CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2019–2020

Esame scritto del 21 Febbraio 2020 — Sessione Estiva Anticipata, II appello

Testo & Svolgimento

. . . . . * . . . . . .

[1] — Nell'anello $\mathbb{Z}[x,y]$ dei polinomi in due variabili a coefficienti interi, consideriamo i due polinomi

$$h(x,y) := y^3 - 3\,x^2\,y + 6\,x\,y + 5\,x - 3\,y - 5 \ , \qquad \ell(x,y) := 3\,y^2 - x - y + 5 \ .$$

(a) Dimostrare che l'anello quoziente $\mathbb{Z}[x,y] \Big/ \big(h(x,y)\big)$ è un dominio.

(b) Dimostrare che l'anello quoziente $\mathbb{Z}[x,y] \Big/ \big(\ell(x,y)\big)$ è un dominio a fattorizzazione unica.

(c) Dimostrare che l'anello quoziente $\mathbb{Z}[x,y] \Big/ \big(\ell(x,y)\big)$ *non* è un dominio a ideali principali.

(d) Dimostrare che l'anello quoziente $\mathbb{Q}[x,y] \Big/ \big(\ell(x,y)\big)$ è un dominio euclideo.

[2] — Sia $\mathbb{Z}_{26}$, l'anello degli interi modulo 26, e sia $U(\mathbb{Z}_{26})$ il gruppo (moltiplicativo) dei suoi elementi invertibili.

(a) Calcolare esplicitamente tutti i sottogruppi di Sylow di $U(Z_{26})$.

(b) Determinare la (unica) decomposizione di $U(Z_{26})$ come prodotto diretto di gruppi ciclici $U(\mathbb{Z}_{26}) \cong C_1 \times \cdots \times C_k$ di ordini $d_i := \big|C_I\big|$ $(\, i = 1, \dots, k \,)$ tali che $d_{i+1} \Big| d_i$ per ogni $i = 1, \dots, k-1$.

[3] — Sia G un gruppo, e sia H un sottogruppo di G con indice finito n, cioè tale che $(G : H\,) = n \in \mathbb{N}_+$. Dimostrare che esiste un sottogruppo normale N di G tale che $N \leq H$ e $(G : N) \,\Big|\, n!$ — cioè l'indice di N in G divide $n!$.

[4] — Sia G un gruppo di ordine 231. Dimostrare che:

(a) esiste in G un sottogruppo ciclico di ordine 33;

(b) esiste in G un sottogruppo ciclico di ordine 77 che è normale;

(c) il centro $Z(G)$ di G è non banale.

[5] — Sia $\mathbb{Q}\big(\alpha\,,\beta\,\big)$ il campo estensione di $\mathbb{Q}$ generato da due elementi α e β con polinomi minimi su $\mathbb{Q}$ dati da $p_\alpha(x) = x^3 - 5$ e $p_\beta(x) = x^2 + 3$.

(a) Determinare una base di $\mathbb{Q}\big(\alpha\,,\beta\,\big)$ su $\mathbb{Q}$.

(b) Determinare un elemento primitivo dell'estensione $\mathbb{Q}\big(\alpha\,,\beta\,\big)$ di $\mathbb{Q}$.

(c) Determinare se l'estensione $\mathbb{Q}\big(\alpha\,,\beta\,\big)$ di $\mathbb{Q}$ sia normale oppure no.

— ⋆ —

SVOLGIMENTO

N.B.: lo svolgimento qui presentato è molto lungo... Questo non significa *che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si approfitta per spiegare — in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con molti particolari tutti gli aspetti della teoria toccati più o meno a fondo dal testo in questione.*

[1] — Procediamo alla soluzione dell'esercizio punto per punto.

(a) Ricordiamo che per un anello quoziente della forma R/I — con I ideale di R — si ha che R/I *è un dominio se e soltanto se* I *è un ideale primo.* Pertanto, nel nostro caso dobbiamo dimostrare che l'ideale $I := \big(h(x,y)\big)$ nell'anello $R := \mathbb{Z}[x,y]$ è *primo.* Ora, l'anello $R := \mathbb{Z}[x,y]$ è commutativo e l'ideale $I := \big(h(x,y)\big)$ è principale, quindi abbiamo che *l'ideale* $I := \big(h(x,y)\big)$ *è primo se e soltanto se l'elemento* $h(x,y)$ *che lo genera è primo.* Infine, osserviamo che l'anello $R := \mathbb{Z}[x,y]$ è un dominio a fattorizzazione unica, quindi ogni suo elemento è primo se e soltanto se è irriducibile: pertanto, dimostrare che l'elemento sia primo significa dimostrare che sia irriducibile, e a tal fine possiamo utilizzare (qualora ci siano le condizioni per applicarlo) un qualsiasi criterio di irriducibilità.

Nel caso in esame, applichiamo il *Criterio di Eisenstein* come segue. Osservando che $R := \mathbb{Z}[x,y] = \big(\mathbb{Z}[x]\big)[y]$ — cioè identificando i polinomi in x e y a coefficienti in $\mathbb{Z}$ con i polinomi in y a coefficienti in $\mathbb{Z}[x]$ — osserviamo che $D := \mathbb{Z}[x]$ è un dominio a fattorizzazione unica (perchè tale è l'anello $\mathbb{Z}$, e allora possiamo applicare il *Teorema del*

Trasporto di Gauss), e quindi agli elementi dell'anello di polinomi $R = D[y]$ possiamo applicare il criterio di irriducibilità di Eisenstein. Nel caso in esame, riscrivendo $h(x,y)$ come polinomio in y a coefficienti in $\mathbb{Z}[x]$ troviamo

$$h(x,y) \,:=\, y^3 - 3\,x^2\,y + 6\,x\,y + 5\,x - 3\,y - 5 \,=\, y^3 - 3\,(x-1)^2\,y + 5\,(x-1)$$

cioè

$$h(x,y) = \sum_{k=0}^{3} a_k\,y^k \;\text{ con }\; a_0 = (x-1),\, a_1 = -3\,(x-1)^2,\, a_2 = 0,\, a_3 = 1 \,\in D := \mathbb{Z}[x] \quad (1.1)$$

Ora, dalla (1.1) osserviamo che l'elemento $q := (x-1) \in D[x] \setminus \{0\}$, che è chiaramente irriducibile in $D := \mathbb{Z}[x]$, ha la proprietà che

$$(x-1) \nmid a_3\,, \quad (x-1) \,\big|\, a_2\,, \quad (x-1) \,\big|\, a_1\,, \quad (x-1) \,\big|\, a_0\,, \quad (x-1)^2 \nmid a_0 \qquad (1.2)$$

pertanto possiamo applicare il *Criterio di Eisenstein* che ci garantisce che il polinomio $h(x,y)$ è irriducibile in $D[y] = R$. Per quanto già discusso, ne segue allora che $h(x,y)$ è anche primo, quindi l'ideale principale $I := \big(h(x,y)\big)$ da esso generato in $R := \mathbb{Z}[x,y]$ è un ideale primo, e quindi il quoziente $R/I = \mathbb{Z}[x,y]\Big/\big(h(x,y)\big)$ è un dominio, q.e.d.

(b) Dimostriamo che l'anello quoziente $\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big)$ è un dominio a fattorizzazione unica osservando che è isomorfo ad un altro anello che sappiamo essere un dominio a fattorizzazione unica.

Consideriamo il morfismo di anelli

$$ev_{x=3\,y^2-y-5} : \mathbb{Z}[x,y] \longrightarrow\!\!\!\!\!\!\rightarrow \mathbb{Z}[y] \;\;,\quad f(x,y) \,\mapsto\, f\big(3\,y^2 - y - 5\,,\, y\big) \qquad (1.3)$$

Tale morfismo è ovviamente suriettivo, in quanto

$$ev_{x=3\,y^2-y-5}\big(p(y)\big) \;=\; p(y) \qquad \forall\;\, p(y) \in \mathbb{Z}[y] \subseteq \mathbb{Z}[x,y] \qquad (1.4)$$

Inoltre, $ev_{x=3\,y^2-y-5}$ ha nucleo

$$Ker\big(ev_{x=3\,y^2-y-5}\big) \;=\; \big(\,x - 3\,y^2 + y + 5\,\big) \;=\; \big(-\ell(x,y)\,\big) \;=\; \big(\,\ell(x,y)\,\big) \qquad (1.5)$$

Infatti, è chiaro che $J := \big(\,x - 3\,y^2 + y + 5\,\big) = \big(-\ell(x,y)\,\big) = \big(\,\ell(x,y)\,\big)$ e anche che vale l'inclusione $J := \big(\,x - 3\,y^2 + y + 5\,\big) \subseteq Ker\big(ev_{x=3\,y^2-y-5}\big)$, in quanto chiaramente si ha $ev_{x=3\,y^2-y-5}\big(\,x - 3\,y^2 + y + 5\,\big) = \big(\,3\,y^2 - y - 5\,\big) - 3\,y^2 + y + 5 \,=\, 0$. Inoltre, per ogni $f(x,y) \in \mathbb{Z}[x,y] = \big(\mathbb{Z}[y]\big)[x]$ possiamo fare la divisione con resto

$$f(x,y) \;=\; \big(\,x - 3\,y^2 + y + 5\,\big)\cdot q(x,y) \,+\, r(x,y) \qquad (1.6)$$

— pensando $d(x,y) \,:=\, x - 3\,y^2 + y + 5 \,=\, x - \big(\,3\,y^2 - y - 5\,\big) \,\in\, \big(\mathbb{Z}[y]\big)[x] = \mathbb{Z}[x,y]$ come polinomio in x a coefficienti in $\mathbb{Z}[x]$ — con $q(x,y), r(x,y) \,\in\, \big(\mathbb{Z}[y]\big)[x] \,=\, \mathbb{Z}[x,y]$ tali che — indicando con $\partial_x\big(k(x,y)\big)$ il *grado rispetto ad* x di un qualsiasi polinomio $k(x,y) \in \big(\mathbb{Z}[y]\big)[x] = \mathbb{Z}[x,y]$ — si abbia $r(x,y) = 0$ oppure $\partial_x\big(r(x,y)\big) \lneq \partial_x\big(d(x,y)\big)$; e

siccome è $\partial_x\big(d(x,y)\big) = 1$, in ogni caso sarà $\partial_x\big(r(x,y)\big) = 0$, quindi $\partial_x\big(r(x,y)\big) \in \mathbb{Z}[y]$, da cui segue in particolare, per la (1.4), che

$$ev_{x=3\,y^2-y-5}\big(r(x,y)\big) \;=\; r(x,y) \tag{1.7}$$

N.B.: la divisione con resto in (1.6) è sempre possibile perché il polinomio divisore $d(x,y) := x - \big(3\,y^2 - y - 5\big)$ è *monico* (come polinomio in x).

Ora, siccome $ev_{x=3\,y^2-y-5}$ è un morfismo e $ev_{x=3\,y^2-y-5}\big(x - 3\,y^2 + y + 5\big) \;=\; 0$, l'identità (1.6) ci dà $ev_{x=3\,y^2-y-5}\big(f(x,y)\big) \;=\; ev_{x=3\,y^2-y-5}\big(r(x,y)\big) \;=\; r(x,y)$. Pertanto, se prendiamo $f(x,y) \in Ker\big(ev_{x=3\,y^2-y-5}\big)$ abbiamo

$$0 \;=\; ev_{x=3\,y^2-y-5}\big(f(x,y)\big) \;=\; r(x,y)$$

così che la (1.6) diventa

$$f(x,y) \;=\; \big(x - 3\,y^2 + y + 5\big)\cdot q(x,y) \;\in\; \big(x - 3\,y^2 + y + 5\big)$$

e quindi la (1.5) è completamente dimostrata.

A questo punto, mettendo insieme la suriettività del morfismo in (1.2) e la descrizione del suo nucleo data in (1.5), il *Teorema Fondamentale di Omomorfismo* per anelli ci consente di concludere che

$$\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big) \;=\; \mathbb{Z}[x,y]\Big/Ker\big(ev_{x=3\,y^2-y-5}\big) \;\cong\; Im\big(ev_{x=3\,y^2-y-5}\big) \;=\; \mathbb{Z}[y]$$

dunque in breve abbiamo un isomorfismo di anelli $\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big) \;\cong\; \mathbb{Z}[y]$. Ora, poiché $\mathbb{Z}$ è un dominio a fattorizzazione unica, per il *Teorema del Trasporto* di Gauss anche l'anello $\mathbb{Z}[y]$ è a sua volta un dominio a fattorizzazione unica, e quindi pure $\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big)$, essendo isomorfo a $\mathbb{Z}[y]$, è un dominio a fattorizzazione unica, q.e.d.

(c) Analogamente a quanto fatto in *(b)*, dimostriamo che l'anello in esame *non* è un dominio a ideali principali osservando che è isomorfo ad un altro anello del quale sappiamo che *non* è un dominio a ideali principali. In dettaglio, abbiamo visto in *(b)* che c'è un isomorfismo di anelli $\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big) \;\cong\; \mathbb{Z}[y]$: ora, sappiamo che l'anello $\mathbb{Z}[y]$ *non* è un dominio a ideali principali, ad esempio perché l'ideale $(2\,,x)$ certamente non è principale; pertanto possiamo dedurre che anche l'anello $\mathbb{Z}[x,y]\Big/\big(\ell(x,y)\big)$ non è un dominio a ideali principali, q.e.d.

(d) La stessa analisi fatta per il punto *(b)* — sostituendo $\mathbb{Z}$ con il suo campo dei quozienti $\mathbb{Q}$ — dimostrare che l'anello quoziente $\mathbb{Q}[x,y]\Big/\big(\ell(x,y)\big)$ è isomorfo all'anello di polinomi $\mathbb{Q}[y]$, tramite un isomorfismo indotto — mediante il Teorema Fondamentale di Omomorfismo per anelli — dal morfismo suriettivo

$$ev^{\mathbb{Q}}_{x=3\,y^2-y-5} : \mathbb{Q}[x,y] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Q}[y] \;\;,\quad f(x,y) \mapsto f\big(3\,y^2 - y - 5\,,\,y\big)$$

analogo quello in (1.3). Ma sappiamo senz'altro che l'anello $\mathbb{Q}[y]$ dei polinomi in *una* variabile a coefficienti nel *campo* $\mathbb{Q}$ è *un dominio euclideo*, quindi possiamo concludere che $\mathbb{Q}[x,y]\Big/\big(\ell(x,y)\big)$, essendo isomorfo a $\mathbb{Q}[y]$, è a sua volta un dominio euclideo, q.e.d.

[2] — Procediamo alla soluzione dell'esercizio punto per punto.

(a) Per cominciare osserviamo che l'anello $\mathbb{Z}_{26}$ è finito e che il prodotto in esso è commutativo, quindi il gruppo $U(\mathbb{Z}_{26})$ considerato al punto *(b)* è un gruppo finito abeliano. In particolare, allora, per ogni primo p che divida l'ordine del gruppo $U(\mathbb{Z}_{26})$ esisterà esattamente *uno e un solo* p–sottogruppo di Sylow in $U(\mathbb{Z}_{26})$.

L'ordine del gruppo $U(\mathbb{Z}_{26})$ è dato da

$$\big|U(\mathbb{Z}_{26})\big| \,=\, \varphi(26) \,=\, \varphi(2\cdot 13) \,=\, \varphi(2)\cdot\varphi(13) \,=\, (2-1)\cdot(13-1) \,=\, 1\cdot 12 \,=\, 12 \,=\, 3\cdot 2^2$$

cioè in breve $\big|U(\mathbb{Z}_{26})\big| \,=\, 12 \,=\, 3\cdot 2^2$. Pertanto, i soli primi che dividano $\big|U(\mathbb{Z}_{26})\big|$ sono 3 e 2, quindi esiste uno e un solo 3–sottogruppo di Sylow Σ_3, di ordine 3, ed esiste uno e un solo 2–sottogruppo di Sylow Σ_2, di ordine $2^2 = 4$. Sappiamo poi che il gruppo $U(\mathbb{Z}_{26})$ è (isomorfo a il) prodotto diretto dei suoi sottogruppi di Sylow, dunque

$$U(\mathbb{Z}_{26}) \;\cong\; \Sigma_3 \times \Sigma_2 \tag{2.1}$$

Il 3–sottogruppo di Sylow Σ_3, essendo di ordine 3 che è primo, è necessariamente isomorfo a $\mathbb{Z}_3$; in particolare è ciclico, generato da un qualsiasi elemento di ordine 3. Invece il 2–sottogruppo di Sylow Σ_2 ha ordine $2^2 = 4$, quindi Σ_2 è (necessariamente) isomorfo a $\mathbb{Z}_4$ *oppure* a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Ora, come si distinguono tra loro i due casi $\Sigma_2 \cong \mathbb{Z}_4$ e $\Sigma \cong \mathbb{Z}_2 \times \mathbb{Z}_2$? La differenza sta in questo: nel gruppo $\mathbb{Z}_4$ (con la somma come operazione) esistono due elemento di ordine 4 — precisamente le classi $[1]_4$ e $[3]_4$ — mentre nel gruppo $\mathbb{Z}_2 \times \mathbb{Z}_2$ — con la somma componente per componente come operazione — *non* esistono elementi di ordine 4 (ogni elemento a ordine 2 oppure 1); in particolare, nel primo caso $\Sigma_2 \cong \mathbb{Z}_4$ è ciclico generato da un qualsiasi elemento di ordine 4, nel secondo caso invece $\Sigma_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ è generato da due qualsiasi elementi di ordine 2 che siano distinti tra loro e dai rispettivi inversi. Quindi, indicando con $\omega(\,\overline{z}\,)$ l'ordine (moltiplicativo, cioè rispetto all'operazione di moltiplicazione!) di un elemento $\overline{z} \in U(\mathbb{Z}_{26})$, avremo

$$\Sigma_2 \;\cong\; \mathbb{Z}_4 \quad\Longleftrightarrow\quad \exists\;\, \overline{z} \in U(\mathbb{Z}_{26}) \,:\, \omega(\,\overline{z}\,) = 4 \tag{2.2}$$

come anche, equivalentemente,

$$\Sigma_2 \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}_2 \quad\Longleftrightarrow\quad \nexists\;\, \overline{z} \in U(\mathbb{Z}_{26}) \,:\, \omega(\,\overline{z}\,) = 4 \tag{2.3}$$

Per sapere quale tra le due possibilità (2.2) e (2.3) si presenta, dobbiamo fare qualche calcolo esplicito, che serve anche a descrivere esplicitamente Σ_2 così come Σ_3. Sappiamo che $U(\mathbb{Z}_{26})$ è dato esplicitamente da

$$U(\mathbb{Z}_{26}) \;=\; \big\{\, \overline{z} \in \mathbb{Z}_{26} \,\big|\, \mathrm{MCD}(z\,,26) = 1 \,\big\} \;=\; \big\{\, \overline{1}\,,\overline{3}\,,\overline{5}\,,\overline{7}\,,\overline{9}\,,\overline{11}\,,\overline{15}\,,\overline{17}\,,\overline{19}\,,\overline{21}\,,\overline{23}\,,\overline{25} \,\big\}$$

A questo punto i calcoli espliciti ci danno

$$\overline{3}^{\,1} = \overline{3}\,,\quad \overline{3}^{\,2} = \overline{9}\,,\quad \overline{3}^{\,3} = \overline{27} = \overline{1}\,,\quad\Longrightarrow\quad \omega(\,\overline{3}\,) \,=\, 3 \quad\Longrightarrow\quad \Sigma_3 \,=\, \big\langle\, \overline{3}\,\big\rangle \,=\, \big\{\, \overline{1}\,,\overline{3}\,,\overline{9}\,\big\}$$

che ci dà una descrizione esplicita dell'unico 3–sottogruppo di Sylow Σ_3, precisamente

$$\Sigma_3 \;=\; \big\{\, \overline{1}\,,\overline{3}\,,\overline{9}\,\big\} \tag{2.4}$$

Analogamente abbiamo anche

$$\overline{5}^{\,1} = \overline{5}\,, \quad \overline{5}^{\,2} = \overline{25} = \overline{-1}\,, \quad \overline{5}^{\,3} = \overline{-5} = \overline{21}\,, \quad \overline{5}^{\,4} = \overline{-25} = \overline{1}\,, \quad \Longrightarrow \quad \omega(\overline{5}) = 4 \quad \Longrightarrow$$
$$\Longrightarrow \quad \Sigma_2 = \langle \overline{5} \rangle = \{ \overline{1}\,, \overline{5}\,, \overline{25}\,, \overline{21} \}$$

che ci dà una descrizione esplicita dell'unico 2–sottogruppo di Sylow Σ_2, che è il sottogruppo *ciclico* di ordine 4 dato da

$$\Sigma_2 \;=\; \langle \overline{5} \rangle \;=\; \{ \overline{1}\,, \overline{5}\,, \overline{25}\,, \overline{21} \} \tag{2.5}$$

Complessivamente, la (2.4) e la (2.5) rispondono al quesito *(a)*.

(b) Come già osservato al punto *(a)*, il gruppo $U(\mathbb{Z}_{26})$ è finito e abeliano: pertanto, l'esistenza di una decomposizione del tipo richiesto è assicurata da un opportuno teorema di classificazione/struttura. Dalla teoria generale sappiamo che un tale gruppo è (isomorfo al) prodotto diretto di tutti i suoi sottogruppi di Sylow: quindi nel caso in esame è

$$U(\mathbb{Z}_{26}) \;\cong\; \Sigma_3 \times \Sigma_2 \tag{2.6}$$

Inoltre, dall'analisi fatta al punto *(a)* sappiamo che $\Sigma_3 \cong \mathbb{Z}_3$ e $\Sigma_2 \cong \mathbb{Z}_4$, che insieme alla (2.6) ci danno

$$U(\mathbb{Z}_{26}) \;\cong\; \Sigma_3 \times \Sigma_2 \;\cong\; \mathbb{Z}_3 \times \mathbb{Z}_4 \;\cong\; \mathbb{Z}_{3\cdot 4} \;=\; \mathbb{Z}_{12}$$

dove l'isomorfismo in $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{3\cdot 4}$ è dato dal Teorema Cinese del Resto. In conclusione, abbiamo

$$U(\mathbb{Z}_{26}) \;\cong\; \mathbb{Z}_{12}$$

che è esattamente la (unica) decomposizione del gruppo $U(\mathbb{Z}_{26})$ in prodotto diretto di gruppi ciclici richiesta: si tratta di un caso particolare, nel senso che la decomposizione è composta da un solo fattore, ma non per questo è meno corretta.

N.B.: si noti invece che la decomposizione $U(\mathbb{Z}_{26}) \cong \mathbb{Z}_3 \times \mathbb{Z}_4$ *non è del tipo richiesto*, in quanto i due fattori ciclici hanno ordini 3 e 4 con $4 \not| 3$ (e anche cambiando l'ordine dei fattori non si avrebbe quanto richiesto).

[3] — Possiamo farci guidare da alcune idee fondamentali:

<u>*Prima idea:*</u> i sottogruppi normali N di un gruppo G sono tutti e soli i nuclei dei morfismi che abbiano G come dominio; in aggiunta, se $\rho : G \longrightarrow \Gamma$ è un tale morfismo (di gruppi) e $N = Ker(\rho)$, allora il *Teorema Fondamentale di Omomorfismo* per gruppi garantisce che ρ induce un morfismo iniettivo $\rho_* : G/N = G/Ker(\rho) \hookrightarrow \Gamma$.

<u>*Seconda idea:*</u> l'indice $(G : K)$ di un sottogruppo K in un gruppo G è la cardinalità dell'insieme delle classi laterali (destre o sinistre, è equivalente) di K in G; quando in più K è (sottogruppo) *normale*, tale cardinalità è l'ordine del gruppo quoziente G/K.

<u>*Terza idea:*</u> per ogni sottogruppo Λ in un gruppo Γ, l'ordine $|\Lambda|$ di Λ divide l'ordine $|\Gamma|$ di Γ.

<u>*Quarta idea:*</u> per ogni $n \in \mathbb{N}_+$, il fattoriale $n!$ è l'ordine del gruppo simmetrico $\mathcal{S}_n$ su n elementi, cioè $n! = |\mathcal{S}_n| = |\mathcal{S}(X_n)|$ dove $\mathcal{S}(X_n)$ indica il gruppo delle permutazioni di

un qualsiasi insieme X_n di cardinalità n, cioè con n elementi: *ad esempio*, un tale insieme X_n è, per ipotesi, $X_n := G/H$ dato che $\left|G/H\right| := (G : H)$.

Quinta idea: ogni morfismo di gruppi $\rho : G \longrightarrow \mathcal{S}(Y)$ corrisponde — in modo biunivoco ed esplicito — ad una azione del gruppo G sull'insieme Y.

Con queste idee in mente, cerchiamo di ottenere $N \trianglelefteq G$ contenente H come nucleo di un opportuno morfismo di gruppi $\rho : G \longrightarrow \Gamma$ in cui sia $\Gamma := \mathcal{S}(X_n)$ con $X_n := G/H$: infatti, dato che $\left|G/H\right| := (G : H)$, le nostre ipotesi dicono proprio che $X_n := G/H$ ha cardinalità n.

Considerando un tale morfismo $\rho : G \longrightarrow \mathcal{S}\big(G/H\big)$ esista, e ponendo $N := Ker\,(\rho)$ esso indurrà un monomorfismo $\rho_* : G/N \lhook\joinrel\longrightarrow \mathcal{S}\big(G/H\big)$, tramite il quale in particolare si ha $G/H \cong Im\,(\rho_*) = Im\,(\rho)$ e quindi $(G : N) = \left|G/N\right| = \big|Im\,(\rho)\big|$. Ora, $Im\,(\rho)$ è un sottogruppo di $\mathcal{S}\big(G/H\big)$, che è un gruppo di di ordine $\left|G/H\right|! = (G : H)! = n!$; allora il *Teorema di Lagrange* dà $\big|Im\,(\rho)\big| \,\Big|\, n!$, e quindi in conclusione $(G : N) \,\Big|\, n!$. Dunque abbiamo trovato che per un *qualsiasi* morfismo di gruppi $\rho : G \longrightarrow \mathcal{S}\big(G/H\big)$, posto $N := Ker\,(\rho)$ si ha $N \trianglelefteq G$ con $(G : N) \,\Big|\, n!$. Ma in aggiunta, *a noi è richiesto che sia anche* $N \leq H$, cioè (dato che comunque N è un sottogruppo) che sia $N \subseteq H$.

N.B.: altrimenti, basterebbe prendere $N := G$, corrispondente al morfismo ρ banale, cioè costante, per il quale si ha $(G : N) = 1$ ...

A questo punto occorre e basta trovare un morfismo di gruppi $\rho : G \longrightarrow \mathcal{S}\big(G/H\big)$ per il quale $N := Ker\,(\rho)$ soddisfi la condizione $N \subseteq H$.

In base alla *quinta idea*, il morfismo cercato $\rho : G \longrightarrow \mathcal{S}\big(G/H\big)$ corrisponde ad un'azione $\sigma : G \times \big(G/H\big) \longrightarrow G/H$. Ora, una tale azione ad esempio è quella indotta dall'azione regolare sinistra di G su sé stesso quest'ultima è data da

$$\lambda : G \times G \longrightarrow G \quad , \qquad\qquad (g\,,\gamma) \;\mapsto\; \lambda(g\,,\gamma) := g\,\gamma \qquad \forall\;\; g \in G\,,\;\gamma \in G$$

e induce l'azione di G su G/H data da

$$\sigma_{_H} : G \times \big(G/H\big) \longrightarrow G/H \quad , \quad \big(g\,,\gamma H\big) \mapsto \sigma\big(g\,,\gamma H\big) := (g\,\gamma)H \quad \forall\;\; g \in G\,,\;\gamma H \in G/H$$

Sia dunque $\rho_{_H} : G \longrightarrow \mathcal{S}\big(G/H\big)$ il morfismo di gruppi corrispondente all'azione $\sigma_{_H}$, e $N := Ker\,(\rho_{_H})$. Per definizione $\rho_{_H}$ è dato da

$$\big(\rho_{_H}(g)\big)(\gamma H) \;:=\; \sigma\big(g\,,\gamma H\big) \;=\; (g\,\gamma)H \qquad\qquad \forall\;\; g \in G\,,\;\gamma H \in G/H$$

e quindi

$$N \;:=\; Ker\,(\rho_{_H}) \;=\; \Big\{\, g \in G \,\Big|\, \rho_{_H}(g) = \mathrm{id}_{_{G/H}} \Big\} \;=\; \Big\{\, g \in G \,\Big|\, (\,g\,\gamma)H = \gamma H \;\; \forall\,\gamma \in G \,\Big\} \quad (3.1)$$

Ma la condizione $(\,g\,\gamma)H = \gamma H \;\; \big(\forall\,\gamma \in G\big)$ implica in particolare (per $\gamma = e_{_G}$) che $gH = H$ che a sua volta equivale a $g \in H$; questo e la (3.1) danno $N \subseteq H$, q.e.d.

[4] — Per rispondere ai diversi quesiti, indaghiamo la struttura del gruppo G studiandone numero e natura dei sottogruppi di Sylow, e come essi "interagiscano" tra loro.

Per cominciare, dato che $|G| = 231 = 3 \cdot 7 \cdot 11$, il gruppo G possiede almeno un p–sottogruppo di Sylow se e soltanto se $p \in \{3, 7, 11\}$. Inoltre, ricordiamo che il numero ν_{p_i} di p_i–sottogruppi di Sylow in un qualsiasi gruppo finito Γ di ordine $|\Gamma| =: n$ la cui fattorizzazione in primi sia $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_1}$ ha queste proprietà:

$$\nu_{p_i} \equiv 1 \pmod{p_i} \quad \& \quad \nu_{p_i} \,\Big|\, \big(n/p_i\big) = \prod_{\substack{j=1 \\ j \neq i}}^{k} p_j^{e_j} \,, \quad \text{in breve} \quad \nu_{p_i} \in \big(1 + p_i \mathbb{N}\big) \bigcap Div\big(n/p_i\big) \tag{4.1}$$

dove $Div\big(n/p_i\big)$ indica l'insieme dei divisori di n/p_i in $\mathbb{N}_+$. Nel caso in esame — con $\Gamma := G$, $n = 231$, $p_1 = 3$, $p_2 = 7$, $p_3 = 11$, $e_1 = e_2 = e_3 = 1$ — la (4.1) ci dà

$$\nu_3 \in \big(1 + 3\,\mathbb{N}\big) \bigcap \{1, 7, 11, 77\} = \{1, 7\} \quad \Longrightarrow \quad \nu_3 \in \{1, 7\} \tag{4.2}$$

$$\nu_7 \in \big(1 + 7\,\mathbb{N}\big) \bigcap \{1, 3, 11, 33\} = \{1\} \quad \Longrightarrow \quad \nu_7 = 1 \tag{4.3}$$

$$\nu_{11} \in \big(1 + 11\,\mathbb{N}\big) \bigcap \{1, 3, 7, 21\} = \{1\} \quad \Longrightarrow \quad \nu_{11} = 1 \tag{4.4}$$

In particolare, la (4.3) dice che esiste un unico 7–sottogruppo di Sylow, che indichiamo con N_7, e la (4.4) dice che esiste un unico 11–sottogruppo di Sylow, che indichiamo con N_{11}. La teoria generale dice che se esiste esattamente uno e un solo p–sottogruppo di Sylow, allora esso è normale: pertanto, nel caso in esame concludiamo che N_7 e N_{11} sono entrambi sottogruppi normali in G, in formule

$$N_7 \trianglelefteq G \quad , \qquad N_{11} \trianglelefteq G \tag{4.5}$$

D'altra parte, i sottogruppi Σ_3, N_7 e N_{11} hanno tutti ordine primo (rispettivamente 3, 7 e 11) e quindi sono necessariamente isomorfi al gruppo ciclico di quell'ordine, cioè

$$H_3 \cong \mathbb{Z}_3 \quad , \qquad N_7 \cong \mathbb{Z}_7 \quad , \qquad N_{11} \cong \mathbb{Z}_{11} \tag{4.6}$$

Procediamo adesso a rispondere ai singoli quesiti.

(a) Sia Σ_3 un 3–sottogruppo di Sylow in G (che certamente esiste); ora, siccome N_{11} è un sottogruppo *normale*, il prodotto insiemistico $\Sigma_3 N_{11}$ coincide con $\Sigma_3 N_{11}$ e (quindi) è un sottogruppo di G, che indichiamo con $H_{33} := \Sigma_3 N_{11}$. Inoltre, per il *Teorema di Lagrange* abbiamo che $\Sigma_3 \cap N_{11} = \{e_{_G}\}$ — perché è un sottogruppo di G il cui ordine divide $|\Sigma| = 3$ e $|N_{11}| = 11$, dunque è 1; ne segue che $H_{33} := \Sigma_3 N_{11}$ è (isomorfo a) un prodotto semidiretto $\Sigma_3 \ltimes N_{11}$, quindi in particolare ha ordine

$$|H_{33}| \,=\, \big|\Sigma_3 \ltimes N_{11}\big| \,=\, |\Sigma_3| \cdot |N_{11}| \,=\, 3 \cdot 11 \,=\, 33$$

dunque H_{33} è un sottogruppo G di ordine 33.

Adesso osserviamo anche che il suddetto prodotto semidiretto $H_{33} = \Sigma_3 \ltimes N_{11}$ è in effetti banale, cioè è il prodotto *diretto* $H_3 \times N_{11}$. Infatti, tale prodotto semidiretto dipende da un morfismo di gruppi $\Phi : \Sigma_3 \longrightarrow Aut_{\mathcal{G}}(N_{11})$, ed è un prodotto diretto solo se tale morfismo Φ è *banale*, nel senso che è il morfismo costante dato da $\Phi(\sigma) = \mathrm{id}_{N_{11}}$ per ogni $\sigma \in \Sigma_3$. Infatti, il gruppo $\Sigma_3 \cong \mathbb{Z}_3$ ha ordine 3, mentre il gruppo $Aut_{\mathcal{G}}(N_{11}) \cong Aut_{\mathcal{G}}(Z_{11}) \cong U(\mathbb{Z}_{10}) \cong \mathbb{Z}_{10}$ ha ordine 10; ma allora l'ordine del gruppo

$Im\,(Phi)$ divide 10 (che è l'ordine del gruppo $Aut_{\mathcal{G}}(Z_{11}) \cong U(\mathbb{Z}_{11})$ di cui $Im\,(Phi)$ è sottogruppo) e inoltre divide 3 (perché $Im\,(Phi)$ è isomorfo a $\Sigma_3 / Ker\,(Phi)$ il cui ordine è l'indice $\big(\Sigma_3 : Ker\,(Phi)\big)$ e come tale divide l'ordine di Σ_3, che è appunto 3), e quindi necessariamente $Im\,(Phi) = 1$ che significa proprio che Φ è il morfismo costante!

A questo punto abbiamo (tenendo in conto (4.6) e il Teorema Cinese del Resto) che

$$H_{33} \cong H_3 \times N_{11} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{3\cdot 11} = \mathbb{Z}_{33} \quad , \qquad \text{cioè} \qquad H_{33} \cong \mathbb{Z}_{33}$$

e quindi concludiamo che H_{33} è un sottogruppo *ciclico* G di ordine 33, q.e.d.

NOTA: in modo del tutto analogo, si può dimostrare anche che il gruppo G contiene il sottogruppo $H_{21} = \Sigma_3 N_7 = N_7 \Sigma_3$ che è (isomorfo a) un prodotto semidiretto $\Sigma_3 \ltimes N_7$, quindi in particolare ha ordine $3 \cdot 7 = 21$. Tuttavia, esistono certamente dei morfismi di gruppi *non banali* (cioè non costanti) da $\Sigma_3 \cong \mathbb{Z}_3$ (che ha ordine 3) a $Aut_{\mathcal{G}}(N_7) \cong Aut_{\mathcal{G}}(\mathbb{Z}_7) \cong U(\mathbb{Z}_7) \cong \mathbb{Z}_6$ (che ha ordine 6): da questo segue allora che esistono anche prodotti semidiretti del tipo $\Sigma_3 \ltimes N_7$ che *non sono* banali, cioè non sono il prodotto diretto; pertanto, non è detto che $H_{21} \cong \Sigma_3 \ltimes N_7$ sia isomorfo al gruppo ciclico $\mathbb{Z}_{21}$ — anzi, esistono senz'altro esempi di casi in cui non lo è.

(b) Sia ora N_7 l'*unico* 7–sottogruppo di Sylow in G — come in (4.5). Operando analogamente a quanto fatto per *(a)*, dato che N_{11} è un sottogruppo *normale*, abbiamo che il prodotto insiemistico $N_{77} := N_7 N_{11} = N_{11} N_7$ è sottogruppo di G. Inoltre, ancora per il *Teorema di Lagrange* abbiamo che $N_7 \cap N_{11} = \{e_{_G}\}$ — perché è un sottogruppo di G il cui ordine divide $|N_7| = 7$ e $|N_{11}| = 11$, dunque è 1 — e quindi N_{77} è (isomorfo a) un prodotto semidiretto $N_7 \ltimes N_{11}$, quindi in particolare ha ordine

$$|N_{77}| \,=\, \big|N_7 \ltimes N_{11}\big| \,=\, |N_7| \cdot |N_{11}| \,=\, 7 \cdot 11 \,=\, 77 \tag{4.8}$$

dunque N_{77} è un sottogruppo di G di ordine 77. In aggiunta, siccome N_7 e N_{11} sono entrambi normali, anche il loro prodotto $N_7 N_{11} =: N_{77}$ è *normale*, in quanto si ha

$$g\, N_{77}\, g^{-1} \,=\, g\, N_7\, N_{11}\, g^{-1} \,=\, g\, N_7\, g^{-1}\, g\, N_{11}\, g^{-1} \,=\, N_7\, N_{11} \,=:\, N_{77} \qquad \forall\ g \in G$$

e quindi abbiamo che N_{77} è un sottogruppo normale di G che è normale.

Infine, osserviamo che nel prodotto semidiretto $N_7 \ltimes N_{11} = N_{77}$ *entrambi* i fattori sono normali: pertanto (per una proprietà generale) tale prodotto è necessariamente *diretto*, così che $N_{77} = N_7 \times N_{11}$. Ne segue allora, per il Teorema Cinese del Resto, che

$$N_{77} \,=\, N_7 \times N_{11} \,\cong\, \mathbb{Z}_7 \times \mathbb{Z}_{11} \,\cong\, \mathbb{Z}_{7\cdot 11} \,\cong\, \mathbb{Z}_{77}$$

Pertanto N_{77} è un sottogruppo ciclico di G di ordine 77, q.e.d.

(c) Dall'analisi al punto *(a)* sappiamo che il sottogruppo N_{11} è contenuto nel sottogruppo $\Sigma_3\, N_{11} =: H_{33}\big(\cong \mathbb{Z}_{33}\big)$ e nel sottogruppo $N_7\, N_{11} =: N_{77}\big(\cong \mathbb{Z}_{77}\big)$, che sono entrambi gruppi (ciclici, e quindi) abeliani: in particolare quindi gli elementi di N_{11} commutano con gli elementi di Σ_3 e con gli elementi di N_7, e ovviamente commutano anche tra di loro. Inoltre, $\Sigma_3 \cap N_{77}$ è sottogruppo di Σ_3 e di $\mathbb{N}_{77}$, quindi — per il Teorema di Lagrange — ha un ordine che divide sia 3 che 77, perciò tale ordine è 1, dunque $\Sigma_3 \cap N_{77} = \{e_{_G}\}$. Allora da $\Sigma_3 \leq G$, $\mathbb{N}_{77} \trianglelefteq G$ deduciamo che $\Sigma_3 \mathbb{N}_{77} \leq G$, e aggiungendo che $\Sigma_3 \cap N_{77} = \{e_{_G}\}$ abbiamo anche che $\Sigma_3 \mathbb{N}_{77} \cong \Sigma_3 \ltimes N_{77}$, da cui anche

$$\big|\Sigma_3 \mathbb{N}_{77}\big| \,=\, \big|\Sigma_3 \ltimes N_{77}\big| \,=\, \big|\Sigma_3\big| \cdot \big|N_{77}\big| \,=\, 3 \cdot 77 \,=\, 231 \,=\, |G|$$

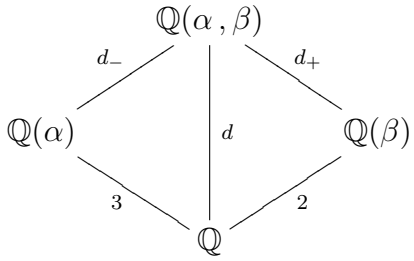
Dunque abbiamo $\Sigma_3 \mathbb{N}_{77} \leq G$ con $\big|\Sigma_3 \mathbb{N}_{77}\big| = 231 = |G|$, da cui $\Sigma_3 \mathbb{N}_{77} = G$.

Ora, abbiamo osservato in precedenza che gli elementi di N_{11} commutano con tutti gli elementi di Σ_3, con tutti gli elementi di N_{11} e con tutti gli elementi di N_7. Ma allora commutano anche con tutti gli elementi del prodotto $\Sigma_3 \mathbb{N}_7 N_{11} = \Sigma_3 \mathbb{N}_{77} = G$, cioè con tutti gli elementi di G. Pertanto

$$N_{11} \subseteq \big\{ z \in G \,\big|\, z\,g = g\,z \;\; \forall\, g \in G \big\} =: Z(G)$$

da cui, siccome N_{11} è non banale, concludiamo che anche $Z(G)$ è non banale, q.e.d.

[5] — Cominciamo osservando che possiamo considerare il seguente diagramma di estensioni di campi



(5.1)

in cui i simboli a fianco dei segmenti indicano il grado della rispettiva estensione di campi, precisamente

$$\big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}(\alpha)\,\big] =: d_- \;\;,\quad \big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}(\beta)\,\big] =: d_+ \;\;,\quad \big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}\,\big] =: d$$
$$\big[\,\mathbb{Q}(\alpha) : \mathbb{Q}\,\big] = 3 \quad , \qquad \big[\,\mathbb{Q}(\beta) : \mathbb{Q}\,\big] = 2$$

Le ultime due identitá sono dovute al fatto che

$$\big[\,\mathbb{Q}(\alpha) : \mathbb{Q}\,\big] \;=\; \partial\big(p_\alpha(x)\big) \;=\; \partial\big(x^3 - 5\big) \;=\; 3$$

e analogamente

$$\big[\,\mathbb{Q}(\beta) : \mathbb{Q}\,\big] \;=\; \partial\big(p_\beta(x)\big) \;=\; \partial\big(x^2 + 3\big) \;=\; 2$$

più precisamente, nel primo caso si ha $\big[\,\mathbb{Q}(\alpha) : \mathbb{Q}\,\big] = 3$ con $\big\{1\,,\alpha\,,\alpha^2\,\big\}$ come base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$, mentre nel secondo caso abbiamo $\big[\,\mathbb{Q}(\beta) : \mathbb{Q}\,\big] = 2$ con $\big\{1\,,\beta\,\big\}$ come base di $\mathbb{Q}(\beta)$ su $\mathbb{Q}$. Per le prime identità invece, abbiamo che

$$\big[\,\mathbb{Q}(\beta) : \mathbb{Q}\,\big] \;=\; 2 \quad\Longrightarrow\quad d_- \;:=\; \big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}(\alpha)\,\big] \;=\; \big[\,\big(\mathbb{Q}(\alpha)\big)(\beta) : \mathbb{Q}(\alpha)\,\big] \;\leq\; 2$$

in quanto il polinomio $p_\beta(x)$, che si annulla in $x = \beta$, appartiene a $\mathbb{Q}[x]$ e quindi anche a $\big(\mathbb{Q}(\alpha)\big)[x]$, per cui β è algebrico su $\mathbb{Q}(\alpha)$ di grado al più $\partial\big(p_\beta(x)\big) = 2$. Analogamente, abbiamo

$$\big[\,\mathbb{Q}(\alpha) : \mathbb{Q}\,\big] \;=\; 3 \quad\Longrightarrow\quad d_+ \;:=\; \big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}(\beta)\,\big] \;=\; \big[\,\big(\mathbb{Q}(\beta)\big)(\alpha) : \mathbb{Q}(\beta)\,\big] \;\leq\; 3$$

in quanto il polinomio $p_\alpha(x)$, che si annulla in $x = \alpha$, appartiene a $\mathbb{Q}[x]$ e quindi anche a $\big(\mathbb{Q}(\beta)\big)[x]$, per cui α è algebrico su $\mathbb{Q}(\beta)$ di grado al più $\partial\big(p_\alpha(x)\big) = 3$.

Come conseguenza, l'insieme $\{1\,,\beta\}$ è certamente un insieme di generatori (lineari) di $\mathbb{Q}(\alpha\,,\beta) = \big(\mathbb{Q}(\alpha)\big)(\beta)$ come spazio vettoriale su $\mathbb{Q}(\alpha)$; siccome poi l'insieme $\{1\,,\alpha\,,\alpha^2\}$ è una base (quindi un insieme di generatori lineari) di $\mathbb{Q}(\alpha)$ come spazio vettoriale su $\mathbb{Q}$, possiamo concludere che l'insieme dei prodotti

$$\mathcal{B} \,:=\, \big\{\,\alpha^a\beta^b\,\big|\,a\in\{0,1,2\}\,,\ b\in\{0,1\}\big\} \,=\, \{1\,,\alpha\,,\alpha^2\,,\beta\,,\alpha\,\beta\,,\alpha^2\beta\,\} \tag{5.2}$$

è a sua volta un insieme di generatori (lineari) di $\mathbb{Q}(\alpha\,,\beta)$ come spazio vettoriale su $\mathbb{Q}$. Parallelamente, lo stesso risultato si ottiene osservando che l'insieme $\{1\,,\alpha\,,\alpha^2\,\}$ è un insieme di generatori (lineari) di $\mathbb{Q}(\alpha\,,\beta) = \big(\mathbb{Q}(\beta)\big)(\alpha)$ come spazio vettoriale su $\mathbb{Q}(\beta)$, e poiché l'insieme $\{1\,,\beta\,\}$ è una base (quindi un insieme di generatori lineari) di $\mathbb{Q}(\beta)$ come spazio vettoriale su $\mathbb{Q}$, possiamo concludere che l'insieme dei prodotti tra elementi del primo insieme con elementi del secondo è di nuovo un insieme di generatori (lineari) di $\mathbb{Q}(\alpha\,,\beta)$ come spazio vettoriale su $\mathbb{Q}$, che però per costruzione risulta essere esattamente l'insieme $\mathcal{B}$ già ottenuto in (5.2). Come conseguenza, siccome l'insieme $\mathcal{B}$ ha 6 elementi ne deduciamo che la dimensione di $\mathbb{Q}(\alpha\,,\beta)$ su $\mathbb{Q}$ è al più 6, cioè

$$d \,:=\, \big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}\,\big] \,=\, dim_{\mathbb{Q}}\big(\mathbb{Q}(\alpha\,,\beta)\big) \,\leq\, 6 \tag{5.3}$$

Ora, per la moltiplicatività del grado in una torre di estensioni, da (5.1) otteniamo

$$d \,:=\, \big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}\,\big] \,=\, \big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}(\alpha)\,\big]\cdot\big[\,\mathbb{Q}(\alpha):\mathbb{Q}\,\big] \,=\, d_-\cdot 3 \,\in\, 3\,\mathbb{N}_+ \tag{5.4}$$

come anche

$$d \,:=\, \big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}\,\big] \,=\, \big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}(\beta)\,\big]\cdot\big[\,\mathbb{Q}(\beta):\mathbb{Q}\,\big] \,=\, d_+\cdot 2 \,\in\, 2\,\mathbb{N}_+ \tag{5.5}$$

Ma (5.4) e (5.5) insieme danno $d\in 3\,\mathbb{N}_+\cap 2\,\mathbb{N}_+ = \text{m.c.m.}(3\,,2)\,\mathbb{N}_+ = 6\,\mathbb{N}_+$ che insieme a (5.3) dà necessariamente

$$\big[\,\mathbb{Q}(\alpha\,,\beta):\mathbb{Q}\,\big] \,=\, d \,=\, 6 \tag{5.6}$$

NOTA: in alternativa, per ottenere (5.6) si può anche procedere dimostrando che l'insieme $\{1\,,\beta\,\}$ è una base di $\mathbb{Q}(\alpha\,,\beta) = \big(\mathbb{Q}(\alpha)\big)(\beta)$ su $\mathbb{Q}(\alpha)$; questo equivale a dimostrare che β ha grado 2 su $\mathbb{Q}(\alpha)$ (sappiamo già che è algebrico, di grado al più 2...), e questo a sua volta equivale a dimostrare che il polinomio $p_\beta(x)$ è irriducibile su $\mathbb{Q}(\alpha)$, il che corrisponde a provare che tale polinomio – dato che ha grado 2 — non ha radici in $\mathbb{Q}(\alpha)$: questo si fa scrivendo un elemento generico $q(\alpha)$ in $\mathbb{Q}(\alpha)$ come $\mathbb{Q}$–combinazione lineare di elementi in $\{1\,,\alpha\,,\alpha^2\}$ — che è base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ — e osservando, tramite calcoli espliciti, che un tale elemento $q(\alpha) = q_0+q_1\,\alpha+q_2\,\alpha^2$ non è *mai* radice di $p_\beta(x) = x^2+3$.

Analogamente (e parallelamente), possiamo procedere invece dimostrando che l'insieme $\{1\,,\alpha\,,\alpha^2\}$ è una base di $\mathbb{Q}(\alpha\,,\beta) = \big(\mathbb{Q}(\beta)\big)(\alpha)$ su $\mathbb{Q}(\beta)$; questo equivale a dimostrare che α ha grado 3 su $\mathbb{Q}(\beta)$ (sappiamo già che è algebrico, di grado al più 3...), e questo a sua volta equivale a dimostrare che il polinomio $p_\alpha(x)$ è irriducibile su $\mathbb{Q}(\beta)$, il che corrisponde a provare che tale polinomio – dato che ha grado 3 — non ha radici in $\mathbb{Q}(\beta)$: questo si fa esprimendo un elemento generico $q(\beta)$ in $\mathbb{Q}(\beta)$ come $\mathbb{Q}$–combinazione lineare di elementi in $\{1\,,\beta\,\}$ — che è base di $\mathbb{Q}(\beta)$ su $\mathbb{Q}$ — e osservando, mediante calcoli espliciti, che un tale elemento $q(\beta) = q_0 + q_1\,\beta$ non è *mai* radice di $p_\alpha(x) = x^3-5$.

I due approcci sono equivalenti, ed entrambi richiedono calcoli relativamente pesanti.

Affrontiamo adesso separatamente i diversi quesiti.

(a) Dall'analisi preliminare svolta in precedenza sappiamo che l'insieme $\mathcal{B}$ in (5.2) è un sistema di generatori (lineari) di $\mathbb{Q}(\alpha\,,\beta)$ come spazio vettoriale su $\mathbb{Q}$; d'altra parte abbiamo anche $\big|\mathcal{B}\big| = 6 = \big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}\,\big] := dim_{\mathbb{Q}}\big(\mathbb{Q}(\alpha\,,\beta)\big)$ — per la (5.6) — quindi possiamo concludere che $\mathcal{B}$ è in effetti una base, come richiesto.

(b) Dato che il campo $\mathbb{Q}$ ha caratteristica zero, il *Teorema dell'Elemento Primitivo* ci garantisce che esisterà appunto un elemento primitivo per l'estensione $\mathbb{Q}(\alpha\,,\beta)$ di $\mathbb{Q}\,$, cioè un elemento $\gamma \in \mathbb{Q}(\alpha\,,\beta)$ tale che $\mathbb{Q}(\alpha\,,\beta)$ si realizzi come estensione *semplice* di $\mathbb{Q}$ generata da $\gamma\,$, in formule $\mathbb{Q}(\alpha\,,\beta) = \mathbb{Q}(\gamma)\,$. In aggiunta, dalla dimostrazione del suddetto teorema (che è costruttiva!), sappiamo che possiamo cercare un elemento primitivo come richiesto in forma di $\mathbb{Q}$–combinazione lineare di α e $\beta\,$, dunque del tipo $\gamma = a\,\alpha + b\,\beta$ con $a, b \in \mathbb{Q}\,$. Tentiamo allora con il candidato più semplice, che — osservando che comunque nel nostro caso deve necessariamente essere $a \neq 0 \neq b\,$, perché $\mathbb{Q}(\beta) \subsetneqq \mathbb{Q}(\alpha\,,\beta) \supsetneqq \mathbb{Q}(\alpha)$ — è dato da $\gamma := \alpha + \beta\,$. Qui di seguito dimostriamo che tale $\gamma := \alpha + \beta$ è effettivamente un elemento primitivo: questo si può fare secondo vari metodi, a seguire ne indichiamo un paio, in ordine di complessità crescente (e quindi semplicità decrescente...).

Come premessa generale, dato che $\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha\,,\beta)\,$, avremo anche

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha\,,\beta) \iff \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = \big[\,\mathbb{Q}(\alpha\,,\beta\gamma) : \mathbb{Q}\,\big] = 6 \iff \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6$$

per cui dobbiamo dimostrare che effettivamente è $\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6\,$. Inoltre, applicando alla torre di estensioni $\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha\,,\beta)$ la *moltiplicatività del grado* si ottiene che $\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big]\Big|\big[\,\mathbb{Q}(\alpha\,,\beta) : \mathbb{Q}\,\big] = 6$ e quindi

$$\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] \;\in\; \{1\,,2\,,3\,,6\,\} \tag{5.7}$$

<u>*Primo Metodo:*</u> Dalla (5.7) segue subito che

$$\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] \neq 6 \iff \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] \leq 3$$

che ha sua volta significa $\partial\big(p_\gamma(x)\big) = \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] \leq 3$ dove $p_\gamma(x)$ indica il *polinomio minimo* di γ su $\mathbb{Q}\,$. Assumiamo allora per assurdo che $\partial\big(p_\gamma(x)\big) \leq 3\,,$ per cui

$$p_\gamma(x) \;=\; q_0 + q_1\,x + q_2\,x^2 + q_3\,x^3 \qquad\qquad \text{con} \qquad q_0\,,q_1\,,q_2\,,q_3 \;\in\; \mathbb{Q} \tag{5.8}$$

Ora calcoliamo esplicitamente il valore $p_\gamma(\gamma)\,$, scrivendolo come combinazione lineare degli elementi della base $\mathcal{B}$ in (5.2), e poi imponiamo la condizione $p_\gamma(\gamma) = 0\,$. Questo implicherà che ciascun coefficiente di ogni elemento della suddetta base dovrà essere 0, e vedremo ciò che questo comporta. I calcoli espliciti — tenendo in conto che $\alpha^3 = 5$ e $\beta^2 = -3$ — ci danno

$$\begin{aligned}
p_\gamma(\gamma) \;&=\; q_0 + q_1\,\gamma + q_2\,\gamma^2 + q_3\,\gamma^3 \;=\; q_0 + q_1\,(\alpha+\beta) + q_2\,(\alpha+\beta)^2 + q_3\,(\alpha+\beta)^3 \;= \\
&=\; q_0 + q_1\,\alpha + q_1\,\beta + q_2\,\alpha^2 + 2\,q_2\,\alpha\,\beta + q_2\,\beta^2 + q_3\,\alpha^3 + 3\,q_3\,\alpha^2\beta + 3\,q_3\,\alpha\,\beta^2 + q_3\,\beta^3 \;= \\
&=\; q_0 + q_1\,\alpha + q_1\,\beta + q_2\,\alpha^2 + 2\,q_2\,\alpha\,\beta + q_2\,(-3) + q_3\cdot 5 + 3\,q_3\,\alpha^2\beta + 3\,q_3\,\alpha\,(-3) + q_3\,(-3)\beta \;= \\
&=\; (\,q_0 - 3\,q_2 + 5\,q_3) + (\,q_1 - 9\,q_3)\,\alpha + q_2\,\alpha^2 + (\,q_1 - 3\,q_3)\,\beta + 2\,q_2\,\alpha\,\beta + 3\,q_3\,\alpha^2\beta
\end{aligned}$$

Da questo allora otteniamo che imporre $p_\gamma(\gamma) = 0$ equivale ad imporre

$$\begin{cases} q_0 - 3\,q_2 + 5\,q_3 = 0 \\ q_1 - 9\,q_3 = 0 \\ q_2 = 0 \\ q_1 - 3\,q_3 = 0 \\ 2\,q_2 = 0 \\ 3\,q_3 = 0 \end{cases} \tag{5.9}$$

Ora, tale sistema ovviamente ha soltanto la soluzione banale $(\,q_0\,q_1\,,q_2\,,q_3) = (0\,,0\,,0\,,0)\,,$ che corrisponde al polinomio nullo $p_\gamma(x) = 0\,;$ ma questo è assurdo — il polinomio minimo per definizione *non* è nullo — quindi abbiamo una contraddizione. Pertanto concludiamo che non può essere $\partial\big(p_\gamma(x)\big) \leq 3\,,$ dunque per quanto già visto dev'essere $\partial\big(p_\gamma(x)\big) = 6$ che a sua volta significa che $\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6$ e quindi $\gamma := \alpha + \beta$ è elemento primitivo dell'estensione di campi $\mathbb{Q}(\alpha\,,\beta)\Big/\mathbb{Q}\,,$ q.e.d.

<u>Secondo Metodo:</u> Questo metodo è una specie di variante del primo, con calcoli un po' più complessi. Il punto è di nuovo dimostrare che $\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6\,;$ adesso però osserviamo che, in generale, si ha

$$\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = t \iff \big\{\,1\,,\gamma\,,\gamma^2\,,\ldots,\gamma^{t-1}\,\big\} \text{ è base di } \mathbb{Q}(\gamma) \text{ su } \mathbb{Q} \tag{5.10}$$

Pertanto, volendo dimostrare che $\big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6\,,$ per la (5.10) basta provare che

$$\big\{\,1\,,\gamma\,,\gamma^2\,,\gamma^3\,,\gamma^4\,,\gamma^5\,\big\} \text{ è base di } \mathbb{Q}(\gamma) \text{ su } \mathbb{Q} \tag{5.11}$$

D'altra parte, siccome $dim_{\mathbb{Q}}\big(\mathbb{Q}(\gamma)\big) = \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] \in \{1\,,2\,,3\,,6\}$ — per la (5.7) — la (5.11) equivale a

$$1\,,\gamma\,,\gamma^2\,,\gamma^3\,,\gamma^4\,,\gamma^5 \text{ sono linearmente indipendenti su } \mathbb{Q} \tag{5.12}$$

Per dimostrare quest'ultimo fatto, sviluppiamo gli elementi in (5.12) come combinazioni lineari dei vettori della base $\mathcal{B}$ in (5.2), da queste estraiamo le stringhe dei rispettivi coefficienti — che sono vettori in $\mathbb{Q}^6$ — e dimostriamo che queste ultime sono tra loro linearmente indipendenti su $\mathbb{Q}\,.$ Per quest'ultimo passaggio, utilizziamo queste stringhe come colonne di una matrice quadrata $M \in Mat_{6\times 6}(\mathbb{Q})$ e dimostriamo che quest'ultima ha rango massimo, cioè 6. In concreto, i calcoli espliciti ci danno quanto segue

$$\begin{aligned} 1 &= 1\cdot 1 + 0\cdot\alpha + 0\cdot\alpha^2 + 0\cdot\beta + 0\cdot\alpha\,\beta + 0\cdot\alpha^2\beta \\ \gamma &= \alpha+\beta = 0\cdot 1 + 1\cdot\alpha + 0\cdot\alpha^2 + 1\cdot\beta + 0\cdot\alpha\,\beta + 0\cdot\alpha^2\beta \\ \gamma^2 &= \alpha^2 + 2\,\alpha\,\beta + \beta^2 = (-3)\cdot 1 + 0\cdot\alpha + 1\cdot\alpha^2 + 0\cdot\beta + 2\cdot\alpha\,\beta + 0\cdot\alpha^2\beta \\ \gamma^3 &= \alpha^3 + 3\,\alpha^2\beta + 3\,\alpha\,\beta^2 + \beta^3 = 5\cdot 1 + (-9)\cdot\alpha + 0\cdot\alpha^2 + (-3)\cdot\beta + 0\cdot\alpha\,\beta + 3\cdot\alpha^2\beta \\ \gamma^4 &= \alpha^4 + 4\,\alpha^3\beta + 6\,\alpha^2\beta^2 + 4\,\alpha\,\beta^3 + \beta^4 = 9\cdot 1 + 5\cdot\alpha + (-18)\cdot\alpha^2 + 20\cdot\beta + (-12)\cdot\alpha\,\beta + 0\cdot\alpha^2\beta \\ \gamma^5 &= \alpha^5 + 5\,\alpha^4\beta + 10\,\alpha^3\beta^2 + 10\,\alpha^2\beta^3 + 5\,\alpha\,\beta^4 + \beta^5 = \\ &= (-150)\cdot 1 + 45\cdot\alpha + 5\cdot\alpha^2 + 9\cdot\beta + 25\cdot\alpha\,\beta + (-30)\cdot\alpha^2\beta \end{aligned}$$

da cui poi, "estraendo le stringhe di coefficienti" come già accennato, si ottiene

$$\begin{array}{rcl} 1 & \rightsquigarrow & (\,1\,,0\,,0\,,0\,,0\,,0\,) \\ \gamma & \rightsquigarrow & (\,0\,,1\,,0\,,1\,,0\,,0\,) \\ \gamma^2 & \rightsquigarrow & (\,-3\,,0\,,1\,,0\,,2\,,0\,) \\ \gamma^3 & \rightsquigarrow & (\,5\,,-9\,,0\,,-3\,,0\,,3\,) \\ \gamma^4 & \rightsquigarrow & (\,9\,,5\,,-18\,,20\,,-12\,,0\,) \\ \gamma^5 & \rightsquigarrow & (\,-150\,,45\,,5\,,9\,,25\,,-30\,) \end{array}$$

e infine accostando queste stringhe (nell'ordine) come colonne formiamo la matrice 6×6

$$M \;:=\; \begin{pmatrix} 1 & 0 & -3 & 5 & 9 & -150 \\ 0 & 1 & 0 & -9 & 5 & 45 \\ 0 & 0 & 1 & 0 & -18 & 5 \\ 0 & 1 & 0 & -3 & 20 & 9 \\ 0 & 0 & 2 & 0 & -12 & 25 \\ 0 & 0 & 0 & 3 & 0 & -30 \end{pmatrix}$$

Resta da calcolare il rango di questa matrice, il che si può fare in veri modi: ad esempio, possiamo operare sulla matrice M una riduzione a scala (non univoca!) tramite eliminazione di Gauss, ottenendo

$$M \;:=\; \begin{pmatrix} 1 & 0 & -3 & 5 & 9 & -150 \\ 0 & 1 & 0 & -9 & 5 & 45 \\ 0 & 0 & 1 & 0 & -18 & 5 \\ 0 & 1 & 0 & -3 & 20 & 9 \\ 0 & 0 & 2 & 0 & -12 & 25 \\ 0 & 0 & 0 & 3 & 0 & -30 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} 1 & 0 & -3 & 5 & 9 & -150 \\ 0 & 1 & 0 & -9 & 5 & 45 \\ 0 & 0 & 1 & 0 & -18 & 5 \\ 0 & 0 & 0 & 3 & 0 & -30 \\ 0 & 0 & 0 & 0 & 24 & 15 \\ 0 & 0 & 0 & 0 & 0 & 171/4 \end{pmatrix}$$

da cui vediamo dunque che il rango di M è 6, q.e.d.

<u>NOTA</u>: Se vogliamo calcolare epslicitamente il polinomio minimo $p_\gamma(x)$ di γ su $\mathbb{Q}$, possiamo procedere tramite calcoli diretti come segue:

$$\begin{array}{l} \gamma := \alpha+\beta \implies \gamma-\beta = \alpha \implies (\gamma-\beta)^3 = \alpha^3 = 5 \implies (\gamma-\beta)^3 - 5 = 0 \implies \\ \implies \quad \gamma^3 - 3\,\gamma^2\beta - 9\,\gamma + 3\,\beta - 5 = 0 \quad \implies \quad \gamma^3 - 9\,\gamma - 5 = 3\left(\gamma^2-1\right)\beta \quad \implies \\ \implies \left(\gamma^3 - 9\,\gamma - 5\right)^2 = \left(3\left(\gamma^2-1\right)\beta\right)^2 \implies \left(\gamma^3 - 9\,\gamma - 5\right)^2 = -27\left(\gamma^2-1\right)^2 \implies \\ \implies \quad \gamma^6 + 81\,\gamma^2 + 25 - 18\,\gamma^4 - 10\,\gamma^3 + 90\,\gamma = -27\left(\gamma^4 - 2\,\gamma^2 + 1\right) \implies \\ \implies \quad \gamma^6 + 81\,\gamma^2 + 25 - 18\,\gamma^4 - 10\,\gamma^3 + 90\,\gamma = -27\,\gamma^4 + 54\,\gamma^2 - 27 \implies \\ \implies \quad \gamma^6 + 81\,\gamma^2 + 25 - 18\,\gamma^4 - 10\,\gamma^3 + 90\,\gamma = -27\left(\gamma^4 - 2\,\gamma^2 + 1\right) \implies \\ \implies \quad \gamma^6 + 9\,\gamma^4 - 10\,\gamma^3 + 27\,\gamma^2 + 90\,\gamma + 52 = 0 \end{array}$$

dove l'ultima identità ci dice che γ è radice del polinomio

$$P(x) \;:=\; x^6 + 9\,x^4 - 10\,x^3 + 27\,x^2 + 90\,x + 52 \;\in\; \mathbb{Q}[\,x\,] \tag{5.13}$$

che in aggiunta è un polinomio monico. Siccome il suo grado è 6 , e abbiamo già appurato separatamente che $\partial\big(p_\gamma(x)\big) = \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6$, possiamo concludere che è proprio $P(x) = p_\gamma(x)$, cioè *il polinomio minimo di* γ *su* $\mathbb{Q}$ *è* $p_\gamma(x) = P(x)$ *come in (5.13).*

Si noti in particolare che questo implica che il polinomio $P(x)$ in (5.13) è irriducibile. Tuttavia, se non avessimo già saputo (per altre vie) che $\partial\big(p_\gamma(x)\big) = \big[\,\mathbb{Q}(\gamma) : \mathbb{Q}\,\big] = 6$, non avremmo potuto concludere così: avremmo invece ancora dovuto dimostrare, indipendentemente, che il polinomio $P(x)$ è irriducibile. Ma dalla sua espressione in (5.13) questo non è affatto evidente: in particolare, non si può applicare il *Criterio di Eisenstein*, mentre il *Criterio della Radice Intera* — che si può applicare (questo sì), perché in effetti $P(x) \in \mathbb{Z}[\,x\,]$ — ci garantisce soltanto che $P(x)$ non ha radici in $\mathbb{Q}$, e quindi non ha fattorizzazioni in cui compaia un fattore di grado 1 — tuttavia a priori potrebbe anche avere una fattorizzazione non banale con tutti i fattori di grado maggiore di 1 .

(c) Per valutare se l'estensione di campi $\mathbb{Q} \subseteq \mathbb{Q}(\alpha\,,\beta)$ sia normale oppure no, ricordiamo un possibile criterio: *Un'estensione finita* $\mathbb{F} \subseteq \mathbb{E}$ *è normale se e soltanto se è campo di spezzamento di un polinomio* $f(x) \in \mathbb{F}[\,x\,]$. Andiamo allora a dimostrare, nel caso in esame, che $\mathbb{Q}(\alpha\,,\beta)$ è campo di spezzamento di un polinomio $f(x) \in \mathbb{Q}[\,x\,]$.

Per definizione, $\mathbb{Q}(\alpha\,,\beta)$ è generato da α e β che sono radici rispettivamente dei polinomi $p_\alpha(x) = x^3 - 5$ e $p_\beta(x) = x^2 + 3$.

Nel secondo di $p_\beta(x) = x^2 + 3$, chiaramente una seconda radice è $-\beta$ che pure appartiene a $\mathbb{Q}(\alpha\,,\beta)$, dunque tale campo contiene tutte le radici di $p_\beta(x) = x^2 + 3$.

Nel caso di $p_\alpha(x) = x^3 - 5$ invece, se $\alpha_1\,,\alpha_2 \in \mathbb{Q}(\alpha\,,\beta)$ sono due radici di $p_\alpha(x) = x^3 - 5$ allora da $\alpha_1^3 - 5 = p_\alpha(\alpha_1) = 0$ e $\alpha_2^3 - 5 = p_\alpha(\alpha_2) = 0$ otteniamo $\alpha_1^3 = 5 = \alpha_2^3$, da cui $\big(\alpha_1\,\alpha_2^{-1}\big)^3 = 1$, cioè $\zeta := \alpha_1\,\alpha_2^{-1}$ è una radice terza dell'unità in $\mathbb{Q}(\alpha\,,\beta)$. Viceversa, se $\zeta \in \mathbb{Q}(\alpha\,,\beta)$ è una radice terza dell'unità ed è primitiva (cioè di ordine 3), allora $\alpha\,,\zeta\,\alpha\,,\zeta\,\alpha^2$ sono tre radici di *distinte* di $p_\alpha(x) = x^3 - 5$. Perciò, *se in* $\mathbb{Q}(\alpha\,,\beta)$ *esiste una radice terza primitiva dell'unità* ζ allora $\mathbb{Q}(\alpha\,,\beta)$ contiene tutte le radici di $p_\alpha(x) = x^3 - 5$. Ora, effettivamente abbiamo che l'elemento

$$\zeta \;:=\; \frac{-1 + \beta}{2} \;\;\in\;\; \mathbb{Q}(\alpha\,,\beta) \tag{5.14}$$

è una radice terza primitiva dell'unità in $\mathbb{Q}(\alpha\,,\beta)$ — la verifica è un calcolo diretto! Così concludiamo che $\mathbb{Q}(\alpha\,,\beta)$ contiene tutte le radici del polinomio $p_\alpha(x) = x^3 - 5 \in \mathbb{Q}[\,x\,]$.

Infine, dall'analisi precedente otteniamo che $\mathbb{Q}(\alpha\,,\beta)$ contiene tutte le radici del polinomio $f(x) := p_\beta(x)\,p_\alpha(x) = \big(\,x^2 + 3\,\big)\big(\,x^3 - 5\,\big) \in \mathbb{Q}[\,x\,]$; d'altra parte, per definizione $\mathbb{Q}(\alpha\,,\beta)$ è generato dalle radici di tale polinomio, quindi $\mathbb{Q}(\alpha\,,\beta)$ è campo di spezzamento di $f(x) \in \mathbb{Q}[\,x\,]$. Possiamo allora concludere che l'estensione $\mathbb{Q} \subseteq \mathbb{Q}(\alpha\,,\beta)$ è normale.

NOTA: se usiamo la notazione $\beta := \sqrt{-3} = i\,\sqrt{3}$ la formula per ζ in (5.14) diventa

$$\zeta \;=\; \frac{-1 + i\,\sqrt{3}}{2}$$

che è l'espressione standard di una radice terza primitiva dell'unità in $\mathbb{C}$, o anche nel sottocampo $\mathbb{Q}[\,i\,]$; questo spiega come la (5.14) stessa possa mai venirci in mente.