ALGEBRA 2 — 2007/2008

Prof. Fabio Gavarini

Sessione estiva anticipata — prova scritta del 26 Febbraio 2008

Svolgimento completo

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

[1] — Si consideri il polinomio $f(x) := x^6 + x^4 - 4\,x^2 - 4 \in \mathbb{Q}[x]$, e sia $\mathbb{Q}_f$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

(a) Determinare esplicitamente il campo $\mathbb{Q}_f$, e in particolare calcolare il grado dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$ ed una sua base.

(b) Calcolare esplicitamente il gruppo di Galois $G(f)$ dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$.

(c) Stabilire se il polinomio $f(x)$ sia risolubile per radicali oppure no.

Soluzione: *(a)* Per definizione, il campo $\mathbb{Q}_f$ è l'estensione di $\mathbb{Q}$ generata dalle radici — in una opportuna chiusura algebrica, quale ad esempio $\mathbb{Q}^a_{\mathbb{C}}$ — del polinomio $f(x)$; cerchiamo allora tali radici. Il polinomio $f(x)$ è triquadratico in x , e precisamente $f(x) = g\big(x^2\big)$ con

$$g(y) \,:=\, y^3 + y^2 - 4\,y - 4 \;\in\; \mathbb{Q}[y]$$

Ora, $g(y)$ si fattorizza in

$$g(y) \,=\, (y-2)\,\big(y^2 + 3\,y + 2\big) \,=\, (y-2)\,(y+1)\,(y+2)$$

quindi $f(x)$ a sua volta si fattorizza in

$$f(x) \,=\, \big(x^2 - 2\big)\,\big(x^2 + 1\big)\,\big(x^2 + 2\big)$$

dal che discende subito che le radici di $f(x)$ sono tutti e soli gli elementi dell'insieme

$$\big\{\, \sqrt{2}\,,\, -\sqrt{2}\,,\, \sqrt{-1}\,,\, -\sqrt{1}\,,\, \sqrt{-2}\,,\, -\sqrt{-2}\,\big\} \;=\; \big\{\, \sqrt{2}\,,\, -\sqrt{2}\,,\, i\,,\, -i\,,\, i\,\sqrt{2}\,,\, -i\,\sqrt{2}\,\big\}$$

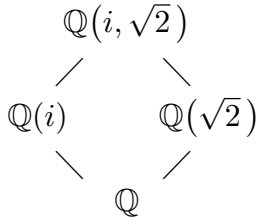
Pertanto $\mathbb{Q}_f = \mathbb{Q}\big(\sqrt{2}\,,\, -\sqrt{2}\,,\, i\,,\, -i\,,\, i\,\sqrt{2}\,,\, -i\,\sqrt{2}\big)$, e poiché chiaramente

$$\mathbb{Q}\big(\sqrt{2}\,,\, -\sqrt{2}\,,\, i\,,\, -i\,,\, i\,\sqrt{2}\,,\, -i\,\sqrt{2}\big) \,=\, \mathbb{Q}\big(\sqrt{2}\,,\, i\,\big)$$

abbiamo più semplicemente

$$\mathbb{Q}_f \,=\, \mathbb{Q}\big(\sqrt{2}\,,\, i\,\big)$$

Per calcolare il grado, osserviamo che abbiamo il seguente diagramma di estensioni:



nel quale le estensioni che appaiono hanno gradi che verificano le seguenti condizioni:

$\big[\mathbb{Q}(i):\mathbb{Q}\big]=2\,,\quad$ perché il polinomio minimo di i su $\mathbb{Q}$ è $x^2+1\,;$ una base di $\mathbb{Q}(i))$ su $\mathbb{Q}$ è $\big\{1\,,\,i\,\big\}\,;$

$\big[\mathbb{Q}\big(\sqrt{2}\,\big):\mathbb{Q}\big]=2\,,\quad$ perché il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$ è $x^2-2\,;$ una base di $\mathbb{Q}\big(\sqrt{2}\,\big)$ su $\mathbb{Q}$ è $\big\{1\,,\,\sqrt{2}\,\big\}\,;$

$\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}(i)\big]\le 2\,,\quad$ perché il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}(i)$ divide $x^2-2\,;$

$\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}\big(\sqrt{2}\,\big)\big]\le 2\,,\quad$ perché il polinomio minimo di i su $\mathbb{Q}\big(\sqrt{2}\,\big)$ divide $x^2+1\,.$

D'altra parte, si ha anche

$$\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}(i)\big]=1\iff\sqrt{2}\in\mathbb{Q}(i)=\big\{\,q_0+q_1i\,\big|\,q_0,q_1\in\mathbb{Q}\big\}$$

e si verifica con un semplice calcolo diretto che invece

$$\sqrt{2}\notin\big\{\,q_0+q_1i\,\big|\,q_0,q_1\in\mathbb{Q}\big\}=\mathbb{Q}(i)$$

cioè non esistono $q_0,q_1\in\mathbb{Q}$ tali che $(q_0+q_1i\,)^2=2\,.$ Pertanto, si conclude infine che $\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}(i)\big]=2\,.$ Inoltre, dal fatto che $\big\{1\,,\,\sqrt{2}\,\big\}$ sia una base di $\mathbb{Q}\big(\sqrt{2}\,\big)$ su $\mathbb{Q}\,,$ segue allora anche che $\big\{1\,,\,\sqrt{2}\,\big\}$ è una base di $\mathbb{Q}\big(i,\sqrt{2}\,\big)$ su $\mathbb{Q}(i)\,.$

In modo del tutto analogo, abbiamo anche che

$$\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}\big(\sqrt{2}\,\big)\big]=1\iff i\in\mathbb{Q}\big(\sqrt{2}\,\big)=\big\{q_0+q_1\sqrt{2}\,\big|\,q_0,q_1\in\mathbb{Q}\big\}$$

e un semplice calcolo diretto dimostra invece che

$$i:=\sqrt{-1}\notin\big\{\,q_0+q_1i\,\big|\,q_0,q_1\in\mathbb{Q}\big\}=\mathbb{Q}\big(\sqrt{2}\,\big)$$

cioè non esistono $q_0,q_1\in\mathbb{Q}$ tali che $(q_0+q_1\sqrt{2}\,)^2=-1\,.$ Pertanto, si conclude dunque che $\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}\big(\sqrt{2}\,\big)\big]=2\,.$ In aggiunta, dal fatto che $\big\{1\,,\,i\,\big\}$ sia una base di $\mathbb{Q}(i)$ su $\mathbb{Q}\,,$ segue allora anche che $\big\{1\,,\,i\,\big\}$ è una base di $\mathbb{Q}\big(i,\sqrt{2}\,\big)$ su $\mathbb{Q}\big(\sqrt{2}\,\big)\,.$

A questo punto, dalla torre di estensioni (ciascuna di grado due)

$$\mathbb{Q}\subseteq\mathbb{Q}(i)\subseteq\mathbb{Q}\big(i,\sqrt{2}\,\big)$$

e dalla moltiplicatività del grado nelle torri di estensioni finite, otteniamo che

$$\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}\big]\;=\;\big[\mathbb{Q}\big(i,\sqrt{2}\,\big):\mathbb{Q}(i)\big]\cdot\big[\mathbb{Q}(i):\mathbb{Q}\big]\;=\;2\cdot2\;=\;4$$

Più precisamente, sappiamo, che una base di $\mathbb{Q}\big(i,\sqrt{2}\,\big)$ su $\mathbb{Q}$ può essere ottenuta prendendo il prodotto — elemento per elemento — di una base di $\mathbb{Q}\big(i,\sqrt{2}\,\big)$ su $\mathbb{Q}(i)\,,$ ad esempio $\big\{1\,,\,\sqrt{2}\,\big\}\,,$ per una base di $\mathbb{Q}(i)$ su $\mathbb{Q}\,,$ ad esempio $\big\{1\,,\,i\,\big\}\colon$ così una possibile base di $\mathbb{Q}\big(i,\sqrt{2}\,\big)$ su $\mathbb{Q}$ è

$$B\;:=\;\big\{1\,,\,\sqrt{2}\,\big\}\cdot\big\{1\,,\,i\,\big\}\;=\;\big\{1\,,\,i\,,\,\sqrt{2}\,,\,i\sqrt{2}\,\big\}\tag{1}$$

In particolare, questo ci dice che

$$\mathbb{Q}_f = \mathbb{Q}\big(i, \sqrt{2}\,\big) = \big\{\, q_0 + q_1\, i + q_2\sqrt{2} + q_3\, i\,\sqrt{2} \;\big|\; q_0, q_1, q_2, q_3 \in \mathbb{Q} \,\big\}$$

(b) Poiché $\mathbb{Q}_f$ è campo di spezzamento su $\mathbb{Q}$ di un polinomio $f(x) \in \mathbb{Q}[x]$, l'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$ è normale e finita, quindi è di Galois: il suo gruppo di Galois $Gal\big(\mathbb{Q}_f/\mathbb{Q}\big)$ è quel che si chiama, per definizione, "gruppo di Galois di $f(x)$", cioè

$$G(f) \;:=\; Gal\big(\mathbb{Q}_f/\mathbb{Q}\big) \;=\; Gal\Big(\mathbb{Q}\big(i, \sqrt{2}\,\big)\Big/\mathbb{Q}\Big)$$

Per descrivere $G(f) = Gal\Big(\mathbb{Q}\big(i, \sqrt{2}\,\big)\Big/\mathbb{Q}\Big)$, osserviamo che ogni $\sigma \in Gal\Big(\mathbb{Q}\big(i, \sqrt{2}\,\big)\Big/\mathbb{Q}\Big)$ deve soddisfare queste condizioni:

$$\sigma(i) \text{ è radice di } x^2+1\,, \qquad\qquad \sigma\big(\sqrt{2}\,\big) \text{ è radice di } x^2-2$$

che equivalgono a

$$\sigma(i) \;\in\; \big\{\, +i\,,\, -i \,\big\}\,, \qquad\qquad \sigma\big(\sqrt{2}\,\big) \;\in\; \big\{\, +\sqrt{2}\,,\, -\sqrt{2}\,\big\} \tag{2}$$

Viceversa, la (2) è anche una condizione *sufficiente*, oltre che necessaria: per ogni scelta di valori

$$\sigma_i \in \big\{\, +i\,,\, -i \,\big\}\,, \qquad\qquad \sigma_{\sqrt{2}} \in \big\{\, +\sqrt{2}\,,\, -\sqrt{2}\,\big\} \tag{3}$$

esiste uno ed un solo $\sigma \in Gal\Big(\mathbb{Q}\big(i, \sqrt{2}\,\big)\Big/\mathbb{Q}\Big) = G(f)$ tale che $\sigma(i) = \sigma_i$ e $\sigma\big(\sqrt{2}\,\big) = \sigma_{\sqrt{2}}$.

Pertanto, tutti gli elementi di $G(f)$ sono determinati — univocamente — da tutte le possibili scelte di valori σ_i e $\sigma_{\sqrt{2}}$ come nella (3). Queste sono in tutto $2 \cdot 2 = 4$, il che corrisponde al fatto che $\big|G(f)\big| = \Big|Gal\big(\mathbb{Q}_f/\mathbb{Q}\big)\Big| = \Big|\big[\mathbb{Q}_f : \mathbb{Q}\big]\Big| = 4$. Tali scelte danno luogo ai seguenti elementi di $G(f)$: indicando con $\sigma_{\sigma_i\,,\,\sigma_{\sqrt{2}}}$ l'unico automorfismo corrispondente alla scelta della coppia $\big(\sigma_i\,,\,\sigma_{\sqrt{2}}\big)$, si ha

$$\begin{aligned}
\sigma_{+i,+\sqrt{2}} \;&:\quad i \mapsto +i \;\;,\quad \sqrt{2} \mapsto +\sqrt{2} \\
\sigma_{-i,+\sqrt{2}} \;&:\quad i \mapsto -i \;\;,\quad \sqrt{2} \mapsto +\sqrt{2} \\
\sigma_{+i,-\sqrt{2}} \;&:\quad i \mapsto +i \;\;,\quad \sqrt{2} \mapsto -\sqrt{2} \\
\sigma_{-i,-\sqrt{2}} \;&:\quad i \mapsto -i \;\;,\quad \sqrt{2} \mapsto -\sqrt{2}
\end{aligned}$$

Inoltre, rispetto alla base $B = \big\{1\,,\, i\,,\, \sqrt{2}\,,\, i\,\sqrt{2}\,\big\}$ di $\mathbb{Q}_f = \mathbb{Q}\big(i, \sqrt{2}\,\big)$ data in (1) tali automorfismi, essendo in particolare trasformazioni lineari del $\mathbb{Q}$–spazio vettoriale $\mathbb{Q}\big(i, \sqrt{2}\,\big)$ in sé, sono descritti esplicitamente dalle formule

$$\begin{aligned}
\sigma_{+i,+\sqrt{2}} \;&:\; 1 \mapsto 1\,,\;\; i \mapsto +i\,,\;\; \sqrt{2} \mapsto +\sqrt{2}\,,\;\; i\,\sqrt{2} \mapsto +i\,\sqrt{2} \\
\sigma_{-i,+\sqrt{2}} \;&:\; 1 \mapsto 1\,,\;\; i \mapsto -i\,,\;\; \sqrt{2} \mapsto +\sqrt{2}\,,\;\; i\,\sqrt{2} \mapsto -i\,\sqrt{2} \\
\sigma_{+i,-\sqrt{2}} \;&:\; 1 \mapsto 1\,,\;\; i \mapsto +i\,,\;\; \sqrt{2} \mapsto -\sqrt{2}\,,\;\; i\,\sqrt{2} \mapsto -i\,\sqrt{2} \\
\sigma_{-i,-\sqrt{2}} \;&:\; 1 \mapsto 1\,,\;\; i \mapsto -i\,,\;\; \sqrt{2} \mapsto -\sqrt{2}\,,\;\; i\,\sqrt{2} \mapsto +i\,\sqrt{2}
\end{aligned}$$

per cui le corrispondenti matrici (rispetto alla base B) sono

$$\sigma_{+i,+\sqrt{2}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad , \qquad \sigma_{-i,+\sqrt{2}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\sigma_{+i,-\sqrt{2}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad , \qquad \sigma_{-i,-\sqrt{2}} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Infine, quanto fatto finora descrive $G(f)$ soltanto come insieme (di automorfismi di $\mathbb{Q}_f$ su $\mathbb{Q}$), ma non dice nulla sulla sua struttura di gruppo. Per quest'ultima, osserviamo che, dalla descrizione esplicita — in termini di generatori (di campo) o di basi (come spazio vettoriale) — degli automorfismi in $G(f)$ fatta qui sopra segue immediatamente anche una decrizione della struttura moltiplicativa: scrivendo per semplicità

$$\sigma_{\epsilon,\eta} := \sigma_{\epsilon\, i\,,\, \eta\sqrt{2}} \qquad \text{per ogni } \ \epsilon, \eta \in \{+,-\}$$

dal calcolo diretto (della composizione di due automorfismi) otteniamo le formule

$$\sigma_{+,+}\,\sigma_{\epsilon,\eta} = \sigma_{\epsilon,\eta}\ , \quad \sigma_{\epsilon,\eta}\,\sigma_{\epsilon,\eta} = \sigma_{+,+}\ , \quad \sigma_{\epsilon,\eta}\,\sigma_{\epsilon',\eta'} = \sigma_{\epsilon',\eta'}\,\sigma_{\epsilon,\eta} \qquad \forall\ \epsilon,\eta,\epsilon',\eta' \in \{+,-\}$$
$$\sigma_{\epsilon,\eta}\,\sigma_{\epsilon',\eta'} = \sigma_{\epsilon'',\eta''} \quad \forall\ \epsilon,\eta,\epsilon',\eta',\epsilon'',\eta'' : \big\{(\epsilon,\eta),(\epsilon',\eta'),(\epsilon'',\eta'')\big\} = \big\{(+,-),(-,+),(-,-)\big\}$$

che consentono di scrivere tutta la tabella moltiplicativa del gruppo. In conseguenza, esistono isomorfismi $G(f) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ di gruppi, per esempio quello dato da

$$\begin{aligned} G(f) &\xrightarrow{\ \cong\ } \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \sigma_{+,+} &\longrightarrow \big(\overline{0},\overline{0}\,\big) \\ \sigma_{+,-} &\longrightarrow \big(\overline{0},\overline{1}\,\big) \\ \sigma_{-,+} &\longrightarrow \big(\overline{1},\overline{0}\,\big) \\ \sigma_{-,-} &\longrightarrow \big(\overline{1},\overline{1}\,\big) \end{aligned}$$

(c) Il campo di spezzamento $\mathbb{Q}_f = \mathbb{Q}\big(i,\sqrt{2}\,\big)$ del polinomio $f(x) \in \mathbb{Q}[x]$ su $\mathbb{Q}$ è ottenuto estendendo $\mathbb{Q}$ tramite gli elementi i e $\sqrt{2}$, quindi $f(x)$ è risolubile per radicali (per la definizione stessa di "risolubilità per radicali").

In alternativa, possiamo usare il criterio per cui

Un polinomio $f(x)$ è risolubile per radicali
se e soltanto se
il suo gruppo di Galois $G(f)$ è risolubile.

Ora, nel nostro caso, anche *senza conoscere* — oppure *prima di conoscere* — la struttura esplicita del gruppo $G(f)$, possiamo osservare che $\big|G(f)\big| = \big[\mathbb{Q}_f : \mathbb{Q}\big] = 4 = 2^2$. Allora, in particolare, da risultati di teoria generale possiamo dedurre che:

$$\big|G(f)\big| = p^n\,,\ \text{con } p \text{ primo},\ n \in \mathbb{N} \quad \Longrightarrow$$
$$\Longrightarrow \quad G(f) \text{ è un } p\text{–gruppo} \quad \Longrightarrow \quad G(f) \text{ è risolubile}$$

oppure (più semplicemente)

$$\big|G(f)\big| = p^2\,,\ \text{con } p \text{ primo} \quad \Longrightarrow \quad G(f) \text{ è abeliano} \quad \Longrightarrow \quad G(f) \text{ è risolubile}$$

In ogni caso, possiamo concludere che $G(f)$ è risolubile. $\square$

[2] — Sia D un dominio unitario a ideali principali, che non è un campo.
Sia I un ideale di D, con $I \neq \{0\}$. Dimostrare che

$$I \text{ è massimale} \quad \Longleftrightarrow \quad \exists\ d \in D : I = (d)\,,\ d \text{ è irriducibile.}$$

<u>Soluzione</u>: Presentiamo due metodi risolutivi, in parte coincidenti.

Primo metodo: Per definizione abbiamo che, per ogni ideale I in D e per ogni elemento $d \in D$, si ha

$$I \text{ è massimale in } D \quad \Longleftrightarrow \quad \begin{cases} I \subsetneqq D \\ \forall\ J \trianglelefteq D \text{ si ha } I \subseteq J \implies J \in \{I, D\} \end{cases} \tag{4}$$

$$d \text{ è irriducibile in } D \quad \Longleftrightarrow \quad \begin{cases} d \notin U(D) \ \bigwedge\ \forall\ a, b \in D\,, \text{ si ha} \\ d = a\,b \implies a \in U(D) \ \bigvee\ b \in U(D) \\ \quad \text{oppure (in modo equivalente)} \\ d = a\,b \implies b \sim d \ \bigvee\ a \sim d \\ \quad \text{oppure (in modo equivalente)} \\ c \,\Big|\, d \implies c \in U(d) \ \bigvee\ c \sim d \end{cases} \tag{5}$$

dove la notazione $x \sim y$ significa "x è associato a y" (in D), mentre $x \,\Big|\, y$ significa "x divide y" (in D).

Ora, poiché D è dominio a ideali principali, anche l'ideale I è principale, cioè esiste un elemento $d \in D$ tale che $I = (d)$. Inoltre, poiché $I \neq \{0\}$, da $I = (d)$ segue anche che $d \neq 0$. Ci resta da dimostrare allora che

$$I = (d) \text{ è massimale} \quad \Longleftrightarrow \quad d \text{ è irriducibile} \tag{6}$$

Sia J un ideale in D. Per ipotesi anch'esso è principale, cioè esiste un $j \in J$ tale che $J = (j)$. A questo punto abbiamo ovviamente

$$(d) = I \subseteq J = (j) \quad \Longleftrightarrow \quad j \,\Big|\, d \tag{7}$$

Allora, mettendo insieme le (4), (5) e (7) si ottiene:

$$I=(d)\ \text{ è massimale } \iff \left\{ \begin{array}{c} (d)=I \subsetneq D=(1) \\ (d)=I \subseteq J=(j) \implies (j)=J \in \big\{ I=(d)\,,\, D=(1) \big\} \end{array} \right\} \iff$$

$$\iff \left\{ \begin{array}{c} 1 \notin (d) \\ (d) \subseteq (j) \ \Rightarrow\ (j) \in \big\{ (d), (1) \big\} \end{array} \right\} \iff \left\{ \begin{array}{c} d \notin U(D) \\ (d) \subseteq (j) \ \Rightarrow\ (j)=(d) \ \vee\ (j)=(1) \end{array} \right\} \iff$$

$$\iff \left(d \notin U(D) \ \bigwedge\ \left(j \,\middle|\, d \implies j \sim d \ \vee\ j \in U(D) \right) \right) \iff d \text{ è irriducibile}$$

e quindi la tesi è dimostrata.

Secondo metodo: Dopo aver osservato (come sopra) che $I=(d)$ con $d \in D \setminus \{0\}$, per dimostrare la (6) possiamo procedere in questo modo.

Prima di tutto, osserviamo che direttamente dalle definizioni di *ideale primo*, di *elemento primo* e di *ideale principale* segue subito che

$$\text{l'}\underline{\textit{ideale}}\ (d)=I \text{ è primo} \iff \text{l'}\underline{\textit{elemento}}\ d \text{ è primo}$$

Da questo, otteniamo che

$$\big[\implies \big] \qquad I \text{ è massimale} \implies I=(d) \text{ è primo (come } \textit{ideale!}) \implies$$
$$\implies d \text{ è primo (come } \textit{elemento!}) \implies d \text{ è irriducibile}$$

perché sappiamo che, in generale — in un qualunque dominio D' — si ha

$$\text{“}I' \text{ massimale} \implies I' \text{ primo”} \qquad \text{(per ogni ideale } I' \trianglelefteq D' \text{)}$$

$$\text{“}d' \text{ primo} \implies d' \text{ irriducibile”} \qquad \text{(per ogni elemento } d' \in D' \text{)}$$

Viceversa, la dimostrazione del fatto che

$$\big[\impliedby \big] \qquad I=(d) \text{ è massimale} \impliedby d \text{ è irriducibile}$$

impiega soltanto la definizione di “elemento irriducibile”, di “ideale massimale” e di “ideale principale”, come nel primo metodo (e non c'è nulla di nuovo da spiegare). $\square$

[3] — Sia $\mathbb{Z}_{42}$ l'anello degli interi modulo 42, e sia $U(\mathbb{Z}_{42})$ il sottoinsieme di $\mathbb{Z}_{42}$ costituito da tutti e soli gli elementi invertibili, *rispetto alla moltiplicazione*, di $\mathbb{Z}_{42}$.

(a) Considerato che $\big(U(\mathbb{Z}_{42})\,;\,\cdot\big)$ è un gruppo (moltiplicativo) abeliano finito, determinarne la struttura ciclica, cioè trovare tutti i primi $p_1, p_2, \ldots, p_s$ e tutti gli interi positivi

$$e_{1,1}, \ldots, e_{1,h_1},\ e_{2,1}, \ldots, e_{2,h_2},\ e_{3,1}, \ldots, e_{s-1,h_{s-1}},\ e_{s,1}, \ldots, e_{s,h_s}$$

tali che, considerando ogni $\mathbb{Z}_{p_i^{\,e_{i,j}}}$ come gruppo additivo, si ha un isomorfismo di gruppi

$$\big(U(\mathbb{Z}_{42})\,;\,\cdot\big) \;\cong\; \mathbb{Z}_{p_1^{\,e_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{\,e_{1,h_1}}} \times \mathbb{Z}_{p_2^{\,e_{2,1}}} \times \cdots \times \mathbb{Z}_{p_s^{\,e_{s,h_s}}}$$

(b - facoltativo) Per ogni primo p, calcolare tutti i p–sottogruppi di Sylow del gruppo moltiplicativo $\big(U(\mathbb{Z}_{42})\,;\,\cdot\big)$.

<u>Soluzione</u>: *(a)* Per cominciare osserviamo che, indicando con φ la funzione di Eulero, si ha

$$\big|\big(U(\mathbb{Z}_{42})\,;\,\cdot\big)\big| \;=\; \varphi(42) \;=\; \varphi(2\cdot 3\cdot 7) \;=\; (2-1)\,(3-1)\,(7-1) \;=\; 12$$

cioè $U(\mathbb{Z}_{42})$ ha ordine $\big|\big(U(\mathbb{Z}_{42})\,;\,\cdot\big)\big| = 12$. Dato che 12 si fattorizza in $12 = 2^2\cdot 3$, se ne deduce che abbiamo due sole possibilità:

(1) $\big(U(\mathbb{Z}_{42})\,;\,\cdot\big) \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, **(2)** $\big(U(\mathbb{Z}_{42})\,;\,\cdot\big) \;\cong\; \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \;=\; \mathbb{Z}_4 \times \mathbb{Z}_3$

Come si distinguono i due casi possibili??? Ad esempio, dagli ordini degli elementi!

Nel **caso (1)**, ci sono esattamente
— 1 elemento di ordine 1 ;
— 3 elementi di ordine 2 ;
— 2 elementi di ordine 3 ;
— 6 elementi di ordine 6 .

Nel **caso (2)**, ci sono esattamente
— 1 elemento di ordine 1 ;
— 1 elemento di ordine 2 ;
— 2 elementi di ordine 4 ;
— 2 elementi di ordine 3 ;
— 2 elementi di ordine 6 ;
— 4 elementi di ordine 12 .

N.B.: nel caso (2) si ha $U(\mathbb{Z}_{42}) \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$, dunque $U(\mathbb{Z}_{42})$ è *ciclico*.

Pertanto, per capire quali dei due casi è effettivamente verificato, basta andare a verificare se nel gruppo $\big(U(\mathbb{Z}_{42})\,;\,\cdot\big)$ *mancano o esistono* elementi di ordine 4, oppure di ordine 12, oppure *quanti sono* gli elementi di ordine 2, oppure di ordine 6. In particolare, *non* è necessario calcolare l'ordine di *tutti* gli elementi, ma ne basteranno alcuni (e precisamente, al massimo 6).

All'atto pratico, il nostro gruppo (moltiplicativo) è

$$\begin{aligned} U(\mathbb{Z}_{42}) &= \left\{ \overline{n} \in \mathbb{Z}_{42} \,\middle|\, 0 \leq n < 42\,,\ M.C.D.(n,42) = 1 \right\} \\ &= \left\{ \overline{1}\,,\, \overline{5}\,,\, \overline{11}\,,\, \overline{13}\,,\, \overline{17}\,,\, \overline{19}\,,\, \overline{23}\,,\, \overline{25}\,,\, \overline{29}\,,\, \overline{31}\,,\, \overline{37}\,,\, \overline{41} \right\} \end{aligned}$$

dove vale la pena di osservare (per semplificare i calcoli) che $\overline{23} = -\overline{19}$, $\overline{25} = -\overline{17}$, $\overline{29} = -\overline{13}$, $\overline{31} = -\overline{11}$, $\overline{37} = -\overline{5}$, $\overline{41} = -\overline{1}$. Ora, il calcolo esplicito — fatto con un minimo di astuzia, per semplificare i conti — ci consente di trovare i seguenti ordini:

$$\begin{gathered} \mathrm{ord}\big(\overline{1}\big) = 1 \\ \mathrm{ord}\big(\overline{13}\big) = \mathrm{ord}\big(\overline{29}\big) = \mathrm{ord}\big(\overline{41}\big) = 2 \\ \mathrm{ord}\big(\overline{25}\big) = \mathrm{ord}\big(\overline{37}\big) = 3 \\ \mathrm{ord}\big(\overline{5}\big) = \mathrm{ord}\big(\overline{11}\big) = \mathrm{ord}\big(\overline{17}\big) = \mathrm{ord}\big(\overline{23}\big) = \mathrm{ord}\big(\overline{31}\big) = 6 \end{gathered}$$

quindi siamo nel **caso (1)**, e dunque in conclusione $U(\mathbb{Z}_{42}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Esempio: poiché $\overline{41} = -\overline{1}$, si ha ovviamente $\mathrm{ord}\big(\overline{41}\big) = \mathrm{ord}\big(\overline{1}\big) = 2$. Inoltre, calcolando a mano trovo che $\overline{13}^{\,2} = \overline{169} = \overline{1}$, per cui $\mathrm{ord}\big(\overline{13}\big) = 2$. *Ma allora*

in $U(\mathbb{Z}_{42})$ gli elementi di ordine 2 sono più di uno

quindi — *senza* bisogno altri calcoli! — *non siamo* nel caso (2), e perciò siamo necessariamente nel caso (1), cioè $U(\mathbb{Z}_{42}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

(b) Per ogni primo p, sia ν_p il numero di p–sottogruppi di Sylow di $U(\mathbb{Z}_{42})$. Ora, *poiché $U(\mathbb{Z}_{42})$ è abeliano, ogni suo sottogruppo è normale*: ciò vale in particolare per tutti i p–sottogruppi di Sylow, che sono tra loro coniugati, e quindi in effetti coincidono (per ciascun p fissato). In altre parole, si ha $\nu_p = 1$ per ogni primo p.

A questo punto, per ogni primo p indichiamo con N_p l'unico p–sottogruppo di Sylow (eventualmente banale!) di $U(\mathbb{Z}_{42})$. Poiché $\big|U(\mathbb{Z}_{42})\big| = \varphi(42) = 12 = 2^2 \cdot 3$, abbiamo

$$N_p = \left\{ \overline{1} \right\} \qquad \forall\ p \text{ primo},\ p \notin \{2\,,3\}$$

e inoltre, in virtù dei calcoli precedenti relativi agli ordini dei vari elementi,

$$N_2 = \left\{ \overline{z} \in U(\mathbb{Z}_{42}) \right\}_{\mathrm{ord}(\overline{z}) \in \{1,2,4\}} = \left\{ \overline{z} \in U(\mathbb{Z}_{42}) \right\}_{\mathrm{ord}(\overline{z}) \in \{1,2\}} = \left\{ \overline{1}\,,\, \overline{13}\,,\, \overline{29}\,,\, \overline{41} \right\}$$

$$N_3 = \left\{ \overline{z} \in U(\mathbb{Z}_{42}) \,\middle|\, \mathrm{ord}\big(\overline{z}\big) \in \{1,3\} \right\} = \left\{ \overline{1}\,,\, \overline{25}\,,\, \overline{37} \right\} \quad . \qquad \square$$

[4] — Siano A e B due insiemi disgiunti. Siano $\mathcal{S}(A)$, $\mathcal{S}(B)$ e $\mathcal{S}\big(A\cup B\big)$ i gruppi simmetrici delle permutazioni su A, su B e su $A\cup B$ rispettivamente. Siano poi

$$\mathcal{S}_A^B \;:=\; \Big\{\, \sigma\in\mathcal{S}\big(A\cup B\big) \,\Big|\, \sigma(A)=A \,\Big\}\;, \qquad \mathcal{S}_B^A \;:=\; \Big\{\, \tau\in\mathcal{S}\big(A\cup B\big) \,\Big|\, \tau(B)=B \,\Big\}$$

Dimostrare che:

(a) $\mathcal{S}_A^B$ e $\mathcal{S}_B^A$ sono sottogruppi di $\mathcal{S}\big(A\cup B\big)$;

(b) $\mathcal{S}_A^B=\mathcal{S}_B^A$;

(c) $\mathcal{S}_A^B\cong\mathcal{S}(A)\times\mathcal{S}(B)$, cioè il gruppo $\mathcal{S}_A^B$ è isomorfo al prodotto diretto dei gruppi $\mathcal{S}(A)$ e $\mathcal{S}(B)$.

<u>Soluzione</u>: *(a)* Per dimostrare che $\mathcal{S}_A^B$ è un sottogruppo di $\mathcal{S}\big(A\cup B\big)$, osserviamo che:

– (1) $e_{\mathcal{S}(A\cup B)}=id_{A\cup B}\in\mathcal{S}_A^B$, per definizione;

– (2) per ogni $\sigma\in\mathcal{S}_A^B$, si ha $\sigma(A)=A$; dato che σ è invertibile, abbiamo allora

$$A \;=\; id_{A\cup B}(A) \;=\; \big(\sigma^{-1}\circ\sigma\big)(A) \;=\; \sigma^{-1}\big(\sigma(A)\big) \;=\; \sigma^{-1}(A)$$

cioè in sintesi $\sigma^{-1}(A)=A$, per cui $\sigma^{-1}\in\mathcal{S}_A^B$;

– (3) per ogni $\sigma_1,\sigma_2\in\mathcal{S}_A^B$, si ha $\sigma_1(A)=A=\sigma_2(A)$, e quindi

$$(\sigma_1\circ\sigma_2)(A) \;=\; \sigma_1\big(\sigma_2(A)\big) \;=\; \sigma_1(A) \;=\; A$$

cioè in conclusione $(\sigma_1\circ\sigma_2)(A)=A$, per cui $(\sigma_1\circ\sigma_2)\in\mathcal{S}_A^B$.

Da (1), (2) e (3) segue che $\mathcal{S}_A^B$ è sottogruppo di $\mathcal{S}_A^B$, q.e.d.

Invertendo i ruoli di A e B si ottiene poi l'analogo risultato per $\mathcal{S}_B^A$.

(b) Sia $\sigma\in\mathcal{S}_A^B$. Per definizione, $\sigma(A)=A$. Ora, B è il complementare di A in $A\cup B$, cioè $B=(A\cup B)\setminus A$; inoltre, σ è una permutazione di $(A\cup B)$ in sé. Pertanto, abbiamo

$$\sigma(B) \;=\; \sigma\big((A\cup B)\setminus A\big) \;=\; (A\cup B)\setminus\sigma(A) \;=\; (A\cup B)\setminus A \;=\; B$$

cioè $\sigma(B)=B$, e quindi $\sigma\in\mathcal{S}_B^A$. Questo dimostra che $\mathcal{S}_A^B\subseteq\mathcal{S}_B^A$.

Invertendo i ruoli di A e B si ottiene l'inclusione inversa — $\mathcal{S}_B^A\subseteq\mathcal{S}_A^B$, dunque $\mathcal{S}_A^B\supseteq\mathcal{S}_B^A$ — quindi $\mathcal{S}_A^B=\mathcal{S}_B^A$, q.e.d.

(c) Presentiamo due metodi risolutivi.

Primo metodo: Sia $\sigma\in\mathcal{S}_A^B$. Allora $\sigma(A)=A$, per cui $\sigma\big|_A$ è un'applicazione suriettiva da A ad A; inoltre, $\sigma\big|_A$ è anche (ovviamente) iniettiva, perché lo è σ stessa, per ipotesi. Pertanto $\sigma\big|_A\in\mathcal{S}(A)$. Analogamente, visto che $\mathcal{S}_A^B=\mathcal{S}_B^A$, invertendo i ruoli di A e B si ha anche che $\sigma\big|_B\in\mathcal{S}(B)$. In conclusione, abbiamo una ben definita applicazione

$$\Phi\,:\,\mathcal{S}_A^B\longrightarrow\mathcal{S}(A)\times\mathcal{S}(B)\;,\quad \sigma\mapsto\Phi(\sigma):=\Big(\sigma\big|_A\,,\,\sigma\big|_B\Big) \tag{8}$$

Dimostriamo ora che la Φ in (8) — dove a destra si considera nell'insieme $\mathcal{S}(A)\times\mathcal{S}(B)$ prodotto cartesiano di $\mathcal{S}(A)$ e $\mathcal{S}(B)$ la struttura di gruppo del prodotto diretto — è un isomorfismo di gruppi.

È immediato verificare che Φ è iniettiva: infatti, per ogni $\sigma',\sigma''\in\mathcal{S}_A^B$ si ha

$$\Phi\big(\sigma'\big)\,=\,\Phi\big(\sigma''\big)\implies\Big(\sigma'\big|_A\,,\,\sigma'\big|_A\Big)\,=\,\Big(\sigma''\big|_A\,,\,\sigma''\big|_B\Big)\implies$$
$$\implies\Big(\,\sigma'\big|_A=\sigma''\big|_A\;\bigvee\;\sigma'\big|_B=\sigma''\big|_B\,\Big)\implies\sigma'\big|_{(A\cup B)}=\sigma''\big|_{(A\cup B)}\implies\sigma'=\sigma''$$

È immediato anche verificare che Φ conserva il prodotto: infatti, per ogni $\sigma',\sigma''\in\mathcal{S}_A^B$,

$$\Phi\big(\sigma'\circ\sigma''\big)\,:=\,\Big(\big(\sigma'\circ\sigma''\big)\big|_A\,,\,\big(\sigma'\circ\sigma''\big)\big|_B\Big)\,=\,\Big(\sigma'\big|_A\circ\sigma''\big|_A\,,\,\sigma'\big|_B\circ\sigma''\big|_B\Big)\,=$$
$$=\,\Big(\sigma'\big|_A\,,\,\sigma'\big|_B\Big)\cdot\Big(\sigma''\big|_A\,,\,\sigma''\big|_B\Big)\,=\,\Phi\big(\sigma'\big)\cdot\Phi\big(\sigma''\big)$$

Infine, Φ è anche suriettiva: infatti, per ogni $\tau_A\in\mathcal{S}(A)$ e $\tau_B\in\mathcal{S}(B)$ resta definita l'applicazione

$$\sigma\,:\,A\cup B\longrightarrow A\cup B\,,\quad x\mapsto\sigma(x):=\begin{cases}\tau_A(x) & \text{se } x\in A\\ \tau_B(x) & \text{se } x\in B\end{cases}$$

e chiaramente si ha che $\sigma\in\mathcal{S}_A^B$. Inoltre, per costruzione, si ha anche

$$\Phi(\sigma)\,:=\,\Big(\sigma\big|_A\,,\,\sigma\big|_B\Big)\,=\,\big(\tau_A\,,\,\tau_B\big)$$

Da questo si conclude allora che Φ è suriettiva, come affermato.

In conclusione, la Φ in (8) è un isomorfismo di gruppi, e quindi il gruppo $\mathcal{S}_A^B$ è isomorfo al prodotto diretto $\mathcal{S}(A)\times\mathcal{S}(B)$.

Secondo metodo: Consideriamo i due sottoinsiemi di $\mathcal{S}\big(A\cup B\big)$ così definiti:

$$\mathcal{S}^A\,:=\,\Big\{\,\sigma\in\mathcal{S}\big(A\cup B\big)\;\Big|\;\sigma\big|_B=id_B\,\Big\}\;,\qquad\mathcal{S}^B\,:=\,\Big\{\,\sigma\in\mathcal{S}\big(A\cup B\big)\;\Big|\;\sigma\big|_A=id_A\,\Big\}$$

Dalle definizioni abbiamo subito che $\mathcal{S}^A\subseteq\mathcal{S}_B^A=\mathcal{S}_A^B$ e $\mathcal{S}^B\subseteq\mathcal{S}_A^B$. Inoltre, tali sottoinsiemi sono anche *sottogruppi normali* di $\mathcal{S}_A^B$. Un modo rapido di verificarlo è il seguente: le applicazioni

$$\mathcal{S}_B^A=\mathcal{S}_A^B\xrightarrow{\Phi_B}\mathcal{S}(B)\,,\quad\sigma\mapsto\Phi_B(\sigma):=\sigma\big|_B\;,\qquad\mathcal{S}_A^B\xrightarrow{\Phi_A}\mathcal{S}(A)\,,\quad\sigma\mapsto\Phi_A(\sigma):=\sigma\big|_A$$

sono chiaramente dei morfismi — suriettivi (ma questo non è rilevante) — di gruppi. Ma per definizione si ha subito che

$$Ker(\Phi_B)\,=\,\mathcal{S}^A\quad,\qquad Ker(\Phi_A)\,=\,\mathcal{S}^B$$

per cui appunto

$$\mathcal{S}^A = Ker(\Phi_B) \trianglelefteq \mathcal{S}_A^B \quad , \qquad \mathcal{S}^B = Ker(\Phi_A) \trianglelefteq \mathcal{S}_A^B \tag{9}$$

Osserviamo poi che

$$\mathcal{S}^A \bigcap \mathcal{S}^B \;=\; \Big\{ \sigma \in \mathcal{S}\big(A \cup B\big) \;\Big|\; \sigma\big|_B = id_B \,,\; \sigma\big|_A = id_A \Big\} \;=\; \big\{ id_{A\cup B} \big\} \tag{10}$$

Infine, per ogni $\sigma \in \mathcal{S}_A^B$ possiamo definire $\sigma_A \,,\, \sigma_B \in \mathcal{S}\big(A \cup B\big)$ così:

$$\sigma_A(x) \;:=\; \begin{cases} \sigma(x) \,, & \forall\; x \in A \\ x \,, & \forall\; x \in B \end{cases} \qquad\qquad \sigma_B(x) \;:=\; \begin{cases} x \,, & \forall\; x \in A \\ \sigma(x) \,, & \forall\; x \in B \end{cases}$$

dalla definizione segue allora che

$$\sigma_A \in \mathcal{S}^A \quad , \quad \sigma_B \in \mathcal{S}^B \quad , \qquad \sigma = \sigma_A \circ \sigma_B = \sigma_B \circ \sigma_A$$

da cui infine otteniamo in particolare che

$$\mathcal{S}_A^B \;=\; \mathcal{S}^A \circ \mathcal{S}^B \qquad \text{o anche} \qquad \mathcal{S}_A^B \;=\; \mathcal{S}^B \circ \mathcal{S}^A \tag{11}$$

In conclusione, la (9), la (10) e la (11) insieme ci dicono che $\mathcal{S}_A^B$ è isomorfo al prodotto diretto dei suoi due sottogruppi (normali) $\mathcal{S}^A$ e $\mathcal{S}^B$, cioè esistono isomorfismi

$$\phi \,:\, \mathcal{S}_A^B \xrightarrow{\;\cong\;} \mathcal{S}^A \times \mathcal{S}^B \qquad \text{e anche} \qquad \psi \,:\, \mathcal{S}_A^B \xrightarrow{\;\cong\;} \mathcal{S}^B \times \mathcal{S}^A \tag{12}$$

Ma adesso possiamo ancora osservare che esistono isomorfismi di gruppi

$$\Psi_A \,:\, \mathcal{S}^A \xrightarrow{\;\cong\;} \mathcal{S}(A) \,,\;\; \tau \;\mapsto\; \Psi_A(\sigma) := \tau\big|_A \,, \qquad \Psi_B \,:\, \mathcal{S}^B \xrightarrow{\;\cong\;} \mathcal{S}(B) \,,\quad \tau \;\mapsto\; \Psi_B(\sigma) := \tau\big|_B$$

e quindi accoppiandoli si ottiene un isomorfismo

$$\big(\Psi_A,\Psi_B\big) : \mathcal{S}^A \times \mathcal{S}^B \xrightarrow{\;\cong\;} \mathcal{S}(A) \times \mathcal{S}(B) \,,\;\; \big(\sigma_A, \sigma_B\big) \mapsto \big(\Psi_A(\sigma_A), \Psi_B(\sigma_B)\big) = \big(\sigma_A\big|_A, \sigma_B\big|_B\big) \tag{13}$$

Infine, componendo l'isomorfismo ϕ in (12) e l'isomorfismo $\big(\Psi_A, \Psi_B\big)$ in (13) otteniamo un isomorfismo

$$\Big(\big(\Psi_A, \Psi_B\big) \circ \phi\Big) \;:\; \mathcal{S}_A^B \xrightarrow{\;\cong\;} \mathcal{S}(A) \times \mathcal{S}(B) \quad , \qquad \sigma \mapsto \Big(\sigma\big|_A, \sigma\big|_B\Big) \tag{14}$$

per cui in conclusione $\mathcal{S}_A^B \cong \mathcal{S}(A) \times \mathcal{S}(B)$, q.e.d.

<u>N.B.:</u> l'isomorfismo ottenuto in (14) è proprio l'isomorfismo Φ già trovato in (8) !!! Dunque i due metodi in effetti danno esattamente lo stesso risultato — si tratta soltanto di due diverse formulazioni della stessa idea. $\square$