il gruppo di Galois G di tale estensione.

(*iii*) Determinare i campi intermedi di tale estensione contenenti $\boldsymbol{Q}(\sqrt{10})$.

Soluzione. (*i*) Si ponga $L = \boldsymbol{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Risulta:

$$[L : \boldsymbol{Q}] = [L : \boldsymbol{Q}(\sqrt{2}, \sqrt{3})] \cdot [\boldsymbol{Q}(\sqrt{2}, \sqrt{3}) : \boldsymbol{Q}(\sqrt{2})] \cdot [\boldsymbol{Q}(\sqrt{2}) : \boldsymbol{Q}] = 2 \cdot 2 \cdot 2 = 8.$$

Posto $f = (X^2 - 2)(X^2 - 3)(X^2 - 5) \in \boldsymbol{Q}[X]$, allora:

$$\Sigma_{f,\boldsymbol{Q}} = \boldsymbol{Q}(\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5}) = L,$$

cioè L è campo di spezzamento del polinomio $f \in \boldsymbol{Q}[X]$. Ne segue che l'estensione $\boldsymbol{Q} \subset L$ è normale.

(*ii*) Dal *TFTG*, $|G| = |G(L \,|\, \boldsymbol{Q})| = [L : \boldsymbol{Q}] = 8$. Sia $\varphi \in G$. Risulta:

$$\varphi(\sqrt{2}) \in \{\pm\sqrt{2}\}, \quad \varphi(\sqrt{3}) \in \{\pm\sqrt{3}\}, \quad \varphi(\sqrt{5}) \in \{\pm\sqrt{5}\}.$$

φ è quindi completamente individuato dai segni che vengono scelti per i tre radicali. Poniamo, per brevità:

$$\mathbf{1} = + + +, \quad \varphi_1 = + + -, \quad \varphi_2 = + - +, \quad \varphi_3 = + - -,$$
$$\boldsymbol{\varphi_4} = - + +, \quad \varphi_5 = - + -, \quad \varphi_6 = - - +, \quad \varphi_7 = - - -.$$

Ad esempio $\varphi_2 : \begin{matrix} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \\ \sqrt{5} \to \sqrt{5}, \end{matrix}$ $\varphi_3 : \begin{matrix} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \\ \sqrt{5} \to -\sqrt{5} \end{matrix}$ ecc..

Si noti che, $\forall\, \varphi_i$, $\varphi_i^{\,2} = \mathbf{1}$. Dunque G ha sette elementi di periodo 2. Ne segue che $G \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$. Tale gruppo ha sette sottogruppi ciclici di ordine 2 e sette sottogruppi di ordine 4 (tutti di Klein), cfr. [AA] pag. 175.

(*iii*) $\boldsymbol{Q}(\sqrt{10})^\sharp$ è un gruppo di Klein [infatti $|\boldsymbol{Q}(\sqrt{10})^\sharp| = [L : \boldsymbol{Q}(\sqrt{10})] = 4$]. Dunque $\boldsymbol{Q}(\sqrt{10})^\sharp$ contiene tre sottogruppi ciclici di ordine 2, che corrispondono a tre sottocampi di L contenenti $\boldsymbol{Q}(\sqrt{10})$: si tratta dei campi intermedi cercati.

Si ha: $\mathbf{1}$, φ_2, φ_5, φ_7 fissano $\sqrt{10}$. Allora

$$\boldsymbol{Q}(\sqrt{10})^\sharp = \langle \varphi_2, \varphi_5 \rangle = \{\mathbf{1}, \varphi_2, \varphi_5, \varphi_7\}.$$

I tre sottocampi cercati sono:

$$L^{\langle \varphi_2 \rangle} = \boldsymbol{Q}(\sqrt{2}, \sqrt{5});$$
$$L^{\langle \varphi_5 \rangle} = \boldsymbol{Q}(\sqrt{3}, \sqrt{10});$$
$$L^{\langle \varphi_7 \rangle} = \boldsymbol{Q}(\sqrt{6}, \sqrt{15}) \quad [= \boldsymbol{Q}(\sqrt{6}, \sqrt{10}) = \boldsymbol{Q}(\sqrt{10}, \sqrt{15})].$$

* * *

Esercizio 5.5.9. È assegnato il polinomio $f = X^6 + X^3 + \overline{2} \in \boldsymbol{Z}_3[X]$.

(*i*) Verificare che f è il cubo di un polinomio irriducibile $g \in \boldsymbol{Z}_3[X]$.

(*ii*) Determinare il campo di spezzamento Σ di f su $\boldsymbol{Z}_3$ e dire se l'estensione $\boldsymbol{Z}_3 \subset \Sigma$ è finita, normale e separabile.

(*iii*) Determinare il gruppo di Galois $G(\Sigma \,|\, \boldsymbol{Z}_3)$.

Soluzione. (*i*) Si ponga: $g = X^2 + X + \overline{2} \in \boldsymbol{Z}_3[X]$. Tale polinomio è irriducibile (infatti $g(\overline{0}), g(\overline{1}), g(\overline{2}) \neq \overline{0}$). Si ha (essendo $car(\boldsymbol{Z}_3) = 3$):

$$g^3 = \big(X^2 + (X + \overline{2})\big)^3 = X^6 + (X + \overline{2})^3 = X^6 + X^3 + \overline{2}^3 = X^6 + X^3 + \overline{2} = f.$$

(*ii*) Poniamo

$$K := \boldsymbol{Z}_3[X]/_{(g)} = \boldsymbol{Z}_3(\alpha) = \{a + b\alpha, \ \forall\, a, b \in \boldsymbol{Z}_3; \ \alpha^2 + \alpha + \overline{2} = \overline{0}\}.$$

Dividendo g per $X - \alpha$ si ottiene

$$g = (X - \alpha)(X + (1 + \alpha)) = (X - \alpha)(X - (\overline{2} + \overline{2}\alpha)).$$

Dunque g è separabile e quindi anche f lo è. Risulta:

$$\Sigma = \Sigma_{f, \boldsymbol{Z}_3} = \boldsymbol{Z}_3(\alpha, \overline{2} + \overline{2}\alpha) = \boldsymbol{Z}_3(\alpha) = K.$$

L'estensione $\boldsymbol{Z}_3 \subset \Sigma$ è finita, normale e separabile, di grado 2.

(*iii*) Dal *TFTG*, $G = G(\Sigma \,|\, \boldsymbol{Z}_3) \cong \boldsymbol{C}_2$. L'unico $\boldsymbol{Z}_3$-automorfismo non banale di G è

$$\varphi : \Sigma \to \Sigma \ \text{ tale che } \ \varphi(\alpha) = \overline{2} + \overline{2}\alpha.$$

* * *

Esercizio 5.5.10. Determinare le radici ottave dell'unità su $\boldsymbol{Z}_5$. Qual'è la minima estensione di $\boldsymbol{Z}_5$ in cui sono contenute? Qual'è il gruppo di Galois di tale estensione su $\boldsymbol{Z}_5$?

Soluzione. Le radici ottave dell'unità su $\boldsymbol{Z}_5$ sono gli zeri del polinomio $f = X^8 - \overline{1} \in \boldsymbol{Z}_5[X]$. Risulta:

$$f = X^8 - \overline{1} = (X^4 - \overline{1})(X^4 + \overline{1}) = (X - \overline{1})(X + \overline{1})(X^2 + \overline{1})(X^4 + \overline{1}).$$

Si osserva subito che i polinomi $X^2 + \overline{1}$, $X^4 + \overline{1}$ si fattorizzano in $\boldsymbol{Z}_5[X]$ rispettivamente nella forma

$$X^2 + \overline{1} = (X - \overline{2})(X - \overline{3}), \quad X^4 + \overline{1} = (X^2 - \overline{2})(X^2 - \overline{3}).$$

I due polinomi $X^2 - \overline{2}$, $X^2 - \overline{3}$ sono poi irriducibili su $\boldsymbol{Z}_5$ [in quanto non hanno zeri in $\boldsymbol{Z}_5$]. Pertanto delle otto radici ottave dell'unità, quattro sono in $\boldsymbol{Z}_5$ $(\overline{1}, \overline{2}, \overline{3}, \overline{4})$ e le rimanenti quattro sono zeri rispettivamente di $X^2 - \overline{2}$, $X^2 - \overline{3}$.

Si ha

$$\boldsymbol{Z}_5[X]/_{(X^2 - \overline{2})} =: \boldsymbol{Z}_5(\alpha) = \{a + b\alpha, \ \forall\, a, b \in \boldsymbol{Z}_5, \ a^2 = \overline{2}\}.$$

I due zeri di $X^2 - \overline{2}$ sono quindi α e $-\alpha = \overline{4}\alpha$. Restano da determinare le ultime due radici ottave dell'unità, zeri del polinomio $X^2 - \overline{3}$.

Ci chiediamo se in $\boldsymbol{Z}_5(\alpha)$ il polinomio $X^2-\overline{3}$ è riducibile. Se lo fosse, esisterebbe $a+b\alpha \in \boldsymbol{Z}_5(\alpha)$ tale che $(a+b\alpha)^2=\overline{3}$. Ne segue $a^2+\overline{2}b^2+\overline{2}ab\alpha-\overline{3}=\overline{0}$, cioè $\overline{2}ab\alpha=\overline{3}-a^2-\overline{2}b^2$. Poiché $\alpha \notin \boldsymbol{Z}_5$, deve risultare $\overline{2}ab=\overline{3}-a^2-\overline{2}b^2=\overline{0}$. Se $a=\overline{0}$, $\overline{3}=\overline{2}b^2$, da cui $b=\overline{2}$. Dunque $\overline{2}\alpha$ è uno zero del polinomio $X^2-\overline{3}\in \boldsymbol{Z}_5(\alpha)[X]$ e l'altro zero è $-\overline{2}\alpha=\overline{3}\alpha$.

Si conclude che

$$\Sigma_{f,\boldsymbol{Z}_5}=\boldsymbol{Z}_5(\alpha) \quad \text{(estensione algebrica semplice di grado 2, su } \boldsymbol{Z}_2)$$

è la minima estensione di $\boldsymbol{Z}_5$ in cui sono contenute tutte le otto radici ottave dell'unità su $\boldsymbol{Z}_5$.

L'estensione $\boldsymbol{Z}_5\subset \boldsymbol{Z}_5(\alpha)$ è separabile e quindi il gruppo di Galois $G(\boldsymbol{Z}_5(\alpha)\,|\,\boldsymbol{Z}_5)$, avendo ordine 2, è isomorfo a $\boldsymbol{C}_2$.

* * *

Esercizio 5.5.11. (*i*) Determinare il campo di spezzamento E del polinomio $X^7-\overline{1}\in \boldsymbol{Z}_2[X]$.

(*ii*) Calcolare il gruppo di Galois $G(E\,|\,\boldsymbol{Z}_2)$.

(*iii*) Determinare i campi intermedi dell'estensione $\boldsymbol{Z}_2\subset E$.

Soluzione. (*i*) Si ha

$$X^7-\overline{1}=(X+\overline{1})(X^6+X^5+X^4+X^3+X^2+X+\overline{1}).$$

Vogliamo verificare se il polinomio $f=X^6+X^5+X^4+X^3+X^2+X+\overline{1}\in \boldsymbol{Z}_2[X]$ è irriducibile.

Si osserva subito che f non ha fattori lineari. Per provare che è irriducibile, basta verificare che non ha fattori monici irriducibili di gradi 2 o 3. Allo scopo conviene (forse) elencare tutti siffatti polinomi e verificare che la divisione euclidea di f per tali polinomi ha resto non nullo. I polinomi monici irriducibili di grado 2 o 3 in $\boldsymbol{Z}_2[X]$ sono i seguenti

$$X^2+X+\overline{1},\ X^3+X^2+\overline{1},\ X^3+X+\overline{1}.$$

Dividendo f per tali polinomi si ottiene sempre resto non nullo. Quindi f è irriducibile.

Si ponga $K=\boldsymbol{Z}_2[X]/_{(f)}=\boldsymbol{Z}_2[\alpha\,|\,\alpha^6=\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+\overline{1}]=:\boldsymbol{Z}_2(\alpha)$. Si tratta di un campo con 64 elementi, estensione algebrica semplice di grado 6 su $\boldsymbol{Z}_2$. In K f ammette lo zero α. Ma anche α^2, α^3, α^4, α^5, $\alpha^6(=\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha+\overline{1})$ sono zeri di f [infatti, per $k=2,\dots,6$, $(\alpha^k)^7=(\alpha^7)^k=\overline{1}^k=\overline{1}$; dunque α^k è uno zero di $X^7-\overline{1}=(X+\overline{1})f$. Essendo $\alpha^k\neq\overline{1}$, α^k è zero di f]. Inoltre i sei zeri considerati sono a due a due distinti [f è separabile]. Ne segue che $E=\Sigma_{f,\boldsymbol{Z}_2}=\boldsymbol{Z}_2(\alpha)$ e $[E:\boldsymbol{Z}_2]=6$.

(*ii*) L'estensione $\boldsymbol{Z}_2\subset E$ è finita, normale e separabile. Dunque $|G(E\,|\,\boldsymbol{Z}_2)|=6$.

Ogni $\boldsymbol{Z}_2$-automorfismo φ di E è completamente individuato dalla sua azione su α. Inoltre $\varphi(\alpha)=\alpha^k$, con $1\le k\le 6$. Se poniamo $\varphi(\alpha)=\alpha^2$, allora

$$\varphi^2(\alpha)=\varphi(\alpha^2)=\varphi(\alpha)^2=\alpha^4,\ \ \varphi^3(\alpha)=\varphi(\alpha^4)=\varphi(\alpha)^4=\alpha^8=\alpha,\ \text{cioè}\ \varphi^3=\mathbf{1}_E.$$

Se invece poniamo $\psi(\alpha)=\alpha^3$, allora

$$\psi^2(\alpha)=\alpha^2,\ \ \psi^3(\alpha)=\alpha^6,\ \ \psi^4(\alpha)=\alpha^4,\ \ \psi^5(\alpha)=\alpha^5,\ \ \psi^6(\alpha)=\alpha,\ \text{cioè}\ \psi^6=\mathbf{1}_E.$$

Essendo $\circ(\psi)=6$, allora $G(E\,|\,\boldsymbol{Z}_2)=\langle\psi\rangle\cong\boldsymbol{C}_6$.

(*iii*) È ben noto che $\boldsymbol{C}_6\cong\langle\psi\rangle$ ammette due sottogruppi propri $\langle\psi^2\rangle$ e $\langle\psi^3\rangle$, di ordini rispettivamente 3, 2. Bisogna quindi determinare i generatori (su $\boldsymbol{Z}_2$) dei due campi fissi $\langle\psi^2\rangle^\flat$ e $\langle\psi^3\rangle^\flat$.

Consideriamo $\langle\psi^2\rangle^\flat$. Risulta: $[\langle\psi^2\rangle^\flat:\boldsymbol{Z}_2]=\frac{6}{3}=2$ e $\langle\psi^2\rangle^\flat=E^{\psi^2}=\{x\in E\,|\,x=\psi^2(x)\}$. Si ha: $\psi^2(\alpha)=\alpha^2$ e quindi $\psi^2(\alpha^2)=\alpha^4$, $\psi^2(\alpha^3)=\alpha^6=\overline{1}+\dots+\alpha^5$, $\psi^2(\alpha^4)=\alpha$, $\psi^2(\alpha^5)=\alpha^3$. Posto $x=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5\in E$, si ha subito che:

$$x=\psi^2(x)\iff a_0=a_0,\ a_3=a_5=\overline{0},\ a_1=a_2=a_4.$$

Pertanto $E^{\psi^2}=\{a+b(\alpha+\alpha^2+\alpha^4),\ \forall\, a,b\in\boldsymbol{Z}_2\}$. Dunque

$$E^{\psi^2}=\boldsymbol{Z}_2(\alpha+\alpha^2+\alpha^4).$$

Tale elemento ha polinomio minimo $X^2+X+\overline{1}$ su $\boldsymbol{Z}_2$, come subito si verifica.

Consideriamo ora $\langle\psi^3\rangle^\flat=E^{\psi^3}$. Procedendo come sopra, si ottiene che

$$x = \psi^3(x) \iff a_0 = a_0,\ a_1 = \overline{0},\ a_2 = a_5,\ a_3 = a_4.$$

Ne segue che $E^{\psi^3} = \{a + b(\alpha^2 + \alpha^5) + c(\alpha^3 + \alpha^4),\ \forall\, a, b, c \in \boldsymbol{Z}_2\}$. Dunque

$$E^{\psi^3} = \boldsymbol{Z}_2(\alpha^2 + \alpha^5,\ \alpha^3 + \alpha^4) = \boldsymbol{Z}_2(\alpha^2 + \alpha^5)$$

[infatti $(\alpha^2 + \alpha^5)^2 = \alpha^3 + \alpha^4$]. Si può facilmente verificare che il polinomio minimo di tale elemento su $\boldsymbol{Z}_2$ è $X^3 + X^2 + \overline{1}$.

* * *

Esercizio 5.5.12. Sono assegnati i polinomi $f = X^3 - 3X + 1,\ g = X^3 + 3X + 1 \in \boldsymbol{Q}[X]$ [si tratta di polinomi irriducibili, come facilmente si verifica].

(*i*) Posto $\zeta = \zeta_9$ (radice primitiva nona dell'unità), verificare che f ammette i tre zeri reali

$$\alpha = \zeta + \zeta^{-1},\quad \beta = \zeta^2 + \zeta^{-2},\quad \gamma = \zeta^4 + \zeta^{-4}$$

e che $\beta, \gamma \in \boldsymbol{Q}(\alpha)$. Dedurne che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{A}_3$.

(*ii*) Verificare che g ammette un unico zero reale. Dedurne che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_3$ e calcolare il campo fisso $\boldsymbol{A}_3^{\flat}$.

Soluzione. (*i*) Che f ammetta tre zeri reali segue facilmente dal Calcolo, studiando il grafico della funzione $Y = f(X)$. Che poi α, β, γ siano numeri reali è evidente [infatti $\alpha = 2\cos\frac{2\pi}{9},\ \beta = 2\cos\frac{4\pi}{9},\ \gamma = 2\cos\frac{8\pi}{9}$].

Si osserva subito che $\zeta^3 = \zeta_3$ (radice primitiva terza dell'unità). Ne segue che $\zeta^{-3} = \zeta_3^{-1} = \zeta_3^2$. Inoltre $\zeta_3^2 + \zeta_3 + 1 = 0$ [in quanto ζ_3 ha polinomio minimo $\Phi_3 = X^2 + X + 1 \in \boldsymbol{Q}[X]$]. Si ha:

$f(\alpha) = \alpha^3 - 3\alpha + 1 = \zeta^3 + \zeta^{-3} + 3\zeta + 3\zeta^{-1} - 3(\zeta + \zeta^{-1}) + 1 = \zeta_3 + \zeta_3^2 + 1 = 0;$

$f(\beta) = \zeta^6 + \zeta^{-6} + 3\zeta^2 + 3\zeta^{-2} - 3(\zeta^2 + \zeta^{-2}) + 1 = \zeta^6 + \zeta^{-6} + 1 = \zeta_3^2 + \zeta_3^{-2} + 1 = \zeta_3^2 + \zeta_3 + 1 = 0;$

$f(\gamma) = \zeta^{12} + \zeta^{-12} + 1 = \zeta^3 + \zeta^{-3} + 1 = 0.$

Risulta: $\alpha^2 = \zeta^2 + \zeta^{-2} + 2\zeta\,\zeta^{-1} = 2 + \beta$. Pertanto $\beta = \alpha^2 - 2$. Inoltre: $\beta^2 = \zeta^4 + \zeta^{-4} + 2 = 2 + \gamma$ e quindi $\gamma = \beta^2 - 2 = (\alpha^2 - 2)^2 - 2 = \alpha^4 - 4\alpha^2 + 2$. Ne segue che $\beta, \gamma \in \boldsymbol{Q}(\alpha)$ e quindi $\Sigma_{f,\boldsymbol{Q}} = \boldsymbol{Q}(\alpha)$. Pertanto $|G(f|\boldsymbol{Q})| = [\Sigma_{f,\boldsymbol{Q}} : \boldsymbol{Q}] = [Q(\alpha) : \boldsymbol{Q}] = 3$. Si conclude quindi che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{A}_3$.

(*ii*) Dal calcolo segue che g ammette un solo zero reale α [infatti $g' = 3X^2 + 3 > 0$ e quindi $Y = f(X)$ è crescente in tutto $\boldsymbol{R}$]. Denotiamo con β, γ gli altri due zeri (complessi coniugati) di g.

Dalla Prop. **5.5** segue subito che $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_3$. Ma, senza far uso di tale risultato, possiamo osservare che $\beta \notin \boldsymbol{Q}(\alpha)$ [in quanto $\beta \notin \boldsymbol{R}$ e $\boldsymbol{Q}(\alpha) \subset \boldsymbol{R}$]; pertanto si ha: $|G(g \,|\, \boldsymbol{Q})| = [\Sigma_{g,\boldsymbol{Q}} : \boldsymbol{Q}] = [\Sigma_{g,\boldsymbol{Q}} : Q(\alpha)] \cdot [\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 6$. Quindi $G(f \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_3$.

Determiniamo ora il campo fisso $\boldsymbol{A}_3^{\flat}$. Si tratta di un'estensione di grado 2 di $\boldsymbol{Q}$. Infatti risulta: $[\boldsymbol{A}_3^{\flat} : \boldsymbol{Q}] = (G(g|\boldsymbol{Q}) : \boldsymbol{A}_3) = (\boldsymbol{S}_3 : \boldsymbol{A}_3) = 2$. In base all'Osserv. **5.4**, $\boldsymbol{A}_3^{\flat}$ è generato su $\boldsymbol{Q}$ dall'elemento $\delta = (\beta - \alpha)(\gamma - \beta)(\gamma - \alpha)$. Poiché $\delta^2 = -4(3)^3 - 27(1)^2 = -135$, allora $\delta = i\sqrt{135}$ e quindi

$$\boldsymbol{A}_3^{\flat} = \boldsymbol{Q}(i\sqrt{135}).$$

Nota. Gli altri campi intermedi dell'estensione $\boldsymbol{Q} \subset \Sigma_{g,\boldsymbol{Q}}$ sono i campi fissi dei tre sottogruppi ciclici di ordine 2 di $\boldsymbol{S}_3$, cioè $\langle(1\,2)\rangle$, $\langle(1\,3)\rangle$, $\langle(2\,3)\rangle$. Si tratta ovviamente di estensioni di grado 3 su $\boldsymbol{Q}$. Risulta ovviamente:

$$\langle(1\,2)\rangle^{\flat} = \boldsymbol{Q}(\gamma),\quad \langle(1\,3)\rangle^{\flat} = \boldsymbol{Q}(\beta),\quad \langle(2\,3)\rangle^{\flat} = \boldsymbol{Q}(\alpha).$$

* * *

ALTRI ESERCIZI

Prove d'esame o di esonero e compiti di verifica A.A. 2005-06 e 2006-07

1. [*Prova d'esonero del 26/04/06*] Sia G un gruppo di ordine 18.

(*i*) Determinare i possibili numeri dei suoi sottogruppi di Sylow.

(*ii*) Per ogni scelta possibile di tali numeri, determinare almeno un corrispondente esempio di gruppo di ordine 18 e descriverne i sottogruppi di Sylow.

Soluzione. (*i*) Poiché $|G| = 2\cdot 3^2$, G ammette 2-Sylow (di ordine 2) e 3-Sylow (di ordine 9).

Sia r il numero dei 2-Sylow. Dal terzo teorema di Sylow, $r \,|\, 9$ e $r \equiv 1$ (*mod* 2). Dunque $r = 1, 3, 9$. Sia s il numero dei 3-Sylow. Poiché ogni 3-Sylow ha indice 2 e quindi è normale, necessariamente $s = 1$. A priori sono possibili tre coppie (r, s):

$$(r,s) = (1,1), \quad (r,s) = (3,1), \quad (r,s) = (9,1).$$

(*ii*) Il caso $(r, s) = (1, 1)$ è ottenuto scegliendo un gruppo G abeliano. Sono possibili due esempi:

$$G = \boldsymbol{C}_{18} \ [\cong \boldsymbol{C}_2 \times \boldsymbol{C}_9] \ \text{ e } \ G = \boldsymbol{C}_2 \times \boldsymbol{C}_3 \times \boldsymbol{C}_3.$$

È noto che $\boldsymbol{C}_{18}$ ha un unico sottogruppo, per ogni divisore positivo di 18. Se $\boldsymbol{C}_{18} = \langle a \,|\, a^{18} = 1\rangle$, il 2-Sylow è $\langle a^9\rangle$ ed il 3-Sylow è $\langle a^2\rangle \cong \boldsymbol{C}_9$. Per descrivere $\boldsymbol{C}_2 \times \boldsymbol{C}_3 \times \boldsymbol{C}_3$ poniamo

$$\boldsymbol{C}_2 = \langle a \,|\, a^2 = 1\rangle, \quad \boldsymbol{C}_3 = \langle b \,|\, b^3 = 1\rangle, \quad \boldsymbol{C}_3 = \langle c \,|\, c^3 = 1\rangle.$$

L'unico 2-Sylow è $\langle (a, 1, 1)\rangle$ mentre l'unico 3-Sylow è $\langle (1, b, 1)\rangle \times \langle (1, 1, c)\rangle \cong \boldsymbol{C}_3 \times \boldsymbol{C}_3$.

Veniamo al caso $(r, s) = (3, 1)$. Un possibile esempio è dato dal prodotto diretto $\boldsymbol{C}_3 \times \boldsymbol{S}_3$. Si ponga

$$\boldsymbol{C}_3 = \langle a \,|\, a^3 = 1\rangle, \quad \boldsymbol{S}_3 = \langle x, y \,|\, x^2 = y^3 = 1,\ yx = x^2 y\rangle.$$

$\boldsymbol{C}_3 \times \boldsymbol{S}_3$ ha esattamente tre elementi di periodo 2: $(1, x)$, $(1, xy)$, $(1, xy^2)$. Quindi ha i tre 2-Sylow corrispondenti $\langle (1, x)\rangle$, $\langle (1, xy)\rangle$, $\langle (1, xy^2)\rangle$. L'unico 3-Sylow è dato dal prodotto diretto $\langle (a, 1)\rangle \times \langle (1, y)\rangle \cong \boldsymbol{C}_3 \times \boldsymbol{C}_3$.

Infine esaminiamo il caso $(r, s) = (9, 1)$. Un possibile esempio è dato dal gruppo diedrale

$$\boldsymbol{D}_9 = \langle \varphi, \rho \,|\, \varphi^9 = \rho^2 = 1,\ \rho \circ \varphi = \varphi^8 \circ \rho\rangle.$$

$\boldsymbol{D}_9$ ha nove elementi di periodo 2 [le nove riflessioni $\rho, \varphi\circ\rho, \ldots, \varphi^8\circ\rho$] e quindi i nove 2-Sylow corrispondenti $\langle\rho\rangle, \langle\varphi\circ\rho\rangle, \ldots, \langle\varphi^8\circ\rho\rangle$. L'unico 3-Sylow è $\langle\varphi\rangle \cong \boldsymbol{C}_9$.

* * *

2. [*Prova d'esonero del 26/04/06*] È assegnato il gruppo $\boldsymbol{O}_2(\boldsymbol{Z})$ delle matrici ortogonali di ordine 2 a valori interi].

(*i*) Elencare gli elementi di $\boldsymbol{O}_2(\boldsymbol{Z})$ e verificare che si tratta di un gruppo diedrale $\boldsymbol{D}_n$ (per un opportuno $n \in \boldsymbol{N}$).

(*ii*) Stabilire un isomorfismo tra $\boldsymbol{O}_2(\boldsymbol{Z})$ e $\boldsymbol{D}_n$.

(*iii*) Elencare le orbite di $\boldsymbol{O}_2(\boldsymbol{Z})$ rispetto all'azione di coniugio.

Soluzione. (*i*) Si ha:

$$\boldsymbol{O}_2(\boldsymbol{Z}) = \{A \in \boldsymbol{GL}_2(\boldsymbol{Z}) \,|\, A^{-1} = A^t\}.$$

Si noti che se $A \in \boldsymbol{O}_2(\boldsymbol{Z})$, $det(A) = \pm 1$. Si ha quindi, $\forall\, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{GL}_2(\boldsymbol{Z})$:

$$A \in \boldsymbol{O}_2(\boldsymbol{Z}) \iff \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \iff \begin{cases} d = a \\ c = -b \end{cases} \text{ oppure } \begin{cases} d = -a \\ c = b. \end{cases}.$$

Pertanto

$$A \in \boldsymbol{O}_2(\boldsymbol{Z}) \iff A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ oppure } A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \text{ con } a^2 + b^2 = 1.$$

In $\boldsymbol{Z}$ l'equazione $a^2+b^2=1$ ha soluzioni $(\pm1,0)$, $(0,\pm1)$. Ne segue che $\boldsymbol{O}_2(\boldsymbol{Z})$ è formato dalle seguenti otto matrici:

$$I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ -I_2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ \alpha=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ -\alpha=\begin{pmatrix}0&-1\\1&0\end{pmatrix},$$
$$\beta=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ -\beta=\begin{pmatrix}-1&0\\0&1\end{pmatrix},\ \gamma=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ -\gamma=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}.$$

Risulta subito che $\circ(-I_2)=\circ(\pm\beta)=\circ(\pm\gamma)=2$, mentre $\circ(\pm\alpha)=4$. Se ne deduce che $\boldsymbol{O}_2(\boldsymbol{Z})\cong\boldsymbol{D}_4$ (gruppo diedrale del quadrato).

(*ii*) Posto $\boldsymbol{D}_4=\langle\,\varphi,\rho\,\big|\,\varphi^4=\rho^2=1,\ \rho\circ\varphi=\varphi^3\circ\rho\,\rangle$, e ricordato che un isomorfismo conserva i periodi degli elementi, un isomorfismo $F:\boldsymbol{D}_4\to\boldsymbol{O}_2(\boldsymbol{Z})$ si ottiene ad esempio ponendo:

$$F(\varphi)=\alpha\ \text{ e }\ F(\rho)=\beta.$$

Si noti che $F(\varphi^3)\,F(\rho)=F(\rho)\,F(\varphi)$. Ciò è sufficiente a concludere che F è un isomorfismo tra i due gruppi.

(*iii*) Per determinare le orbite (rispetto al coniugio) conviene operare su $\boldsymbol{D}_4$.

Si verifica subito che $\boldsymbol{Z}(\boldsymbol{D}_4)=\langle\varphi^2\rangle$. Quindi $\boldsymbol{O}(1)=\{1\}$, $\boldsymbol{O}(\varphi^2)=\{\varphi^2\}$. Inoltre si verifica facilmente che $\boldsymbol{O}(\varphi)=\{\varphi,\varphi^3\}$, $\boldsymbol{O}(\rho)=\{\varphi,\varphi^2\circ\rho\}$, $\boldsymbol{O}(\varphi\circ\rho)=\{\varphi\circ\rho,\varphi^3\circ\rho\}$. Conseguentemente $\boldsymbol{O}_2(\boldsymbol{Z})$ ha cinque orbite:

$$\{I_2\},\ \{-I_2\},\ \{\alpha,-\alpha\},\ \{\beta,-\beta\},\ \{\gamma,-\gamma\}.$$

* * *

3. [*Prova d'esame del 12/06/06*] Sia G il prodotto diretto dei due gruppi alterni $\boldsymbol{A}_3$, $\boldsymbol{A}_4$.

(*i*) Determinare i periodi degli elementi di G.

(*ii*) Determinare i sottogruppi di Sylow di G.

(*iii*) Determinare gli eventuali sottogruppi di ordine 6 di G.

[*Consiglio*: per evitare confusioni, denotare gli elementi di $\boldsymbol{A}_3$ come permutazioni delle lettere a,b,c; denotare invece gli elementi di $\boldsymbol{A}_4$ come permutazioni delle cifre $1,2,3,4$ (come è usuale)].

Soluzione. (*i*) Si ha: $\boldsymbol{A}_3=\{(a),(a\,b\,c),(a\,c\,b)\}$;

$\boldsymbol{A}_4=\{(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3),(1\,2\,3),(1\,3\,2),(1\,2\,4),(1\,4\,2),(1\,3\,4),(1\,4\,3),(2\,3\,4),(2\,4\,3)\}$.

Il gruppo $G=\boldsymbol{A}_3\times\boldsymbol{A}_4$ è formato dai seguenti 36 elementi:

$1_G=((a),(1))$;

$x_1:=((a),(1\,2)(3\,4))$, $x_2:=((a),(1\,3)(2\,4))$, $x_3:=((a),(1\,4)(2\,3))$;

$y_1:=((a\,b\,c),(1))$, $y_2:=((a\,b\,c),(1\,2)(3\,4))$, $y_3:=((a\,b\,c),(1\,3)(2\,4))$, $y_4:=((a\,b\,c),(1\,4)(2\,3))$;

$z_1:=((a\,c\,b),(1))$, $z_2:=((a\,c\,b),(1\,2)(3\,4))$, $z_3:=((a\,c\,b),(1\,3)(2\,4))$, $z_4:=((a\,c\,b),(1\,4)(2\,3))$;

$u_1=((a),(1\,2\,3))$, $u_2=((a),(1\,3\,2))$, $u_3=((a),(1\,2\,4))$, ..., $u_8=((a),(2\,4\,3)$;

$v_1=((a\,b\,c),(1\,2\,3))$, $v_2=((a\,b\,c),(1\,3\,2))$, $v_3=((a\,b\,c),(1\,2\,4))$, ..., $v_8=((a\,b\,c),(2\,4\,3)$;

$w_1=((a\,c\,b),(1\,2\,3))$, $w_2=((a\,c\,b),(1\,3\,2))$, $w_3=((a\,c\,b),(1\,2\,4))$, ..., $w_8=((a\,c\,b),(2\,4\,3)$.

Ricordato che $\circ((x,y))=mcm(\circ(x),\circ(y))$, si ha:

$$\circ(1_G)=1;\ \circ(x_1)=\circ(x_2)=\circ(x_3)=2;\ \circ(y_1)=\circ(z_1)=3;$$
$$\circ(y_2)=\circ(y_3)=\circ(y_4)=\circ(z_2)=\circ(z_3)=\circ(z_4)=6;$$
$$\circ(u_1)=\ ...\ =\circ(u_8)=\circ(v_1)=\ ...\ =\circ(v_8)=\circ(w_1)=\ ...\ =\circ(w_8)=3.$$

(*ii*) Poiché $|G|=2^2\cdot3^2$, G possiede 2-Sylow e 3-Sylow, rispettivamente di ordini 4, 9.

Il numero s dei 2-Sylow verifica le condizioni

$$s\,\big|\,9\ \text{ e }\ s\equiv1\ (mod\ 2).$$

A priori, $s=1,3,9$. Ma G ammette soltanto tre elementi di periodo 2 e nessuno di periodo 4. Dunque G ha un solo 2-Sylow, che è un gruppo di Klein. Si tratta del gruppo

$$\langle(a)\rangle\times\boldsymbol{V}=\{1_G,\,x_1,\,x_2,\,x_3\}$$

[Ovviamente tale gruppo è normale in G]. Il numero t dei 3-Sylow verifica le condizioni

$$t \,\big|\, 4 \ \text{ e } \ t \equiv 1 \ (mod\, 3).$$

A priori, $t = 1, 4$. È noto che un gruppo di ordine 9 o è ciclico o è prodotto diretto di due gruppi $\boldsymbol{C}_3$. Poiché in G mancano elementi di periodo 9, i 3-Sylow sono di tipo $\boldsymbol{C}_3 \times \boldsymbol{C}_3$. Poiché $\boldsymbol{A}_4$ possiede quattro ciclici di ordine 3: $\langle (1\,2\,3) \rangle$, $\langle (1\,2\,4) \rangle$, $\langle (1\,3\,4) \rangle$, $\langle (2\,3\,4) \rangle$, allora:

$$\boldsymbol{A}_3 \times \langle (1\,2\,3) \rangle,\ \boldsymbol{A}_3 \times \langle (1\,2\,4) \rangle,\ \boldsymbol{A}_3 \times \langle (1\,3\,4) \rangle,\ \boldsymbol{A}_3 \times \langle (2\,3\,4) \rangle$$

sono quattro 3-Sylow di G e quindi sono tutti i 3-Sylow di G [ovviamente non normali in G].

(*iii*) G ammette sei elementi di periodo 6 e quindi ha esattamente tre sottogruppi ciclici $\boldsymbol{C}_6$. Si tratta di

$$\langle y_2 \rangle \ (= \langle z_2 \rangle),\ \ \langle y_3 \rangle \ (= \langle z_3 \rangle),\ \ \langle y_4 \rangle \ (= \langle z_4 \rangle).$$

Ci chiediamo se G ammetta sottogruppi $H \cong \boldsymbol{S}_3$. Ogni $\boldsymbol{S}_3$ contiene tre elementi di periodo 2 e quindi H necessariamente contiene il gruppo di Klein $\langle (a) \rangle \times \boldsymbol{V}$: assurdo (dal teorema di Lagrange).

* * *

4. [*Prova d'esame del 6/02/07*] (*i*) Determinare il gruppo $\boldsymbol{Isom}(\boldsymbol{S}_1)$ delle isometrie del piano euclideo $\boldsymbol{E}^2$ che fissano la circonferenza unitaria $\boldsymbol{S}_1$ [di centro O e raggio 1].

(*ii*) Sia $\omega : \boldsymbol{Isom}(\boldsymbol{S}_1) \times \boldsymbol{S}_1 \to \boldsymbol{S}_1$ l'azione così definita:

$$\omega(\varphi, P) = \varphi(P), \ \ \forall\, (\varphi, P) \in \boldsymbol{Isom}(\boldsymbol{S}_1) \times \boldsymbol{S}_1.$$

Determinare le orbite di ω e lo stabilizzatore del punto $P_0 = (0, 1) \in \boldsymbol{S}_1$.

Soluzione. (*i*) Cominciamo col provare che ogni isometria $\varphi \in \boldsymbol{Isom}(\boldsymbol{S}_1)$ fissa il centro O di $\boldsymbol{S}_1$. Siano $P, Q \in \boldsymbol{S}_1$ diametralmente opposti. Poiché $\varphi(P)$, $\varphi(Q) \in \boldsymbol{S}_1$ e $d(P, Q) = 2 = d(\varphi(P), \varphi(Q))$, anche $\varphi(P)$, $\varphi(Q)$ sono diametralmente opposti. Poiché ogni isometria trasforma il punto medio di un segmento nel punto medio del segmento immagine, allora $\varphi(O) = O$, come richiesto.

Le isometrie che fissano O sono tutte e sole le rotazioni di centro O e le riflessioni di asse una retta per O. In un riferimento cartesiano assegnato, sono rispettivamente rappresentate dalle matrici

$$A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \quad B_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}, \ \ \forall\, \alpha \in [0, 2\pi).$$

Tali matrici, come noto, formano il gruppo $\boldsymbol{O}_2(\boldsymbol{R})$ delle matrici ortogonali. Dunque si è provato che

$$\boldsymbol{Isom}(\boldsymbol{S}_1) \subseteq \boldsymbol{O}_2(\boldsymbol{R}).$$

Viceversa, si verifica subito che, $\forall\, P = (\cos t, \sin t) \in \boldsymbol{S}_1$:

$\omega(A_\alpha, P) = A_\alpha\, {}^t P = {}^t(\cos(\alpha + t), \sin(\alpha + t)) \in \boldsymbol{S}_1$, $\omega(B_\alpha, P) = B_\alpha\, {}^t P = {}^t(\cos(\alpha - t), \sin(\alpha - t)) \in \boldsymbol{S}_1$.
Dunque vale anche l'inclusione opposta $\boldsymbol{O}_2(\boldsymbol{R}) \subseteq \boldsymbol{Isom}(\boldsymbol{S}_1)$.

(*ii*) L'azione ω è ovviamente transitiva [infatti, $\forall\, P, Q \in \boldsymbol{S}_1$, esiste una rotazione φ di centro O che trasforma P in Q]. Dunque ω ha un'unica orbita.

Lo stabilizzatore di P_0 è formato dalle matrici $A \in \boldsymbol{O}_2(\boldsymbol{R})$ tali che $A\, {}^t(0, 1) = {}^t(0, 1)$. Si ha:

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \iff \begin{cases} -\sin\alpha = 0 \\ \cos\alpha = 1 \end{cases} \iff \alpha = 0 \iff A = I_2;$$

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \iff \begin{cases} \sin\alpha = 0 \\ -\cos\alpha = 1 \end{cases} \iff \alpha = \pi \iff A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

[corrispondente alla riflessione ρ_y intorno all'*asse* y]. Si conclude che $\boldsymbol{St}_{P_0} = \langle \rho_y \rangle$ [gruppo ciclico di ordine 2].

* * *

5. [*Prova d'esame del 10/07/06*] Nell'anello $\mathfrak{M}_3(\boldsymbol{Z}_2)$ delle matrici quadrate di ordine 3 a valori in $\boldsymbol{Z}_2$, sia $\mathcal{H}$ l'insieme delle matrici invertibili e triangolari superiori.

(*i*) Verificare che $\mathcal{H}$ è un gruppo e indicarne il tipo.

(*ii*) Sia ω l'azione di moltiplicazione righe per colonne di $\mathcal{H}$ sull'insieme $(\boldsymbol{Z}_2)^3$. Determinare le orbite di ω e lo stabilizzatore del punto $P = (\overline{1}, \overline{1}, \overline{1}) \in (\boldsymbol{Z}_2)^3$.

Soluzione. (*i*) Risulta:

$$A \in \mathcal{H} \iff A = \begin{pmatrix} \overline{1} & a & b \\ \overline{0} & \overline{1} & c \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \text{ con } a, b, c \in \boldsymbol{Z}_2.$$

$\mathcal{H}$ è quindi formato dalle otto matrici

$$\mathbf{1} = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \alpha = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \beta = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \gamma = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix},$$

$$\delta = \begin{pmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \epsilon = \begin{pmatrix} \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \zeta = \begin{pmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}, \quad \eta = \begin{pmatrix} \overline{1} & \overline{1} & \overline{1} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}.$$

Poiché le matrici triangolari superiori formano un gruppo (rispetto al prodotto righe per colonne) e lo stesso è vero per le matrici invertibili, allora $\mathcal{H}$ è un gruppo. Si noti che $\epsilon\,\zeta = \gamma$, mentre $\zeta\,\epsilon = \beta$. Dunque $\mathcal{H}$ non è commutativo. Calcolando i periodi degli elementi, si osserva che

$$\circ(\alpha) = \circ(\beta) = \circ(\gamma) = \circ(\delta) = \circ(\eta) = 2, \text{ mentre } \circ(\epsilon) = \circ(\zeta) = 4.$$

Ciò basta per affermare che $\mathcal{H}$ è isomorfo al gruppo diedrale $\boldsymbol{D}_4$.

(*ii*) $\omega : \mathcal{H} \times (\boldsymbol{Z}_2)^3 \to (\boldsymbol{Z}_2)^3$ è l'azione di moltiplicazione righe per colonne:

$$\omega(A, P) = A\,P, \ \forall\, A \in \mathcal{H}, \ \forall\, P \in (\boldsymbol{Z}_2)^3.$$

Posto $O = (\overline{0}, \overline{0}, \overline{0})$, risulta ovviamente $\boldsymbol{O}(O) = \{(\overline{0}, \overline{0}, \overline{0})\}$.

Posto $U_x = (\overline{1}, \overline{0}, \overline{0})$, risulta $\boldsymbol{O}(U_x) = \{U_x, \alpha\,U_x, \beta\,U_x, \dots, \eta\,U_x\} = \{(\overline{1}, \overline{0}, \overline{0})\}$.

Posto $U_y = (\overline{0}, \overline{1}, \overline{0})$, risulta $\boldsymbol{O}(U_y) = \{U_y, \alpha\,U_y, \beta\,U_y, \dots, \eta\,U_y\} = \{(\overline{0}, \overline{1}, \overline{0}), (\overline{1}, \overline{1}, \overline{0})\}$.

Posto $U_z = (\overline{0}, \overline{0}, \overline{1})$, risulta $\boldsymbol{O}(U_z) = \{U_z, \alpha\,U_z, \dots, \eta\,U_z\} = \{(\overline{0}, \overline{0}, \overline{1}), (\overline{1}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{1}, \overline{1})\}$.

Si conclude che le orbite sono quattro. Si ha infine:

$$\boldsymbol{St}_P = \{A \in \mathcal{H} \,\big|\, A\,P = P\}.$$

Posto $A = \begin{pmatrix} \overline{1} & a & b \\ \overline{0} & \overline{1} & c \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$, si ha

$$A\,P = P \iff \begin{cases} \overline{1} + a + b = \overline{1} \\ \overline{1} + c = \overline{1} \\ \overline{1} = \overline{1} \end{cases} \iff \begin{cases} c = \overline{0} \\ a + b = \overline{0} \end{cases} \iff \begin{cases} c = \overline{0} \text{ e } a = b = \overline{0} \\ \text{oppure} \\ c = \overline{0} \text{ e } a = b = \overline{1} \end{cases} \iff A = \mathbf{1}, \delta.$$

Pertanto $\boldsymbol{St}_P = \langle \delta \rangle$ (gruppo ciclico di ordine 2).

* * *

6. [*Prova di verifica del 7/03/07*] Determinare i sottogruppi propri del gruppo diedrale dell'ottagono regolare $\boldsymbol{D}_8$ e disegnarne il reticolo.

Soluzione. Si ha:

$$\boldsymbol{D}_8 = \langle \varphi, \rho \mid \varphi^8 = \rho^2 = 1, \ \rho \circ \varphi = \varphi^7 \circ \rho \rangle.$$

$\boldsymbol{D}_8$ ha ordine 16 e quindi i suoi sottogruppi propri hanno possibili ordini: 2, 4, 8. Inoltre $\boldsymbol{D}_8$ ha :

- nove elementi di periodo 2: ρ, φ^4, $\varphi \circ \rho$, $\varphi^2 \circ \rho$, $\varphi^3 \circ \rho$, $\varphi^4 \circ \rho$, $\varphi^5 \circ \rho$, $\varphi^6 \circ \rho$, $\varphi^7 \circ \rho$;
- quattro elementi di periodo 8: φ, φ^3, φ^5, φ^7;
- due elementi di periodo 4: φ^2, φ^6.

Ne segue che $\boldsymbol{D}_8$ ha:

- nove sottogruppi ciclici $\boldsymbol{C}_2$: $\langle \rho \rangle$, $\langle \varphi^4 \rangle$, $\langle \varphi \circ \rho \rangle \dots$, $\langle \varphi^7 \circ \rho \rangle$;
- un solo sottogruppo ciclico $\boldsymbol{C}_8$: $\langle \varphi \rangle$;
- un solo sottogruppo ciclico $\boldsymbol{C}_4$: $\langle \varphi^2 \rangle$.

Per ottenere altri sottogruppi di Klein in $\boldsymbol{D}_8$, basta scegliere due elementi di periodo 2 che commutino tra loro. Osserviamo che φ^4 commuta con gli altri otto elementi $\varphi^k \circ \rho$ (per $k = 0, \dots 7$).

Infatti $\varphi^4\circ(\varphi^k\circ\rho) = \varphi^{4+k}\circ\rho$, mentre $(\varphi^k\circ\rho)\circ\varphi^4 = \varphi^k\circ(\rho\circ\varphi^4) = \varphi^k\circ(\varphi^4\circ\rho) = \varphi^{4+k}\circ\rho$. Dunque esistono almeno quattro sottogruppi di Klein:

$$\boldsymbol{V}_1 = \langle\varphi^4,\, \rho\rangle = \{1,\, \varphi^4,\, \rho,\, \varphi^4\circ\rho\}, \quad \boldsymbol{V}_2 = \langle\varphi^4,\, \varphi\circ\rho\rangle = \{1,\, \varphi^4,\, \varphi\circ\rho,\, \varphi^5\circ\rho\},$$
$$\boldsymbol{V}_3 = \langle\varphi^4,\, \varphi^2\circ\rho\rangle = \{1,\, \varphi^4,\, \varphi^2\circ\rho,\, \varphi^6\circ\rho\}, \quad \boldsymbol{V}_4 = \langle\varphi^4,\, \varphi^3\circ\rho\rangle = \{1,\, \varphi^4,\, \varphi^3\circ\rho,\, \varphi^7\circ\rho\}.$$

Si può verificare che, se $\varphi^i\circ\rho$ e $\varphi^j\circ\rho$ commutano (con $0 \le i < j \le 7$), allora $(\varphi^j\circ\rho)\circ(\varphi^i\circ\rho) = \varphi^4$. Dunque ogni sottogruppo di Klein di $\boldsymbol{D}_8$ contiene φ^4 e pertanto non esistono altri sottogruppi di Klein oltre ai precedenti.

Veniamo agli eventuali sottogruppi non ciclcici di ordine 8. Conoscendo la struttura dei gruppi di ordine 8, è noto che tali eventuali sottogruppi possono essere isomorfi a:

$$\boldsymbol{D}_4,\ \mathbf{Q},\ \boldsymbol{C}_2\times\boldsymbol{C}_4,\ \boldsymbol{C}_2\times\boldsymbol{C}_2\times\boldsymbol{C}_2.$$

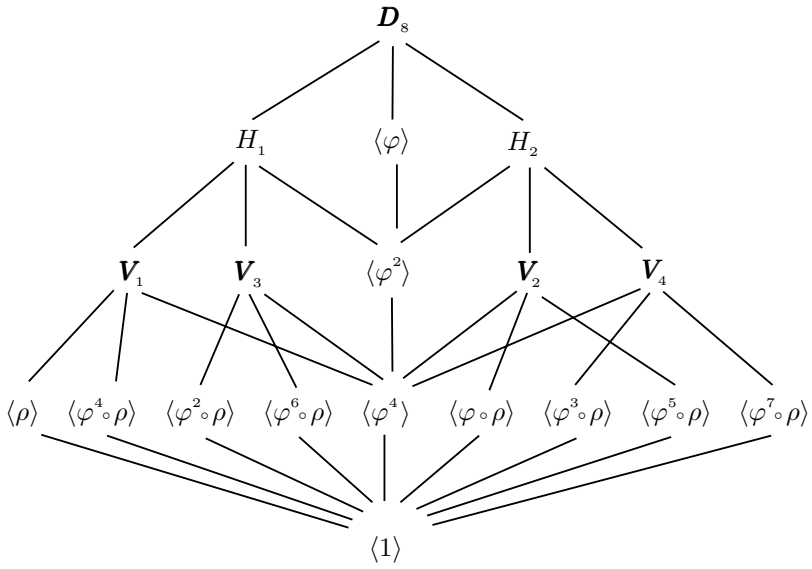
Ma è noto che:

- il gruppo (delle unità di quaternioni) $\mathbf{Q}$ possiede sei elementi di periodo 4;
- il gruppo $\boldsymbol{C}_2\times\boldsymbol{C}_4$ possiede quattro elementi di periodo 4;
- il gruppo $\boldsymbol{C}_2\times\boldsymbol{C}_2\times\boldsymbol{C}_2$ possiede sette sottogruppi di Klein.

Dunque questi tipi di sottogruppi non sono presenti in $\boldsymbol{D}_8$. Ogni eventuale sottogruppo non ciclico di ordine 8 è quindi un $\boldsymbol{D}_4$ (gruppo diedrale del quadrato). E' noto che ogni $\boldsymbol{D}_4$ possiede due elementi di periodo 4 e cinque di periodo 2; inoltre ha due sottogruppi di Klein. Conseguentemente ogni eventuale sottogruppo $H \cong \boldsymbol{D}_4$ contiene $\langle\varphi^2\rangle$. Pertanto $\boldsymbol{D}_8$ possiede i due sottogruppi:

$$H_1 = \langle\varphi^2,\, \rho\rangle = \{1,\, \varphi^2,\, \varphi^4,\, \varphi^6,\, \rho,\, \varphi^2\circ\rho,\, \varphi^4\circ\rho,\, \varphi^6\circ\rho\},$$
$$H_2 = \langle\varphi^2,\, \varphi\circ\rho\rangle = \{1,\, \varphi^2,\, \varphi^4,\, \varphi^6,\, \varphi\circ\rho,\, \varphi^3\circ\rho,\, \varphi^5\circ\rho,\, \varphi^7\circ\rho\}.$$

Non sono possibili in $\boldsymbol{D}_8$ altri $\boldsymbol{D}_4$. Se infatti $H = \langle\varphi^2,\, \varphi^k\circ\rho\rangle$ (con $0 \le k \le 7$), allora $H = H_1$ o $H = H_2$. Concludendo, il reticolo dei sottogruppi di $\boldsymbol{D}_8$ è il seguente:



* * *

7. [*Prova d'esame del 28/09/06*] È assegnato il gruppo diciclico

$$\mathbf{Q}_6 = \langle x,\, y \mid x^6 = 1,\ y^2 = x^3 = (xy)^2\rangle.$$

(*i*) Indicare gli elementi di $\mathbf{Q}_6$ ed esprimere i prodotti $y\cdot x$, $y\cdot x^2$, $y\cdot x^3$, $y\cdot x^4$, $y\cdot x^5$ come opportuni elementi della forma $x^k y$ (con $1 \le k \le 5$).

(*ii*) Determinare i periodi degli elementi di $\mathbf{Q}_6$ e dedurne il reticolo dei sottogruppi di $\mathbf{Q}_6$. Di ciascun sottogruppo ottenuto dire se è normale in $\mathbf{Q}_6$.

Soluzione. (*i*) $\mathbf{Q}_6$ contiene i dodici elementi

$$1,\, x,\, x^2,\, x^3,\, x^4,\, x^5,\, y,\, xy,\, x^2y,\, x^3y,\, x^4y,\, x^5y.$$

Inoltre, dalla relazione $xy\,xy = y^2$, segue:

$$xy\,xy = y^2 \implies xyx = y \implies x^5xyx = x^5y \implies 1\,yx = x^5y \implies yx = x^5y.$$

Dal fatto che $y\cdot x = x^5y$ segue che non esistono in $\mathbf{Q}_6$ altri elementi oltre ai dodici sopra elencati.

Calcoliamo i successivi prodotti $y\cdot x^k$ (con $2 \le k \le 5$). Si ha:

$$y\cdot x^2 = (yx)x = (x^5y)x = x^5(yx) = x^5(x^5y) = x^4y;$$
$$y\cdot x^3 = (yx)x^2 = (x^5y)x^2 = x^5(yx^2) = x^5(x^4y) = x^3y;$$
$$y\cdot x^4 = (yx)x^3 = (x^5y)x^3 = x^5(yx^3) = x^5(x^3y) = x^2y;$$
$$y\cdot x^5 = (yx)x^4 = (x^5y)x^4 = x^5(yx^4) = x^5(x^2y) = xy.$$

(*ii*) Si ha:

$$\circ(1) = 12; \quad \circ(x) = \circ(x^5) = 6; \quad \circ(x^2) = \circ(x^4) = 3; \quad \circ(x^3) = 2;$$
$$\circ(y) = \circ(xy) = \circ(x^2y) = \circ(x^3y) = \circ(x^4y) = \circ(x^5y) = 4.$$

Poiché $\mathbf{Q}_6$ ha un solo elemento di periodo 2, $\mathbf{Q}_6$ non può contenere né sottogruppi di Klein, né sottogruppi isomorfi a $\boldsymbol{S}_3$. Ne segue che $\mathbf{Q}_6$ contiene soltanto sottogruppi ciclici. Precisamente, dall'analisi dei periodi, si ha:

$\langle x\rangle = \{1, x, x^2, x^3, x^4, x^5\}$ è l'unico sottogruppo isomorfo a $\boldsymbol{C}_6$;

$\langle x^2\rangle = \{1, x^2, x^4\}$ è l'unico sottogruppo isomorfo a $\boldsymbol{C}_3$;

$\langle x^3\rangle = \{1, x^3\}$ è l'unico sottogruppo isomorfo a $\boldsymbol{C}_2$.

Esistono infine sei elementi di periodo 4, che generano tre ciclici $\boldsymbol{C}_4$. Sono:

$$\langle y\rangle = \{1, y, x^3, x^3y\}, \quad \langle xy\rangle = \{1, xy, x^3, x^4y\}, \quad \langle x^2y\rangle = \{1, x^2y, x^3, x^5y\}.$$

Si noti che $\langle x\rangle$, $\langle x^2\rangle$, $\langle x^3\rangle$ sono normali in $\mathbf{Q}_6$ [in quanto unici nel rispettivo ordine]. Invece i tre $\boldsymbol{C}_4$ (che sono 2-Sylow di $\mathbf{Q}_6$) sono non normali [ma coniugati tra loro, in base al secondo teorema di Sylow].

* * *

8. [*Prova di verifica del 16/03/07*] È assegnato il gruppo diciclico

$$\mathbf{Q}_8 = \langle x, y \mid x^8 = 1, y^2 = (xy)^2 = x^4\rangle.$$

(*i*) Determinare il reticolo dei suoi sottogruppi.

(*ii*) Verificare la formula di Burnside su $\mathbf{Q}_8$ (rispetto all'azione di coniugio) e calcolare le orbite.

Soluzione. (*i*) Dalla relazione $xy\,xy = y^2$ segue subito che $yx = x^7y$. Se ne deduce che $\mathbf{Q}_8$ ha ordine 16 ed i suoi elementi sono:

$$1, x, x^2, \ldots., x^7, y, xy, x^2y, \ldots., x^7y.$$

Si verifica facilmente che $yx^k = x^{8-k}y$ (con $1 \le k \le 7$). Inoltre $y^{-1} = x^4y$ [infatti $y^{-1} = y^3 = y^2y = x^4y$]. Esaminando i periodi degli elementi, si ottiene che $\mathbf{Q}_8$ possiede

- quattro elementi di periodo 8: x, x^3, x^5, x^7;
- un solo elemento di periodo 2: x^4;
- dieci elementi di periodo 4: $x^2, x^6, y, xy, x^2y, \ldots, x^7y$.

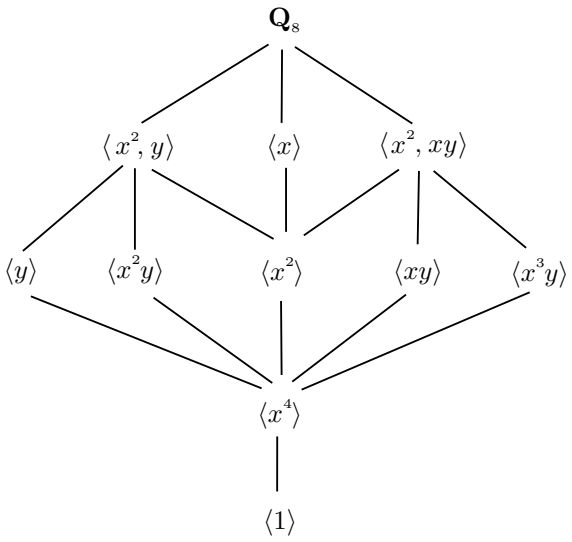
Conseguentemente, $\mathbf{Q}_8$ possiede

- un solo sottogruppo ciclico $\boldsymbol{C}_8$: $\langle x\rangle$;
- un solo sottogruppo ciclico $\boldsymbol{C}_2$: $\langle x^4\rangle$;
- cinque sottogruppi ciclici $\boldsymbol{C}_4$: $\langle x^2\rangle$, $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$, $\langle x^3y\rangle$.

Poiché $\mathbf{Q}_8$ ha un solo elemento di periodo 4, non ha sottogruppi di Klein. Per lo stesso motivo, $\mathbf{Q}_8$ non possiede gruppi diedrali $\boldsymbol{D}_4$, né gruppi isomorfi a $\boldsymbol{C}_2\times\boldsymbol{C}_4$, né gruppi isomorfi a $\boldsymbol{C}_2\times\boldsymbol{C}_2\times\boldsymbol{C}_2$. Tra i gruppi non ciclici di ordine 8, $\mathbf{Q}_8$ può quindi possedere soltanto gruppi di quaternioni, che, come noto, posseggono sei elementi di periodo 4 ed uno solo di periodo 2 (necessariamente x^4). Ogni eventuale gruppo di quaternioni $\mathbf{Q}$ contiene necessariamente il sottogruppo $\langle x^2\rangle$. Infatti, $\forall\, x^iy, x^jy \in \mathbf{Q}$, con $0 \le i < j \le 7$ e $j \ne 4+i$, risulta: $x^iy\cdot x^jy = x^ix^{8-j}x^4 = x^{4+i-j} \in \mathbf{Q}$. Poiché $\mathbf{Q}$ non ha elementi di periodo 8, allora $4+i-j \equiv 2, 6\ (mod\ 8)$ e dunque $\mathbf{Q} \supset \langle x^2\rangle$. Ma allora in $\mathbf{Q}_8$ c'è spazio soltanto per i due seguenti gruppi di quaternioni:

$\mathbf{Q}' = \langle x^2, y\rangle = \{1, x^2, y, x^2y, x^4, x^4y, x^6, x^6y\}$ $[= \langle x^2, x^2y\rangle = \langle x^2, x^4y\rangle = \langle x^2, x^6y\rangle]$;
$\mathbf{Q}'' = \langle x^2, xy\rangle = \{1, x^2, xy, x^3y, x^4, x^5y, x^6, x^7y\}$ $[= \langle x^2, x^3y\rangle = \langle x^2, x^5y\rangle = \langle x^2, x^7y\rangle]$.

Il reticolo dei sottogruppi di $\mathbf{Q}_8$ è quindi il seguente.



(*ii*) La formula di Burnside (rispetto all'azione di coniugio) fornisce il numero n delle orbite di $\mathbf{Q}_8$:

$$n = \tfrac{1}{|\mathbf{Q}_8|} \sum_{g\in\mathbf{Q}_8} |\boldsymbol{C}(g)|$$

[dove $\boldsymbol{C}(g)$ è il centralizzante di g]. Si tratta quindi di calcolare i centralizzanti di tutti i sedici elementi di $\mathbf{Q}_8$.

Si osserva subito che x^4 è l'unica potenza di x che commuta con y. Dunque $\boldsymbol{Z}(\mathbf{Q}_8) = \langle x^4\rangle$ e pertanto $\boldsymbol{C}(1) = \boldsymbol{C}(x^4) = \mathbf{Q}_8$. Le altre sei potenze x^k (con $1 \le k \le 7$, $k \ne 4$) non commutano con y dunque $\boldsymbol{C}(x^k) = \langle x\rangle$. Relativamente agli otto elementi y, xy, x^2y, ..., x^7y, si osserva che nessuno di essi commuta con x^2. Pertanto il loro centralizzante coincide con il sottogruppo da essi generato [cioè $\boldsymbol{C}(y) = \langle y\rangle$, $\boldsymbol{C}(xy) = \langle xy\rangle$, ecc.]. La formula di Burnside fornisce:

$$\tfrac{1}{16}\big(2{\cdot}16 + 6{\cdot}8 + 8{\cdot}4\big) = \tfrac{112}{16} = 7.$$

Calcoliamo le sette orbite di $\mathbf{Q}_8$. Ovviamente

$$\boldsymbol{O}(1) = \{1\}, \quad \boldsymbol{O}(x^4) = \{x^4\}.$$

Risulta poi: $|\boldsymbol{O}(x)| = \frac{|\mathbf{Q}_8|}{|\boldsymbol{C}(x)|} = \frac{16}{8} = 2$. Inoltre $yxy^{-1} = yx\,x^4y = yx^5y = x^3y^2 = x^7$. Allora $\boldsymbol{O}(x) = \{x, x^7\}$. Analogamente: $|\boldsymbol{O}(x^2)| = \frac{16}{8} = 2$ e $yx^2y^{-1} = \ldots = x^6$ e quindi $\boldsymbol{O}(x^2) = \{x^2, x^6\}$; $|\boldsymbol{O}(x^3)| = \frac{16}{8} = 2$ e $yx^3y^{-1} = \ldots = x^5$ e quindi $\boldsymbol{O}(x^2) = \{x^3, x^5\}$.

Calcoliamo infine le due ultime orbite. Si ha: $|\boldsymbol{O}(y)| = \frac{16}{4} = 4$ e

$$xyx^{-1} = xyx^7 = xxy = x^2y, \quad x^2yx^{-2} = x^2yx^6 = x^2x^2y = x^4y, \quad x^3yx^{-3} = x^3yx^5 = x^3x^3y = x^6y.$$

Dunque $\boldsymbol{O}(y) = \{y, x^2y, x^4y, x^6y\}$. Infine, per esclusione, $\boldsymbol{O}(xy) = \{y, x^3y, x^5y, x^7y\}$.

* * *

9. [*Prova di verifica del 16/03/07*] È assegnato il gruppo diciclico

$$\mathbf{Q}_{10} = \langle x, y \mid x^{10} = 1, y^2 = x^5 = (xy)^2\rangle.$$

(*i*) Determinare il reticolo dei suoi sottogruppi.

(*ii*) Determinare i quozienti di $\mathbf{Q}_{10}$ modulo i suoi sottogruppi normali.

Nota. Si utilizzi il seguente fatto: a meno di isomorfismi, i gruppi di ordine 10 sono due: $\boldsymbol{C}_{10}$, $\boldsymbol{D}_5$.

Soluzione. (*i*) Risulta subito che $yx = x^9y$. Se ne deduce che $\mathbf{Q}_{10}$ è formato dai venti elementi x^ky^i, con $0 \le k \le 9$, $0 \le i \le 1$. Esaminando i periodi degli elementi, si ottiene che $\mathbf{Q}_8$ possiede

- quattro elementi di periodo 10: x, x^3, x^7, x^9;

- quattro elementi di periodo 5: x^2, x^4, x^6, x^8;

- un solo elemento di periodo 2: x^5;

- dieci elementi di periodo 4: y, xy, x^2y, ..., x^9y.

Conseguentemente, $\mathbf{Q}_{10}$ possiede

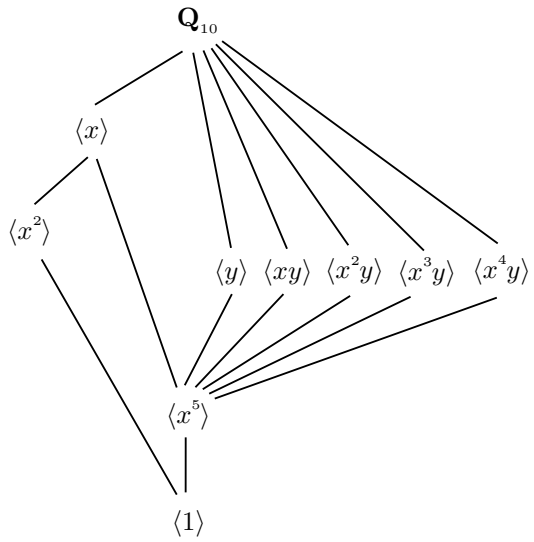
- un solo sottogruppo ciclico $\boldsymbol{C}_{10}$: $\langle x\rangle$;

- un solo sottogruppo ciclico $\boldsymbol{C}_5$: $\langle x^2\rangle$;

- un solo sottogruppo ciclico $\boldsymbol{C}_2$: $\langle x^5\rangle$;

- cinque sottogruppi ciclici $\boldsymbol{C}_4$: $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$, $\langle x^3y\rangle$, $\langle x^4y\rangle$.

Non possedendo che un solo elemento di periodo 2, $\mathbf{Q}_{10}$ non ha sottogruppi di Klein e neppure sottogruppi $\boldsymbol{D}_5$. In base alla nota precedente concludiamo che $\mathbf{Q}_{10}$ non ha altri sottogruppi propri. Dunque il suo reticolo di sottogruppi è il seguente.



(*ii*) I sottogruppi $\langle x\rangle$, $\langle x^2\rangle$, $\langle x^5\rangle$ sono normali (in quanto unici del rispettivo ordine). Invece i sottogruppi $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$, $\langle x^3y\rangle$, $\langle x^4y\rangle$ non sono normali (in quanto sono 2-Sylow, coniugati tra loro). I tre gruppi quozienti sono

$$\mathbf{Q}_{10}/_{\langle x\rangle} \cong \boldsymbol{C}_2, \quad \mathbf{Q}_{10}/_{\langle x^2\rangle}, \quad \mathbf{Q}_{10}/_{\langle x^5\rangle}.$$

Il gruppo $\mathbf{Q}_{10}/_{\langle x^2\rangle}$ ha ordine 4. Il suo elemento $\langle x^2\rangle y$ ha periodo 4 [infatti $(\langle x^2\rangle y)^2 = \langle x^2\rangle y^2 = \langle x^2\rangle x^5 = \langle x^2\rangle x$ e $(\langle x^2\rangle y)^4 = (\langle x^2\rangle x)^2 = \langle x^2\rangle$]. Ne segue che $\mathbf{Q}_{10}/_{\langle x^2\rangle} \cong \boldsymbol{C}_4$.

Il gruppo $\mathbf{Q}_{10}/_{\langle x^5\rangle}$ ha ordine 10. Se fosse ciclico, avrebbe un solo elemento di periodo 2. Ma, per $k = 0, \dots, 4$, gli elementi $\langle x^5\rangle x^k y$ (che sono a due a due distinti) hanno periodo 2 [infatti $(\langle x^5\rangle x^k y)^2 = \langle x^5\rangle (x^k y)^2 = \langle x^5\rangle y^2 = \langle x^5\rangle x^5 = \langle x^5\rangle$]. Si conclude che $\mathbf{Q}_{10}/_{\langle x^5\rangle} \cong \boldsymbol{D}_5$.

* * *

10. [*Prova di verifica del 21/03/07*] Classificare, a meno di isomorfismi, i gruppi di ordine 10.

Soluzione. Sia G un gruppo di ordine 10. G contiene 2-Sylow (di ordine 2) e 5-Sylow (di ordine 5). Siano r ed s rispettivamente il numero dei 2-Sylow e dei 5-Sylow. Dal terzo teorema di Sylow,

$$r \,\big|\, 5 \;\text{ e }\; r \equiv 1 \;(mod\, 2), \quad s \,\big|\, 2 \;\text{ e }\; s \equiv 1 \;(mod\, 5).$$

Ne segue subito che $s = 1$ e $r = 1$ oppure $r = 5$. Poiché $s = 1$, G contiene un unico 5-Sylow $K = \langle x \,\big|\, x^5 = 1\rangle$, normale in G. Sia poi $H = \langle y \,\big|\, y^2 = 1\rangle$ un 2-Sylow di G.

G possiede gli elementi

$$1,\ x,\ x^2,\ x^3,\ x^4,\ y,\ xy,\ x^2y,\ x^3y,\ x^4y.$$

Tali elementi sono a due a due distinti [se $x^k y^i = x^h y^j$, con $0 \le h, k \le 4$, $0 \le i, j \le 1$, allora $x^{k-h} = y^{j-i} = 1$ (per ragioni di periodo) e pertanto $h = k$, $i = j$] e dunque "riempono" tutto G.

Consideriamo in G il prodotto $y\cdot x$: vogliamo esprimerlo come elemento della forma $x^h y^i$ (con $0 \le h \le 4,\ 0 \le i \le 1$). Poiché K è normale in G, si ha:

$$yxy = yxy^{-1} \in yKy^{-1} = K \quad \text{e dunque } yxy = x^i \quad (\text{con } 0 \le h \le 4).$$

Si ha: $x^{i^2} = x^i \dots x^i = (yxy)(yxy)\dots(yxy) = yx^i y$. Allora (essendo $y^2 = 1$):

$$x = y^2 x y^2 = y(yxy)y = yx^i y = x^{i^2}, \text{ cioè } x^{i^2} = x.$$

Ne segue che $i^2 \equiv 1\ (mod\ 5)$. Tale equazione congruenziale ha soluzioni $i = 1,\ 4$. Pertanto

$$yxy = \begin{cases} x \\ x^4, \end{cases} \quad \text{ovvero} \quad yx = \begin{cases} xy \\ x^4 y. \end{cases}$$

Nel caso $yx = xy$, G è abeliano e quindi anche H è normale. Risulta subito che $H \cap K = \{1\}$ e $HK = G$. Ne segue che $G \cong H \times K \cong \boldsymbol{C}_2 \times \boldsymbol{C}_5 \cong \boldsymbol{C}_{10}$. Nel caso $yx = x^4 y$, risulta

$$G = \langle x, y \,|\, x^5 = y^2 = 1,\ yx = x^4 y \rangle \ \text{(gruppo diedrale del quadrato)}.$$

Concludendo, i gruppi di ordine 10 sono, a meno di isomorfismi, due: $\boldsymbol{C}_{10}$ e $\boldsymbol{D}_5$.

* * *

11. [*Prova di verifica del 23/03/07*] (*i*) Dimostrare che l'ideale (13) non è primo in $\boldsymbol{Z}[i]$, provando che $\boldsymbol{Z}[i]/_{(13)} \cong \boldsymbol{Z}_{13} \times \boldsymbol{Z}_{13}$ (anello non integro).

(*ii*) Determinare $x, y \in \boldsymbol{Z}[i]$ tali che $xy \in (13)$, ma $x, y \notin (13)$.

Soluzione. (*i*) Risulta:

$$\boldsymbol{Z}[i]/_{(13)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(13, X^2+1)/_{(X^2+1)}} \cong \frac{\boldsymbol{Z}[X]/_{(13)}}{(13, X^2+1)/_{(13)}} \cong \boldsymbol{Z}_{13}[X]/_{(X^2+\overline{1})}.$$

Poiché (in $\boldsymbol{Z}_{13}[X]$) $X^2 + \overline{1} = (X - \overline{5})(X + \overline{5})$, allora l'anello $\boldsymbol{Z}[i]/_{(13)}$ è non integro. Poiché l'ideale $(X - \overline{5},\ X + \overline{5})$ coincide con $\boldsymbol{Z}_{13}[X]$ [infatti $X + \overline{5} - (X - \overline{5}) = \overline{10}$ è invertibile in $\boldsymbol{Z}_{13}[X]$], allora

$$\boldsymbol{Z}_{13}[X]/_{(X^2+\overline{1})} \cong \boldsymbol{Z}_{13}[X]/_{(X+\overline{5})(X-\overline{5})} \cong \boldsymbol{Z}_{13}[X]/_{(X+\overline{5})} \times \boldsymbol{Z}_{13}[X]/_{(X-\overline{5})} \cong \boldsymbol{Z}_{13} \times \boldsymbol{Z}_{13}.$$

(*ii*) I polinomi $X \pm \overline{5}$ di $\boldsymbol{Z}_{13}[X]$ corrispondono (risp.) agli elementi $i \pm 5$ in $\boldsymbol{Z}[i]$. Si ha:

$$(i + 5)(i - 5) = -26 = -2 \cdot 13 \in (13),$$

ma, come ora verifichiamo, $i + 5,\ i - 5 \notin (13)$.

Infatti, se per assurdo $i + 5 \in (13)$, $i + 5 = 13(a + bi)$, $\exists\, a, b \in \boldsymbol{Z}$. Passando alle rispettive norme: $\mathcal{N}(i + 5) = \mathcal{N}(13(a + bi)) = \mathcal{N}(13)\mathcal{N}(a + bi)$. Dunque $26 = 169(a^2 + b^2)$: assurdo. In modo analogo si verifica che $i - 5 \notin (13)$.

* * *

12. [*Prova d'esonero del 26/04/06*] È assegnato l'elemento $z = 1 + 2\sqrt{-5} \in \boldsymbol{Z}[\sqrt{-5}]$.

(*i*) Fattorizzare z come prodotto di elementi irriducibili.

(*ii*) Calcolare (se esiste) $MCD(z, \overline{z})$.

(*iii*) Verificare se z è un elemento primo in $\boldsymbol{Z}[\sqrt{-5}]$.

Soluzione. (*i*) Si ha: $\mathcal{N}(z) = 1 + 4 \cdot 5 = 21$. Se $z = z_1 z_2$, risulta: $21 = \mathcal{N}(z_1)\mathcal{N}(z_2)$. Assumiamo che $\mathcal{N}(z_1) \le \mathcal{N}(z_2)$. Allora

$$(\mathcal{N}(z_1), \mathcal{N}(z_2)) = (3, 7) \ \text{oppure} \ (\mathcal{N}(z_1), \mathcal{N}(z_2)) = (1, 21).$$

Nel primo caso, posto $z_1 = a + b\sqrt{-5}$, si avrebbe $a^2 + 5b^2 = 3$; ma tale equazioni non ha soluzioni intere (come subito si osserva) e dunque in $\boldsymbol{Z}[\sqrt{-5}]$ non esistono elementi di norma 3 (e neppure 7). Si conclude che z ammette solo fattorizzazioni in cui un elemento ha norma 1, cioè è invertibile. Dunque z è irriducibile.

(*ii*) Anche $\overline{z}$ è irriducibile [infatti ha fattori coniugati a quelli di z]. Da (*i*) segue che z ha fattori $\{\pm 1, \pm z\}$, mentre $\overline{z}$ ha fattori $\{\pm 1, \pm\overline{z}\}$. I fattori comuni sono soltanto ± 1. Si conclude che $MCD(z, \overline{z}) = 1$.

(*iii*) Si ha:

$$\boldsymbol{Z}[\sqrt{-5}]\big/_{(z)} \cong \frac{\boldsymbol{Z}[X]\big/_{(X^2+5)}}{(1+2X,\, X^2+5)\big/_{(X^2+5)}} \cong \boldsymbol{Z}[X]\big/_{(1+2X,\, X^2+5)}.$$

Sia $I := (1+2X,\, X^2+5)$. Vogliamo verificare se I è primo. Si osserva che

$$I \ni (X^2+5) - 5(1+2X) = X^2 - 10X = X(X-10).$$

Se I è primo, allora $X \in I$ oppure $X - 10 \in I$. Assumiamo verificata la prima eventualità. Allora

$$\boldsymbol{Z}[X]\big/_I \cong \frac{\boldsymbol{Z}[X]\big/_{(X)}}{I\big/_{(X)}} \cong \boldsymbol{Z}\big/_{(1+2\cdot 0,\, 0^2+5))} \cong \boldsymbol{Z}\big/_{\boldsymbol{Z}} = 0.$$

Dunque $I = \boldsymbol{Z}$ e ciò è assurdo [un ideale primo non coincide con l'intero anello].

Sia invece $X - 10 \in I$. Allora

$$\boldsymbol{Z}[X]\big/_I \cong \frac{\boldsymbol{Z}[X]\big/_{(X-10)}}{I\big/_{(X-10)}} \cong \boldsymbol{Z}\big/_{(21,\, 105)} = \boldsymbol{Z}\big/_{(21)} \cong \boldsymbol{Z}_{21},$$

anello non integro: assurdo. Abbiamo provato che z non è primo.

Nota. Una dimostrazione più semplice è la seguente: poiché $z \,\big|\, z\overline{z} = 21 = 3\cdot 7$, basta verificare che $z \not| 3$ e $z \not| 7$.

Se infatti $z \,\big|\, 3$, allora $3 = (a + b\sqrt{-5})(1 + 2\sqrt{-5})$, per opportuni $a, b \in \boldsymbol{Z}$. Allora si avrebbe $3 = (a - 10b) + (2a + b)\sqrt{-5}$, da cui $a - 10b = 3$, $b = -2a$. Ne segue $7a = 1$: assurdo (in $\boldsymbol{Z}$). Se invece $z \,\big|\, 7$, allora, procedendo nello stesso modo, si ottiene $a - 10b = 7$, $b = -2a$, da cui $3a = 1$: assurdo (in $\boldsymbol{Z}$).

* * *

13. [*Prova d'esame del 10/07/06*] È assegnato il dominio $A = \boldsymbol{Z}[\sqrt{-6}]$.

(*i*) Verificare che A non è un *UFD*.

(*ii*) Fattorizzare l'elemento $2\sqrt{-6}$ in tutti i modi possibili, come prodotto di fattori irriducibili in A.

(*iii*) Verificare se l'ideale $I = (2 + 3\sqrt{-6})$ è primo in A.

Soluzione. (*i*) Come per ogni dominio $\boldsymbol{Z}[\sqrt{d}]$, con $d < -2$ e privo di fattori quadratici, basta verificare che l'elemento 2 è irriducibile ma non primo.

Infatti, se $2 = uv$, con $u, v \in A$, si ha: $4 = \mathcal{N}(u)\mathcal{N}(v)$. Siccome in A nessun elemento può avere norma 2, allora ad esempio $\mathcal{N}(u) = \pm 1$, cioè u è invertibile. Dunque 2 è irriducibile. Inoltre

$$A\big/_{(2)} \cong \boldsymbol{Z}[X]\big/_{(X^2+6,\, 2)} \cong \boldsymbol{Z}_2[X]\big/_{(X^2+\overline{6})} = \boldsymbol{Z}_2[X]\big/_{(X^2)}$$

e tale anello è ovviamente non integro $[X + (X^2)$ è uno 0-divisore]. Dunque 2 non è primo.

(*ii*) Si ha:

$$\mathcal{N}(2\sqrt{-6}) = 24 = 2\cdot 12, \text{ oppure } = 3\cdot 8, \text{ oppure } = 4\cdot 6.$$

Poiché in A non esistono elementi di norma 2 e 3, se $2\sqrt{-6} = uv$, allora $\mathcal{N}(u) = 4$, $\mathcal{N}(v) = 6$ (o viceversa). Ne segue $u = \pm 2$, $v = \pm\sqrt{-6}$. Inoltre gli elementi ± 2, $\pm\sqrt{-6}$ sono irriducibili. Ciò è già stato verificato per 2. Per $\sqrt{-6}$ si procede nello stesso modo: posto $\sqrt{-6} = uv$, con $u, v \in A$, allora $6 = \mathcal{N}(u)\mathcal{N}(v)$. Ma in A non esistono elementi di norma 2 e 3. Quindi u (ovvero v) è invertibile. Si conclude che $2\sqrt{-6}$ ammette soltanto le fattorizzzazioni (equivalenti)

$$2\sqrt{-6} = 2\cdot\sqrt{-6}, \quad 2\sqrt{-6} = (-2)\cdot(-\sqrt{-6}).$$

(*iii*) Si osservi che $\mathcal{N}(2+3\sqrt{-6}) = 58 = 2\cdot 29$. Da ciò segue subito che $2+3\sqrt{-6}$ è irriducibile. Ma non è detto a priori che sia primo. Si ha:

$$A\big/_I \cong \frac{\boldsymbol{Z}[X]\big/_{(X^2+6)}}{(2+3X,\, X^2+6)\big/_{(X^2+6)}} \cong \boldsymbol{Z}[X]\big/_{(2+3X,\, X^2+6)}.$$

Posto $H := (2 + 3X,\, X^2 + 6)$, si osserva subito che

$$H \ni X^2 + 6 - 3(2 + 3X) = X^2 - 9X = X(X - 9).$$

Ne segue che I contiene $\sqrt{-6}(\sqrt{-6} - 9)$ $[= -3(2 + 3\sqrt{-6})]$. Per concludere che I non è primo, basta verificare che I non contiene $\sqrt{-6}$ e $\sqrt{-6} - 9$. Se infatti fosse $\sqrt{-6} = \alpha(2 + 3\sqrt{-6})$, con

$\alpha \in A$, allora $6 = \mathcal{N}(\alpha)\cdot 58$, da cui $29 \,|\, 6$: assurdo. Se invece fosse $-9+\sqrt{-6} = \beta(2+3\sqrt{-6})$, con $\beta \in A$, allora $87 = \mathcal{N}(\beta)\cdot 58$, da cui $3 = N(\beta)\cdot 2$: assurdo.

* * *

14. [*Prova d'esame del 28/09/06*] (*i*) Verificare che l'anello $A = \boldsymbol{Z}[X]/_{(X^3-2)}$ è un dominio d'integrità. Indicarne un elemento non invertibile (e non nullo).

(*ii*) Posto $x := X + (X^3-2)$, verificare se gli elementi $1+x$, $1+x^2$, $1+x+x^2$ sono irriducibili in A.

(*iii*) Fattorizzare $2 + (X^3-2)$ come prodotto di fattori iriducibili in A.

Soluzione. (*i*) Il polinomio $X^3 - 2 \in \boldsymbol{Z}[X]$ è irriducibile (dal criterio di Eisenstein). Ne segue che è un elemento primo [infatti $\boldsymbol{Z}[X]$ è un *UFD*]. Pertanto A è un dominio d'integrità.

Si ponga $A = \boldsymbol{Z}[x \,|\, x^3 = 2]$. Verifichiamo che ad esempio $2 \in A$ non è invertibile. Infatti $A \subset \boldsymbol{Q}[X]/_{(X^3-2)} = \boldsymbol{Q}(\sqrt[3]{2})$ ed in tale campo 2 ha inverso $\frac{1}{2}$. Se 2 fosse invertibile in A, avrebbe lo stesso inverso. Ma $\frac{1}{2} \notin A$.

(*ii*) Si ha:

$$A/_{(1+x)} \cong \frac{\boldsymbol{Z}[X]/_{(X^3-2)}}{(1+X, X^3-2)/_{(X^3-2)}} \cong \boldsymbol{Z}[X]/_{(1+X, X^3-2)} \cong \frac{\boldsymbol{Z}[X]/_{(X+1)}}{(X+1, X^3-2)/_{(X+1)}} \cong \boldsymbol{Z}/_{((-1)^3-2)} \cong \boldsymbol{Z}_3.$$

Dunque $A/_{(1+x)}$ è un campo e pertanto $(1+x)$ è primo (massimale). Pertanto $1+x$ è irriducibile.

Analogamente,

$$A/_{(1+x^2)} \cong \boldsymbol{Z}[X]/_{(1+X^2, X^3-2)} \cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(X+1, X^3-2)/_{(X^2+1)}} = \boldsymbol{Z}[i]/_{(i^3-2)} = \boldsymbol{Z}[i]/_{(-i-2)} \cong$$

$$\cong \frac{\boldsymbol{Z}[X]/_{(X^2+1)}}{(X+2, X^2+1)/_{(X^2+1)}} \cong \frac{\boldsymbol{Z}[X]/_{(X+2)}}{(X+2, X^2+1)/_{(X+2)}} \cong \boldsymbol{Z}/_{(5)} \cong \boldsymbol{Z}_5.$$

Anche in questo caso $A/_{(1+x^2)}$ è un campo e quindi $1+x^2$ è irriducibile.

Veniamo ora all'elemento $1+x+x^2$. Poniamo $J := (1+X+X^2, X^3-2)$. Se verifichiamo che $J = \boldsymbol{Z}[X]$, allora $1+x+x^2$ è invertibile in A (e dunque non irriducibile). Posto $f := X^3-2$, $g := 1+X+X^2$, si verifica infatti subito che $g(X-1) - f = 1$. Dunque $1 \in J$.

Nota. Si ha, in A: $1 = 2-1 = x^3-1 = (x-1)(x^2+x+1)$.

(*iii*) Si ha, in A: $2 = x^3 = x\cdot x\cdot x$. Se verifichiamo che x è irriducibile, allora abbiamo una fattorizzazione di 2 cercata. Si ha infatti:

$$A/_{(x)} \cong \frac{\boldsymbol{Z}[X]/_{(X^3-2)}}{(X, X^3-2)/_{(X^3-2)}} \cong \boldsymbol{Z}[X]/_{(X, X^3-2)} = \boldsymbol{Z}[X]/_{(X, 2)} \cong \boldsymbol{Z}_2 \text{ (campo)}.$$

* * *

15. [*Prova d'esame del 12/06/06*] Sia p un primo e siano $F = Y - X^2 - \overline{1}$, $G = X + Y^2 \in \boldsymbol{Z}_p[X,Y]$. Sia I l'ideale generato da F, G.

(*i*) Esprimere l'anello quoziente $\boldsymbol{Z}_p[X,Y]/_I$ come quoziente dell'anello $\boldsymbol{Z}[X]$.

(*ii*) Dire se l'ideale I è primo o massimale, per $p = 2$ e $p = 3$.

Soluzione. (*i*) Si ponga $J = (F)$. Si ha:

$$\boldsymbol{Z}_p[X,Y]/_J \cong \boldsymbol{Z}_p[X][Y]/_{(Y-(X^2+\overline{1}))} \cong \boldsymbol{Z}_p[X]$$

[quest'ultimo isomorfismo trasforma un arbitrario polinomio $H(Y) \in \boldsymbol{Z}_p[X][Y]$ nel polinomio $H(X^2+\overline{1}) \in \boldsymbol{Z}_p[X]$]. In particolare,

$$\boldsymbol{Z}_p[X,Y]/_I \cong \frac{\boldsymbol{Z}_p[X,Y]/_J}{I/_J} \cong \boldsymbol{Z}_p[X]/_{(G(X^2+\overline{1}))} = \boldsymbol{Z}_p[X]/_{(X+(X^2+\overline{1})^2)} \cong \boldsymbol{Z}[X]/_{(p,\, X+(X^2+\overline{1})^2)}$$

(*ii*) Per $p=2$, $X+(X^2+\overline{1})^2 = X+X^4+\overline{1}$ e tale polinomio è irriducibile in $\boldsymbol{Z}_2[X]$. Infatti non ha zeri in $\boldsymbol{Z}_2$ e l'unico polinomio irriducibile di grado 2 in $\boldsymbol{Z}_2[X]$ [cioè $X^2+X+\overline{1}$] non ne è fattore, come subito si verifica eseguendo la divisione euclidea. Ne segue che $\boldsymbol{Z}_2[X,Y]\big/_I$ è un campo, cioè I è massimale.

Sia $p=3$. In tal caso $X+(X^2+\overline{1})^2 = X^4+\overline{2}X^2+X+\overline{1}$. Tale polinomio si fattorizza su $\boldsymbol{Z}_3[X]$ nella forma

$$X^4+\overline{2}X^2+X+\overline{1} = (X+\overline{1})(X^3+\overline{2}X^2+\overline{1}).$$

Ne segue che $\boldsymbol{Z}_3[X,Y]\big/_I$ non è integro, cioè I non è primo.

* * *

16. [*Prova d'esame del 6/02/07*] È assegnato l'anello $A = \boldsymbol{Z}_2[X,Y]\big/_I$, con $I=(X^2,\,Y^3)$.

(*i*) Verificare che A è un anello finito, indicarne il generico elemento e la cardinalità.

(*ii*) Verificare che A possiede un unico ideale primo.

(*iii*) Determinare l'inverso dell'elemento $(\overline{1}+X+Y)+I \in A$.

Soluzione. (*i*) Poiché $(X^2)\subset I$, allora

$$A\big/_I \cong \frac{\boldsymbol{Z}_2[X,Y]\big/_{(X^2)}}{I\big/_{(X^2)}} =: B\big/_J, \;\text{ con }\; B := \boldsymbol{Z}_2[X,Y]\big/_{(X^2)},\;\; J := I\big/_{(X^2)}.$$

Si ha: $B \cong \boldsymbol{Z}_2[x\,|\,x^2=\overline{0}][Y]$ e quindi

$$A\big/_I \cong B\big/_J = \boldsymbol{Z}_2[x,\,y\,|\,x^2=y^3=\overline{0}] =$$
$$= \{a+bx+cy+dxy+ey^2+fxy^2,\;\forall\, a,b,c,d,e,f\in\boldsymbol{Z}_2;\; x^2=y^3=\overline{0}\}.$$

Si tratta quindi di un anello finito, con $2^6=64$ elementi.

(*ii*) Sia $P\big/_I$ un ideale di A, con P ideale di $\boldsymbol{Z}_2[X,Y]$, $P\supseteq I$. È noto che

$$\text{l'ideale } P\big/_I \text{ è primo in } A \iff \text{l'ideale } P \text{ è primo in } \boldsymbol{Z}_2[X,Y].$$

Se $P\supseteq I=(X^2,\,Y^3)$ e P è primo, allora $P\supseteq(X,Y)$, massimale in $\boldsymbol{Z}_2[X,Y]$. Dunque $P=(X,Y)$. Ne segue che l'unico ideale massimale (e quindi primo) di A è $(X,Y)\big/_I =: (x,y)$.

(*iii*) Gli elementi di $A-(x,y)$ sono tutti e soli gli elementi invertibili di A. In particolare, $\overline{1}+x+y$ è invertibile in A. Per calcolarne l'inverso si ponga:

$$\overline{1} = (\overline{1}+x+y)(a+bx+cy+dxy+ey^2+fxy^2).$$

Sviluppando il prodotto, raccogliendone a fattor comune gli addendi e confrontando i due membri dell'uguaglianza, si ottiene il sistema lineare (a valori in $\boldsymbol{Z}_2$):

$$\begin{cases} a=\overline{1}, & d+b+c=\overline{1},\\ a+b=\overline{0}, & c+e=\overline{0},\\ a+c=\overline{0}, & e+d+f=\overline{0}. \end{cases}$$

Ne segue: $a=b=c=e=f=\overline{1}$, $d=\overline{0}$. Pertanto in A:

$$(\overline{1}+x+y)^{-1} = \overline{1}+x+y+y^2+xy^2.$$

* * *

17. [*Prova di verifica del 28/03/07*] È assegnato l'ideale (X^2+1) in $\boldsymbol{Q}[X,Y]$.

i) Determinare l'anello quoziente $\boldsymbol{Q}[X,Y]\big/_{(X^2+1)}$ e dedurne che (X^2+1) è un ideale primo, non massimale in $\boldsymbol{Q}[X,Y]$.

ii) Dimostrare che lo spettro $Spec\big(\boldsymbol{Q}[X,Y]_S\big)$, con $S=\boldsymbol{Q}[X,Y]-(X^2+1)$, è formato da un solo primo non nullo.

Soluzione. *i*) Si consideri l'applicazione $\varphi:\boldsymbol{Q}[X,Y]\to\boldsymbol{C}[Y]$ tale che $\varphi(X)=i$, $\varphi(Y)=Y$ e

$$\varphi\big(\textstyle\sum a_{hk}X^hY^k\big) = \sum a_{hk}i^hY^k,\;\; \forall\, \sum a_{hk}X^hY^k \in \boldsymbol{Q}[X,Y].$$

Si verifica facilmente che φ è un omomorfismo di anelli.

Proviamo che $Ker\varphi = (X^2+1)$. Ovviamente $\varphi(X^2+1) = i^2+1 = 0$ e quindi $(X^2+1) \subseteq Ker\varphi$. Viceversa, sia $F \in Ker\varphi$. Dividendo F per X^2+1 [in $\boldsymbol{Q}[Y][X]$), si ottiene

$$F = (X^2+1)\cdot Q + R, \text{ con } R = A(Y) + X\,B(Y),\ A(Y),\ B(Y) \in \boldsymbol{Q}[Y].$$

Si ha: $0 = \varphi(F) = 0\cdot Q + A(Y) + i\,B(Y)$. Ne segue che $A(Y) = B(Y) = 0$, cioè $R = 0$. Pertanto $F \in (X^2+1)$, cioè $Ker\varphi \subseteq (X^2+1)$.

Calcoliamo $Im\varphi$. Risulta, $\forall\, F = \sum a_{hk}X^hY^k \in \boldsymbol{Q}[X,Y]:\ \varphi(F) = \sum a_{hk}i^hY^k \in \boldsymbol{Q}(i)[Y]$.

Viceversa, $\forall\, P = \sum(\alpha_h + i\beta_h)Y^h \in \boldsymbol{Q}(i)[Y]$ (con $\alpha_h + i\beta_h \in \boldsymbol{Q}(i)$) si ha: $\varphi\big(\sum(\alpha_h + X\beta_h)Y^h\big) = P$ e dunque $P \in Im\varphi$. Pertanto $Im\varphi = \boldsymbol{Q}(i)[Y]$.

Allora $\boldsymbol{Q}[X,Y]\big/_{(X^2+1)} \cong \boldsymbol{Q}(i)[Y]$ (dominio d'integrità non campo) e quindi (X^2+1) è un ideale primo non massimale in $\boldsymbol{Q}[X,Y]$.

(*ii*) Risulta:

$$Spec\big(\boldsymbol{Q}[X,Y]_S\big) = \big\{\mathfrak{p}_S,\ \ \forall\,\mathfrak{p} \in Spec(\boldsymbol{Q}[X,Y]) \text{ tale che } \mathfrak{p} \subseteq (X^2+1)\big\}.$$

Certamente l'ideale $(X^2+1)\boldsymbol{Q}[X,Y]_S$ è primo in $\boldsymbol{Q}[X,Y]_S$ ed anzi è l'unico massimale in $\boldsymbol{Q}[X,Y]_S$. Vogliamo verificare che tale ideale è l'unico elemento di $Spec\big(\boldsymbol{Q}[X,Y]_S\big)$, dimostrando che

$$\mathfrak{p} \subset (X^2+1) \implies \mathfrak{p} = (0).$$

Per assurdo, sia $\mathfrak{p} \neq (0)$ e $T \in \mathfrak{p}^{\cdot}$. Poiché $T \in \mathfrak{p} \subset (X^2+1)$, allora $T = B_1\cdot(X^2+1)$, $\exists\, B_1 \in \boldsymbol{Q}[X,Y]^{\cdot}$. Poiché $X^2+1 \notin \mathfrak{p}$ e $T \in \mathfrak{p}$, allora $B_1 \in \mathfrak{p}$. Ne segue che $B_1 = B_2(X^2+1)$, $\exists\, B_2 \in \boldsymbol{Q}[X,Y]^{\cdot}$. Allora $T = B_2\cdot(X^2+1)^2$.

Analogamente, $B_2 \in \mathfrak{p}$ [perché $(X^2+1)^2 \notin \mathfrak{p}$] e quindi $B_2 = B_3\cdot(X^2+1)$, $\exists\, B_3 \in \boldsymbol{Q}[X,Y]^{\cdot}$, cioè $T = B_3\cdot(X^2+1)^3$. Proseguendo in questo modo, $T = B_k\cdot(X^2+1)^k$, $\forall\, k \geq 1$. Ciò è palesemente assurdo (per ragioni di grado).

* * *

18. [*Prova di verifica del 4/04/07*] Sia A un *ED*, con valutazione euclidea $v : A^{\cdot} \to \boldsymbol{N}$. Fissato un elemento $s \in A^{\cdot}$, si consideri la parte moltiplicativa $S = \{s^k\}_{k\geq 0}$. Verificare che la seguente applicazione

$$\tilde{v} : A_S^{\cdot} \to \boldsymbol{N} \text{ tale che } \tilde{v}\big(\tfrac{a}{s^k}\big) = v(a'),\ \text{se } \tfrac{a}{s^k} = \tfrac{a'}{s^h},\ \text{con } MCD(a',s) = 1,$$

è una ben definita valutazione euclidea [e dunque anche A_S è un *ED*].

Nota. È vero, più in generale, che ogni anello di frazioni di un *ED* è un *ED*.

Soluzione. Proviamo che l'elemento a' (definito nella definizione di $\tilde{v}$) esiste ed è completamente individuato (a meno di un fattore invertibile) da $\frac{a}{s^k}$.

Infatti, essendo s irriducibile, allora $MCD(a,s) = 1$ oppure $s \,\big|\, a$. In quest'ultimo caso, $a = a's^r$, con $MCD(a',s) = 1$ e dunque $\frac{a}{s^k} = \frac{a'}{s^{k-r}}$. Se poi $\frac{a}{s^k} = \frac{a'}{s^h} = \frac{a''}{s^t}$, con $MCD(a',s) = MCD(a'',s) = 1$, allora $a's^t = a''s^h$ e quindi (dal Lemma di Euclide) $a' \,\big|\, a''$ e $a'' \,\big|\, a'$. Dunque $a' = a''u$, $\exists u \in \mathcal{U}(A)$.

Poiché è noto che, alterando un elemento per un elemento invertibile, la valutazione euclidea non cambia (cfr. Eserc. **3.3.12**), allora $v(a') = v(a'')$. Dunque $\tilde{v}$ è un'applicazione ben definita.

Per provare che $\tilde{v}$ è una valutazione euclidea, bisogna verificare due condizioni:

(*i*) $\tilde{v}\big(\tfrac{a}{s^k}\cdot\tfrac{b}{s^h}\big) \geq \tilde{v}\big(\tfrac{a}{s^k}\big),\ \ \forall\, \tfrac{a}{s^k},\ \tfrac{b}{s^h} \in A_S^{\cdot}$.

Infatti: $\tilde{v}\big(\tfrac{a}{s^k}\cdot\tfrac{b}{s^h}\big) = \tilde{v}\big(\tfrac{ab}{s^{h+k}}\big)$. Se $\frac{a}{s^k} = \frac{a'}{s^t}$ e $\frac{b}{s^h} = \frac{b'}{s^n}$, con a', b' coprimi con s, allora $\frac{ab}{s^{h+k}} = \frac{a'b'}{s^{t+n}}$, con $MCD(a'b',s) = 1$. Dunque $\tilde{v}\big(\tfrac{a}{s^k}\cdot\tfrac{b}{s^h}\big) = \tilde{v}\big(\tfrac{ab}{s^{h+k}}\big) = v(a'b') \geq v(a') = \tilde{v}\big(\tfrac{a}{s^k}\big)$, come richiesto.

(*ii*) $\forall\ \forall\, \tfrac{a}{s^k},\ \tfrac{b}{s^t} \in A_S^{\cdot},\ \exists Q, R \in A_S$ tali che $\frac{a}{s^k} = \frac{b}{s^t}\cdot Q + R$, con $R = 0$ oppure $\tilde{v}(R) < \tilde{v}\big(\tfrac{a}{s^k}\big)$.

Sia $\frac{b}{s^t} = \frac{b'}{s^\ell}$, con $MCD(s,b') = 1$. Essendo A un *ED*, si ha: $a = b'q + r$, con $r = 0$ oppure $v(r) < v(b')$. Ne segue:

$$\tfrac{a}{s^k} = b'\cdot\tfrac{q}{s^k} + \tfrac{r}{s^k} = \tfrac{b'}{s^\ell}\cdot\tfrac{qs^\ell}{s^k} + \tfrac{r}{s^k} = \tfrac{b}{s^t}\cdot Q + R,\ \text{con } Q := \tfrac{qs^\ell}{s^k},\ R := \tfrac{r}{s^k}.$$

Se $r = 0$, allora $R = 0$. Se $r \neq 0$, allora $\tilde{v}(R) = \tilde{v}\big(\tfrac{r}{s^k}\big) = \tilde{v}\big(\tfrac{r'}{s^n}\big)$, con $\frac{r}{s^k} = \frac{r'}{s^n}$ e $MCD(r',s) = 1$. Ne segue che $rs^n = r's^k$ e quindi (dal Lemma di Euclide) $r' \,\big|\, r$ Allora $r = r'c$, $\exists\, c \in A$, e quindi $v(r) = v(r'c) \geq v(r') = \tilde{v}(R)$, cioè $\tilde{v}(R) < \tilde{v}\big(\tfrac{a}{s^k}\big)$, come richiesto.

* * *

19. [*Prova d'esonero del 9/06/06*] Verificare che $\boldsymbol{Z}_2(X^2)$ è un sottocampo di $\boldsymbol{Z}_2(X^3, X^7)$ e che l'estensione $\boldsymbol{Z}_2(X^2) \subseteq \boldsymbol{Z}_2(X^3, X^7)$ è algebrica semplice. Indicarne il grado e dire se è normale e separabile.

Soluzione. Si ha: $\frac{(X^7)^2}{(X^3)^4} = X^2$. Dunque $\boldsymbol{Z}_2(X^2) \subseteq \boldsymbol{Z}_2(X^3, X^7)$. Inoltre $\frac{X^7}{(X^3)^2} = X$. Quindi $\boldsymbol{Z}_2(X^3, X^7) = \boldsymbol{Z}_2(X)$. Si ha subito che $X \notin \boldsymbol{Z}_2(X^2)$ ed il polinomio minimo di X in $\boldsymbol{Z}_2(X^2)[T]$ è $T^2 - X^2$. [Tale polinomio è ovviamente irriducibile in quanto $X \notin \boldsymbol{Z}_2(X^2)$]. Risulta pertanto

$$[\boldsymbol{Z}_2(X^3, X^7) : \boldsymbol{Z}_2(X^2)] = 2.$$

Poiché l'estensione ha grado 2, è normale. Infine $T^2 - X^2 = (T - X)^2$ (in $\boldsymbol{Z}_2(X)[T]$). Dunque l'estensione non è separabile.

* * *

20. [*Prova d'esonero del 9/06/06*] Assegnato il pentagono regolare standard $\boldsymbol{\mathcal{P}}_5$, verificare se sono costruibili con riga e compasso:

(*i*) un quadrato $\boldsymbol{\mathcal{Q}}$, il cui perimetro coincide con quello di $\boldsymbol{\mathcal{P}}_5$.

(*ii*) un quadrato $\boldsymbol{\mathcal{Q}}'$, la cui area eguaglia quella di $\boldsymbol{\mathcal{P}}_5$.

[Si assuma come noto il fatto che $\cos(\frac{2\pi}{5}) = \frac{G^{-1}}{2}$, dove $G = \frac{1+\sqrt{5}}{2}$ è il rapporto aureo].

Soluzione. (*i*) UP è un lato di $\boldsymbol{\mathcal{P}}_5$ (cfr. figura). Si ha:

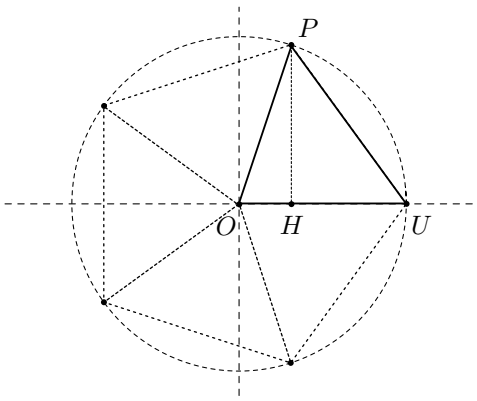
$$\overline{UP} = \sqrt{(\tfrac{G^{-1}}{2} - 1)^2 + (\sin(\tfrac{2\pi}{5}) - 0)^2} = \sqrt{\tfrac{G^{-2}}{4} + 1 - G^{-1} + 1 - \tfrac{G^{-2}}{4}} = \sqrt{2 - G^{-1}} = \sqrt{\tfrac{5-\sqrt{5}}{2}}.$$

Allora $\boldsymbol{\mathcal{P}}_5$ ha perimetro $5\sqrt{\frac{5-\sqrt{5}}{2}}$ e dunque $\boldsymbol{\mathcal{Q}}$ ha lato $\ell = \frac{5}{4}\sqrt{\frac{5-\sqrt{5}}{2}}$.

Si tratta di verificare che ℓ è costruibile con riga e compasso [abbr. *R&C*]. Basta verificare che $[\boldsymbol{Q}(\ell) : \boldsymbol{Q}] = 4$ e che esiste una catena di estensioni di grado 2 tra $\boldsymbol{Q}$ e $\boldsymbol{Q}(\ell)$, cioè

$$\boldsymbol{Q} \subset K \subset \boldsymbol{Q}(\ell).$$

Basta porre: $\alpha = \frac{5-\sqrt{5}}{2}$, $\beta = \sqrt{\alpha}$ e $K = \boldsymbol{Q}(\alpha)$. Ovviamente $\boldsymbol{Q}(\ell) = \boldsymbol{Q}(\beta)$, $[\boldsymbol{Q}(\beta) : K] = 2$ e $[K : \boldsymbol{Q}] = 2$.



(*ii*) L'interno di $\boldsymbol{\mathcal{P}}_5$ è unione di cinque triangoli congruenti al triangolo OPU (cfr. figura). Ne segue che l'area $\mathcal{A}(\boldsymbol{\mathcal{P}}_5)$ è cinque volte quella di tale triangolo. Calcoliamo tale area:

$$\mathcal{A}(OPU) = \tfrac{1}{2}\overline{OU}\cdot\overline{PH} = \tfrac{1}{2}\cdot 1\cdot\sin(\tfrac{2\pi}{5}) = \tfrac{1}{2}\sqrt{1 - \tfrac{G^{-2}}{4}} = \tfrac{1}{4}\sqrt{4 - G^{-2}}.$$

Dunque

$$\mathcal{A}(\boldsymbol{\mathcal{P}}_5) = \tfrac{5}{4}\sqrt{4 - G^{-2}} = \tfrac{5}{4}\sqrt{4 - G^{-2}} = \tfrac{5}{4}\sqrt{\tfrac{5+\sqrt{5}}{2}}.$$

Un quadrato $\boldsymbol{\mathcal{Q}}'$ richiesto ha lato $\ell' = \sqrt{\frac{5}{4}\sqrt{\frac{5+\sqrt{5}}{2}}}$. Si tratta di verificare che ℓ' è costruibile con *R&C*. Si ponga $\alpha = \frac{5+\sqrt{5}}{2}$ e $\beta = \sqrt{\alpha}$. Allora $\ell' = \sqrt{\frac{5}{4}\beta}$ e

$$\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha) \subset \boldsymbol{Q}(\beta) \subset \boldsymbol{Q}(\ell')$$

Inoltre $[\boldsymbol{Q}(\ell') : \boldsymbol{Q}] = 8$. Ciò è sufficiente a concludere che ℓ' è costruibile con *R&C*.

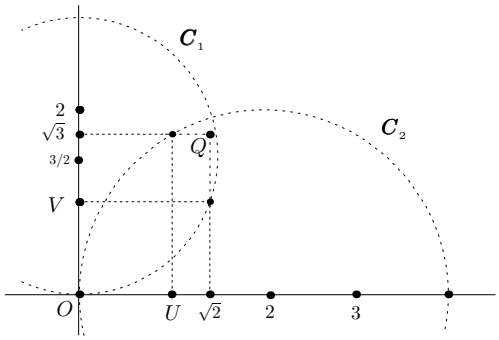
* * *

21. [*Prova di verifica del 4/05/07*] Assegnato in $\boldsymbol{E}^2$ un riferimento cartesiano antiorario $RC(O,U)$, costruire con *R&C* il punto $Q = (\sqrt{2}, \sqrt{3})$.

Soluzione. La radice quadrata di un numero razionale viene costruita con *R&C* utilizzando il secondo teorema di Euclide. Si costruiscono le due circonferenze:

$$\boldsymbol{C}_1, \text{ di centro } (0, \tfrac{3}{2}) \text{ e raggio } \tfrac{3}{2}; \quad \boldsymbol{C}_2, \text{ di centro } (2,0) \text{ e raggio } 2.$$

La retta parallela all'*asse x* e passante per V interseca $\boldsymbol{C}_1$ nel punto $(\sqrt{2}, 1)$. La retta parallela all'*asse y* e passante per U interseca $\boldsymbol{C}_2$ nel punto $(1, \sqrt{3})$. Interesecando le due rette $X = \sqrt{2}$, $Y = \sqrt{3}$, si costruisce il punto $Q = (\sqrt{2}, \sqrt{3})$.



* * *

22. [*Prova di verifica del 4/05/07*] Dimostrare che è possibile "quadrare" con *R&C* un triangolo equilatero di lato 1.

Se $\mathcal{T}$ è il triangolo di vertici A, B, C in $\boldsymbol{\mathcal{P}}_0$, è possibile "quadrare" $\mathcal{T}$ con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$?

Soluzione. Un triangolo equilatero $\mathcal{T}$ di lato 1 ha area $\mathcal{A} = \frac{1}{2}\,1 \cdot \frac{\sqrt{3}}{2} = \frac{\sqrt{3}}{4}$. Pertanto:

$$\mathcal{T} \text{ è quadrabile con } R\&C \iff \exists\, \ell \in \boldsymbol{R},\ \ell > 0, \text{ costruibile con } R\&C, \text{ tale che } \ell^2 = \mathcal{A}$$
$$\iff \ell = \tfrac{1}{2}\sqrt[4]{3} \text{ è costruibile con } R\&C.$$

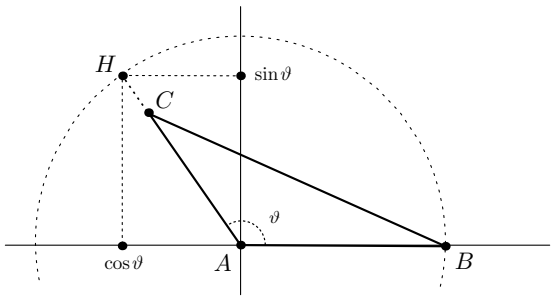
Il numero reale $\sqrt[4]{3}$ è facilmente costruibile con *R&C*. Basta infatti costruire con *R&C* (utilizzando il secondo teorema di euclide) prima $\sqrt{3}$ e poi $\sqrt{\sqrt{3}}$. Ne segue che ℓ è costruibile con *R&C*.

Sia ora $\mathcal{T} = ABC$ un triangolo con vertici in $\boldsymbol{\mathcal{P}}_0$. È noto che l'area $\mathcal{A} = \mathcal{A}(\mathcal{T})$ è data da

$$\tfrac{1}{2}\,\|\,\overrightarrow{AB} \wedge \overrightarrow{AC}\,\| = \tfrac{1}{2}\,\overline{AB}\cdot\overline{AC}\,\sin\vartheta.$$

Poiché $A, B, C \in \boldsymbol{\mathcal{P}}_0$, i numeri reali $\overline{AB}$ e $\overline{AC}$ sono costruibili con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$. Verifichiamo che anche $\sin\vartheta$ è costruibile con *R&C* a partire da $\boldsymbol{\mathcal{P}}_0$.

A tale scopo conviene scegliere il riferimeno cartesiano $RC(A,B)$, come illustrato in figura.



Il punto $\sin\vartheta$ è così costruito: si interseca la retta $R(A,C)$ con la circonferenza $\boldsymbol{C}(A,1)$ e si ottiene il punto H; poi si interseca con l'*asse y* la retta per H parallela all'*asse x*.

Avendo provato che $\mathcal{A} = \mathcal{A}(\mathcal{T})$ è costruibile con $R\&C$ a partire da $\boldsymbol{\mathcal{P}}_0$, allora è costruibile il numero reale $\sqrt{\mathcal{A}}$, e quindi è costruibile con $R\&C$ il quadrato avente per lato $\sqrt{\mathcal{A}}$.

* * *

23. [*Prova di verifica del 9/05/07*] È vero che l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{\sqrt{2}+\sqrt[3]{2}})$ è radicale?

Soluzione. Ovviamente $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{2}+\sqrt[3]{2}) \subseteq \boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ e l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ è radicale ed ha grado 6. Se verifichiamo che anche l'estensione $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{2}+\sqrt[3]{2})$ ha grado 6, risulta allora che $\boldsymbol{Q}(\sqrt{2}+\sqrt[3]{2}) = \boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ e dunque $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{2}+\sqrt[3]{2})$ è radicale. Dall'esercizio precedente segue subito che l'assegnata estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\sqrt{\sqrt{2}+\sqrt[3]{2}})$ è radicale.

Si ponga $\alpha = \sqrt{2}+\sqrt[3]{2}$. Da $\alpha - \sqrt{2} = \sqrt[3]{2}$, elevando al cubo si ottiene $\alpha^3 - 6\alpha - 2 = \sqrt{2}(3\alpha^2 - 2)$. Quadrando, $\alpha^6 - 6\alpha^4 - 4\alpha^3 + 12\alpha^2 - 24\alpha - 4 = 0$. Dunque α è zero del polinomio

$$f = X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4 \in \boldsymbol{Q}[X].$$

Si tratta ora di verificare che tale polinomio è irriducibile in $\boldsymbol{Q}[X]$. Certamente f non ha fattori lineari [basta verificare che $f(\pm1)$, $f(\pm2)$, $f(\pm4) \neq 0$] e perciò neppure fattori di grado 5. per provare che non ha fattori di gradi 2, 3, 4 è sufficiente verificare che non esiste alcun polinomio di tali gradi a coefficienti in $\boldsymbol{Q}$ che ammette α come zero. Si ponga:

$$p = X^2 + aX + b,\ \ q = X^3 + aX^2 + bX + c,\ \ h = X^4 + aX^3 + bX^2 + cX + d,\ \text{ con } a,b,c,d \in \boldsymbol{Q}.$$

Se $p(\alpha) = 0$, allora

$$2 + b + a\sqrt{2} + a\sqrt[3]{2} + \sqrt[3]{4} + 2\sqrt{2}\sqrt[3]{4} = 0.$$

Si tratta di una combinazione lineare non banale dell'insieme $S := \{1,\ \sqrt{2},\ \sqrt[3]{2},\ \sqrt[3]{4},\ \sqrt{2}\sqrt[3]{2},\ \sqrt{2}\sqrt[3]{4}\}$ (che è una base di $\boldsymbol{Q}(\sqrt{2},\sqrt[3]{2})$ su $\boldsymbol{Q}$. Da qui un assurdo.

Se $q(\alpha) = 0$, si ottiene:

$$(c + 2a + 2) + (2 + b)\sqrt{2} + (6 + b)\sqrt[3]{2} + a\sqrt[3]{4} + 2\sqrt{2}\sqrt[3]{4} + 2a\sqrt{2}\sqrt[3]{2}.$$

Si è ottenuta un'altra combinazione lineare non banale di S: assurdo.

Infine, se $h(\alpha) = 0$, allora

$$(4 = d + 2a + 2b) + (8 + 2a + c)\sqrt{2} + (2 + 6a + c)\sqrt[3]{2} + (12 + b)\sqrt[3]{4} + (8 + 2b)\sqrt{2}\sqrt[3]{4} + 3a\sqrt{2}\sqrt[3]{2} = 0.$$

Anche tale combinazione lineare di S è non banale: assurdo.

Si conclude che f è irriducibile e, come richiesto, che $[\boldsymbol{Q}(\sqrt{2}+\sqrt[3]{2}) : \boldsymbol{Q}] = 6$.

Nota. Una sequenza radicale di $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{\sqrt{2}+\sqrt[3]{2}})$ è data da $\{\sqrt{2}, \sqrt[3]{2},\ \sqrt{\sqrt{2}+\sqrt[3]{2}}\}$.

* * *

24. [*Prova d'esonero del 9/06/06*] Si consideri l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$, con $\alpha = \sqrt{3} + i\sqrt{5}$.

(*i*) Determinare il polinomio minimo dell'elemento α su $\boldsymbol{Q}$.

(*ii*) Verificare se l'estensione assegnata è normale.

(*iii*) Determinare i campi intermedi dell'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$.

Soluzione. (*i*) Si ha: $\alpha^2 = -2 + 2i\sqrt{15}$. Allora $(\alpha^2+2)^2 = 4i^2 \cdot 15 = -60$. Dunque $\alpha^4 + 4\alpha^2 + 64 = 0$ e pertanto α è zero del polinomio $m = X^4 + 4X^2 + 64 \in \boldsymbol{Q}[X]$.

Il polinomio m si fattorizza in $\boldsymbol{C}[X]$ nella forma

$$m = (X - \sqrt{-2 + 2i\sqrt{15}})(X - \sqrt{-2 - 2i\sqrt{15}})(X + \sqrt{-2 + 2i\sqrt{15}})(X + \sqrt{-2 - 2i\sqrt{15}}).$$

Il prodotto di due di questi quattro fattori non è contenuto in $\boldsymbol{Q}[X]$ e quindi m è irriducibile su $\boldsymbol{Q}$. Ne segue che m è il polinomio minimo di α su $\boldsymbol{Q}$.

(*ii*) Risulta: $\boldsymbol{Q}(\alpha) \subseteq \boldsymbol{Q}(\sqrt{3},\, i\sqrt{5})$ e $[\boldsymbol{Q}(\sqrt{3},\, i\sqrt{5}) : \boldsymbol{Q}] = 4$. Ne segue, per confronto dei gradi, che $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\sqrt{3},\, i\sqrt{5})$. Ma $\boldsymbol{Q}(\sqrt{3},\, i\sqrt{5}) = \Sigma_{f,\boldsymbol{Q}}$, con $f = (X^2 - 3)(X^2 + 5)$. Dunque l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$ è normale.

(*iii*) Essendo l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$ finita, normale e separabile, $|G(\boldsymbol{Q}(\alpha)\,|\,\boldsymbol{Q})| = 4$. Ogni automorfismo $\varphi \in G(\boldsymbol{Q}(\alpha)\,|\,\boldsymbol{Q})$ è completamente individuato assegnando $\varphi(\sqrt{3})$ e $\varphi(i\sqrt{5})$. Inoltre $\varphi(\sqrt{3}) = \pm\sqrt{3}$ e $\varphi(i\sqrt{5}) = \pm i\sqrt{5}$. Pertanto i quattro $\boldsymbol{Q}$-automorfismi sono:

$$\mathbf{1} = \varphi_1 : \begin{cases} \sqrt{3} \to \sqrt{3} \\ i\sqrt{5} \to i\sqrt{5}, \end{cases} \quad \varphi_2 : \begin{cases} \sqrt{3} \to \sqrt{3} \\ i\sqrt{5} \to -i\sqrt{5}, \end{cases} \quad \varphi_3 : \begin{cases} \sqrt{3} \to -\sqrt{3} \\ i\sqrt{5} \to i\sqrt{5}, \end{cases} \quad \varphi_4 : \begin{cases} \sqrt{3} \to -\sqrt{3} \\ i\sqrt{5} \to -i\sqrt{5}. \end{cases}$$

Risulta subito che $\circ(\varphi_2) = \circ(\varphi_3) = \circ(\varphi_4) = 2$ e dunque $G(\boldsymbol{Q}(\alpha)\,|\,\boldsymbol{Q}) \cong \boldsymbol{V}$ (gruppo di Klein).

I tre campi intermedi dell'estensione sono $\langle\varphi_2\rangle^\flat$, $\langle\varphi_3\rangle^\flat$, $\langle\varphi_4\rangle^\flat$, cioè:

$$\langle\varphi_2\rangle^\flat = \boldsymbol{Q}(\alpha)^{\langle\varphi_2\rangle} = \boldsymbol{Q}(\sqrt{3}), \quad \langle\varphi_3\rangle^\flat = \boldsymbol{Q}(\alpha)^{\langle\varphi_3\rangle} = \boldsymbol{Q}(i\sqrt{5}), \quad \langle\varphi_4\rangle^\flat = \boldsymbol{Q}(\alpha)^{\langle\varphi_4\rangle} = \boldsymbol{Q}(i\sqrt{15}).$$

* * *

25. [*Prova d'esonero del 9/06/06*] (*i*) Determinare il campo K generato su $\boldsymbol{Z}_7$ dalle radici terze e dalle radici quarte dell'unità $\overline{1} \in \boldsymbol{Z}_7$.

(*ii*) Assegnato il polinomio $f = (X^4 - \overline{2})(X^3 - \overline{2}) \in \boldsymbol{Z}_7[X]$, determinare il campo di spezzamento $E = \Sigma_{f,\boldsymbol{Z}_7}$ ed il suo grado su $\boldsymbol{Z}_7$. [*Suggerimento*: per determinare gli zeri di f utilizzare (*i*)].

(*iii*) Determinare il gruppo di Galois $G(E\,|\,\boldsymbol{Z}_7)$.

Soluzione. (*i*) Risulta:

$$X^3 - \overline{1} = (X - \overline{1})(X^2 + X + \overline{1}) = (X - \overline{1})(X - \overline{2})(X - \overline{4}).$$

Dunque le radici terze di $\overline{1}$ in $\boldsymbol{Z}_7$ sono $\overline{1}$, $\overline{2}$, $\overline{4}$. Risulta poi:

$$X^4 - \overline{1} = (X^2 - \overline{1})(X^2 + \overline{1}) = (X - \overline{1})(X - \overline{6})(X^2 + \overline{1}).$$

Il polinomio $X^2 + \overline{1}$ non ha zeri in $\boldsymbol{Z}_7$ e dunque è irriducibile. Si consideri il campo $\boldsymbol{Z}_7(\alpha) = \boldsymbol{Z}_7[X]/_{(X^2+\overline{1})}$ [di cardinalità 49]. In tale campo $X^2 + \overline{1} = (X - \alpha)(X + \alpha) = (X - \alpha)(X - \overline{6}\alpha)$. Dunque le radici quarte di $\overline{1}$ in $\boldsymbol{Z}_7$ sono $\overline{1}$, $\overline{6}$, α, $\overline{6}\alpha$. Si conclude che

$$K = \boldsymbol{Z}_7(\overline{1}, \overline{2}, \overline{4}, \overline{6}, \alpha, \overline{6}\alpha) = \boldsymbol{Z}_7(\alpha).$$

(*ii*) Per ottenere i quattro zeri di $X^4 - \overline{2} \in \boldsymbol{Z}_7[X]$, basta determinarne uno e moltiplicarlo per le quattro radici quarte di $\overline{1}$. Analogo ragionamento vale per gli zeri di $X^3 - \overline{2}$. Risulta:

$$X^4 - \overline{2} = X^4 - \overline{4}^2 = (X^2 - \overline{4})(X^2 + \overline{4}) = (X - \overline{2})(X + \overline{2})(X^2 + \overline{4}) \in \boldsymbol{Z}_7[X].$$

Uno zero di $X^4 - \overline{2}$ è quindi $\overline{2}$. I quattro zeri di $X^4 - \overline{2}$ sono pertanto $\overline{2}$, $\overline{2}\cdot\overline{6} = \overline{5}$, $\overline{2}\alpha$, $\overline{5}\alpha$.

Il polinomio $X^3 - \overline{2}$ non ha zeri in $\boldsymbol{Z}_7$ e quindi è irriducibile. Nel campo $L = \boldsymbol{Z}_7[X]/_{(X^3-\overline{2})} =: \boldsymbol{Z}(\beta)$ [di cardinalità 7^3] uno zero di $X^3 - \overline{2}$ è β e quindi i tre zeri sono: β, $\overline{2}\beta$, $\overline{4}\beta$.

Verifichiamo che $\beta \notin K\ (= \boldsymbol{Z}_7(\alpha))$. Altrimenti si avrebbe $\beta = a + b\alpha \in \boldsymbol{Z}_7(\alpha)$ e quindi

$$\overline{2} = (a + b\alpha)^3 = a^3 + \overline{3}a^2 b\alpha + \overline{3}ab^2\alpha^2 + b^3\alpha^3 = a^3 + \overline{3}a^2 b\alpha - \overline{3}ab^2 - b^3\alpha.$$

Ne segue

$$(a^3 - \overline{3}ab^2 - \overline{2}) + \alpha(\overline{3}a^2 b - b^3) = \overline{0}, \text{ da cui } \begin{cases} a^3 - \overline{3}ab^2 = \overline{2} \\ (\overline{3}a^2 - b^2)b = \overline{0}. \end{cases}$$

Ma tale sistema è incompatibile in $\boldsymbol{Z}_7$. Se infatti $b = \overline{0}$, $a^3 = \overline{2}$ (assurdo in $\boldsymbol{Z}_7$); se invece $b \neq \overline{0}$, si ricava che $ab^2 = \overline{1}$, da cui $a^3 = \overline{5}$ (ancora assurdo in $\boldsymbol{Z}_7$).

Segue allora che $X^3 - \overline{2}$ è irriducibile in $\boldsymbol{Z}_7(\alpha)[X]$. Quindi $E = \Sigma_{f,\boldsymbol{Z}_7} = \boldsymbol{Z}_7(\alpha, \beta)$ e

$$[E : \boldsymbol{Z}_7] = [E : \boldsymbol{Z}_7(\alpha)]\cdot[\boldsymbol{Z}_7(\alpha) : \boldsymbol{Z}_7] = 3\cdot 2 = 6.$$

(*iii*) L'estensione $\boldsymbol{Z}_7 \subset E$ è finita, normale e separabile. Dunque $G(E\,|\,\boldsymbol{Z}_7) = [E : \boldsymbol{Z}_7] = 6$. Ogni automorfismo $\varphi \in G(E\,|\,\boldsymbol{Z}_7)$ è completamente individuato da $\varphi(\alpha)$ e $\varphi(\beta)$. Ovviamente $\varphi(\alpha) \in \{\alpha, -\alpha\,(= \overline{6}\alpha)\}$ mentre $\varphi(\beta) \in \{\beta, \overline{2}\beta, \overline{4}\beta\}$ [infatti φ conserva gli zeri di $X^2 + \overline{1}$ e di $X^3 - \overline{2}$]. Posto $\varphi : \begin{cases} \alpha \to -\alpha \\ \beta \to \overline{2}\beta, \end{cases}$ risulta:

$$\varphi^2 : \begin{cases} \alpha \to \alpha \\ \beta \to \overline{4}\beta, \end{cases} \quad \varphi^3 : \begin{cases} \alpha \to -\alpha \\ \beta \to \beta, \end{cases} \quad \varphi^4 : \begin{cases} \alpha \to \alpha \\ \beta \to \overline{2}\beta, \end{cases} \quad \varphi^5 : \begin{cases} \alpha \to \alpha \\ \beta \to \overline{4}\beta, \end{cases} \quad \varphi^6 : \begin{cases} \alpha \to \alpha \\ \beta \to \beta. \end{cases}$$

Dunque $\circ(\varphi) = 6$ e $G(E \,|\, \boldsymbol{Z}_7) = \langle\varphi\rangle \cong \boldsymbol{C}_6$.

* * *

26. [*Prova d'esame del 6/02/07*] Sia $\alpha = \sqrt{2-\sqrt{3}} \in \boldsymbol{R}$ e si consideri l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$.

(*i*) Determinare il polinomio minimo m di α ed il grado dell'estensione.

(*ii*) Verificare se l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$ è normale.

(*iii*) Calcolare il guppo di Galois dell'estensione e indicare i campi intermedi.

Soluzione. (*i*) Si ha: $\alpha^2 = 2-\sqrt{3} \implies (\alpha^2-2)^2 = 3 \implies \alpha^4 - 4\alpha^2 + 1 = 0$. Dunque α è zero del polinomio $m = X^4 - 4X^2 + 1 \in \boldsymbol{Q}[X]$. Tale polinomio si fattorizza in $\boldsymbol{R}[X]$ nella forma

$$m = (X - \sqrt{2-\sqrt{3}})(X + \sqrt{2-\sqrt{3}})(X - \sqrt{2+\sqrt{3}})(X + \sqrt{2+\sqrt{3}}).$$

Il prodotto di due di questi quattro fattori non appartiene a $\boldsymbol{Q}[X]$. Ne segue che m è irriducibile su $\boldsymbol{Q}$ e quindi è il polinomio minimo di α su $\boldsymbol{Q}$. Ovviamente $[\boldsymbol{Q}(\alpha) : \boldsymbol{Q}] = 4$.

(*ii*) Posto $\beta := \sqrt{2+\sqrt{3}}$, risulta subito che $\alpha\beta = 1$. Allora i quattro zeri di m sono $\pm\alpha, \pm\frac{1}{\alpha}$. Ne segue che

$$\Sigma_{m,\,\boldsymbol{Q}} = \boldsymbol{Q}(\alpha,\, -\alpha,\, \tfrac{1}{\alpha},\, -\tfrac{1}{\alpha}) = \boldsymbol{Q}(\alpha)$$

e quindi l'estensione $\boldsymbol{Q} \subset \boldsymbol{Q}(\alpha)$ è normale.

(*iii*) Dal *TFTG*, $|G(\boldsymbol{Q}(\alpha) \,|\, \boldsymbol{Q})| = 4$. Gli automorfismi $\varphi \in G(\boldsymbol{Q}(\alpha) \,|\, \boldsymbol{Q})$ sono completamente individuati dall'immagine di α. Ovviamente $\varphi(\alpha) \in \{\alpha, -\alpha, \frac{1}{\alpha}, -\frac{1}{\alpha}\}$. Si ponga:

$$\mathbf{1} = \varphi_1 : \alpha \to \alpha; \quad \varphi_2 : \alpha \to -\alpha; \quad \varphi_3 : \alpha \to \tfrac{1}{\alpha}, \quad \varphi_4 : \alpha \to -\tfrac{1}{\alpha}.$$

Risulta: $\varphi_2^{\,2}(\alpha) = \varphi_2(-\alpha) = -\varphi_2(\alpha) = \alpha$ e dunque $\varphi_2^{\,2} = \mathbf{1}$. Analogamente

$\varphi_3^{\,2}(\alpha) = \varphi_3(\frac{1}{\alpha}) = \frac{1}{\varphi_3(\alpha)} = \alpha$ e dunque $\varphi_3^{\,2} = \mathbf{1}$;

$\varphi_4^{\,2}(\alpha) = \varphi_4(-\frac{1}{\alpha}) = -\varphi_4(\frac{1}{\alpha}) = \alpha$ e dunque $\varphi_4^{\,2} = \mathbf{1}$.

Essendo $\circ(\varphi_2) = \circ(\varphi_3) = \circ(\varphi_4) = 2$, si conclude che $G(\boldsymbol{Q}(\alpha) \,|\, \boldsymbol{Q})$ è un gruppo di Klein.

I campi fissi corrispondenti ai tre sottogruppi propri del gruppo di Klein sono:

$$\langle\varphi_2\rangle^{\flat}, \quad \langle\varphi_3\rangle^{\flat}, \quad \langle\varphi_4\rangle^{\flat}.$$

Posto $x = a + b\alpha + c\alpha^2 + d\alpha^3 \in \boldsymbol{Q}(\alpha)$ [con $a, b, c, d \in \boldsymbol{Q}$], si ha, per $i = 2, 3, 4$:

$$x \in \langle\varphi_i\rangle^{\flat} \iff \varphi_i(x) = x.$$

Consideriamo φ_2. Si ha:

$$\varphi_2(x) = x \iff a - b\alpha + c\alpha^2 - d\alpha^3 = a + b\alpha + c\alpha^2 + d\alpha^3 \iff b = d = 0.$$

Pertanto

$$\langle\varphi_2\rangle^{\flat} = \boldsymbol{Q}(1, \alpha^2) = \boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\sqrt{3}).$$

Analogamente: $\varphi_3(x) = x \iff a + b\frac{1}{\alpha} + c\frac{1}{\alpha^2} + d\frac{1}{\alpha^3} = a + b\alpha + c\alpha^2 + d\alpha^3 \iff$

$\iff a\alpha^3 + b\alpha^2 + c\alpha + d = a\alpha^3 + b\alpha^4 + c\alpha^5 + d\alpha^6 = a\alpha^3 + b(4\alpha^2 - 1) + c(4\alpha^3 - \alpha) + d(15\alpha^2 - 4) \iff$

$\iff a\alpha^3 + b\alpha^2 + c\alpha + d = (a + 4c)\alpha^3 + (4b + 15d)\alpha^2 - c\alpha - (4d + b) \iff$

$$\iff \begin{cases} a = a + 4c, & b = 4b + 15d \\ c = -c, & d = -b - 4d. \end{cases} \iff \begin{cases} c = 0 \\ b = -5d. \end{cases}$$ Pertanto

$$\langle\varphi_3\rangle^{\flat} = \boldsymbol{Q}(1, \alpha^3 - 5\alpha) = \boldsymbol{Q}(\alpha^3 - 5\alpha).$$

Infine, procedendo in modo analogo: $\varphi_4(x) = x \iff a\alpha^3 - b\alpha^2 + c\alpha - d = a\alpha^3 + b\alpha^4 + c\alpha^5 + d\alpha^6 \iff$

$$\iff \begin{cases} a + 4c = a, & 5b + 15d = 0 \\ c = -c, & -b - 3d = 0 \end{cases} \iff \begin{cases} c = 0 \\ b = -3d. \end{cases}$$ Pertanto

$$\langle\varphi_4\rangle^{\flat} = \boldsymbol{Q}(1, \alpha^3 - 3\alpha) = \boldsymbol{Q}(\alpha^3 - 3\alpha).$$

* * *

27. [*Prova d'esame del 12/06/06*] È assegnata l'estensione algebrica semplice $\boldsymbol{Q} \subset \boldsymbol{Q}(G^{-1/3})$, con $G = \frac{1+\sqrt{5}}{2}$ (rapporto aureo).

(*i*) Determinare il polinomio minimo di $G^{-1/3}$ su $\boldsymbol{Q}$ e verificare che l'estensione assegnata è non normale.

(*ii*) Determinare la chiusura normale N di tale estensione e valutarne il grado su $\boldsymbol{Q}$.

(*iii*) Determinare il gruppo di Galois $G(\boldsymbol{Q}(G^{-1/3}) \,|\, \boldsymbol{Q})$.

Soluzione. (*i*) Si ponga $X = G^{-1/3}$. Allora $X^3 = G^{-1} = \frac{\sqrt{5}-1}{2}$. Dunque $X^3 + \frac{1}{2} = \frac{\sqrt{5}}{2}$. Quadrando,

$$X^6 + X^3 + \tfrac{1}{4} = \tfrac{5}{4}, \text{ cioè } X^6 + X^3 - 1 = 0.$$

Allora $G^{-1/3}$ è uno zero del polinomio $f = X^6 + X^3 - 1 \in \boldsymbol{Q}[X]$. Per verificare se f è irriducibile su $\boldsymbol{Q}$ (e quindi è il polinomio minimo richiesto) conviene scriverne una fattorizzazione in fattori irriducibili in $\boldsymbol{R}[X]$. Risulta subito:

$$\begin{aligned} f &= (X^3 + \tfrac{1}{2} + \tfrac{\sqrt{5}}{2})(X^3 + \tfrac{1}{2} - \tfrac{\sqrt{5}}{2}) = (X^3 + G)(X^3 - G^{-1}) = \\ &= (X + G^{1/3})(X^2 + G^{1/3}X + G^{2/3})\,(X - G^{-1/3})(X^2 + G^{-1/3}X + G^{-2/3}). \end{aligned}$$

Poiché nessuno di tali fattori irriducibili su $\boldsymbol{R}$ è in $\boldsymbol{Q}[X]$ e nessun prodotto di due di essi è in $\boldsymbol{Q}[X]$, allora f non ammette fattorizzazioni proprie su $\boldsymbol{Q}$ e dunque è irriducibile su $\boldsymbol{Q}$. Inoltre f ha due zeri reali $G^{-1/3}$ e $-G^{1/3}$ [entrambi in $\boldsymbol{Q}(G^{-1/3})$] e quattro zeri complessi non reali (a due a due coniugati):

$$\zeta_3 G^{-1/3},\ \zeta_3^2 G^{-1/3},\ -\zeta_3 G^{1/3},\ -\zeta_3^2 G^{1/3}.$$

Ne segue subito che l'estensione assegnata [contenuta in $\boldsymbol{R}$] è non normale.

(*ii*) Ovviamente

$$N = \Sigma_{f,\boldsymbol{Q}} = \boldsymbol{Q}(G^{-1/3}, \zeta_3 G^{-1/3}, \zeta_3^2 G^{-1/3}, -G^{1/3}, -\zeta_3 G^{1/3}, -\zeta_3^2 G^{1/3}) = \boldsymbol{Q}(G^{-1/3}, \zeta_3).$$

ζ_3 è zero del polinomio ciclotomico $X^2 + X + 1$. Inoltre $\zeta_3 \notin \boldsymbol{Q}(G^{-1/3})$ (essendo complesso non reale). Dunque $X^2 + X + 1$ è irriducibile su $\boldsymbol{Q}(G^{-1/3})$. Pertanto

$$[N : \boldsymbol{Q}] = [N : \boldsymbol{Q}(G^{-1/3})] \cdot [\boldsymbol{Q}(G^{-1/3}) : \boldsymbol{Q}] = 2 \cdot 6 = 12.$$

(*iii*) Il polinomio minimo f di $G^{-1/3}$ ha due zeri distinti in $\boldsymbol{Q}(G^{-1/3})$: $G^{-1/3}$ e $-G^{1/3}$. È noto che in tal caso $G(\boldsymbol{Q}(G^{-1/3}) \,|\, \boldsymbol{Q}) \cong \boldsymbol{S}_2$. L'unico automorfismo non identico di tale gruppo scambia tra loro i due zeri di f.

* * *

28. [*Prova d'esame del 12/06/06*] Sia E l'estensione di $\boldsymbol{Z}_3$ generata dalle radici 12-sime dell'unità $\overline{1}$ di $\boldsymbol{Z}_3$. Determinare il gruppo di Galois $G(E \,|\, \boldsymbol{Z}_3)$, esplicitandone gli automorfismi. Descrivere gli eventuali campi intermedi dell'estensione $\boldsymbol{Z}_3 \subseteq E$.

Soluzione. Risulta: $E = \Sigma_{f,\boldsymbol{Z}_3}$, con $f = X^{12} - \overline{1} \in \boldsymbol{Z}_3[X]$. Si ha:

$$f = (X^6 - \overline{1})(X^6 + \overline{1}) = (X^2 - \overline{1})^3 (X^2 + \overline{1})^3 = (X - \overline{1})^3 (X - \overline{2})^3 (X^2 + \overline{1})^3.$$

Dunque f ha i due zeri tripli $\overline{1}$, $\overline{2} \in \boldsymbol{Z}_3$; inoltre $X^2 + \overline{1}$ è irriducibile su $\boldsymbol{Z}_3$ (non ha zeri). Pertanto il campo di spezzamento E cercato è:

$$E = \boldsymbol{Z}_3[X]\big/_{(X^2+\overline{1})} := \boldsymbol{Z}_3(\alpha) = \{a + b\alpha,\ \ \forall\, a, b \in \boldsymbol{Z}_2;\ \alpha^2 = \overline{2}\}$$

[campo di cardinalità 9]. In E il polinomio $X^2 + \overline{1}$ ammette i due zeri α, $\overline{2}\alpha$.

L'estensione $\boldsymbol{Z}_3 \subset E$ è finita, normale e separabile [infatti $X^2 + \overline{1} \notin \boldsymbol{Z}_3[X^3]$] e dunque

$$|G(E \,|\, \boldsymbol{Z}_3)| = [E : \boldsymbol{Z}_3] = 2.$$

Pertanto $G(E \,|\, \boldsymbol{Z}_3) \cong \boldsymbol{C}_2$, con generatore $\varphi : E \to E$ tale che $\varphi(\alpha) = \overline{2}\alpha$. Quindi

$$\varphi(x) = a + \overline{2}b\alpha,\ \ \forall\, x = a + b\alpha \in E.$$

Non esistono campi intermedi tra $\boldsymbol{Z}_3$ ed E, in quanto $\boldsymbol{C}_2$ non ha sottogruppi propri.

* * *

29. [*Prova d'esame del 10/07/06*] Sia K il sottocampo di $\boldsymbol{C}$ generato dalle radici quadrate e dalle radici terze di i.

(*i*) Verificare che $\boldsymbol{Q}(i) \subseteq K$ e determinare il grado di tale estensione.

(*ii*) Esprimere K come campo di spezzamento di un polinomio in $\boldsymbol{Q}(i)[X]$ e come campo di spezzamento di un polinomio in $\boldsymbol{Q}[X]$.

(*iii*) Indicare i campi intermedi tra $\boldsymbol{Q}(i)$ e K.

Soluzione. (*i*) Le radici quadrate e le radici terze di i sono rispettivamente gli zeri di $X^2 - i$ e $X^3 - i \in \boldsymbol{C}[X]$. Una radice quadrata di i è ad esempio

$$\alpha = \cos\tfrac{\pi}{4} + i \sin\tfrac{\pi}{4} = \tfrac{\sqrt{2}}{2}\,(1 + i),$$

mentre una radice terza di i è ad esempio

$$\beta = \cos\tfrac{\pi}{6} + i \sin\tfrac{\pi}{6} = \tfrac{1}{2}(\sqrt{3} + i).$$

Ricordato che le radici quadrate di 1 sono ± 1 e le radici terze di 1 sono 1, ζ_3, ζ_3^2, allora

$$K = \boldsymbol{Q}(\alpha,\, -\alpha,\, \beta,\, \beta\zeta_3,\, \beta\zeta_3^2).$$

Poiché $\beta\zeta_3^2 = -i$ [come subito si verifica], allora

$$K = \boldsymbol{Q}(i,\, \sqrt{2},\, \sqrt{3}).$$

Dunque $\boldsymbol{Q}(i) \subset K$ e $[K : \boldsymbol{Q}(i)] = 4$ [essendo $X^2 - 2$ e $X^2 - 3$ polinomi minimi di $\sqrt{2}$, $\sqrt{3}$ su $\boldsymbol{Q}(i)$].

(*ii*) Risulta:

$$K = \Sigma_{f,\boldsymbol{Q}(i)}, \text{ con } f = (X^2 - i)(X^3 - i) \in \boldsymbol{Q}(i)[X]$$

[ovvero con $f = (X^2 - 2)(X^2 - 3) \in \boldsymbol{Q}(i)[X]$]. Analogamente:

$$K = \Sigma_{g,\boldsymbol{Q}}, \text{ con } g = (X^2 + 1)(X^2 - 2)(X^2 - 3) \in \boldsymbol{Q}[X].$$

(*iii*) L'estensione $\boldsymbol{Q}(i) \subset K$ è finita, normale e separabile. Allora $|G(K \,|\, \boldsymbol{Q}(i)| = 4$. Gli automorfismi di $G(K \,|\, \boldsymbol{Q}(i)$ sono completamente individuati dall'azione su $\sqrt{2}$ e $\sqrt{3}$. Inoltre $\sqrt{2}$ viene trasformato in $\pm\sqrt{2}$, mentre $\sqrt{3}$ viene trasformato in $\pm\sqrt{3}$. Pertanto i tre automorfismi non banali φ_1, φ_2, φ_3 cercati sono rispettivamente identificabili con $(+-)$, $(-+)$, $(--)$ [segni delle immagini dei due radicali; ad esempio $\varphi_1(\sqrt{2}) = +\sqrt{2}$, $\varphi_1(\sqrt{3}) = -\sqrt{3}$, ecc.].

Il gruppo $G(K \,|\, \boldsymbol{Q}(i)$ è quindi un gruppo di Klein ed i suoi tre sottogruppi propri sono in corrispondenza biunivoca con i tre campi intermedi cercati. Si tratta di

$$\langle\varphi_1\rangle^\flat = \boldsymbol{Q}(i,\, \sqrt{2}), \quad \langle\varphi_2\rangle^\flat = \boldsymbol{Q}(i,\, \sqrt{3}), \quad \langle\varphi_3\rangle^\flat = \boldsymbol{Q}(i,\, \sqrt{6}).$$

* * *

30. [*Prova d'esame del 28/09/06*] È assegnato in $\boldsymbol{Z}_2[X]$ il polinomio irriducibile $f = X^3 + X + \overline{1}$. Si consideri il campo $\boldsymbol{Z}_2(\alpha) := \boldsymbol{Z}_2[X]/_{(f)}$.

(*i*) Verificare se l'estensione algebrica semplice $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(\alpha)$ è normale e separabile.

(*ii*) Determinare il grado dell'estensione $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(\sqrt{\alpha})$ e calcolare il guppo di Galois dell'estensione, indicandone gli automorfismi.

Soluzione. (*i*) Dividendo f per $X + \alpha$ si ottiene:

$$f = (X + \alpha)(X^2 + \alpha X + (\overline{1} + \alpha^2)).$$

Verifichiamo se il polinomio $g := X^2 + \alpha X + (\overline{1} + \alpha^2) \in \boldsymbol{Z}_2(\alpha)[X]$ è riducibile. Posto $x := a + b\alpha + c\alpha^2$ [con $a, b, c \in \boldsymbol{Z}_2$], risulta:

$$\begin{aligned} g(x) = \overline{0} &\iff (a + b\alpha + c\alpha^2)^2 + \alpha(a + b\alpha + c\alpha^2) + (\overline{1} + \alpha^2) = \overline{0} \iff \\ &\iff (a^2 + c + \overline{1}) + \alpha(c^2 + a + c) + \alpha^2(b^2 + c^2 + b + \overline{1}) = \overline{0}. \end{aligned}$$

Ad esempio, posto $a = b = \overline{0}$, allora $c = \overline{1}$ e dunque α^2 è uno zero di g. Dividendo g per $X + \alpha^2$, si ottiene $g = (X + \alpha^2)(X + \alpha + \alpha^2)$. Si conclude che

$$f = (X + \alpha)(X + \alpha^2)(X + \alpha + \alpha^2).$$

Quindi f ha tre zeri distinti, tutti in $\boldsymbol{Z}_2(\alpha)$. Pertanto $\boldsymbol{Z}_2(\alpha)$ è campo di spezzamento di f su $\boldsymbol{Z}_2$. L'estensione $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(\alpha)$ è quindi normale e separabile, di grado 3.

(*ii*) Ovviamente $\boldsymbol{Z}_2(\alpha) \subseteq \boldsymbol{Z}_2(\sqrt{\alpha})$. Ci chiediamo se viceversa $\sqrt{\alpha} \in \boldsymbol{Z}_2(\alpha)$. Posto $\sqrt{\alpha} = a+b\alpha+c\alpha^2$, quadrando si ottiene: $\alpha = a^2+c^2\alpha+(b^2+c^2)\alpha^2$. Ne segue $\begin{cases} a = 0 \\ b = c = \overline{1}. \end{cases}$ Pertanto $\sqrt{\alpha} = \alpha+\alpha^2 \in \boldsymbol{Z}_2(\alpha)$. Dunque $\boldsymbol{Z}_2(\alpha) = \boldsymbol{Z}_2(\sqrt{\alpha})$.

Dal *TFTG*, $|G(\boldsymbol{Z}_2(\sqrt{\alpha}) \,|\, \boldsymbol{Z}_2)| = [\boldsymbol{Z}_2(\sqrt{\alpha}) : \boldsymbol{Z}_2] = [\boldsymbol{Z}_2(\alpha) : \boldsymbol{Z}_2] = 3$. Pertanto $G(\boldsymbol{Z}_2(\sqrt{\alpha}) \,|\, \boldsymbol{Z}_2) \cong \boldsymbol{C}_3$ [gruppo ciclico di ordine 3]. Ogni $\boldsymbol{Z}_2$-automorfismo di $\boldsymbol{Z}_2(\sqrt{\alpha})$ stabilisce una permutazione degli zeri di f. I tre automorfismi cercati sono:

$$\mathbf{1} : \begin{cases} \alpha \to \alpha \\ \alpha^2 \to \alpha^2 \\ \alpha+\alpha^2 \to \alpha+\alpha^2, \end{cases} \qquad \varphi : \begin{cases} \alpha \to \alpha^2 \\ \alpha^2 \to \alpha+\alpha^2 \\ \alpha+\alpha^2 \to \alpha, \end{cases} \qquad \varphi^2 : \begin{cases} \alpha \to \alpha+\alpha^2 \\ \alpha^2 \to \alpha \\ \alpha+\alpha^2 \to \alpha^2. \end{cases}$$

* * *

31. [*Prova d'esame del 10/07/06*] Sono assegnati in $\boldsymbol{Z}_2[X]$ i polinomi $f = X^2+X+\overline{1}$, $g = X^3+X+\overline{1}$.

(*i*) Verificare che f, g sono irriducibili su $\boldsymbol{Z}_2$ e determinare il campo di spezzamento $E = \Sigma_{fg,\,\boldsymbol{Z}_2}$ del polinomio fg su $\boldsymbol{Z}_2$.

(*ii*) Determinare il gruppo di Galois $G(E|\,\boldsymbol{Z}_2)$.

(*iii*) Determinare i campi intermedi dell'estensione $\boldsymbol{Z}_2 \subset E$.

Soluzione. (*i*) Risulta $f(\overline{0})$, $f(\overline{1}) \neq \overline{0}$ e, analogamente, $g(\overline{0})$, $g(\overline{1}) \neq \overline{0}$. Dunque i due polinomi sono irriducibili su $\boldsymbol{Z}_2$.

Sia $\boldsymbol{Z}_2(\alpha) := \boldsymbol{Z}_2[X]\big/_{(f)} = \{\overline{0},\, \overline{1},\, \alpha,\, \alpha+\overline{1};\ \alpha^2 = \alpha+\overline{1}\}$. Nel campo $\boldsymbol{Z}_2(\alpha)$, f ha i due zeri α, $\alpha+\overline{1}$. In $\boldsymbol{Z}_2(\alpha)$, g è irriducibile. Infatti:

$$\begin{aligned} &g(\overline{0}),\, g(\overline{1}) \neq \overline{0}; \\ &g(\alpha) = \alpha^3+\alpha+\overline{1} = (\alpha^2+\alpha)+\alpha+\overline{1} = \alpha^2+\overline{1} = \alpha \neq \overline{0}; \\ &g(\alpha+\overline{1}) = (\alpha+\overline{1})^3+(\alpha+\overline{1})+\overline{1} = \,\ldots\, = \alpha+\overline{1} \neq \overline{0}. \end{aligned}$$

Sia $K := \boldsymbol{Z}_2(\alpha)[X]\big/_{(g)} = \boldsymbol{Z}_2(\alpha)[\beta \,|\, \beta^3+\beta+\overline{1} = \overline{0}] =: \boldsymbol{Z}_2(\alpha,\, \beta)$. Si tratta di un campo con $4^3 = 64$ elementi. Dividendo g per $X+\beta$ si ottiene

$$g = (X+\beta)\,h, \ \text{ con } \ h = X^2+\beta X+\beta^2+\overline{1} \in K[X].$$

Risulta:

$$h(\beta^2) = (\beta^2)^2+\beta^3+\beta^2+\overline{1} = (\beta^2+\beta)+(\beta+\overline{1})+\beta^2+\overline{1} = \overline{0}$$

e quindi β^2 è un altro zero di g (in K). Il terzo zero di g si ottiene dividendo h per $X+\beta^2$ e si ottiene $\beta^2+\beta$. Pertanto

$$g = (X+\beta)(X+\beta^2)(X+\beta^2+\beta) \in K[X].$$

Concludendo, $E = \Sigma_{fg,\,\boldsymbol{Z}_2} = \boldsymbol{Z}_2(\alpha,\, \alpha+\overline{1},\, \beta,\, \beta^2,\, \beta^2+\beta) = \boldsymbol{Z}_2(\alpha,\, \beta)$. Inoltre

$$[E : \boldsymbol{Z}_2] = [\boldsymbol{Z}_2(\alpha,\, \beta) : \boldsymbol{Z}_2(\alpha)] = [\boldsymbol{Z}_2(\alpha) : \boldsymbol{Z}_2] = 3{\cdot}2 = 6.$$

(*ii*) L'estensione $\boldsymbol{Z}_2 \subset E$ è finita, normale e separabile. Dal *TFTG*(*i*) segue che $|G(E|\,\boldsymbol{Z}_2)| = 6$.

Sia $\varphi \in G(E|\,\boldsymbol{Z}_2)$. Poiché $f(\varphi(\alpha)) = \overline{0}$ e $g(\varphi(\beta)) = \overline{0}$, allora $\varphi(\alpha) \in \{\alpha,\, \alpha+\overline{1}\}$, mentre $\varphi(\beta) \in \{\beta,\, \beta^2,\, \beta^2+\beta\}$. Si ponga:

$$\varphi : \begin{matrix} \alpha \to \alpha+\overline{1} \\ \beta \to \beta^2. \end{matrix}$$

Risulta, successivamente:

$$\varphi^2 : \begin{matrix} \alpha \to \alpha \\ \beta \to \beta^2+\beta, \end{matrix} \quad \varphi^3 : \begin{matrix} \alpha \to \alpha+\overline{1} \\ \beta \to \beta, \end{matrix} \quad \varphi^4 : \begin{matrix} \alpha \to \alpha \\ \beta \to \beta^2, \end{matrix} \quad \varphi^5 : \begin{matrix} \alpha \to \alpha+\overline{1} \\ \beta \to \beta^2+\beta, \end{matrix} \quad \varphi^6 : \begin{matrix} \alpha \to \alpha \\ \beta \to \beta. \end{matrix}$$

Dunque $\circ(\varphi) = 6$ e quindi $G(E|\,\boldsymbol{Z}_2) = \langle\varphi\rangle \cong \boldsymbol{C}_6$.

(*iii*) È noto che $\boldsymbol{C}_6 = \langle\varphi\rangle$ ha due soli sottogruppi propri:

$$\langle\varphi^2\rangle, \quad \langle\varphi^3\rangle$$

(di ordini rispettivamente 3, 2). I corrispondenti campi fissi sono

$$\langle\varphi^2\rangle^\flat = E^{\langle\varphi^2\rangle} = \boldsymbol{Z}_2(\alpha) \text{ e } \langle\varphi^3\rangle^\flat = E^{\langle\varphi^3\rangle} = \boldsymbol{Z}_2(\beta).$$

Le due estensioni $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(\alpha)$, $\boldsymbol{Z}_2 \subset \boldsymbol{Z}_2(\beta)$ sono ovviamente normali.

* * *

32. [*Prova di verifica del 28/05/07*] Siano x, y rispettivamente zeri dei polinomi $f = X^2 + \overline{1}$, $g = X^3 + X^2 + \overline{2} \in \boldsymbol{Z}_3[X]$. Si consideri l'estensione $\boldsymbol{Z}_3 \subseteq \boldsymbol{Z}_3(x, y)$.

(*i*) Dire se tale estensione è normale e indicarne il grado.

(*ii*) Calcolarne il gruppo di Galois.

(*iii*) Verificare che $\boldsymbol{Z}_3(xy) = \boldsymbol{Z}_3(x, y)$ e determinare il polinomio minimo di xy su $\boldsymbol{Z}_3$.

Soluzione. (*i*) I due polinomi f, g sono irriducibili in $\boldsymbol{Z}_3[X]$ (in quanto non hanno zeri in $\boldsymbol{Z}_3$).

Sia $K := \boldsymbol{Z}_3[X]/_{(g)} \cong \boldsymbol{Z}_3[y \,|\, g(y) = \overline{0}]$. Si tratta di un campo di cardinalità 27. Il polinomio g si fattorizza in $K[X]$ nella forma:

$$g = (X - x)(X^2 + (\overline{1} + y)X + y(\overline{1} + y)).$$

Gli zeri di $h := X^2 + (\overline{1} + y)X + y(\overline{1} + y)$ sono dati da

$$\overline{2}^{-1}\big(-\overline{1} - y \pm \sqrt{(\overline{1} + y)^2 - \overline{4}(y(\overline{1} + y)}\big) = \overline{2}\,\big(\overline{2} + \overline{2}y \pm \sqrt{\overline{1} + y)}\big).$$

Per valutare se $\sqrt{\overline{1} + y)} \in K$, basta verificare se l'equazione

$$(a + by + cy^2)^2 = \overline{1} + y$$

ammette soluzioni $a, b, c \in \boldsymbol{Z}_3$.

Si ottiene: $(a + by + cy^2)^2 = (a^2 + \overline{2}c^2 + \overline{2}bc) + y(c^2 + \overline{2}ab) + y^2(b^2 + c^2 + \overline{2}ac + bc)$. Il sistema

$$\begin{cases} a^2 + \overline{2}c^2 + \overline{2}bc = \overline{1} \\ c^2 + \overline{2}ab = \overline{1} \\ b^2 + c^2 + \overline{2}ac + bc = \overline{0} \end{cases}$$

è risolto ad esempio da $a = \overline{0}$, $b = c = \overline{1}$. Dunque $(y + y^2)^2 = \overline{1} + y$ e pertanto $\sqrt{\overline{1} + y)} = y + y^2$. Allora h ha zeri

$$\overline{2}(\overline{2} + \overline{2}y + y + y^2) = \overline{1} + \overline{2}y^2 \text{ e } \overline{2}(\overline{2} + \overline{2}y - y - y^2) = (\overline{1} + y)^2.$$

Ne segue che $K = \Sigma_{g,\boldsymbol{Z}_3} = \boldsymbol{Z}_3(y)$.

Ora consideriamo il polinomio $f = X^2 + \overline{1}$ e ci chiediamo se è riducibile in $K[X]$. Ciò avviene $\iff \exists\, a, b, c \in \boldsymbol{Z}_3$ tali che $(a + by + cy^2)^2 + \overline{1} = \overline{0}$, ovvero se il sistema

$$\begin{cases} a^2 + \overline{2}c^2 + \overline{2}bc = \overline{2} \\ c^2 + \overline{2}ab = \overline{0} \\ b^2 + c^2 + \overline{2}ac + bc = \overline{0} \end{cases}$$

ammette soluzioni in $\boldsymbol{Z}_3$.

Ponendo successivamente $c = \overline{0}$, $c = \overline{1}$, $c = \overline{2}$, si verifica che nei tre casi il sistema è incompatibile. Ne segue che il polinomio f è irriducibile in $K[X]$ e pertanto $K[X]/_{(f)}$ è un campo di cardinalità $27^2 = 729$.

Risulta:

$$K[X]/_{(f)} \cong K[x \,|\, x^2 = \overline{2}] \cong \boldsymbol{Z}_3(x, y).$$

Poiché f ha zeri $x, \overline{2}x$, entrambi in $\boldsymbol{Z}_3(x, y)$, si conclude che $\boldsymbol{Z}_3(x, y) = \Sigma_{fg,\boldsymbol{Z}_3}$. Pertanto l'estensione $\boldsymbol{Z}_3 \subset \boldsymbol{Z}_3(x, y)$ è normale e si ha:

$$[\boldsymbol{Z}_3(x, y) : \boldsymbol{Z}_3] = [\boldsymbol{Z}_3(x, y) : K] \cdot [K : \boldsymbol{Z}_3] = 6.$$

(*ii*) Siccome l'estensione $\boldsymbol{Z}_3 \subset \boldsymbol{Z}_3(x, y)$ è finita, separabile e normale, allora $|G(\boldsymbol{Z}_3(x, y)|\boldsymbol{Z}_3)| = 6$. Ogni automorfismo $\varphi \in G(\boldsymbol{Z}_3(x, y)|\boldsymbol{Z}_3)$ è individuato dalle due immagini

$$\varphi(y) \in \{y, \overline{1} + \overline{2}y^2, (\overline{1} + y)^2\} \text{ e } \varphi(x) \in \{x, \overline{2}x\}.$$

Se poniamo

$$\varphi : \begin{cases} y \to \overline{1} + \overline{2}y^2 \\ x \to \overline{2}x, \end{cases} \quad \text{allora } \varphi^2 : \begin{cases} y \to (\overline{1} + y)^2 \\ x \to x, \end{cases} \quad \varphi^3 : \begin{cases} y \to y \\ x \to \overline{2}x. \end{cases}$$

Essendo $\circ(\varphi) > 3$, necessariamente $\circ(\varphi) = 6$ e quindi $G(\boldsymbol{Z}_3(x, y)|\boldsymbol{Z}_3) \cong \boldsymbol{C}_6$.

(*iii*) Per provare che $\boldsymbol{Z}_3(x, y) = \boldsymbol{Z}_3(xy)$ è sufficiente verificare che $x, y \in \boldsymbol{Z}_3(xy)$. Utilizziamo le identità $x^2 = \overline{2}$ e $y^3 + y^2 = \overline{1}$.

Da $y^3 + y^2 = \overline{1}$ segue $y^2(\overline{1} + y) = \overline{1}$. Allora $\overline{1} + y = \frac{\overline{1}}{y^2} = \frac{\overline{2}}{\overline{2}y^2} = \frac{\overline{2}}{(xy)^2}$ e quindi $y = -\overline{1} + \overline{2}\frac{\overline{1}}{(xy)^2} = \overline{2}(\overline{1} + \frac{\overline{1}}{(xy)^2})$. Perciò $y \in \boldsymbol{Z}_3(xy)$.

Da $x^2 = \overline{2}$ segue: $\overline{2}\,x^3y^3 = \overline{2}(\overline{2}xy^3) = xy^3$ e quindi $x = \frac{\overline{2}(xy)^3}{y^3} = \frac{\overline{2}(xy)^3}{\overline{1}+\overline{2}y^2} = \frac{\overline{2}(xy)^3}{\overline{1}+(xy)^2}$. Perciò anche $x \in \boldsymbol{Z}_3(xy)$.

Da (*i*) segue che xy ammette polinomio minimo di grado 6 su $\boldsymbol{Z}_3$. Per ottenere tale polinomio osserviamo che:

$$(xy)^6 = \overline{2}y + y^2, \quad (xy)^4 = y^2 + y + \overline{2}, \quad (xy)^2 = \overline{2}y^2.$$

Cerchiamo (se esistono) $a, b, c \in \boldsymbol{Z}_3$ tali che $(xy)^6 + a(xy)^4 + b(xy)^2 + c = 0$. Con semplici calcoli si ottiene $a = c = \overline{1}$, $b = \overline{2}$. Pertanto

$$F := X^6 + X^4 + \overline{2}X^2 + \overline{1} \in \boldsymbol{Z}_3[X]$$

ammette xy come zero. Ne segue che necessariamente F è irriducibile su $\boldsymbol{Z}_3$. Ovviamente infine $\boldsymbol{Z}_3[X]/_{(F)} \cong \boldsymbol{Z}_3(xy)$.

* * *

Bibliografia

[AA] **G.Campanella**. *Appunti di Algebra.* Nuova Cultura, 2005.

[AA2] **G.Campanella**. *Appunti di Algebra. Duecento esercizi svolti.* Nuova Cultura, 2005.

R.B.Allenby. *Rings,Fields and Groups. An introduction to Abstract Algebra.* Arnold, 1983.

M.A.Armstrong. *Groups and Symmetry.* UTM Springer, 1988.

M.Artin. *Algebra.* Prentice Hall, 1991.

M.F.Atiyah - I.G.MacDonald. *Introduction to Commutative Algebra.* Addison - Wesley, 1969.

L.Childs. *A Concrete Introduction to Higher Algebra.* Springer, 1983.

H.M.Edwards. *Galois Theory.* Springer, 1984.

R.W.Gilmer. *Multiplicative Ideal Theory.* Dekker, 1972.

M.Girardi - G.Israel. *Teoria dei campi.* Feltrinelli, 1976.

I.N.Herstein. *Algebra.* Editori Riuniti, 1982.

A.Machì. *Introduzione alla teoria dei gruppi.* Feltrinelli, 1974.

G.M. Piacentini Cattaneo. *Algebra.* Decibel - Zanichelli, 1996.

I. Stewart. *Galois Theory.* Chapman & All, 1973 - 1989 - 2004.

J.Stillwell. *Elements of Algebra: geometry, numbers, equations.* Springer, 1994.

J.P.Tignol. *Galois theory of algebraic equations.* World Scientific, 2001.