Università degli Studi di Roma "Tor Vergata"

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2019–2020

Esame scritto del 23 Settembre 2020 — Sessione Autunnale, II appello

N.B.: compilare il compito in modo sintetico ma **esauriente**, *spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

— SVOLGIMENTO —

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

[1] — Sia A l'anello prodotto diretto $A := \mathbb{Z} \times \mathbb{Z}$.

(a) Dimostrare che A è anello a ideali principali.

(b) Determinare tutti gli ideali primi di A .

(c) Determinare tutti gli ideali massimali di A .

[2] — Sia $\mathbb{K} := \mathbb{Q}_{(x^2-5)(x^3-7)}$ il campo di spezzamento su $\mathbb{Q}$ del polinomio $\big(x^2 - 5\big)\big(x^3 - 7\big)$ in $\mathbb{Q}[x]$.

(a) Determinare il grado $\big[\mathbb{K} : \mathbb{Q}\big]$ dell'estensione di campi $\mathbb{K}/\mathbb{Q}$.

(b) Determinare il numero di sottogruppi normali nel gruppo $Gal\big(\mathbb{K}/\mathbb{Q}\big)$.

(c) Determinare esplicitamente tutte le estensioni $\mathbb{F}$ intermedie tra $\mathbb{Q}$ e $\mathbb{K}$ tali che l'estensione $\mathbb{F}/\mathbb{Q}$ sia normale.

[3] — Sia G un gruppo di ordine 385, il quale contenga un sottogruppo H di ordine 77.

(a) Dimostrare che H è l'unico sottogruppo in G di ordine 77.

(b) Dimostrare che esistono in G due sottogruppi K_1 e K_2 che sono *caratteristici* e tali che $\{e_G\} \subsetneqq K_1 \subsetneqq K_2 \subsetneqq G$.

[4] — Sia dato il polinomio $f(x) := x^2 + 7\,x + 13$ in $\mathbb{Z}[x]$.

(a) Dimostrare che $f(x)$ è irriducibile in $\mathbb{Z}[x]$.

(b) Determinare se l'anello quoziente $A := \mathbb{Z}[x] \Big/ \big(f(x)\big)$ sia un dominio, o un campo, o nessuno dei due.

[5] — *(a)* Nel gruppo simmetrico $\mathcal{S}_8$, determinare il numero di elementi σ tali che $\sigma^2 = \big(5\,,2\big)\big(3\,,6\big)$.

(b) Sia p un primo, G un p-gruppo finito, N un sottogruppo normale non banale di G, e

$$N^G \;:=\; \Big\{\, n \in N \,\Big|\, g\,n\,g^{-1} = n \;\;\forall\, g \in G \,\Big\}$$

l'insieme dei punti di N fissati dall'azione di coniugazione di G ristretta ad N. Dimostrare che $\big|N^G\big| \geq p$.

ESAME SCRITTO DI

ALGEBRA 2

(2019-2020 GAVARINI)

23/09/2020

SVOLGIMENTO

— ∘ —

1 Sia $A := \mathbb{Z} \times \mathbb{Z}$

(a) Dimostrare che A è a ideali principali.

(b) Determinare tutti gli ideali primi di A.

(c) Determinare tutti gli ideali massimali di A.

Soluzione:

(a) Consideriamo le due applicazioni

$\pi_d : A := \mathbb{Z}_4 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4, \ (z_s, z_d) \longmapsto z_d$

$\pi_s : A := \mathbb{Z}_4 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4, \ (z_s, z_d) \longmapsto z_s$

che sono, entrambe epimorfismi di anelli (le "proiezioni" del prodotto diretto sul fattore sinistro e sul fattore destro).

Sia I un ideale di A.

Siccome π_s e π_d sono epimorfismi, $\pi_d(I)$ e $\pi_s(I)$ sono ideali di $\mathbb{Z}_4$, che è a ideali principali, $\Rightarrow \exists \ \zeta_d, \zeta_s$ tali che

$\pi_d(I) = \mathbb{Z}_4 \cdot \zeta_d$, $\pi_s(I) = \mathbb{Z}_4 \cdot \zeta_s$

Ora, $\forall \ z := (z_s, z_d) \in I \Rightarrow z_s = \pi_s(z)$, $z_d = \pi_d(z)$, $\forall$ cioè $\forall \ z = (z_s, z_d) \in I \Rightarrow$

così

$$\Rightarrow \begin{cases} z_s = \pi_s(a) \in \pi_s(I) = \mathbb{Z}_4 \cdot \zeta_s \\ z_d = \pi_d(a) \in \pi_d(I) = \mathbb{Z}_4 \cdot \zeta_d \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} \exists\, c_s \in \mathbb{Z}_4 : \; z_s = c_s \cdot \zeta_s \\ \exists\, c_d \in \mathbb{Z}_4 : \; z_d = c_d \cdot \zeta_d \end{cases} \Rightarrow$$

$$\Rightarrow a := (z_s, z_d) = (c_s \cdot \zeta_s, c_d \cdot \zeta_d) =$$

$$= (c_s, c_d) \cdot (\zeta_s, \zeta_d) \in (\mathbb{Z}_4 \times \mathbb{Z}_4) \cdot \underline{\zeta} = A \cdot \underline{\zeta}$$

dove $\underline{\zeta} := (\zeta_s, \zeta_d) \in \mathbb{Z}_4 \times \mathbb{Z}_4 =: A$

QUINDI $a \in A \cdot \underline{\zeta} \quad (\forall a \in I)$

DUNQUE $I \subseteq A \cdot \underline{\zeta} \qquad (1)$

dove $A \cdot \underline{\zeta}$ è l'ideale principale di A generato da $\underline{\zeta}$.

VICEVERSA, siccome per costruzione è $\pi_i(I) = \mathbb{Z}_4 \cdot \zeta_i \quad (\forall i = d, s)$ abbiamo in particolare che

ζ_s e ζ_d si "incontrano" nella forma

$$\zeta_s = \pi_s(\zeta_s, \delta), \quad \zeta_d = \pi_d(\sigma, \zeta_d)$$

per opportuni $\delta, \sigma \in \mathbb{Z}_4$ tali che

$$(\zeta_s, \delta), (\sigma, \zeta_d) \in I.$$

ALLORA

$$I \ni (\zeta_s, \delta) \Rightarrow$$

$$\Rightarrow I \ni (\zeta_s, \delta)\cdot(1, \emptyset) = (\zeta, \emptyset)$$

e analogamente $I \ni (\emptyset, \zeta_d)$

$$\Longrightarrow (\zeta_s, \zeta_d) =$$

$$= (\zeta_s, \emptyset) + (\emptyset, \zeta_d) \in I$$

per le proprietà degli ideali!

DUNQUE abbiamo

$$\underline{\zeta} := (\zeta_s, \zeta_d) \in I, \Rightarrow$$

$\supseteq$ $A \cdot \underline{\zeta} \subseteq \underline{I}$, che è proprio l'inclusione inversa della (1). PERCIÒ

$$\underline{I} = A \cdot \underline{\zeta}$$

così $\underline{I}$ è l'ideale principale in A generato da $\underline{\zeta} := (\zeta_s, \zeta_d)$.

(b+c) Sia $\underline{I}$ un ideale di A.

Dalla parte (a) sappiamo che $\underline{I}$ è principale, dunque della forma $\underline{I} = A \cdot \underline{\zeta}$, $\underline{\zeta} = (\zeta_s, \zeta_d)$

Supponiamo che

$\underline{I}$ è primo $\iff$ $A/\underline{I}$ è dominio

ORA,

$$A/I = (\mathbb{Z}_4 \times \mathbb{Z}_4) \Big/ (\mathbb{Z}_4 \times \mathbb{Z}_4)(z_s, z_d) =$$

$$= \mathbb{Z}_4 \times \mathbb{Z}_4 \Big/ (\mathbb{Z}_4 \cdot z_s) \times (\mathbb{Z}_4 \cdot z_d) \cong$$

$$\cong \mathbb{Z}_4/\mathbb{Z}_4 \cdot z_s \times \mathbb{Z}_4/\mathbb{Z}_4 \cdot z_d =$$

$$= \mathbb{Z}_{4 z_s} \times \mathbb{Z}_{4 z_d}$$

CIOÈ $A/I = \mathbb{Z}_{4 z_s} \times \mathbb{Z}_{4 z_d}$

Oltretutto ricordiamo che per ogni prodotto diretto $A_1 \times A_2$ si ha $A_1 \times A_2$, è un dominio/campo $\iff$ (con $\{i,j\} = \{1,2\}$) A_i è dominio/campo & $A_j = \{0\}$

cioè un fattore deve essere un dominio/campo mentre l'altro fattore dev'essere banale.

Nel caso in esame, con $A_1 := \mathbb{Z}_{\Delta\zeta_s}$ e $A_2 := \mathbb{Z}_{\Delta\zeta_d}$, abbiamo

$$A/I \cong \mathbb{Z}_{\Delta\zeta_s} \times \mathbb{Z}_{\Delta\zeta_d} \text{ è dominio/campo}$$

$$\Updownarrow$$

$$\mathbb{Z}_{\Delta\zeta_s} \text{ è dominio/campo} \;\&\; \mathbb{Z}_{\Delta\zeta_d} = \{0\}$$

OPPURE

$$\mathbb{Z}_{\Delta\zeta_d} \text{ è dominio/campo} \;\&\; \mathbb{Z}_{\Delta\zeta_s} = \{0\}$$

$$\Updownarrow$$

$$\zeta_s \text{ è primo } (\text{in } \mathbb{Z}_\Delta) \;\&\; \zeta_d \in \{+1,-1\}$$

OPPURE

$$\zeta_d \text{ è primo } (\text{in } \mathbb{Z}_\Delta) \;\&\; \zeta_s \in \{+1,-1\}$$

dove abbiamo sfruttato il fatto che $\forall\, n \in \mathbb{Z}_4$ si ha

$$\mathbb{Z}_{4_n} := \mathbb{Z}_4 / n\cdot\mathbb{Z}_4 \quad \text{è dominio}$$

$$\Updownarrow$$

$$n \text{ è primo (in } \mathbb{Z}_4)$$

$$\Updownarrow$$

$$\mathbb{Z}_{4_n} := \mathbb{Z}_4 / n\cdot\mathbb{Z}_4 \quad \text{è campo}$$

Questo risponde a entrambi i quesiti (b) e (c). □

(continua...)

2 $\mathbb{K} := \mathbb{Q}_{(x^2-5)(x^3-7)} =$

= campo di spezzamento di

$f(x) := (x^2-5)(x^3-7)$ su $\mathbb{Q}$.

(a) Determinare $[\mathbb{K} : \mathbb{Q}]$.

(b) Determinare il numero di sottogruppi normali nel gruppo $Gal(\mathbb{K}/\mathbb{Q})$.

(c) Determinare tutte le estensioni intermedie $\mathbb{F}$ tali che $\mathbb{F}/\mathbb{Q}$ sia normale.

Soluzione:

(a) Consideriamo in $\mathbb{K}$ gli elementi

$\sqrt{5} :=$ radice di x^2-5

$\sqrt[3]{7} :=$ radice di x^3-7

$\zeta_3 :=$ radice di x^3-1, con $\zeta_3 \neq 1$

Allora $\mathbb{K}$ è generato su $\mathbb{Q}$ da $\sqrt{5}$, $\sqrt[3]{7}$ e ζ_3, cioè

$$\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt[3]{7}, \zeta_3)$$

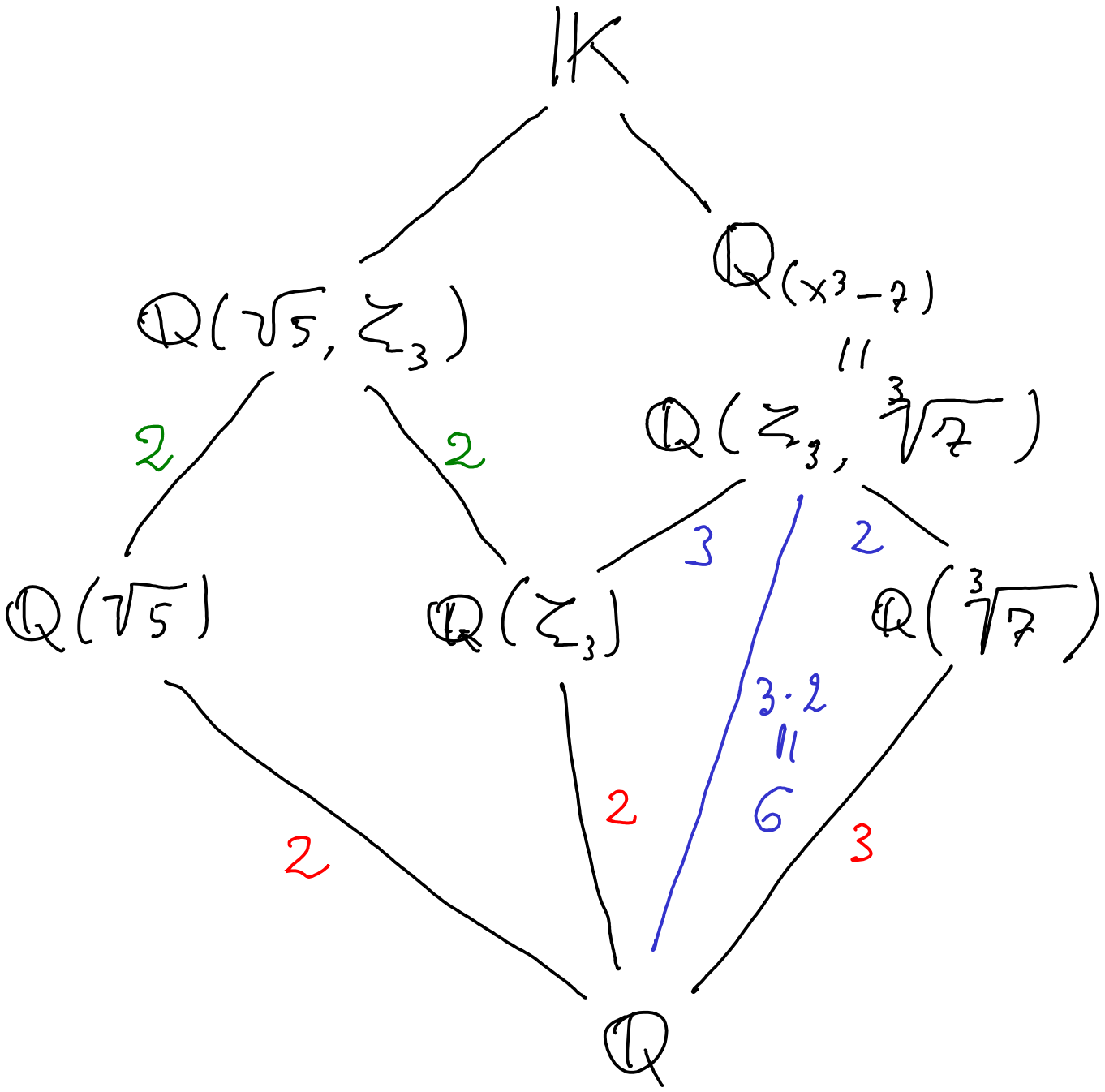
Inoltre,

$\sqrt{5}$ ha grado 2 su $\mathbb{Q}$
(il polinomio minimo è $x^2 - 5$)

$\sqrt[3]{7}$ ha grado 3 su $\mathbb{Q}$
(il polinomio minimo è $x^3 - 7$)

ζ_3 ha grado 2 su $\mathbb{Q}$
(il polinomio minimo è $x^2 + x + 1$)

Otteniamo allora il seguente diagramma di estensioni di campi (intermedi, tra $\mathbb{K}$ e $\mathbb{Q}$):



Dove ad esempio troviamo che

$$[\mathbb{Q}(\zeta_3, \sqrt[3]{7}) : \mathbb{Q}] =: d = 6$$

perché necessariamente è
(per la moltiplicatività del
grado, e per quanto già visto)

$$[\mathbb{Q}(\zeta_3, \sqrt[3]{7}) : \mathbb{Q}] =$$

$$= [(\mathbb{Q}(\zeta_3))(\sqrt[3]{7}) : \mathbb{Q}(\zeta_3)] \cdot [\mathbb{Q}(\zeta_3) : \mathbb{Q}] =$$

$$= d' \cdot 2, \quad \text{con } d' \leq 3$$

$$[\mathbb{Q}(\zeta_3, \sqrt[3]{7}) : \mathbb{Q}] =$$

$$= [(\mathbb{Q}(\sqrt[3]{7}))(\zeta_3) : \mathbb{Q}(\sqrt[3]{7})] \cdot [\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] =$$

$$= d'' \cdot 3, \quad \text{con } d'' \leq 2$$

e analogamente abbiamo

$$[\mathbb{Q}(\zeta_3, \sqrt{5}) : \mathbb{Q}] =$$

$$= [(\mathbb{Q}(\zeta_3))(\sqrt{5}) : \mathbb{Q}(\zeta_3)] \cdot [\mathbb{Q}(\zeta_3) : \mathbb{Q}] =$$

$$= \delta \cdot 2, \quad \text{con } \delta \leq 2$$

e poi osserviamo che $\delta = 2$ perché il polinomio $X^2 - 5$, di cui $\sqrt{5}$ è radice, è

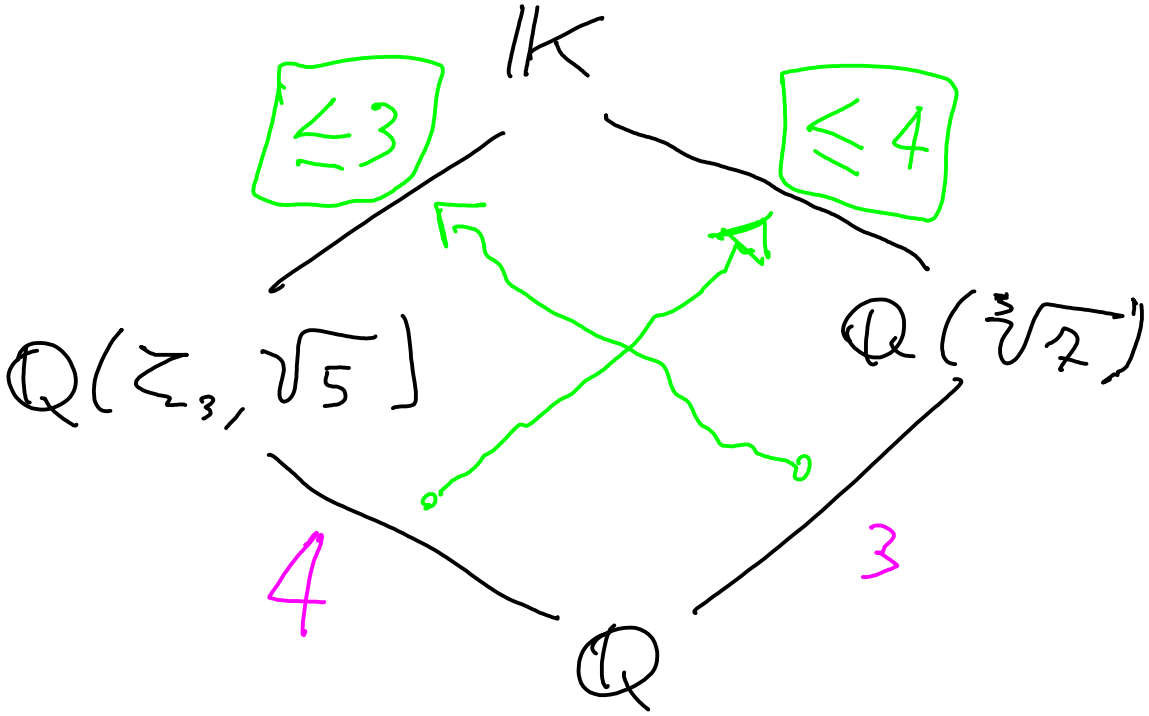
irriducibile in $\mathbb{Q}(\zeta_3)[X]$ in quanto nessun elemento di

$$\mathbb{Q}(\zeta_3) = \{ q_0 + q_1 \zeta_3 \mid q_0, q_1 \in \mathbb{Q} \}$$

(in cui $\zeta_3^2 = -1 - \zeta_3$) ha quadrato uguale a 5; concludiamo che

$$[\mathbb{Q}(\zeta_3, \sqrt{5}) : \mathbb{Q}] = 6 \cdot 2 = 2 \cdot 2 = 4$$

come abbiamo



da cui possiamo concludere che $[\mathbb{K} : \mathbb{Q}] = 4 \cdot 3 = 12$

cioè $\boxed{[\mathbb{K} : \mathbb{Q}] = 12}$

(b) Il campo

$$\mathbb{K} := \mathbb{Q}_{(x^2-5)\cdot(x^3-2)}$$

contiene i due campi di spezzamento

$$\mathbb{Q}_{(x^2-5)} =: \mathbb{K}_+$$

$$\mathbb{Q}_{(x^3-2)} =: \mathbb{K}_-$$

la cui unione genera $\mathbb{K}$ su $\mathbb{Q}$; da questo segue che

$$G := Gal(\mathbb{K}/\mathbb{Q}) \cong G_+ \times G_-$$

con $G_\pm := Gal(K_\pm / \mathbb{Q})$.

Ora, in un prodotto diretto come $G_+ \times G_-$ i sottogruppi normali sono tutti e soli della forma $N_+ \times N_-$ con

$$N_+ \trianglelefteq G_+ \quad e \quad N_- \trianglelefteq G_- ;$$

perciò dobbiamo conoscere i sottogruppi normali di G_+ e di G_-.

ORA, abbiamo

$$\mathbb{Q}_{(x^2-5)} = \mathbb{Q}(\sqrt{5})$$

$$\mathbb{Q}_{(x^3-7)} = \mathbb{Q}(\sqrt[3]{7}, \zeta_3)$$

e per i loro gruppi di Galois

(su $\mathbb{Q}$) si hanno isomorfismi

$$\mathbb{Q}(\sqrt{5})$$
$$\parallel$$
$$G_+ := Gal(\mathbb{Q}(x^2-5)/\mathbb{Q}) \cong \mathbb{Z}_{/2}$$

$$\left(\sigma : +\sqrt{5} \longmapsto -\sqrt{5}\right) \longleftrightarrow [1]_2$$

e

$$\mathbb{Q}(\sqrt[3]{7}, \zeta_3)$$
$$\parallel$$
$$G_- := Gal(\mathbb{Q}(x^3-7)/\mathbb{Q}) \cong \mathbb{Z}_{/2} \times \mathbb{Z}_{/3}$$

$$\left(\tau : \begin{cases} \zeta_3 \longmapsto \zeta_3^{-1} \\ \sqrt[3]{7} \longmapsto \sqrt[3]{7} \end{cases}\right) \longleftrightarrow ([1]_2, [0]_3)$$

$$\left(\rho : \begin{cases} \zeta_3 \longmapsto \zeta_3 \\ \sqrt[3]{7} \longmapsto \zeta_3 \cdot \sqrt[3]{7} \end{cases}\right) \longleftrightarrow ([0]_2, [1]_3)$$

ALLORA

- per $G_+ \cong \mathbb{Z}_{/2}$ i sottogruppi normali N_+ sono 2 $\left(\{[0]_2\} \text{ e } \mathbb{Z}_{/2}\right)$

- per $G_- \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ i sottogruppi normali N_+ sono in tutto 3

$$\left(\{([\emptyset]_2, [\emptyset]_3)\},\ \{[\emptyset]_2\} \times \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_3 \right)$$

IN CONSEGUENZA,

i sottogruppi normali $N_+ \times N_-$ in $G_+ \times G_-$ sono in totale

$$2 \cdot 3 = 6 .$$

(c) Per il Teorema di Corrispondenza di Galois, sappiamo già a priori che le estensioni $\mathbb{F}$ con $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{K}$ e $\mathbb{F}/\mathbb{Q}$ normale sono tante quanti i sottogruppi normali in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Perciò, da quanto già visto sono 6.

Inoltre, sempre dal Teorema di corrispondenza di Galois abbiamo la biiezione

$$N \longleftrightarrow \mathbb{F} := \mathbb{K}^N$$

dove

$$\mathbb{K}^N := \{ k \in \mathbb{K} \mid \nu(k) = k, \ \forall \nu \in N \}$$

Da questo troviamo:

$$N = \{id\} \cong \{[0]_2\} \times \{([0]_2, [0]_3)\} \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{K}$$

$$N \cong \{[0]_2\} \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{Q}_{(x^2-5)} = \mathbb{Q}(\sqrt{5})$$

$$N \cong \{[0]_2\} \times (\{[0]_2\} \ltimes \mathbb{Z}_3) \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{Q}(\sqrt{5}, \zeta_3) =$$

$$= \mathbb{Q}_{(x^3-5)\cdot(x^2+x+1)}$$

$$N \cong \mathbb{Z}_2 \times \{([0]_2, [0]_3)\} \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{Q}_{(x^3-7)} = \mathbb{Q}(\sqrt[3]{7}, \zeta_3)$$

$$N \cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \ltimes \mathbb{Z}_3) = Gal(\mathbb{K}/\mathbb{Q}) \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{K}^{Gal(\mathbb{K}/\mathbb{Q})} = \mathbb{Q}$$

$$N \cong \mathbb{Z}_2 \times (\{[0]_2\} \ltimes \mathbb{Z}_3) \longleftrightarrow$$

$$\longleftrightarrow \mathbb{K}^N = \mathbb{Q}(\zeta_3) = \mathbb{Q}_{(x^2+x+1)}$$

Questo conclude la risposta al quesito (c). □

3 Sia G un gruppo e H un sottogruppo di G, con $|G| = 385$, $|H| = 77$

(a) Dimostrare che H è l'unico sottogruppo di G di ordine 77.

(b) Dimostrare che $\exists\, K_1, K_2 \leq G$ tali che K_1, K_2 sono caratteristici e $\{e_G\} \subsetneq K_1 \subsetneq K_2 \subsetneq G$.

Soluzione:

(a) Sia $H_+ \leq G$ con $H_+ \neq H$.

Consideriamo l'applicazione

$$\alpha : H \times H_+ \longrightarrow G$$
$$(h, h_+) \longmapsto h \cdot h_+$$

Per l'equivalenza associata ρ_α si ha

$$(h, h_+) \rho_\alpha (\hat{h}, \hat{h}_+) \iff$$

$$\iff h \cdot h_+ = \hat{h} \cdot \hat{h}_+ \iff$$

$$\iff h_+ \cdot \hat{h}_+^{-1} = h^{-1} \cdot \hat{h} \in H_+ \cap H$$

$H_+ \ni$ $\quad \in H$

Questo implica che ogni classe di ρ_α-equivalenza in $H \times H_+$ è della forma

$$[(h, h_+)]_{\rho_\alpha} = \{(h\eta, \eta^{-1} h_+) \mid \eta \in H \cap H_+\}$$

in particolare ha cardinalità

$$|[(h, h_+)]_{\rho_\alpha}| = |H \cap H_+|$$

e quindi

$$\left| \frac{H \times H_+}{\rho_\alpha} \right| = \frac{|H \times H_+|}{|H \cap H_+|} =$$

$$= \frac{|H| \cdot |H_+|}{|H \cap H_+|} = \frac{77^2}{|H \cap H_+|}$$

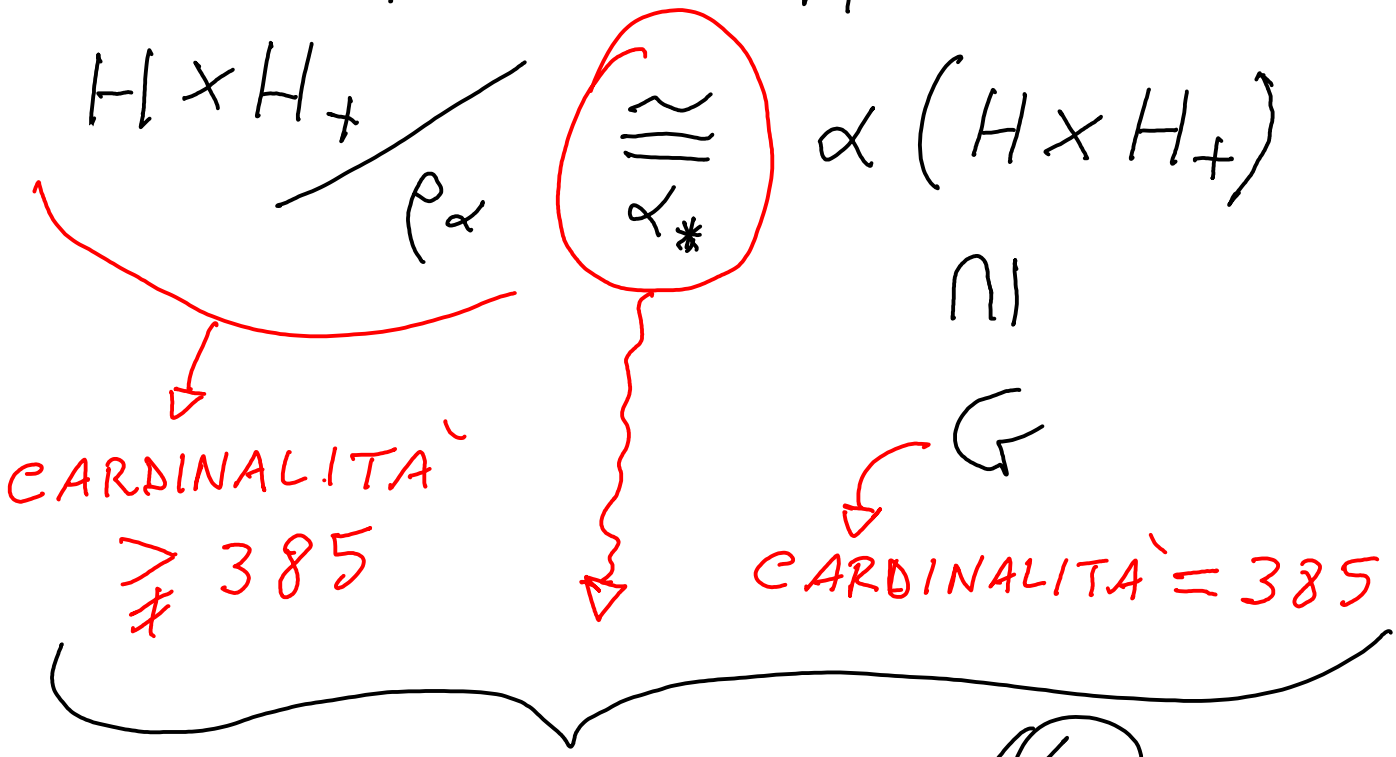
Ora, sia $H_+ \neq H$ segue che $H \cap H_+ \subsetneq H$, e per il Teorema di Lagrange (per $|H| = 77 = 7 \cdot 11$) si ha che $|H \cap H_+| \in \{1, 7, 11\}$, quindi

$$\left| \frac{H \times H_+}{\rho_\alpha} \right| \in \{77^2, 77 \cdot 11, 77 \cdot 7\}$$

che in ogni caso è più di

$$\left| \frac{H \times H_+}{\rho_\alpha} \right| \geq 7 \cdot 11 \cdot 5 = 385$$

D'altra parte, sappiamo che



abbiamo un assurdo, ↯

Dunque non può essere $H_+ \neq H$, il che prova l'unicità di H.

(b) Sappiamo da (a) che

$\exists!\ H \leq G : |H| = 77$

Allora, $\forall\, \varphi \in Aut_g(G)$ si ha

$\varphi(H) \leq G$ e $|\varphi(H)| = |H| = 77$

$\Rightarrow \varphi(H) = H$, per l'unicità di H.

Pertanto H è caratteristico in G, con $|H| = 77 \lneq |G|$

quindi

$$\{e_G\} \subsetneq H \subsetneq G$$

Poniamo allora $K_2 := H$

Sia ora K_1 un 7-sottogruppo di Sylow di H (e quindi di G).

Per $\nu_7 := |\{7\text{-sottogruppi di Sylow in } G\}|$ si ha

$$\nu_7 \in (1+7\cdot\mathbb{N}) \cap \{1,5,11,55\} = \{1\}$$

così $\nu_7 = 1$ e allora

K_1 è caratteristico in G,

con $\{e_G\} \subsetneq K_1 \subsetneq K_2 \subsetneq G$. □

4 $f(x) := x^2 + 7x + 13 \in \mathbb{Z}_4[x]$

(a) Dimostrare che $f(x)$ è irriducibile in $\mathbb{Z}_4[x]$.

(b) Determinare se

$$A := \mathbb{Z}_4[x] / (f(x))$$

sia un dominio, o un campo, o nessuno dei due.

Soluzione:

(a) $\mathbb{Z}_4$ è un dominio a fattorizzazione unica (= DFU), quindi lo è anche $\mathbb{Z}_4[x]$.

Dato che $f(x)$ è monico, possiamo ridurlo modulo p ($\forall$ primo p) e se

la sua riduzione modulo p è irriducibile allora lo è anche $f(x)$.

Per $p := 2$ si ha

$$\overline{f}(X) = X^2 + X + \overline{1} \in \mathbb{Z}_2[X]$$

che non ha radici in $\mathbb{Z}_2$ (ché $\overline{f}(\overline{0}) = \overline{f}(\overline{1}) = \overline{1} \neq \overline{0}$) e quindi – siccome ha grado 2 – è irriducibile in $\mathbb{Z}_2[X]$; $\Rightarrow$ $\Rightarrow$ $f(X)$ è irriducibile in $\mathbb{Z}[X]$

(b) Come già osservato, $\mathbb{Z}[X]$ è un DFU, $\Rightarrow$ ogni irriducibile è primo in $\mathbb{Z}[X]$; $\Rightarrow$ per il punto (a), $f(X)$ è elemento primo in $\mathbb{Z}[X]$; $\Rightarrow$ per un fatto generale (valido in ogni

dominio), l'ideale principale $I_f := (f(x))$ generato dall'elemento primo $f(x)$ è un ideale primo, $\Rightarrow$

$\Rightarrow$ $A/(f(x))$ è un dominio

D'altra parte, il quoziente

$A/(f(x))$ non è un campo

ad esempio perché l'ideale $I_f := (f(x))$ non è massimale - ché $(f(x)) \subsetneq (f(x), 2) \subsetneq \mathbb{Z}_4[x]$ - oppure perché $\nexists\, (\overline{3})^{-1} \in \mathbb{Z}_4[x]$;

infatti $\mathbb{Z}_4[x]/(f(x)) =: A$ si descrive come

$$A = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \cdot \bar{x} = \{a + b\bar{x} \mid a, b \in \mathbb{Z}_4\}$$

con operazioni

$$(a + b\bar{x}) + (a' + b'\bar{x}) =$$
$$= (a + a') + (b + b')\bar{x}$$

$$(a + b\bar{x}) \cdot (a' + b'\bar{x}) =$$
$$= (aa' - 13bb') + (ab' + ba' - 2bb')\bar{x}$$

da cui si vede subito che

$$\nexists\ (\bar{3})^{-1} \in \mathbb{Z}_4[x]/(f(x))$$

(CONTINUA...)

5 (a) Determinare il numero di elementi $\sigma \in S_8$ tali che

$$\sigma^2 = (5,2)(3,6)$$

(b) Sia p primo, $G \neq \{e_G\}$ un p-gruppo finito, $N \trianglelefteq G$, $N \neq \{e_G\}$, e

$$N^G := \{n \in N \mid gng^{-1} = n \ \forall g \in G\}$$

Dimostrare che $|N^G| \geq p$.

Soluzione:

(a) Da $\sigma^2 = (5,2)(3,6)$ segue che $\sigma^4 = id$; siccome $\sigma^2 \neq id$ concludiamo che $\text{ord}(\sigma) = 4$, cioè σ ha ordine 4.

Ora scriviamo σ come prodotto

di cicli disgiunti

$$\sigma = x_1 \circ x_2 \circ \cdots \circ x_n$$

(dove ogni x_i è una permutazione ciclica); allora

$$\text{ord}(\sigma) = \text{m.c.m.}(\text{ord}(x_1), \ldots, \text{ord}(x_n))$$

Ma $\text{ord}(\sigma) = 4$, quindi $\Rightarrow$

$\Rightarrow \text{ord}(x_i) \in \{2, 4\} \quad \forall i = 1, \ldots, n,$

$$\Rightarrow x_i = \begin{cases} (a_i\ b_i) \\ (a_i\ b_i\ c_i\ d_i) \end{cases} \quad (\forall i = 1, \ldots, n)$$

cioè ogni x_i ha lunghezza 2 o 4

ovvero σ ha una delle forme

$$\sigma_1 = (a\ b\ c\ d) \cdot (e\ f\ g\ h)$$

$$\sigma_2 = (a\ b\ c\ d) \cdot (e\ f) \cdot (g\ h)$$

$$\sigma_3 = (a\ b\ c\ d) \cdot (e\ f)$$

oppure $\sigma_4 = x_1 \circ \cdots \circ x_s$ con $s \leq 4$ e ogni x_i ha lunghezza 2 $\Longrightarrow$

$\Rightarrow$ MA in tal caso sarebbe $\sigma_4^2 = id$, $\lightning$

$\Rightarrow$ QUINDI le possibilità sono, a priori, soltanto $\sigma_1, \sigma_2, \sigma_3$. ORA

$$\sigma_1^2 = ((a\,b\,c\,d)\cdot(e\,f\,g\,h))^2 =$$

$$= (a\,b\,c\,d)^2 \circ (e\,f\,g\,h)^2 =$$

$$= (a\,c)(b\,d)(e\,g)(f\,h) \neq (5\,2)(3\,6)$$

$\longrightarrow$ $\sigma \neq \sigma_1$

$$\sigma_2^2 = ((a\,b\,c\,d)(e\,f)(g\,h))^2 =$$

$$= (a\,b\,c\,d)^2 (e\,f)^2 (g\,h)^2 =$$

$$= (a\,b\,c\,d)^2 = (a\,c)(b\,d), \Rightarrow$$

$\Rightarrow$ [$\sigma_2^2 = (a\,c)(b\,d) = (5\,2)(3\,6) \iff$

$\iff \{\{a,c\},\{b,d\}\} = \{\{5,2\},\{3,6\}\}$]

(l'ordine non conta!) QUINDI

può essere

$(a\,b\,c\,d) = (5\,3\,2\,6) =: x_1$

o $(a\,b\,c\,d) = (5\,6\,2\,3) =: x_1$

Analogamente è

$$\sigma_3^2 = ((a\,b\,c\,d)(e\,f))^2 =$$

$$= (a\,b\,c\,d)^2 (e\,f)^2 = (a\,b\,c\,d)^2$$

e quindi si trova come prima

$$(a\,b\,c\,d) = \begin{cases} (5\,3\,2\,6) \\ (5\,6\,2\,3) \end{cases}$$

DUNQUE
σ è della forma

$$\sigma = x_1 \circ x_2 \circ x_3 \quad \text{o} \quad \sigma = x_1 \circ x'$$

con $x_1 \in \{(5\,3\,2\,6), (5\,6\,2\,3)\}$

2 scelte

e x_1, x_2, x_3 cicli di lunghezza 2 su elementi scelti in

$$\{1, \dots, 8\} \setminus \{5,3,2,6\} = \{1,4,7,8\}$$

→ 3 scelte per x_1 e x_2

\+ → 6 scelte per x'

IN TOTALE, per σ abbiamo

$$(2 \times 3) + (2 \times 6) = 18 \text{ scelte}$$

QUINDI la risposta al quesito (a) è 18.

(b) Consideriamo l'azione di G su sé stesso per coniugazione, cioè

$$(g, \gamma) \longmapsto g \cdot \gamma := g \gamma g^{-1}$$

$$\forall\, (g, \gamma) \in G \times G$$

Dall'ipotesi $N \trianglelefteq G$ segue che questa azione si restringe a un'azione

$$G \times N \longrightarrow N, \quad (g, \nu) \longmapsto g \cdot \nu g^{-1}$$

di G su N; $\Rightarrow$ allora N è unione disgiunta delle G-orbite di questa azione - che sono le classi di coniugazione degli elementi di N - diciamo $N = \coprod_{\mathcal{O}^N \in N/G} \mathcal{O}^N$, dove ogni $\mathcal{O}^N$ è una classe di coniugazione (di un $n \in N$) e N/G è lo spazio di tali classi. Ora,

$$N = \coprod_{\mathcal{O}^N \in N/G} \mathcal{O}^N \Rightarrow |N| = \sum_{\mathcal{O}^N \in N/G} |\mathcal{O}^N| \quad (\star)$$

dove in ⊛ abbiamo:

$|N| = p^s$, con $s > 0$, per ipotesi,

$|\mathcal{O}^N| = p^{e_{\mathcal{O}^N}}$ con $e_{\mathcal{O}^N} \geq 0$ (che però dipende dall'orbita $\mathcal{O}^N$) perché $\mathcal{O}^N$ è G-orbita e G è un p-gruppo

(perciò $|\mathcal{O}^N| = |G/\mathcal{St}_n^G| =$

$= \dfrac{|G|}{|\mathcal{St}_n^G|} = \dfrac{p^n}{p^e} = p^{e_{\mathcal{O}^N}}$

$\forall\, n \in \mathcal{O}^N$)

QUINDI la ⊛ diventa

$$p^s = \sum_{\mathcal{O}^N \in N/G} p^{e_{\mathcal{O}^N}} \qquad (*)$$

Ma per costruzione si ha

$N^G = \{ n \in N \mid \mathcal{O}_G(n) = \{n\} \} =$

$= \{ n \in N \mid |\mathcal{O}_G(n)| = 1 \}$

cioè N^G è l'insieme dei punti di N che hanno G-orbita (= classe di coniugazione) banale cioè fatta di 1! elemento.

Allora l'identità ⊛ diventa

$$p^s = \sum_{n \in N^G} 1 + \sum_{\substack{\mathcal{O}^N \in N/G \\ |\mathcal{O}^N| > 1}} p^{e_{\mathcal{O}^N}} =$$

$$= |N^G| + \sum_{\substack{\mathcal{O}^N \in N/G \\ |\mathcal{O}^N| > 1}} p^{e_{\mathcal{O}^N}} \Rightarrow$$

$$\Rightarrow |N^G| = p^s - \sum_{\substack{\mathcal{O}^N \in N/G \\ |\mathcal{O}^N| > 1}} p^{e_{\mathcal{O}^N}}$$

dove tutti gli esponenti sulla destra sono ≥ 1, quindi $|N^G|$ è multiplo di p (in $\mathbb{N}_+$) e così in particolare $|N^G| \geq p$. □