Esercizi di Algebra 2

Corso di Laurea in Matematica

Università degli Studi di Palermo

BOZZA

Giuseppe Metere e Manuel Mancini

27 dicembre 2022

Indice

Introduzione

Queste note contengono esercizi svolti di algebra, tratti da temi d'esame e dalle esercitazioni per il corso di Algebra 2 dell'Università degli Studi di Palermo. Sono state predisposte allo scopo di accompagnare la preparazione degli studenti per la prova scritta dell'esame, e non hanno alcuna pretesa di originalità.

Capitolo 1

Teoria dei gruppi

1.1 Proprietà universali, gruppi liberi e presentazioni di gruppi

Esercizio 1.1: prova d'esame del 16/09/2020 - n° 2

Sia $f\colon G \to H$ un omomorfismo di gruppi, e $N < G$ un sottogruppo normale di G tale che $f(N) = \{1_H\}$. Dimostrare che f fattorizza univocamente per la proiezione canonica $\pi\colon G \to G/N$, i.e. che esiste uno e un solo omomorfismo di gruppi $k\colon G/N \to H$ tale che $k \circ \pi = f$.

Soluzione. Ricordiamo che π è definita dalla posizione $\pi(x) = xN$, per $x \in G$. Allora è immediato definire $k(xN) = f(x)$. Infatti k è ben definita: se è dato $y \in G$ tale che $yN = xN$, allora esiste $n \in N$ tale che $y = xn$. Pertanto, si avrà

$$k(yN) = f(y) = f(xn) = f(x)f(n) = f(x)1_H = f(x) = k(xN)\,.$$

Inoltre k è omomorfismo, poiché

$$k(xN\,x'N) = k(xx'N) = f(xx') = f(x)\,f(x') = k(xN)\,k(x'N)\,.$$

Infine, k soddisfa $k \circ \pi = f$. In effetti, se $x \in G$, si ha

$$k \circ \pi(x) = k(\pi(x)) = k(xN) = f(x)\,.$$

L'unicità di k è immediata: se anche $k'\colon G/N\colon H$ soddisfa le condizioni, abbiamo, per ogni $xN \in G/N$

$$k'(xN) = k'(\pi(x)) = k(\pi(x)) = k(xN)\,.$$

Esercizio 1.2: prima prova parziale del 10/11/2020 - n° 2

Dimostrare che il gruppo G con presentazione

$$G = \langle x, y \mid x^3, y^4, xyx^2y^3 \rangle$$

è isomorfo a $(\mathbb{Z}_{12}, +)$.

Soluzione. È sufficiente dimostrare che $|G| = 12$ e che G sia ciclico, ovvero che ammetta un elemento di periodo 12.

G è generato da un elemento x di periodo 3 e da un elemento y di periodo 4. Allora la terza relazione si può scrivere nel seguente modo:

$$1_G = xyx^2y^3 = xyx^{-1}y^{-1},$$

ovvero i generatori x e y di G commutano. Da ciò segue che G è un gruppo abeliano e i suoi elementi sono le potenze

$$x^i y^j, \quad con \quad i = 0, 1, 2, \ j = 0, 1, 2, 3$$

Dunque G ha esattamente 12 elementi. Inoltre

$$o(xy) = mcm\{o(x), o(y)\} = mcm\{3, 4\} = 12,$$

così G è un gruppo ciclico. Si conclude che $G \cong (\mathbb{Z}_{12}, +)$.

Esercizio 1.3: prova d'esame del 28/06/2021 - n° 2

Si consideri il gruppo moltiplicativo

$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}_2 \right\}$$

Dopo avere dimostrato che G è un gruppo non abeliano di ordine 8, si descrivano i suoi sottogruppi propri, specificando quali di essi siano normali.
A quale dei due gruppi non abeliani di ordine 8 è isomorfo G? Motivare la risposta.

Soluzione. La moltiplicazione riga per colonna di due matrici unitriangolari superiori ci permette di scrivere il gruppo G come l'insieme delle terne $(a, b, c) \in \mathbb{Z}_2^3$ con moltiplicazione

$$(a, b, c)(x, y, z) = (a + x, b + y, c + z + ay).$$

ed elemento neutro $(0, 0, 0)$. Allora G è un gruppo di ordine 8 ed è non abeliano in quanto

$$(1, 0, 1)(0, 1, 1) = (1, 1, 1) \neq (1, 1, 0) = (0, 1, 1)(1, 0, 1).$$

G possiede due elementi di periodo 4, precisamente le terne $(1, 1, 0)$ e $(1, 1, 1)$, e cinque elementi di periodo 2. Così G ha esattamente cinque sottogruppi di ordine 2

$$\langle(1, 0, 0)\rangle; \langle(0, 1, 0)\rangle; \langle(0, 0, 1)\rangle; \langle(1, 0, 1)\rangle; \langle(0, 1, 0)\rangle;$$

e tre sottogruppi di ordine 4, di cui uno ciclico

$$\langle(1, 1, 0)\rangle = \{(0, 0, 0), (1, 1, 0), (0, 0, 1), (1, 1, 1)\},$$

e due isomorfi al gruppo di Klein

$$\{(0, 0, 0), (1, 0, 0), (0, 0, 1), (1, 0, 1)\},$$

$$\{(0, 0, 0), (0, 1, 0), (0, 0, 1), (0, 1, 1)\}.$$

I tre sottogruppi di ordine 4 sono tutti normali, in quanto hanno indice 2 in G. Si verifica inoltre che l'unico sottogruppo normale di ordine 2 è quello generato dalla terna $(0, 0, 1)$ ed esso coincide con il centro $Z(G)$. Infine la mappa

$$(1, 1, 0) \mapsto \rho, \ (1, 0, 0) \mapsto \sigma$$

definisce un isomorfismo di gruppi $f : G \leftrightarrows D_4$. Si osserva infatti che vale la relazione

$$[(1, 1, 0)(1, 0, 0)]^2 = (0, 0, 0).$$

Allo stesso risultato si poteva arrivare anche per esclusione, ragionando sull'ordine degli elementi, e osservando che l'unico altro gruppo non abeliano di ordine 8 è il gruppo dei quaternioni Q_8.

1.2 Azioni di gruppi, equazione delle classi di un gruppo e G-insiemi

Esercizio 1.4: Prima Prova Parziale del 10/11/2020 - n° 1

Si consideri la funzione $f\colon \mathbb{R}\times\mathbb{C}\to\mathbb{C}$ definita dalla formula $f(t,z)=z\cdot e^{it}$, per $t\in\mathbb{R}$ e $z\in\mathbb{C}$.

(i) Dimostrare che f definisce un'azione $t*z=f(t,z)$ del gruppo $(\mathbb{R},+)$ sull'insieme $\mathbb{C}$ dei numeri complessi.

(ii) Calcolare orbita e stabilizzatore di un generico $z\in\mathbb{C}$.

Soluzione.

(i) Per ogni $z\in\mathbb{C}$, si ha

$$0*z=z\cdot e^{i0}=z\,.$$

Inoltre, per $s,t\in\mathbb{R}$, si calcola:

$$s*(t*z)=s*(z\cdot e^{it})=(z\cdot e^{it})\cdot e^{is}=z\cdot e^{i(s+t)}=(s+t)*z\,.$$

(ii) Per $z=0_{\mathbb{C}}$ si ha

$$\mathsf{Orb}(0)=\{0\}\,,\qquad \mathsf{Stab}(0)=\mathbb{R}\,.$$

Per $z_0\in\mathbb{C}^*$, invece si calcola

$$\mathsf{Orb}(z_0)=\{z_0\cdot e^{it}\,|\,t\in\mathbb{R}\}\,,$$

cioè la circonferenza con centro nell'origine, passante per z_0;

$$\mathsf{Stab}(z_0)=\{t\in\mathbb{R}\,|\,z\cdot e^{it}=z\}\,,$$

cioè il sottogruppo additivo dei reali $\{2k\pi\,|\,k\in\mathbb{Z}\}$.

Esercizio 1.5: prova d'esame del 10/11/2020 - n° 2

Scrivere l'equazione delle classi di un gruppo non abeliano di ordine 39.

Soluzione. Poiché G non è abeliano, $Z(G) \neq G$. Se fosse $|Z(G)| = 13$, si avrebbe che $G/Z(G)$ sarebbe ciclico, e quindi G abeliano; analogamente, se fosse $|Z(G)| = 3$. Quindi possiamo concludere $|Z(G)| = 1$.

Poiché i centralizzanti degli elementi di G sono sottogruppi il cui ordine divide l'ordine di G, essi possono avere ordine 13 o ordine 3. Quindi, si ha la relazione $39 = 1 + 3a + 13b$, con a e b interi non negativi. L'unica soluzione $a = 4$ $b = 2$ ci da l'equazione delle classi di G:

$$39 = 1 + 3 + 3 + 3 + 3 + 13 + 13$$

Esercizio 1.6: prova d'esame del 20/01/2021 - n° 1

Calcolare la cardinalità della classe di coniugio dell'elemento

$$\sigma = (12)(34)$$

nel gruppo di permutazioni S_n, con $n \geq 4$. Successivamente, dopo averne ricordato la definizione, calcolare la cardinalità del centralizzante di σ in S_n.

Soluzione. Una permutazione $\tau \in S_n$ è coniugata a σ se e solo se τ e σ hanno la stessa struttura ciclica. Quindi, la classe di coniugio $\bar{\sigma}$ di σ ha tanti elementi quante sono le coppie di due cicli distinti di S_n:

$$\bar{\sigma} = \{\tau \in S_n \,|\, \tau = (ab)(cd)\}\,.$$

Quindi si calcola $|\bar{\sigma}| = \frac{n(n-1)(n-2)(n-3)}{8}$, dove abbiamo diviso per 8 perché la stessa permutazione $(ab)(cd)$ può essere scritta anche scambiando a con b, c con d e (ab) con (cd). Infine, per il teorema Orbita/Stabilizzatore, si ha che

$$|S_n| = |\bar{\sigma}| \cdot |Z_{Sn}(\sigma)|\,,$$

Da cui si calcola $|Z_{Sn}(\sigma)| = 8(n-4)!$.

Esercizio 1.7: prova d'esame del 3/02/2021 - n° 2

Sia Γ un sottogruppo di ordine 8 del gruppo simmetrico $\mathbb{S}_7$. Dimostrare che esiste $i \in \{1, \ldots, 7\}$ tale che, per ogni $\gamma \in \Gamma$, si abbia $\gamma(i) = i$.
Suggerimento: studiare l'equazione delle classi dell'azione canonica di Γ su $\{1, \ldots, 7\}$.

Soluzione. Considero l'azione canonica

$$\Gamma \times \{1, ..., 7\} \to \{1, ..., 7\}$$

$$(\gamma, i) \to \gamma(i)$$

Si deve dimostrare che la cardinalità del sottoinsieme X degli elementi di $\{1, ..., 7\}$ che sono fissati da tutti gli elementi di Γ è non nulla. Ma Γ è un 2-gruppo e dall'equazione delle classi dell'azione canonica di Γ su $\{1, ..., 7\}$ si ricava che

$$7 = |\{1, ..., 7\}| \equiv |X| \ (mod\ 2),$$

così $|X| \geq 1$.

Esercizio 1.8: prova d'esame del 17/02/2021 - n° 2

Sia $X = \{1, 2, 3, 4, 5\}$. Si consideri l'azione $*$ del gruppo simmetrico $\mathbb{S}_5$ sull'insieme $X^3 = X \times X \times X$ definita da,

$$\sigma * (x, y, z) = (\sigma(x), \sigma(y), \sigma(z))$$

per $\sigma \in \mathbb{S}_5$, e $(x, y, z) \in X^3$. Determinare le orbite di $*$ e dedurre, per ogni orbita, la cardinalità del relativo stabilizzatore.
Suggerimento: studiare le orbite di $(1, 1, 1)$, $(1, 2, 1)$, $(1, 2, 3)$.

Soluzione. Studiamo le orbite dell'azione e l'ordine dei relativi stabilizzatori.

(i) $Orb(1, 1, 1) = \{(\sigma(1), \sigma(1), \sigma(1)) \mid \sigma \in \mathbb{S}_5\} = \{(x, x, x) \mid x \in X\}$. Inoltre

$$|Stab(1, 1, 1)| = \frac{|\mathbb{S}_5|}{|Orb(1, 1, 1)|} = \frac{120}{5} = 24.$$

(ii) $Orb(1, 2, 1) = \{(\sigma(1), \sigma(2), \sigma(1)) \mid \sigma \in \mathbb{S}_5\} = \{(x, y, x) \mid x, y \in X, x \neq y\}$. Inoltre

$$|Stab(1, 2, 1)| = \frac{|\mathbb{S}_5|}{|Orb(1, 2, 1)|} = \frac{120}{20} = 6.$$

(iii) $Orb(1, 1, 2) = \{(\sigma(1), \sigma(1), \sigma(2)) \mid \sigma \in \mathbb{S}_5\} = \{(x, x, y) \mid x, y \in X, x \neq y\}$. Inoltre

$$|Stab(1, 1, 2)| = \frac{|\mathbb{S}_5|}{|Orb(1, 1, 2)|} = \frac{120}{20} = 6.$$

(iv) In modo analogo $Orb(2,1,1) = \{(x,y,y) \mid x,y \in X, x \neq y\}$. Inoltre

$$|Stab(2,1,1)| = \frac{|\mathbb{S}_5|}{|Orb(2,1,1)|} = \frac{120}{20} = 6.$$

(v) Infine $Orb(1,2,3) = \{(\sigma(1),\sigma(2),\sigma(3)) \mid \sigma \in \mathbb{S}_5\} = \{(x,y,z) \mid x,y,z \in X, x \neq y, x \neq z, y \neq z\}$. Inoltre

$$|Stab(1,2,3)| = \frac{|\mathbb{S}_5|}{|Orb(1,2,3)|} = \frac{120}{60} = 2.$$

In effetti $Stab(1,2,3) = \{(1),(45)\}$.

Si osserva che quelle trovate sono tutte le orbite dell'azione in quanto esse costituiscono una partizione dell'insieme X^3.

Esercizio 1.9: prova d'esame del 14/04/2021 - n° 2

Dati H, K sottogruppi di un gruppo G, definiamo l'insieme

$$X = \{hk \,|\, h \in H \text{ e } k \in K\} \subseteq G\,.$$

Verificare che la legge $(h,k) * x = hxk^{-1}$ (per $h \in H$, $k \in K$ e $x \in X$) definisce un'azione $*$ transitiva del gruppo $H \times K$ sull'insieme X.

Soluzione. Dimostriamo che $*$ definisce un'azione.

(a) $1_{H\times K} * x = (1_G, 1_G) * x = 1_G x 1_G^{-1} = x$, per ogni $x \in X$;

(b) $(h',k')*[(h,k)*x] = (h',k')*(hxk^{-1}) = h'(hxk^{-1})k'^{-1} = (h'h)x(k'k)^{-1} = (h'h,k'k) * x = [(h',k')(h,k)] * x$, per ogni $(h,k),(h',k') \in H \times K$ e per ogni $x \in X$.

Inoltre l'azione è transitiva perché, per ogni $x \in X$, $x = hk$ con $h \in H$ e $k \in K$. Dunque

$$x = hk = h1_G(k^{-1})^{-1} = (h,k^{-1}) * 1_G,$$

così $X = Orb(1_G)$.

Esercizio 1.10: prova d'esame del 9/06/2021 - n° 2

Dato il gruppo $G = GL_3(\mathbb{Z}_2)$ delle matrici invertibili a coefficienti in nel campo $\mathbb{Z}_2$, si consideri l'azione di G sull'insieme di vettori colonna $X = \mathbb{Z}_2^3$ data dalla moltiplicazione di matrici.

(i) Dimostrare che l'orbita di $\underline{v} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ è l'insieme $X \setminus \{0\}$.

(ii) Determinare l'ordine dello stabilizzatore di $\underline{v}$ e descriverne la struttura.

Soluzione.

(i) Sia $A \in GL_3(\mathbb{Z}_2)$. Allora $A \cdot \underline{v} = A^1$, dove A^1 indica la prima colonna della matrice A. Poiché A è invertibile, A^1 può essere qualunque vettore di X, tranne il vettore nullo. Dunque l'orbita del vettore $\underline{v}$ è proprio $X \setminus \{0\}$.

(ii) Dal Teorema Orbita-Stabilizzatore si deduce che

$$|Stab(\underline{v})| = \frac{|G|}{|Orb(\underline{v})|}.$$

Per determinare la cardinalità di G ragioniamo nel seguente modo: la prima colonna di una generica matrice di G può essere scelta in modo arbitrario a meno di escludere la colonna nulla, ovvero può variare in $2^3-1 = 7$ modi. Fissata la prima colonna, la seconda non deve essere un multiplo della prima e quindi può essere scelta in $2^3-2 = 6$ modi. Infine l'ultima colonna non deve essere una combinazione lineare delle prime due e quindi può variare in $2^3 - 2^2 = 4$ modi. Così $|G| = 7 \cdot 6 \cdot 4 = 168$ e dunque l'ordine dello stabilizzatore di $\underline{v}$ è

$$|Stab(\underline{v})| = \frac{168}{7} = 24.$$

Infine è facile verificare che $Stab(\underline{v})$ consiste di tutte le matrici invertibili di $GL_3(\mathbb{Z}_2)$ tali che la prima colonna è proprio il vettore $\underline{v}$.

Esercizio 1.11: prova d'esame del 12/07/2021 - n° 1

Sia dato l'insieme $V = \{(x_1, x_2, x_3) \in (\mathbb{F}_5)^3 \mid x_1 + x_2 + x_3 = 0\}$.

(i) Calcolare la cardinalità di V.

(ii) Verificare che la legge $*\colon S_3 \times V \to V$ data da

$$\sigma * (x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

definisce un'azione del gruppo simmetrico S_3 su V.

(iii) Determinare le orbite di tale azione.

Soluzione.

(i) V è un sottospazio vettoriale di dimensione 2 di $(\mathbb{F}_5)^3$, dunque ha cardinalità $5^2 = 25$.

(ii) Per ogni $(x_1, x_2, x_3) \in V$ si ha

$$id_{S_3} * (x_1, x_2, x_3) = (x_{id(1)}, x_{id(2)}, x_{id(3)}) = (x_1, x_2, x_3).$$

Inoltre, per ogni $\sigma, \tau \in S_3$ e per ogni $(x_1, x_2, x_3) \in V$ si ha

$$\sigma * (\tau * (x_1, x_2, x_3)) = \sigma * (x_{\tau^{-1}(1)}, x_{\tau^{-1}(2)}, x_{\tau^{-1}(3)}) = \sigma * (y_1, y_2, y_3) =$$

(dove $y_i = x_{\tau^{-1}(i)}$, per ogni $i = 1, 2, 3$)

$$= (y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}, y_{\sigma^{-1}(3)}) = (x_{\tau^{-1}(\sigma^{-1}(1))}, x_{\tau^{-1}(\sigma^{-1}(2))}, x_{\tau^{-1}(\sigma^{-1}(1))}) =$$

$$= (x_{(\sigma\circ\tau)^{-1}(1)}, x_{(\sigma\circ\tau)^{-1}(2)}, x_{(\sigma\circ\tau)^{-1}(3)}) = (\sigma \circ \tau) * (x_1, x_2, x_3).$$

(iii) Ricordando che, per ogni $(x_1, x_2, x_3) \in V$,

$$Orb(x_1, x_2, x_3) = \{\sigma * (x_1, x_2, x_3) \mid \sigma \in S_3\},$$

si ha

- $Orb(0, 0, 0) = \{(0, 0, 0)\}$;
- $Orb(0, 1, 4) = \{(0, 1, 4), (1, 0, 4), (4, 1, 0), (0, 4, 1), (1, 4, 0), (4, 0, 1)\}$;
- $Orb(0, 2, 3) = \{(0, 2, 3), (2, 0, 3), (3, 2, 0), (0, 3, 2), (2, 3, 0), (3, 0, 2)\}$;
- $Orb(1, 1, 3) = \{(1, 1, 3), (1, 3, 1), (3, 1, 1)\}$;
- $Orb(1, 2, 2) = \{(1, 2, 2), (2, 2, 1), (2, 1, 2)\}$;
- $Orb(4, 4, 2) = \{(4, 4, 2), (4, 2, 4), (2, 4, 4)\}$;
- $Orb(4, 3, 3) = \{(4, 3, 3), (3, 4, 3), (3, 3, 4)\}$.

1.3 Teoremi di Sylow e applicazioni

Esercizio 1.12: prova d'esame del 16/09/2020 - n° 1

Sia p un numero primo, $\mathbb{F}_p$ il campo con p elementi, e $\Gamma = GL_2(\mathbb{F}_p)$ il gruppo delle matrici invertibili 2×2 a valori in $\mathbb{F}_p$.

(i) Dimostrare che l'ordine di Γ è $(p^2-1)(p^2-p)$.

(ii) Dedurre che i p-sottogruppi di Sylow di Γ sono $p+1$.

Soluzione.

(i) Sia $\alpha \in \Gamma$, allora $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $a, b, c, d \in \mathbb{F}_p$ tali che $ad - bc \neq 0$. Quante sono le possibili matrici che soddisfano questa condizione? Procediamo in questo modo: per la prima riga possiamo scegliere a e b in $\mathbb{F}_p$ con la condizione che non siano entrambi nulli, quindi abbiamo p^2-1 scelte; per la seconda riga possiamo scegliere c e d con la condizione che la seconda riga non sia un multiplo della prima, quindi abbiamo $p^2 - p$ scelte. In conclusione, in Γ ci sono esattamente $(p^2-1)(p^2-p)$ matrici.

(ii) Poiché $(p^2-1)(p^2-p) = p(p+1)(p-1)^2$, è chiaro che l'ordine dei p-sottogruppi di Sylow è p. Di conseguenza, il sottogruppo $P \leq \Gamma$ generato dalla matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, i.e.

$$P = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{t.c.} \quad x \in \mathbb{F}_p \right\}$$

è un p-sottogruppo di Sylow di Γ. Essendo i p-sottogruppi di Sylow tutti coniugati fra loro, si ha che il loro numero è precisamente $n_p = [\Gamma : N_\Gamma(P)]$. Possiamo allora calcolare il normalizzante $N_\Gamma(P)$.

Sia α definita come al punto (i). Si ha che $\alpha \in N_\Gamma(P)$ se e solo se coniuga $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ con un'altra matrice di P. Si può calcolare

$$\alpha \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \alpha^{-1} = \frac{1}{ad-bc} \begin{pmatrix} ad - bc - ac & a^2 \\ -c^2 & ad - bc + ac \end{pmatrix}.$$

Concludiamo che $\alpha \in N_\Gamma(P)$ se e solo se $c = 0$. Di conseguenza, si ha $|N_\Gamma(P)| = p(p-1)^2$, e quindi $n_p = p+1$.

Esercizio 1.13: prova d'esame del 20/01/2021 - n° 2

Determinare il numero degli elementi di ordine 7 in un gruppo semplice di ordine 168.

Soluzione. Sia $|G| = 168 = 2^3 \cdot 3 \cdot 7$. I 7-sottogruppi di Sylow di |G| sono sottogruppi ciclici di ordine 7: ognuno di essi contiene esattamente 6 elementi di periodo 7 più l'identità. Detto n_7 il numero di 7-sottogruppi di Sylow, si ha

$$n_7 \equiv 1 \pmod 7 \qquad \text{e} \qquad n_7 | 24\,,$$

da cui si ricava $n_7 \in \{1, 8\}$. Ora, poiché G è un gruppo semplice, $n_7 \neq 1$ (altrimenti l'unico 7-Sylow sarebbe normale), e quindi $n_7 = 8$. Per il teorema di Lagrange, due 7-sottogruppi di Sylow distinti hanno intersezione banale; d'altro canto, tutti gli elementi di periodo 7 appartengono a qualche 7-sottogruppo di Sylow. In conclusione, calcoliamo $6 \cdot 8 = 48$ elementi di periodo 7 in G.

Esercizio 1.14: prova d'esame del 3/02/2021 - n° 1

Si consideri il gruppo moltiplicativo delle matrici:

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \ : \ a \in \mathbb{Z}_7,\ b \in \{1, 2, 4\} \right\}$$

(i) Determinare gli elementi di ordine 7 e di ordine 3 di G.

(ii) Descrivere esplicitamente i sottogruppi di Sylow di G.

Soluzione.

(i) Si osserva che $|G| = 21$. Per induzione su $n \in \mathbb{N}$ si dimostra che

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} 1 & a + ab + ab^2 + \ldots + ab^{n-1} \\ 0 & b^n \end{pmatrix}$$

In particolare

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^3 = \begin{pmatrix} 1 & a(1 + b + b^2) \\ 0 & b^3 \end{pmatrix},$$

così gli elementi di periodo 3 di G sono tutte e sole le matrici con $b \in \{2, 4\}$ e $a \in \mathbb{Z}_7$. In modo analogo si ottiene che

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^7 = \begin{pmatrix} 1 & a + ab + ab^2 + ab^3 + ab^4 + ab^5 + ab^6 \\ 0 & b \end{pmatrix},$$

così gli elementi di periodo 7 di G sono le matrici con $b = 1$ e $a \neq 0$. Si osserva che in questo modo abbiamo ottenuto tutte la matrici di G (ad esclusione delle matrice identità), dunque non esiste nessun elemento di G di periodo 21, ovvero G non è ciclico.

(ii) Dal terzo Teorema di Sylow si ricava che $n_7 \equiv 1 \ (mod \ 7)$ e $n_7|3$, dunque $n_7 = 1$. Allora esiste un unico 7-sottogruppo di Sylow di G di cardinalità 7 ed esso sarà formato dalle matrici

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

ovvero dall'unità e da tutti e soli gli elementi di periodo 7 di G.
Inoltre si ricava che $n_3 \equiv 1 \ (mod \ 7)$ e $n_3|7$, dunque $n_3 = 1$ oppure $n_3 = 7$. Sicuramente $n_3 \neq 1$, perchè in G ci sono 14 elementi di periodo 3, così esistono sette 3-sottogruppi di Sylow di G a due a due distinti e ciascuno essi sarà formato dall'unità e da due matrici di periodo 3 di G. In particolare, in ogni 3-sottogruppo di Sylow di G troveremo una matrice con $b = 2$ e una matrice con $b = 4$.

Esercizio 1.15: prova d'esame del 17/02/2021 - n° 1

Provare che un gruppo di ordine 300 non è semplice.

Soluzione. Sia G un gruppo di ordine $300 = 2^2 \cdot 3 \cdot 5^2$. Allora il numero di 5-sottogruppi di Sylow di G è tale che

$$n_5 \equiv 1 \ (mod \ 5) \ \ e \ \ n_5|12$$

Dunque $n_5 \in \{1, 6\}$. Se $n_5 = 1$, allora esiste un unico 5-sottogruppo di Sylow di G e quindi G non è semplice. Suppongo invece che $n_5 = 6$ e considero l'azione di coniugio del gruppo G sull'insieme X dei suoi sei 5-sottogruppi di Sylow. Tale azione è equivalente ad un omomorfismo di gruppi

$$\varphi : G \to Sym(X),$$

con $|Sym(X)| = 6!$. Chiaramente φ non è un monomorfismo, perché $|G| = 300$ non divide $6!$. D'altro canto φ non è l'omomorfismo banale, perché altrimenti per ogni $P \in X$ e per ogni $g \in G$ si avrebbe $gPg^{-1} = P$, il che non può essere perché P non è un sottogruppo normale di G. Allora $Ker(\varphi)$ è un sottogruppo normale proprio di G e, dunque, G non è un gruppo semplice.

Esercizio 1.16: prova d'esame del 14/04/2021 - n° 1

Dimostrare che i 2-sottogruppi di Sylow del gruppo di permutazioni $\mathbb{S}_6$ sono tutti isomorfi a $\mathbb{D}_4 \times \mathbb{Z}_2$, e determinarne il numero.

Soluzione. Si osserva subito che $|\mathbb{S}_6| = 6! = 2^4 \cdot 3^2 \cdot 5$. Per dimostrare che tutti i 2-sottogruppi di Sylow di $\mathbb{S}_6$ sono isomorfi a $\mathbb{D}_4 \times \mathbb{Z}_2$ è sufficiente osservare che $\mathbb{S}_6$ contiene i sottogruppi

$$H = \langle (1234), (12)(34) \rangle \cong \mathbb{D}_4,$$

$$K = \langle (56) \rangle \cong \mathbb{Z}_2.$$

Risulta che

(a) il generatore di K commuta con i generatori di H, così $HK = KH$ e $HK \leq G$;

(b) $H \cap K = \{(1)\}$, così $|HK| = |H||K| = 8 \cdot 2 = 16$ e $HK \cong H \times K \cong \mathbb{D}_4 \times \mathbb{Z}_2$;

(c) $H \times K$ è un 2-sottogruppo di Sylow di $\mathbb{S}_6$.

Dunque tutti i 2-sottogruppi di Sylow di $\mathbb{S}_6$ sono isomorfi a $\mathbb{D}_4 \times \mathbb{Z}_2$. Infine il numero n_2 di tali sottogruppi si ottiene moltiplicando il numero di modi di scegliere 4 elementi tra 6 per il numero di immersioni non isomorfe del gruppo $\mathbb{D}_4$ in $\mathbb{S}_6$, ovvero

$$n_2 = \binom{6}{4} \cdot 3 = 45.$$

In effetti $45 \equiv 1 \ (mod\ 2)$ e $45 \left| \frac{6!}{2^4} = 45. \right.$

Esercizio 1.17: prova d'esame del 9/06/2021 - n° 1

Sia p un numero primo. Dimostrare che, per $n > 1$, un gruppo di ordine $p^n(p+1)$ non può essere semplice.

Soluzione. Sia $n > 1$ e supponiamo per assurdo che un gruppo G di ordine $p^n(p+1)$ sia semplice. Allora, dal terzo Teorema di Sylow, si deduce che il numero n_p di p-sottogruppi di Sylow di G è $p+1$. L'azione di coniugio di G sull'insieme dei suoi p-sottogruppi di Sylow produce un omomorfismo di gruppi $f : G \to S_{p+1}$. Studiamo il nucleo di f. Se fosse $\mathsf{Ker}(f) = G$, per la transitività dell'azione, G avrebbe un unico p-sottogruppo di Sylow: contraddizione.

Se invece fosse $\mathsf{Ker}(f) = 1$, allora f sarebbe un monomorfismo, e si otterrebbe nuovamente una contraddizione, in quanto $|f(G)| = |G| = p^n(p+1)$ non divide $(p+1)!$ per $n > 1$. In conclusione, $\mathsf{Ker}(f)$ è un sottogruppo normale proprio di G, che quindi non è semplice.

Esercizio 1.18: prova d'esame del 28/06/2021 - n° 1

Sia G un gruppo finito, e p un primo che divide $|G|$. Detta N l'intersezione dei p-sottogruppi di Sylow di G, dimostrare che:
(i) N è un p-sottogruppo normale di G;
(ii) se K è un p-sottogruppo normale di G, allora $K \leq N$.

Soluzione. Sia $|G| = p^k m$, con $(p, m) = 1$ e sia P un p-sottogruppo di Sylow di G. Allora

$$N = \bigcap_{g \in G} gPg^{-1}.$$

(i) Per ogni $x \in G$ si ha che

$$xNx^{-1} = \bigcap_{g \in G} (xg)P(xg)^{-1} = N,$$

dunque N è un sottogruppo normale di G.

(ii) Sia K un p-sottogruppo normale di G. Allora K è contenuto in un p-sottogruppo di Sylow di G e, per ogni $x \in G$, si ha che $xKx^{-1} = K$. Così K è contenuto in tutti i p-sottogruppi di Sylow di G e, dunque, $K \subseteq N$.

Esercizio 1.19: prova d'esame del 15/09/2021 - n° 1

Delle due proposizioni scritte sotto, solo una è vera. Dimostrare l'affermazione vera e portare un controesempio per quella falsa.

(i) Presi due sottogruppi di S_6 di ordine 4, essi sono isomorfi.

(ii) Presi due sottogruppi di S_6 di ordine 9, essi sono isomorfi.

Soluzione. L'affermazione (i) è falsa. Infatti, in S_6 il sottogruppo $\langle(1234)\rangle$ è ciclico di ordine 4, mentre, per esempio, $\langle(12), (34)\rangle$ è isomorfo al gruppo di Klein.

L'affermazione (ii) è vera. Infatti, poiché

$$S_6 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 2^4 \cdot 3^2 \cdot 5$$

ogni sottogruppo di ordine 9 è un 3-sottogruppo di Sylow, ed essi sono tutti coniugati fra loro (per Sylow II) e a fortiori isomorfi.

Esercizio 1.20: prova d'esame del 15/09/2021 - n° 2

Sia G un gruppo semplice di ordine 168, e sia H un sottogruppo di G tale che $|H|$ è multiplo di 7.

(i) Calcolare il numero di elementi di G di periodo 7.

(ii) Dopo aver verificato che H contiene un 7-sottogruppo di Sylow P, determinare l'ordine del normalizzante $N_G(P)$. Infine dedurre che non può essere $|H| = 14$.

Soluzione.

(i) Scriviamo $168 = 2^3 \cdot 3 \cdot 7$. Per il terzo Teorema di Sylow, si ha che il numero dei 7-sottogruppi di Sylow è

$$n_7 \equiv 1 \mod 7 \qquad n_7 \mid 24$$

Dalla semplicità di G, deduciamo $n_7 \neq 1$, per cui necessariamente $n_7 = 8$. Per il teorema di Lagrange, gli otto sottogruppi di Sylow hanno intersezione banale. Inoltre, essendo ciclici, contengono ciascuno sei elementi di ordine 7. Infine, ovviamente ogni elemento di ordine 7 di G appartiene a un qualche 7-sottogruppo di Sylow. Di conseguenza, abbiamo $6 \cdot 8 = 48$ elementi di ordine 7 in G.

(ii) Per il teorema di Cauchy, H contiene un sottogruppo P di ordine 7, che è necessariamente un 7-sottogruppo di Sylow di G. Ricordiamo ora che l'indice del normalizzante di P in G è pari alla cardinalità dell'orbita di P per l'azione di coniugo, i.e. (per Sylow II) proprio il numero n_7 dei sottogruppi di Sylow coniugati a P; da questo si deduce immediatamente $|N_G(P)| = 21$. Infine, se fosse $|H| = 14$ si avrebbe $[H : P] = 2$, da cui P normale in H. Ma allora, $H \leq N_G(P)$, e per il teorema di Lagrange, questa è una contraddizione, perché 14 non divide 21.

1.4 Gruppi abeliani finiti

Esercizio 1.21: prova d'esame del 12/07/2021 - n° 4

Classificare, a meno di isomorfismi, il gruppo abeliano degli elementi invertibili dell'anello $\mathbb{Z}_{32}$.

Soluzione. Il gruppo degli elementi invertibili dell'anello $\mathbb{Z}_{32}$ è un gruppo abeliano di ordine $\varphi(32) = 16$

$$\mathcal{U}(\mathbb{Z}_{32}) = \{[1], [3], [5], [7], [9], [11], [13], [15], [17], [19], [21], [23], [25], [27], [29], [31]\}.$$

Esso contiene un sottogruppo ciclico di ordine 2 ed un sottogruppo ciclico di ordine 8 ad intersezione banale:

$$H = \langle [31] \rangle = \{[1], [31]\},$$

$$K = \langle [3] \rangle = \{[1], [3], [9], [27], [17], [19], [25], [11]\}.$$

K è un sottogruppo normale, in quanto ha indice 2 in $\mathcal{U}(\mathbb{Z}_{32})$. Dunque possiamo concludere che

$$\mathcal{U}(\mathbb{Z}_{32}) = HK \cong \mathbb{Z}_2 \times \mathbb{Z}_8.$$

Capitolo 2

Teoria dei campi

2.1 Estensioni di campi

Esercizio 2.1: Seconda Prova Parziale del 22/01/2021 - n° 2

Dimostrare che la mappa

$$\Phi\colon \quad a+b\sqrt{2} \quad \mapsto \quad a-\sqrt{2}$$

con $a, b \in \mathbb{Q}$, definisce un isomorfismo di campi $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$.

Soluzione. Per prima cosa, è necessario dimostrare che Φ definisce un omomorfismo di anelli unitari. Infatti, Φ preserva la somma:

$$\begin{aligned}\Phi(a+b\sqrt{2})+\Phi(c+d\sqrt{2}) &= a-b\sqrt{2}+c-d\sqrt{2}\\ &= a+c-(b+d)\sqrt{2}\\ &= \Phi\left((a+c)+(b+d)\sqrt{2}\right)\\ &= \Phi\left((a+b\sqrt{2})+(c+d\sqrt{2})\right),\end{aligned}$$

preserva il prodotto:

$$\begin{aligned}\Phi(a+b\sqrt{2})\cdot\Phi(c+d\sqrt{2}) &= (a-b\sqrt{2})\cdot(c-d\sqrt{2})\\ &= ac+2bd-(ac+bd)\sqrt{2}\\ &= \Phi\left(ac+2bd+(ac+bd)\sqrt{2}\right)\\ &= \Phi\left((a+b\sqrt{2})\cdot(c+d\sqrt{2})\right)\end{aligned}$$

e preserva banalmente anche l'unità. Poiché $\mathbb{Q}(\sqrt{2})$ è un campo, si vede subito che l'ideale $\ker(\Phi) = (0)$, quindi Φ è iniettiva. Infine, tale mappa è

suriettiva, perché, per ogni $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, si ha

$$\Phi(a - b\sqrt{2}) = a + b\sqrt{2}\,.$$

Sia ora Ψ un generico automorfismo del campo $\mathbb{Q}(\sqrt{2})$. Ovviamente, $\Psi(1) = 1$ per definizione, e infatti ogni Ψ fissa il sottocampo primo $\mathbb{Q}$. Poiché Φ preserva il prodotto, valgono le uguaglianze

$$(\Psi(\sqrt{2}))^2 = \Psi(\sqrt{2}) \cdot \Psi(\sqrt{2}) = \Psi(\sqrt{2} \cdot \sqrt{2}) = \Phi(2) = 2$$

da cui otteniamo $\Psi(\sqrt{2}) = \pm\sqrt{2}$. Ora, Ψ, visto come applicazione lineare tra spazi vettoriali su $\mathbb{Q}$, è determinato dai valori che assume sulla base $\{1, \sqrt{2}\}$. In conclusione, se $\Psi(\sqrt{2}) = \sqrt{2}$, allora $\Psi = Id$, se invece $\Psi(\sqrt{2}) = -\sqrt{2}$, allora $\Psi = \Phi$.

Esercizio 2.2: prova d'esame del 3/02/2021 - n° 4

Data l'estensione di campi $F \to E$, sia $p(x) \in F[x]$ un polinomio non costante. Dimostrare che se $\alpha \in E$ è trascendente su F, allora anche $p(\alpha)$ è trascendente su F.

Soluzione. Se per assurdo $p(\alpha) \in E$ fosse un elemento trascendente su F, allora esisterebbe un polinomio $f(x) \in F[x]$ tale che $f(p(\alpha)) = 0$. In tal modo α sarebbe radice del polinomio $(f \circ p)(x) \in F[x]$, e ciò è un assurdo in quanto $\alpha \in E$ è trascendente su F.

Esercizio 2.3: prova d'esame del 17/02/2021 - n° 4

Determinare il massimo comune divisore dei polinomi

$$p(x) = x^4 + 3x^3 + 2x^2 + 4 \quad \text{e} \quad q(x) = x^2 + 3x + 2$$

nell'anello di polinomi $\mathbb{Z}_5[x]$.

Soluzione. Dividendo il polinomio $p(x)$ per il polinomio $q(x)$ si ottiene che

$$p(x) = q(x)x^2 - 1$$

Dunque

$$1 = -p(x) + x^2 q(x)$$

è un'identità di Bézout per i polinomi $p(x)$ e $q(x)$. Ne segue che

$$MCD(p(x), q(x)) = 1.$$

In alternativa, si osserva che $q(x) = (x+2)(x+1)$ e le sue radici 3 e 4 non sono radici del polinomio $p(x)$, dunque

$$MCD(p(x), q(x)) = 1.$$

Esercizio 2.4: prova d'esame del 9/06/2021 - n° 3

Data una estensione di campi $F \to E$ di grado finito, sia $f(x) \in F[x]$ un polinomio di grado p primo, irriducibile su F. Dimostrare che se $f(x)$ è riducibile su E, allora p divide il grado $[E : F]$.
Vale il viceversa?

Soluzione. Sia α una radice di $f(x)$. Allora $[F(\alpha) : F] = deg(f(x)) = p$, in quanto $f(x)$ è irriducibile su F, e $[E(\alpha) : E] < p$, poiché $f(x)$ è riducibile su E. Inoltre

$$[E(\alpha) : F] = [E(\alpha) : F(\alpha)][F(\alpha) : F] = p[E(\alpha) : F(\alpha)],$$

$$[E(\alpha) : F] = [E(\alpha) : E][E : F].$$

Così il numero primo p divide il prodotto $[E(\alpha) : E][E : F]$ e, poiché p non divide $[E(\alpha) : E]$, si conclude che p divide il grado $[E : F]$.

Esercizio 2.5: prova d'esame del 9/06/2021 - n° 4

Sia I l'ideale generato dal polinomio x^4+x^3+x+3 in $\mathbb{Z}_5[x]$. Verificare se l'anello quoziente $\mathbb{Z}_5[x]/I$ sia un campo.

Soluzione. Si verifica facilmente che il polinomio $f(x) = x^4+x^3+x+3$ non ha radici sul campo $\mathbb{Z}_5$. Allora supponiamo che $f(x)$ si spezzi nel prodotto di due fattori di secondo grado

$$f(x) = (x^2 + ax + b)(x^2 + Ax + B),$$

oppure

$$f(x) = (2x^2 + ax + b)(3x^2 + Ax + B).$$

Di seguito si analizzerà solamente il primo caso, dal quale si ottiene il sistema

$$\begin{cases} a + A = 1 \\ B + b + aA = 0 \\ aB + bA = 1 \\ bB = 3 \end{cases}$$

Dalla quarta equazione si trova che $(b, B) = (1, 3)$ oppure $(b, B) = (4, 2)$ (le altre due possibilità sono speculari). Nel primo caso si raggiunge un assurdo in quanto le prime due equazioni si riducono a

$$\begin{cases} a + A = 1 \\ aA = 1 \end{cases}$$

e non si hanno soluzioni in $\mathbb{Z}_5$. Nel secondo caso il sistema si riduce a

$$\begin{cases} a + A = 1 \\ aA = -1 \\ 2a + 4b = 1 \end{cases}$$

Le prime due equazioni sono soddisfatte solo per la coppia $(a, A) = (3, 3)$, ma sostituendo tale risultato nella terza equazione si ottiene

$$2 \cdot 3 + 4 \cdot 3 = 1 + 2 = 3 \neq 1.$$

L'altro caso si risolve in modo analogo e si conclude che l'anello quoziente $\mathbb{Z}_5[x]/I$ è un campo, in quanto il polinomio $f(x) = x^4+x^3+x+3$ è irriducibile su $\mathbb{Z}_5$.

Esercizio 2.6: prova d'esame del 28/06/2021 - n° 4

In un campo F di caratteristica 5, consideriamo un elemento α che non ammetta radice quinta in F, i.e. tale che non esista $a \in F$, $a^5 = \alpha$. Dimostrare che il polinomio $f(x) = x^5 - \alpha$ è irriducibile in $F[x]$.

Soluzione. Il polinomio $f(x) = x^5 - \alpha$ non ammette radici sul campo F in quanto non esiste la radice quinta di α in F. Supponiamo allora che $f(x)$ si spezzi nel prodotto di un fattore di secondo grado e di un fattore di terzo grado

$$f(x) = p(x) \cdot q(x).$$

I metodo

Se a è radice di $p(x)$, a è anche radice di $x^5 - \alpha$. Per Forbenius, $x^5 - \alpha = x^5 - a^5 = (x - a)^5$, da cui $p(x) = x^2 - 2ax + a^3$. Concludiamo $-2a \in F \Rightarrow a \in F$, contraddizione.

II metodo

Senza perdere in generalità, analizziamo solo il caso in cui entrambi i fattori siano monici:

$$p(x) = x^2 + ax + b \qquad q(x) = x^3 + cx^2 + dx + e.$$

Moltiplicando e confrontando i coefficienti, otteniamo il sistema di equazioni:

$$\begin{cases} a + c = 0 \\ b + ac + d = 0 \\ bc + ad + e = 0 \\ bd + ae = 0 \\ be = \alpha \end{cases}$$

Risolvendo il sistema dall'alto verso il basso per sostituzione si ottiene

$$\begin{cases} c = -a \\ d = a^2 - b \\ e = -a^3 + 2ab \\ b^2 + 2ab + a^4 = (b + a^2)^2 = 0 \\ be = \alpha \end{cases}$$

e dunque

$$\begin{cases} b = -a^2 \\ e = -a^3 - 2a^3 = -3a^3 = 2a^3 \end{cases}$$

Infine, sostituendo nella quinta ed ultima equazione, si ottiene

$$be = (-a^2)(2a^3) = 3a^5 = (3a)^5 = \alpha$$

e tale equazione non ha soluzione perché non esiste in F la radice quinta di α. Dunque il polinomio $f(x) = x^5 - \alpha$ è irriducibile sul campo F.

Esercizio 2.7: prova d'esame del 12/07/2021 - n° 3

Sia K un campo con caratteristica $p > 0$. Dimostrare che l'insieme $K' = \{\alpha^p \mid \alpha \in K\}$ è un sottocampo di K.

Soluzione. K' è un sottocampo di K in quanto è l'immagine dell'endomorfismo di Frobenius $F : K \to K$, definito da $F(\alpha) = \alpha^p$, per ogni $\alpha \in K$. Si osserva che, se K è un campo finito, allora F è un automorfismo e $K' = K$.

Esercizio 2.8: prova d'esame del 15/09/2021 - n° 4

Sia $\omega = e^{2\pi i/3} \in \mathbb{C}$ e A l'anello $\mathbb{Z}[\omega]$, i.e. il sottoanello di $\mathbb{C}$ generato da ω. Sia infine $(2) \subset A$ l'ideale principale di $2 \in A$. Dimostrare che l'anello quoziente $A/(2)$ è un campo finito. Quale?

Soluzione. Il sottoanello di $\mathbb{C}$ generato da ω può essere descritto come insieme di coppie di interi:

$$A = \mathbb{Z}[\omega] = \{a + b\omega \,|\, a, b \in \mathbb{Z} \text{ e } \omega^2 = -\omega - 1\}$$

Ora, poiché l'ideale principale generato da $2 \in A$ è dato dall'insieme $\{2k + 2h\omega \,|\, k, h \in \mathbb{Z}\}$, si verifica subito che le classi dell'anello quoziente $A/(2)$ sono univocamente determinati dalla parità di a e b nell'espressione $a + b\omega$, e possono quindi essere rappresentati dagli elementi 0, 1, ω e $1 + \omega$. Contempliamo la tavola di moltiplicazione:

$\cdot$	1	ω	$1+\omega$
1	1	ω	$1+\omega$
ω	ω	$1+\omega$	1
$1+\omega$	$1+\omega$	1	ω

Si vede che ogni elemento diverso da zero ammette inverso, pertanto trattasi di un campo. Per il teorema di classificazione dei campi finiti, il campo in questione è $\mathbb{F}_4$.

Una soluzione alternativa usa le proprietà astratte dell'anello A. Esso, infatti, può essere descritto dalla proprietà universale dell'anello di polinomi $\mathbb{Z}[x]$, come quoziente $\mathbb{Z}[x]/(x^2+x+1)$. Allora si hanno i seguenti isomorfismi canonici di anelli unitari:

$$A/(2) \cong \frac{\mathbb{Z}[x]/(x^2+x+1)}{(2)} \cong \frac{\mathbb{Z}[x]}{(x^2+x+1, 2)}$$

$$\cong \frac{\mathbb{Z}[x]/(2)}{(x^2+x+1)} = \frac{\mathbb{F}_2[x]}{(x^2+x+1)} \cong \mathbb{F}_4$$

2.2 Estensioni algebriche semplici e polinomio minimo di un elemento algebrico

Esercizio 2.9: prova d'esame del 16/09/2020 - n° 3

Dato il polinomio $p(x) = x^5 - 3$ a coefficienti razionali, dimostrare che esso ammette cinque radici distinte $\theta_1, \theta_2, \ldots, \theta_5 \in \mathbb{C}$, e che i campi $\mathbb{Q}(\theta_1), \mathbb{Q}(\theta_2), \ldots, \mathbb{Q}(\theta_5)$ sono distinti a due a due.

Soluzione. Il polinomio $p(x) = x^3 - 5$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstain, con $p = 3$ ed ammette radici multiple per il criterio di separabilità.

Per $i = 1, \dots, 5$ definiamo $F_i = \mathbb{Q}(\theta_i)$. Delle cinque radici, una, e una sola (diciamo θ_1), è reale, per cui F_1 è un sottocampo dei reali, e di conseguenza $F_1 \neq F_i$, per $i = 2, \dots, 5$. Per dimostrare ora che i restanti quattro campi $F_2, \dots, F_5$ sono diversi tra loro, assumiamo che $F_i = F_j$ con $2 \leq i, j \leq 5$. Sia σ un isomorfismo $F_i \to F_1$ tale che $\sigma(\theta_i) = \theta_1$ (un tale isomorfismo esiste, come ampiamente discusso a lezione). Poiché abbiamo assunto $F_i = F_j$, si ha che $\theta_j \in F_i$, e inoltre:

$$p(\sigma(\theta_j)) = \sigma(p(\theta_j)) = \sigma(0) = 0\,.$$

Quindi, $\sigma(\theta_j)$ è una radice *reale* di $p(x)$, e per quanto ricordato sopra, $\sigma(\theta_j) = \theta_1$. Tuttavia, anche $\sigma(\theta_i) = \theta_1$. Essendo σ iniettiva, questo implica $\theta_i = \theta_j$.

Esercizio 2.10: prova d'esame del 16/09/2020 - n° 4

Verificare se il polinomio $q(x) = x^2 - \sqrt{2}$ sia riducibile su $\mathbb{Q}(\sqrt{2})$.

Soluzione. Essendo di secondo grado, il polinomio $q(x)$ è riducibile su $\mathbb{Q}(\sqrt{2})$ se e solo se ammette una radice, i.e. se e solo se esistono $a, b \in \mathbb{Q}$ tali che $(a + b\sqrt{2})^2 = \sqrt{2}$. Si ottiene il sistema:

$$\begin{cases} a^2 + 2b^2 = 0 \\ 2ab = 1 \end{cases}$$

che non ammette soluzioni razionali.

Esercizio 2.11: prova d'esame del 20/01/2021 - n° 3

Si consideri il polinomio $p(x) = x^4 + 3x + 3$.

(i) Verificare che $p(x)$ è un polinomio irriducibile su $\mathbb{Q}$.

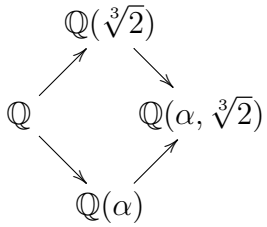
(ii) Calcolare il grado dell'estensione $\mathbb{Q} \hookrightarrow \mathbb{Q}(\alpha)$, dove α è una radice di $p(x)$.

(iii) Dedurre che $p(x)$ è irriducibile su $\mathbb{Q}(\alpha)$.

Soluzione.

(i) Il polinomio $p(x)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein con $p = 3$.

(ii) Si consideri il diagramma commutativo di estensioni di campi



Essendo $p(x)$ irriducibile su $\mathbb{Q}$, si ha che $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. D'altro canto, anche $x^3 - 2$ è irriducibile su $\mathbb{Q}$, e $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Per la legge dei gradi si ha:

$$4 \cdot 3 = 12 \mid [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] .$$

Ora, poiché $p(\alpha) = 0$, detto $m(x)$ il polinomio minimo di α su $\mathbb{Q}(\sqrt[3]{2})$, si ha che $m(x) \mid p(x)$. Dunque, $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \leq 4$,

$$[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \cdot 3 \leq 4 \cdot 3 = 12.$$

In conclusione, otteniamo $[\mathbb{Q}(\alpha, \sqrt[3]{2}) : \mathbb{Q}] = 12$.

(iii) Infine, dal punto (ii) otteniamo immediatamente che il grado di $m(x)$ è 4, e poiché come abbiamo visto $m(x) \mid p(x)$, si ha che il polinomio $p(x) = m(x)$ è irriducibile in quanto polinomio minimo di α su $\mathbb{Q}(\alpha, \sqrt[3]{2})$.

Esercizio 2.12: Seconda Prova Parziale del 22/01/2021 - n° 1

Si consideri il polinomio $p(x) = x^3 - 2x - 2$.

(i) Verificare che $p(x)$ è un polinomio irriducibile su $\mathbb{Q}$.

(ii) Detta α una radice di $p(x)$, determinare una base $\mathcal{B}$ di $\mathbb{Q}(\alpha)$, visto come spazio vettoriale su $\mathbb{Q}$.

(iii) Scrivere il valore dell'elemento

$$(1 + \alpha + \alpha^2)^{-1} \in \mathbb{Q}(\alpha)$$

come combinazione lineare dei valori della base $\mathcal{B}$.

Soluzione.

(i) Il polinomio $p(x)$ è irriducibile per il criterio di Eisenstein.

(ii) $\mathcal{B} = \{1, \alpha, \alpha^2\}$

(iii) Poniamo
$$(1 + \alpha + \alpha^2)(a + b\alpha + c\alpha^2) = 1$$
e svolgiamo i calcoli modulo $p(x)$, cioè con la condizione $\alpha^3 = 2\alpha + 2$. Otteniamo il sistema
$$\begin{cases} a + 2b + 2c = 1 \\ a + 3b + 4c = 0 \\ a + b + 3c = 0 \end{cases}$$
che ha soluzione $(a, b, c) = (5/3, 1/3, -2/3)$. L'elemento da calcolare risulta quindi essere:
$$\frac{1}{3}(5 + \alpha - 2\alpha^2)\,.$$

Esercizio 2.13: prova d'esame del 14/04/2021 - n° 4

Determinare il polinomio minimo di $\sqrt{2}\sqrt{6 + \sqrt{3}}$ su $\mathbb{Q}$.

Soluzione. Poniamo
$$x = \sqrt{2}\sqrt{6 + \sqrt{3}}.$$
Segue che
$$x^2 = 12 + 2\sqrt{3},$$
così
$$x^2 - 12 = 2\sqrt{3},$$
ed elevando entrambi i membri nuovamente al quadrato
$$x^4 - 24x^2 + 144 = 12.$$
Dunque considero il polinomio $p(x) = x^4 - 24x^2 + 132 \in \mathbb{Q}[x]$. Esso è monico ed ammette $\sqrt{2}\sqrt{6 + \sqrt{3}}$ come radice. Infine $p(x)$ è irriducibile su $\mathbb{Q}$ in quanto, ponendo $t = x^2$, l'equazione
$$t^2 - 24t + 132 = 0$$

ammette due soluzioni distinte non razionali $t_{1,2} = 12 \pm 2\sqrt{3}$ e la fattorizzazione in $\mathbb{R}[x]$ è unica. Così $p(x)$ è proprio il polinomio minimo di $\sqrt{2}\sqrt{6+\sqrt{3}}$ su $\mathbb{Q}$.

Esercizio 2.14: prova d'esame del 12/07/2021 - n° 4

Si consideri l'estensione $\mathbb{Q}(\pi^3) \hookrightarrow \mathbb{Q}(\pi)$.

(i) Verificare che $\pi^2 \notin \mathbb{Q}(\pi^3)$.

(ii) Determinare il polinomio minimo di π^2 su $\mathbb{Q}(\pi^3)$.

Soluzione.

(i) Se fosse $\pi^2 \in \mathbb{Q}(\pi^3)$, allora si avrebbe che

$$\pi^2 = \frac{a_n(\pi^3)^n + ... + a_1\pi^3 + a_0}{b_m(\pi^3)^m + ... + b_1\pi^3 + b_0},$$

dove $a_0, ..., a_n, b_0, ..., b_m \in \mathbb{Q}$ e $a_n \neq 0 \neq b_m$. Così si otterrebbe un'equazione polinomiale a coefficienti razionali

$$b_m\pi^{3m+2} + ... + b_1\pi^5 + b_0\pi^2 - (a_n\pi^{3n} + ... + a_1\pi^3 + a_0) = 0$$

e ciò implicherebbe che π sarebbe radice del polinomio a coefficienti razionali

$$p(x) = b_m x^{3m+2} + ... + b_1x^5 + b_0x^2 - (a_n x^{3n} + ... + a_1x^3 + a_0),$$

il che è un assurdo.

(ii) Il polinomio $p(x) = x^3 - \pi^6 = x^3 - (\pi^3)^2 \in \mathbb{Q}(\pi^3)[x]$ ammette π^2 come radice ed è irriducibile su $\mathbb{Q}(\pi^3)$ in quanto la sua fattorizzazione su $\mathbb{R}[x]$ è

$$p(x) = x^3 - (\pi^2)^3 = (x - \pi^2)(x^2 + \pi^2 x + \pi^4).$$

Dunque il polinomio minimo di π^2 su $\mathbb{Q}(\pi^3)$ è proprio $p(x)$.

Esercizio 2.15: prova d'esame del 15/09/2021 - n° 3

Dopo avere verificato che il polinomio $m(x) = x^3 - x^2 + 1$ è irriducibile su $\mathbb{Q}$, si consideri il campo $L = \mathbb{Q}(\alpha)$, dove α ha polinomio minimo $m(x)$ su $\mathbb{Q}$.

(i) Determinare una base di L su $\mathbb{Q}$.

(ii) Scrivere il valore
$$\frac{\alpha^5}{\alpha^3 + \alpha + 3}$$
come combinazione lineare degli elementi della base trovata.

Soluzione. Per il lemma di Gauss, il polinomio $m(x)$ non ha radici razionali, ed essendo di terzo grado, questo implica che $m(x)$ è irriducibile.

(i) Essendo $m(x)$ di terzo grado, si ha ad esempio la base
$$\mathcal{B} = \{1, \alpha, \alpha^2\}$$

(ii) Per svolgere il resto dell'esercizio, useremo sistematicamente la riduzione $\alpha^3 = \alpha^2 - 1$. Calcoliamo il reciproco di $\alpha^2 + \alpha + 2$ utilizzando l'identità di Bézout:
$$5 = (\alpha^3 - \alpha^2 + 1)(\alpha^2 + \alpha + 2) - (\alpha - 2)(\alpha^2 + \alpha + 2)$$
$$5 = (\alpha^3 - \alpha^2 - \alpha + 3)(\alpha^2 + \alpha + 2)$$
$$5 = (-\alpha + 2)(\alpha^2 + \alpha + 2)$$
Si ottiene subito:
$$\frac{\alpha^5}{\alpha^3 + \alpha + 3} = \frac{-\alpha - 1}{\alpha^2 + \alpha + 2} = \frac{1}{5}(-\alpha - 1)(\alpha + 2) = \frac{1}{5}(\alpha^2 - \alpha - 2)\,.$$

2.3 Campo di spezzamento di un polinomio

Esercizio 2.16: prova d'esame del 20/01/2021 - n° 4

Calcolare il grado del campo di spezzamento di $x^4 + 4$ sul campo F nei casi seguenti:
$$(i)\quad F = \mathbb{Q} \qquad (ii)\quad F = \mathbb{R}$$

Soluzione. Il polinomio in questione si scompone in $\mathbb{Z}[x]$ come segue,

$$x^4 + 4 = (x^2 + x + 1)(x^2 - x + 1)\,.$$

e ha esattamente 4 radici complesse $x = \pm 1 \pm i$. Quindi si ha immediatamente:

$$\text{(i)}\ \ \Sigma = \mathbb{Q}(i) \qquad \text{(ii)}\ \ \Sigma = \mathbb{R}(i) = \mathbb{C}$$

Esercizio 2.17: prova d'esame del 17/02/2021 - n° 3

Si consideri il polinomio $f(x) = x^6 - 5 \in \mathbb{Q}[x]$.

(i) Scrivere il polinomio $f(x)$ come prodotto dei suoi fattori irriducibili su $\mathbb{Q}(\sqrt[6]{5})$.

(ii) Calcolare il grado dell'estensione $\mathbb{Q} \to \Sigma$, dove Σ è il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

Soluzione.

(i) Si osserva che

$$x^6 - 5 = (x^3 - \sqrt{5})(x^3 + \sqrt{5}) =$$

$$= (x - \sqrt[6]{5})(x^2 + \sqrt[6]{5}x + \sqrt[3]{5})(x + \sqrt[6]{5})(x^2 - \sqrt[6]{5}x + \sqrt[3]{5})$$

e i polinomi di secondo grado $x^2 + \sqrt[6]{5}x + \sqrt[3]{5}$ e $x^2 - \sqrt[6]{5}x + \sqrt[3]{5}$ sono irriducibili su $\mathbb{Q}(\sqrt[6]{5})$ in quanto non hanno radici in tale campo.

(ii) Il campo di spezzamento Σ del polinomio $f(x)$ sul campo $\mathbb{Q}$ si ottiene estendendo il campo $\mathbb{Q}(\sqrt[6]{5})$ con una radice sesta primitiva dell'unità, ad esempio $\omega = e^{\frac{\pi i}{3}}$, la quale soddisfa la relazione $\omega^2 - \omega + 1 = 0$. Infatti risulta che $\sqrt[6]{5}\omega$ è radice del polinomio $x^2 - \sqrt[6]{5}x + \sqrt[3]{5}$ e $\sqrt[6]{5}\omega^2$ è radice di $x^2 + \sqrt[6]{5}x + \sqrt[3]{5}$. Inoltre si ha che

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

in quanto il polinomio $x^2 - x + 1$ è un polinomio monico, irriducibile su $\mathbb{Q}(\sqrt[6]{5})$ ed ammette ω come radice, ovvero è il polinomio minimo di ω sul campo $\mathbb{Q}(\sqrt[6]{5})$. Sfruttando il Teorema dei Gradi, si conclude che

$$[\Sigma : \mathbb{Q}] = [\Sigma : \mathbb{Q}(\sqrt[6]{5})][\mathbb{Q}(\sqrt[6]{5}) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

2.4 Campi finiti e campi in caratteristica p

Esercizio 2.18: prova d'esame del 10/11/2020 - n° 4

Sia $f(x)$ un polinomio irriducibile di terzo grado sul campo $\mathbb{F}_p$, con p numero primo. Dimostrare che il campo di spezzamento di $f(x)$ su $\mathbb{F}_p$ ha p^3 o p^6 elementi.

Soluzione. Sia α una radice di f. Si ha $[F_p(\alpha) : \mathbb{F}_p] = 3$, e $f(x) = (x-\alpha)g(x)$ in $\mathbb{F}_p(\alpha)[x]$, con $g(x)$ polinomio di secondo grado. Ci sono due possibilità. Se $g(x)$ è riducibile in $\mathbb{F}_p(\alpha)[x]$, esso non può che scomporsi nel prodotto di due fattori lineari; pertanto $\mathbb{F}_p(\alpha)$ è il campo di spezzamento che si cercava, e ha esattamente p^3 elementi. In caso contrario, sia β una radice di $g(x)$. Il campo $\mathbb{F}_p(\alpha, \beta)$ è il campo di spezzamento cercato, ha grado 2 su $\mathbb{F}_p(\alpha)$, e quindi grado 6 su $\mathbb{F}_p$.

Esercizio 2.19: prova d'esame del 14/04/2021 - n° 3

Determinare il grado del campo di spezzamento del polinomio $f(x) = x^{21} - [1]$ su $\mathbb{F}_3$.

Soluzione. La caratteristica di $\mathbb{F}_3$ è 3, dunque $f(x) = (x^7 - [1])^3$, così il campo di spezzamento di $f(x)$ coincide con il campo di spezzamento di $g(x) = x^7 - [1]$. Inoltre

$$g(x) = \Phi_1(x)\Phi_7(x) = (x - [1])\Phi_7(x),$$

dove $\Phi_7(x)$ è il settimo polinomio ciclotomico a coefficienti in $\mathbb{F}_3$. Ogni radice a di $\Phi_7(x)$ è tale che $a^7 = [1]$, quindi a ha periodo 7 nel gruppo moltiplicativo del campo di spezzamento Σ di $f(x)$, con $|\Sigma| = 3^n$ (in quanto Σ è un $\mathbb{F}_3$-spazio vettoriale). Da questo, si deduce che 7 divide $3^n - 1$ e la minima estensione di campi di $\mathbb{F}_3$ per cui ciò accade si ottiene per $n = 6$. Quindi, per il *Teorema di Cauchy* per i gruppi, $a \in \mathbb{F}_{3^6} = \mathbb{F}_3(a)$ e quest'ultimo è il campo di spezzamento Σ cercato.

2.5 Polinomi Ciclotomici

Esercizio 2.20: prova d'esame del 3/02/2021 - n° 3

Sia $\Phi_{15}(x)$ il 15-esimo polinomio ciclotomico a coefficienti razionali, e sia Σ il campo di spezzamento di $\Phi_{15}(x)$ su $\mathbb{Q}$.

(i) Determinare il grado dell'estensione $\mathbb{Q} \to \Sigma$.

(ii) Calcolare $\Phi_{15}(x)$.

Soluzione.

(i) Il polinomio ciclotomico $\Phi_{15}(x)$ è irriducibile sul campo $\mathbb{Q}$ e le sue radici sono tutte e sole le radici primitive quindicesime dell'unità

$$\varepsilon^k = e^{\frac{2k\pi i}{15}},$$

con $(k, 15) = 1$, ovvero $k = 1, 2, 4, 7, 8, 11, 13, 14$. Segue che il campo di spezzamento di $\Phi_{15}(x)$ sul campo $\mathbb{Q}$ è dato dall'estensione algebrica semplice $\mathbb{Q}(\varepsilon)$. Si può concludere che

$$[\Sigma : \mathbb{Q}] = deg(\Phi_{15}(x)) = \varphi(15) = 8,$$

dove φ è la funzione di Eulero.

(ii) Dalla teoria sui polinomi ciclotomici, è ben noto che

$$\prod_{d|15} \Phi_d(x) = x^{15} - 1$$

Ne segue che

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} =$$

$$= \frac{x^{15} - 1}{(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)} =$$

$$= \frac{x^{15} - 1}{x^7 + x^6 + x^5 - x^2 - x - 1}$$

La divisione polinomiale ci restituisce il risultato

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Esercizio 2.21: prova d'esame del 28/06/2021 - n° 3

Sia $\zeta = e^{2\pi i/5} \in \mathbb{C}$. Dopo aver calcolato il grado $[\mathbb{Q}(\zeta) : \mathbb{Q}]$, verificare che si ha $\mathbb{Q} \subset \mathbb{Q}(\zeta + \zeta^4) \subset \mathbb{Q}(\zeta)$.

Soluzione. Il grado $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ è 4 in quanto il polinomio minimo dell'estensione di campi $\mathbb{Q} \hookrightarrow \mathbb{Q}(\zeta)$ è il quinto polinomio ciclotomico $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

L'inclusione $\mathbb{Q}(\zeta + \zeta^4) \subseteq \mathbb{Q}(\zeta)$ è immediata in quanto $\zeta \in \mathcal{C} \setminus \mathbb{R}$, mentre

$$\zeta + \zeta^4 = \zeta + \bar{\zeta} = 2\Re(\zeta) \in \mathbb{R}.$$

Per verificare che vale l'inclusione propria $\mathbb{Q} \subset \mathbb{Q}(\zeta + \zeta^4)$, dimostriamo che $\zeta + \zeta^4$ non è un numero razionale.

I metodo

Calcoliamo

$$(\zeta + \zeta^4)^2 = \zeta^2 + 2 + \zeta^3 =$$

da cui

$$\zeta + \zeta^4 + \zeta^2 + 2 + \zeta^3 = 1$$

dove abbiamo usato il fatto che la somma di tutte le n radici n-esime dell'unità è 0.

Quindi, $\zeta + \zeta^4$ soddisfa l'equazione $z^2 + z = 1$ che fornisce l'unica soluzione reale positiva:

$$z = \frac{-1 + \sqrt{5}}{4} \in \mathbb{R} \setminus \mathbb{Q}.$$

II metodo

Poiché $\zeta + \zeta^4 = 2\cos\left(\frac{2\pi}{5}\right)$, è opportuno osservare che

$$\cos\left(\frac{4\pi}{5}\right) = \cos\left(2\pi - \frac{4\pi}{5}\right) = \cos\left(\frac{6\pi}{5}\right).$$

Sia $x = \frac{2\pi}{5}$, così $\cos(2x) = \cos(3x)$ e, usando le formule di duplicazione del coseno, si ottiene

$$2\cos^2(x) - 1 = 4\cos^3(x) - 3\cos(x).$$

Ponendo $y = \cos(x)$, si ha che

$$(y - 1)(4y^2 + 2y - 1) = 0,$$

e, escludendo la soluzione $y = 1$ e ricordando che nel primo quadrante il coseno assume valori compresi tra 0 e 1, si ottiene che

$$y = \cos(x) = \cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4} \in \mathbb{R} \setminus \mathbb{Q}.$$

Così $\zeta + \zeta^4$ non è un numero razionale.

Bibliografia

[1] P. Aluffi, Algebra: Chapter 0, *Graduate Studies in Mathematics*, American Mathematical Society (2008).