Universitá degli studi di Bari
Dipartimento di Matematica

Eserciziario di Algebra 2

Tutor: Angela MONTI

Titolare del Corso: Prof. Roberto LA SCALA
Anno Accademico 2013/2014

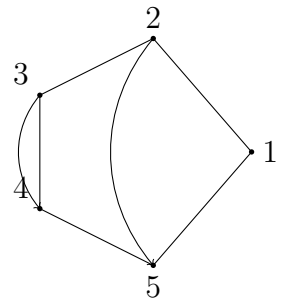
Prefazione

Prima di chiarire gli obiettivi e le finalità dell'eserciziario preparato, ritengo doveroso chiarire che lo stesso è stato elaborato sotto la guida vigile ed attenta del Prof. Roberto LA SCALA.
Nell'approntare gli esercizi da somministrare e proporre agli studenti del Corso di Algebra 2, ho inteso considerare prove che potessero favorire lo sviluppo delle capacità logico-sintetiche e logico-analitiche, ma anche favorire in essi la consapevolezza che l'impegno e l'attenzione possono consentire la risoluzione autonoma degli esercizi proposti.
Credo inoltre che non sia superfluo precisare che le prove e gli esercizi proposti abbiano riguardato le tematiche fondamentali dell'esame di Algebra 2, al fine di fornire agli studenti gli strumenti necessari per sostenere le prove d'esame.

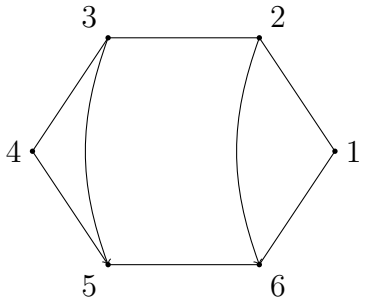
Teoria dei gruppi

Esercizio 1. *Sia D_5 il gruppo diedrale di ordine* 10*, costituito dalle simmetrie del pentagono. Calcolare tutti gli omomorfismi $\phi : D_5 \to \mathbb{Z}_6$.*
Svolgimento

Non è essenziale per questo esercizio, ma osserviamo che è possibile realizzare facilmente ogni gruppo diedrale D_n come sottogruppo di S_n. Infatti se numeriamo i vertici del poligono regolare con n lati, abbiamo che D_n agisce fedelmente su $\{1, 2, \ldots, n\}$, ovvero è dato un monomorfismo (immersione) $D_n \to S_n$. Ad esempio



$D_5 = \langle (12345), (25)(34) \rangle$ dove (12345) rappresenta la rotazione e (25)(34) la riflessione.



$D_6 = \langle (123456), (26)(35) \rangle$ dove (123456) rappresenta la rotazione e (26)(35) la riflessione. Questa realizzazione del gruppo diedrale ci libera dalla necessità di ricordare la tavola di moltiplicazione di $D_n = \langle \sigma, \tau \rangle$, dedotta dall'identità fondamentale $\tau\sigma\tau = \sigma^{-1}$ (quindi $\tau\sigma^i\tau = \sigma^{-i}$) che è la seguente

- $\sigma^i\sigma^j = \sigma^{i+j}$

- $\sigma^i(\sigma^j\tau) = \sigma^{i+j}\tau$
- $(\sigma^i\tau)\sigma^j = \sigma^{i-j}\tau$
- $(\sigma^i\tau)(\sigma^j\tau) = \sigma^{i-j}$

Dal teorema fondamentale di isomorfismo sappiamo che determinare un omomorfismo di gruppi

$$\phi : G \to G'$$

significa determinare

- un sottogruppo normale $N = ker(\phi) \triangleleft G$,
- un sottogruppo $H = im(\phi) < G'$,
- un isomorfismo di gruppi $G/N \simeq H$, tale che $g \cdot N \to \phi(g)$.

Dunque cominciamo con il considerare i possibili nuclei $N \triangleleft D_5$. Il gruppo D_5 ha ordine 10 e quindi, per il teorema di Lagrange, gli ordini possibili per i sottogruppi sono $1, 2, 5, 10$.

1. Se $N = ker(\phi) = 1$, allora avremmo un monomorfismo (omomorfismo ingettivo) $D_5 \to \mathbb{Z}_6$, ma chiaramente questo non è possibile in quanto $|D_5| = 10 > 6 = |\mathbb{Z}_6|$.
2. Se invece $N = ker(\phi) = D_5$, allora abbiamo l'omomorfismo banale (notiamo che quest'ultimo lo ritroviamo sempre).
3. Ora osserviamo che 2 e 5 sono numeri primi, pertanto se $|N| = 2$ oppure $|N| = 5$, allora N è un sottogruppo ciclico di D_5. Gli elementi di $D_5 < S_5$ sono

$$id, (12)(35), (13)(45), (14)(23), (15)(24), (25)(34), (12345),$$

$$(13524), (14253), (15432)$$

È facile verificare che gli elementi di periodo 2 non generano sottogruppi normali, per esempio

$$(12345)(12)(35)(12345)^{-1} = (14)(23).$$

Abbiamo un solo sottogruppo di periodo 5

$$N = \{id, (12345), (13524), (14253), (15432)\},$$

che chiaramente è normale in quanto ha indice 2. Notiamo che $D_5/N = \{N, (12)(35)N\} \simeq \mathbb{Z}_2$, pertanto come immagine di ϕ cerchiamo un sottogruppo $H < \mathbb{Z}_6$ che sia isomorfo a $\mathbb{Z}_2$. Poiché $\mathbb{Z}_6$ è un gruppo ciclico e 2 divide 6 allora, per il teorema di corrispondenza, esiste esattamente un unico sottogruppo di questo tipo

$$H = \langle 3 \rangle = \{0, 3\}.$$

Quindi ogni isomorfimo $D_5/N \leftrightarrow H$ va bene per definire ϕ. Trattandosi di gruppi di ordine 2 ce n'è uno solo

$$N \to 0, (12)(35)N \to 3.$$

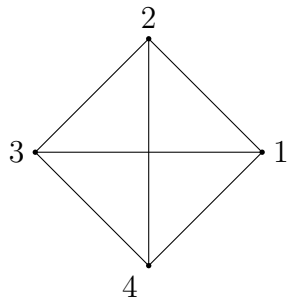
Pertanto esistono esattamente due omomorfismi da D_5 in $\mathbb{Z}_6$, nessuno dei quali è surgettivo.

Esercizio 2. *Il gruppo diedrale D_4 fissa un quadrato rispetto al gruppo delle trasformazioni del piano, che corrispondono al gruppo ortogonale $O_2(\mathbb{R})$. In particolare D_4 agisce fedelmente (mappa ingettiva) sull'insieme X_v dei vertici del quadrato, sull'insieme X_l dei lati e sull'insieme X_d delle diagonali del quadrato. Calcolare lo stabilizzatore di un elemento di ciascuno degli insiemi X_v, X_l e X_d.*

Svolgimento

Possiamo ragionare in termini geometrici, ma sfruttando l'azione fedele di D_4 su $X_v = \{1, 2, 3, 4\}$ (omomorfismo iniettivo $D_4 \to S(X_v) = S_4$) possiamo

identificare D_4 con il sottogruppo di S_4.



$D_4 = \langle (1234), (24) \rangle = \{id, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$ ed inoltre

$$X_v = \{1,2,3,4\},\ X_l = \big\{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\big\},\ X_d = \big\{\{1,3\},\{2,4\}\big\}$$

L'azione sui sottoinsiemi $\{i,j\}$ è chiaramente la seguente

$$\sigma \cdot \{i,j\} = \{\sigma(i), \sigma(j)\} \text{ dove } \sigma \in D_4.$$

È chiaro che D_4 non può agire fedelmente su X_d, in quanto $|D_4| > |S_2|$. Si può facilmente verificare che D_4 agisce fedelmente su X_l, ovvero solo l'identità agisce identicamente sugli elementi di X_l. Inoltre

$$Stab(1) = \{id, (24)\}, Stab(2) = \{id, (13)\} \text{ etc...}$$

Calcoliamo orbita e stabilizzatore di $\{1,2\}$.

$$Orb(\{1,2\}) = \big\{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\big\} = X_l$$

$$Stab(\{1,2\}) = \big\{id, (12)(34)\big\}$$

Risulta dunque verificata la relazione fondamentale

$$|D_4| = |Orb||Stab| = 4 \cdot 2 = 8$$

Per quanto riguarda $\{1,3\}$ risulta $Orb(\{1,3\}) = \big\{\{1,3\},\{2,4\}\big\} = X_d$ e $Stab(\{1,3\}) = \{id,(13),(24),(13)(24)\}$. Notiamo che le azioni di D_4 su X_v, X_l, X_d sono tutte transitive (l'insieme coincide con un'unica orbita).

Esercizio 3. *Decomporre come prodotto diretto di gruppi ciclici il gruppo abeliano* $U(\mathbb{Z}_{72})$.

Svolgimento

Osserviamo subito che la fattorizzazione di 72 è $72 = 2^3 \cdot 3^2$. Il teorema cinese del resto ci dice che l'omomorfismo di anelli

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$

$$1 \to (1,1)$$

$$x \to (x,x)$$

è un isomorfismo se $GCD(m,n) = 1$. Ne segue che $U(\mathbb{Z}_{mn}) \simeq U(\mathbb{Z}_m \times \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Abbiamo dunque

$$U(\mathbb{Z}_{2^3.3^2}) \simeq U(\mathbb{Z}_{2^3}) \times U(\mathbb{Z}_{3^2})$$

e l'isomorfismo è dato dalla mappa

$$x \to (x,x).$$

Ragioniamo separatamente per i gruppi abeliani $U(\mathbb{Z}_{2^3})$ e $U(\mathbb{Z}_{3^2})$. Si può dimostrare che $U(\mathbb{Z}_{p^k})$ con $p > 2$ è un gruppo ciclico. Infatti

$$|U(\mathbb{Z}_{3^2})| = \psi(3^2) = 3^2 - 3 = 6$$

quindi i possibili periodi per gli elementi di $U(\mathbb{Z}_{3^2})$ sono 1, 2, 3, 6. Risulta $2^2 = 4$ e $2^3 = 8$, pertanto 2 ha periodo 6 e quindi $U(\mathbb{Z}_{3^2}) = \langle 2 \rangle$. Inoltre

$$|U(\mathbb{Z}_{2^3})| = \psi(2^3) = 2^3 - 2^2 = 4$$

e poiché $4 = 2^2$, per il 2-gruppo abeliano $U(\mathbb{Z}_{2^3})$ abbiamo esattamente due

casi: ciclico oppure isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Controlliamo quindi i periodi

$$3^2 = 9 \equiv 1 \bmod 8,\ 5^2 = 25 \equiv 1 \bmod 8$$

e quindi

$$U(\mathbb{Z}_{2^3}) = \langle 3 \rangle \times \langle 5 \rangle.$$

Vogliamo ottenere la decomposizione del gruppo $U(\mathbb{Z}_{2^3.3^2})$. Dobbiamo quindi calcolare le controimmagini di (3,1), (5,1) e (1,2) attraverso l'isomorfismo

$$U(\mathbb{Z}_{2^3.3^2}) \to U(\mathbb{Z}_{2^3}) \times U(\mathbb{Z}_{3^2})$$

$$x \to (x, x)$$

Dobbiamo semplicemente applicare il teorema cinese del resto ai seguenti sistemi di congruenze

$$\begin{cases} x \equiv 3 \bmod 8 \\ x \equiv 1 \bmod 9 \end{cases}$$

$$\begin{cases} x \equiv 5 \bmod 8 \\ x \equiv 1 \bmod 9 \end{cases}$$

$$\begin{cases} x \equiv 1 \bmod 8 \\ x \equiv 2 \bmod 9 \end{cases}$$

L'identità di Bezout è

$$1 = (-1)8 + (1)9 = -8 + 9$$

e quindi le soluzioni sono $1(-8)+3(9) = 19$, $1(-8)+5(9) = 37$, $2(-8)+1(9) = -7 \equiv 65 \bmod 72$. Abbiamo quindi

$$U(\mathbb{Z}_{72}) = \langle 19 \rangle \times \langle 37 \rangle \times \langle 65 \rangle.$$

A scopo di verifica è preferibile controllare che i periodi di 19, 37 e 65 siano effettivamente 2, 2 e 6 in $U(\mathbb{Z}_{72})$.

Esercizio 4. *Provare che il gruppo degli automorfismi di D_5 è costituito da 20 elementi.*

Svolgimento

Sappiamo che il gruppo D_5 ha la seguente presentazione:

$$D_5 = \langle \sigma, \tau \mid \sigma^5 = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$$

Allora D_5 è generato da due elementi e le relazioni verificate da tali elementi derivano tutte dalle tre relazioni date. Un omomorfismo $\phi : D_5 \to G$ è assegnato non appena sono dati due elementi a, $b \in G$ che verificano le relazioni fondamentali soddisfatte da σ e τ. Inoltre poiché abbiamo

$$D_5 = \langle \sigma \rangle \rtimes \langle \tau \rangle = \{\sigma^i, \sigma^i\tau\}_{i,j=0,\dots,4}$$

l'omomorfismo ϕ è dato esplicitamente come

$$\phi(\sigma^i) = a^i,\ \phi(\sigma^i\tau) = a^i b$$

Il fatto che a e b verificano (almeno) le relazioni soddisfatte da σ e τ, garantisce che presentazioni diverse di uno stesso elemento di D_5 hanno come immagine attraverso ϕ uno stesso elemento di G, ovvero ϕ è ben definita. In altri termini

$$1 = \sigma^5 = \tau^2 = \tau\sigma\tau\sigma,\ \phi(1) = a^5 = b^2 = baba = 1$$

Il nucleo di ϕ sarà costituito dalle eventuali altre relazioni soddisfatte da a e b.

Osserviamo che questo discorso possiamo applicarlo ad ogni gruppo presentato e non solo a D_5. Nel nostro caso vogliamo trovare omomorfismi bigettivi del tipo

$$D_5 \to D_5$$

dunque ci serve una coppia di elementi di D_5 che verifichino le stesse relazioni di σ e τ. Osserviamo che σ ha periodo 5, che è un numero primo; allora per

ogni $i > 0$ σ^i ha periodo 5. Inoltre

$$\sigma^j \tau \sigma^j \tau = \sigma^j \sigma^{-j} = 1$$

ovvero $\sigma^j \tau$ ha periodo 2 per ogni j. Resta da verificare la relazione

$$(\sigma^j \tau)\sigma^i(\sigma^j \tau) = \sigma^{-i}.$$

Ma infatti $(\sigma^j \tau)\sigma^i(\sigma^j \tau) = \sigma^j \tau \sigma^{i+j} \tau = \sigma^j \sigma^{-i-j} = \sigma^{-i}$. Allora l'assegnazione

$$\sigma \to \sigma^i,\ \tau \to \sigma^j \tau$$

definisce un omomorfismo $\phi : D_5 \to D_5$.
Resta da verificare che $ker(\phi) = \{1\}$ ma, trattandosi di un endomorfismo di un gruppo finito, questo è equivalente a provare

$$im(\phi) = \langle \sigma^i, \sigma^j \tau \rangle = D_5.$$

Chiaramente $\sigma \in \langle \sigma^i \rangle$ (in quanto il periodo è un primo) e quindi $\sigma^j \in \langle \sigma^i \rangle \subseteq im(\phi)$ per cui si ha

$$\tau = \sigma^{-j} \cdot \sigma^j \tau \in im(\phi)$$

ovvero $D_5 = \langle \sigma, \tau \rangle \subseteq im(\phi)$. Il numero di coppie $(\sigma^i, \sigma^j \tau)$, con $i = 1, 2, 3, 4$ e $j = 0, 1, 2, 3, 4$ è dunque $4 \cdot 5 = 20$, ovvero il numero degli automorfismi di D_5 risulta essere uguale a 20.

Esercizio 5. *Nel gruppo S_5 si consideri il seguente sottogruppo*

$$G = \langle (12), (14)(25) \rangle.$$

1. *Stabilire se G è un sottogruppo di Sylow di S_5.*
2. *Calcolare le classi di coniugio di G.*
3. *Calcolare tutti i sottogruppi normali di G.*
4. *Determinare il centro Z di G.*

5. Classificare a meno di isomorfismi i gruppi G e G/Z.

Svolgimento

$|S_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$, dunque i sottogruppi di Sylow di S_5 sono ciclici di ordine 5 e 3, oppure sono di ordine 8. Dato che G contiene elementi di periodo 2, se è un sottogruppo di Sylow, allora può avere solo ordine 8. I gruppi non abeliani di ordine 8 sono D_4 e Q (il gruppo dei quaternioni), mentre quelli abeliani sono $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
Ci aspettiamo quindi che G sia un qualche prodotto di due suoi sottogruppi, ma

$$|\langle(12)\rangle \cdot \langle(14)(25)\rangle| = 4 < 8.$$

Proviamo quindi i prodotti

$$(12)(14)(25) = (1425),\ (14)(25)(12) = (1524).$$

Chiaro che G non è abeliano ed inoltre (1425), $(1524) \in G$. Poniamo $H = \langle(12)\rangle = \{id, (12)\}$ e $K = \langle(1425)\rangle = \{id, (1425), (12)(45), (1524)\}$. Ovviamente $H \cdot K \subseteq G$. Inoltre, poiché

$$(12)(1425) = (12)(12)(14)(25) = (14)(25)$$

abbiamo $G = \langle(12), (1425)\rangle = H \ltimes K$ (K ha indice 2 in G). È chiaro che $G \simeq D_4$. Esplicitamente gli elementi di G raggruppati per struttura ciclica sono:

$$\{id/(12), (45)/(12)(45), (14)(25), (15)(24)/(1425), (1524)\}.$$

Poiché $G \subseteq S_5$ abbiamo che le classi di coniugio sono contenute nei sottoinsiemi di elementi che hanno la stessa struttura ciclica. Inoltre il numero di elementi di una classe (orbita) divide l'ordine del gruppo $|G| = 8$, ma non può essere uguale perché c'è la classe $\{id\}$. Dunque il sottoinsieme $\{(12)(45), (14)(25), (15)(24)\}$ deve necessariamente spezzarsi in più classi. Sappiamo che il centro di $D_n = \langle\sigma, \tau\rangle$ con n pari è $Z = \{1, \sigma^{n/2}\}$ ovvero

nel nostro caso

$$(1425)^2 = (12)(45),\ Z = \{id, (12)(45)\}.$$

Possiamo dunque concludere (ricordando che gli elementi del centro hanno classi di coniugio ridotte ad un singolo elemento) che le classi di coniugio di G sono:

$$\{id\},\ \{(12)(45)\},\ \{(12), (45)\},\ \{(14)(25), (15)(24)\},\ \{(1425), (1524)\}.$$

I sottogruppi normali sono sottogruppi (che contengono la classe $\{id\}$) che risultano unione di classi di coniugio. Per Lagrange possono avere cardinalità 1, 2, 4, 8. Allora essi risultano:

$$\{id\},$$

$$\{id, (12)(45)\} = Z,$$

$$\{id, (12), (45), (12)(45)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,$$

$$\{id, (14)(25), (15)(24), (12)(45)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,$$

$$\{id, (1425), (1524), (12)(45)\} \simeq \mathbb{Z}_4,$$

$$G.$$

Il gruppo G/Z ha ordine $8/2 = 4$ ed è quindi abeliano isomorfo a $\mathbb{Z}_4$ oppure a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Analizziamo il periodo delle classi laterali

$$Z = \{id, (12)(45)\}\ |Z| = 1,$$

$(1425)Z = \{(1425), (1524)\}$ $(1425)^2 Z = (12)(45)Z = Z$ quindi $|(1425)Z| = 2$

$$(12)^2 Z = Z \text{ quindi } |(12)Z| = 2.$$

Concludiamo quindi che $G/Z \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Teoria degli anelli

Esercizio 6. *Descrivere l'insieme dei divisori dello zero, l'insieme degli elementi nilpoenti e l'insieme degli elementi unitari dell'anello*

$$A = \mathbb{Q}[x]/(x^4 + 2x^2).$$

Svolgimento

Gli elementi di A sono rappresentati univocamente come i laterali del tipo

$$g + (f) \text{ con } g = 0 \text{ oppure } deg(g) < deg(f) = 4$$

dove $f(x) = x^4 + 2x^2$. È facile verificare che si ha l'unione disgiunta

$$A = \{0\} \cup \{\text{divisori dello zero}\} \cup U(A)$$

dove

$$g + (f) \in U(A) \Leftrightarrow GCD(f, g) = 1$$

$$g + (f) \neq (f) \text{ è divisore } \Leftrightarrow GCD(f, g) \neq 1.$$

La fattorizzazione unica di f è immediata

$$f = x^4 + 2x^2 = x^2(x^2 + 2) \text{ in } \mathbb{Q}[x].$$

Calcoliamo i divisori dello zero (il complementare in $A - \{0\}$ darà l'insieme degli elementi unitari). I gradi ammessi per i rappresentanti delle classi laterali sono $0, 1, 2, 3$. In grado zero abbiamo le costanti, che sono elementi unitari in $\mathbb{Q}[x]$ e dunque pure in A. In grado 1 abbiamo l'insieme dei polinomi monici non coprimi con f, quindi polinomi divisibili da qualche fattore primo di f. Ma allora abbiamo solo $\{x\}$. In grado 2 abbiamo

$$\{x(x + a), x^2 + 2 \mid a \in \mathbb{Q}\}.$$

In grado 3 si ha

$$\{x(x^2+ax+b), (x^2+2)(x+a) \mid a,b \in \mathbb{Q}\}.$$

Un elemento $a \in A$ è per definizione nilpotente se $a^k = 0$ per qualche $k \in \mathbb{N}$. Nel nostro caso abbiamo una classe $g + (f)$ tale che

$$g^k + (f) = (f) \Leftrightarrow g^k \in (f) \Leftrightarrow f \text{ divide } g^k$$

ma è chiaro che ciò accade quando tutti i fattori irriducibili di f dividono g. Poiché tali fattori sono x ed x^2+2 ed inoltre $deg(g)$ deve essere minore di 4 abbiamo, a meno di costanti,

$$g = x(x^2+2)$$

infatti $g^2 \equiv 0 \bmod f$.

Esercizio 7. *Fattorizzare in* $\mathbb{Z}[i]$ *l'elemento* $w = 8+5i$.
Svolgimento

Essendo $\mathbb{Z}[i]$ un dominio euclideo, abbiamo che si tratta anche di un dominio a fattorizzazione. Naturalmente gli elementi primi (quindi irriducibili) di $\mathbb{Z}[i]$ possono essere diversi da quelli di $\mathbb{Z} \subset \mathbb{Z}[i]$. Gli elementi primi di $\mathbb{Z}[i]$ si chiamano *primi di Gauss*. Notiamo subito che se $z \in \mathbb{Z}[i]$ non è primo di Gauss, ovvero se

$$z = u \cdot v \text{ con } u,v \in \mathbb{Z}[i] \text{ e } u,v \notin U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$$

allora

$$\nu(z) = \nu(u) \cdot \nu(v) \text{ con } \nu(u), \nu(v) \neq 1$$

ovverp $\nu(z) \in \mathbb{N}$ non è un numero primo. Dunque se $\nu(z)$ è un numero primo, allora z è un primo di Gauss.
Se $z = a+ib$, con $a \neq 0$ e $b \neq 0$, si prova che $\nu(z)$ è un numero primo se e solo se z è primo di Gauss. Inoltre se z è associato ad un numero intero n (quindi $a = 0$ oppure $b = 0$), allora z è primo di Gauss solo se n è un numero

primo. Osserviamo però che non tutti i numeri primi sono primi di Gauss. Per esempio

$$2 = (1-i)(1+i) = -i(1+i)^2 \text{ e } 5 = (1+2i)(1-2i).$$

Notiamo che $2 = 1^2 + 1^2$ e $5 = 1^2 + 2^2$. In effetti si può dimostrare la *classificazione dei primi di Gauss*.
Un elemento $z = a + ib \in \mathbb{Z}[i]$ è primo (irriducibile) se e solo se

1. $a \neq 0$, $b \neq 0$ e $\nu(z) \in \mathbb{Z}$ è un numero primo, oppure
2. z è associato a $p \in \mathbb{Z}$ un numero primo tale che:
   - p non è la norma di un primo di Gauss o equivalentemente
   - p non è la somma di due quadrati di interi o equivalentemente
   - $p \neq 2$ e $p \not\equiv 1 \bmod 4$.

Ricordiamo infatti che un numero primo p è somma di due quadrati se e solo se $p = 2$ oppure $p \equiv 1 \bmod 4$. In effetti lo abbiamo visto per 2 e $5 \equiv 1 \bmod 4$. Inoltre anche per 13 e 17 (che sono congrui ad 1 modulo 4) abbiamo

$$13 = (2+3i)(2-3i) \text{ e } 17 = (1+4i)(1-4i) \text{ etc...}$$

che dunque nono sono primi di Gauss. Notiamo infine che

$$z = a + ib \text{ è primo } \Leftrightarrow \ \bar{z} = a - ib \text{ è primo}$$

in quanto $z \to \bar{z}$ è un automorfismo dell'anello $\mathbb{Z}[i]$.
Ora possiamo fattorizzare l'elemento w. Calcoliamo la fattorizzazione della valutazione

$$\nu(w) = 8^2 + 5^2 = 145 = 5 \cdot 29$$

pertanto w non è primo. Osserviamo inoltre quali sono i primi che hanno valutazione 5 e 29

$$5 \to (1+2i), (1-2i) \text{ oppure gli associati}$$

$$29 \to (5+2i), (5-2i) \text{ oppure gli associati}$$

pertanto in w avremo un prodotto di due di questi fattori (uno derivante da 5 e l'altro da 29). Si ha che

$$8+5i = i(1-2i)(5+21).$$

Esercizio 8. *Determinare gli elementi invertibili, i divisori dello zero e gli elementi nilpotenti dell'anello* $\mathbb{Z}[i]/(10)$.
Svolgimento

Consideriamo la fattorizzazione di 10 in $\mathbb{Z}[i]$

$$10 = 2 \cdot 5 = (1+i)(1-i)(1+2i)(1-2i)$$

ma osserviamo che il numero $1-i$ non solo è coniugato di $1+i$ ma è pure associato ad esso. Infatti

$$1-i = -i \cdot (1+i) \ \ -i \in U(\mathbb{Z}[i]).$$

Dunque è più corretto dire che la fattorizzazione unica di 2 è

$$2 = -i(1+i)^2$$

e quindi

$$10 = -i(1+i)^2(1+2i)(1-2i).$$

Poiché $\mathbb{Z}[i]$ è un dominio euclideo si ha che i divisori dello zero di $\mathbb{Z}[i]/(10)$ sono le classi laterali $a+ib+(10)$ con $GCD(a+ib, 10) \neq 1$, ovvero qualcuno dei fattori primi di 10 deve dividere $a+ib$. L'anello $\mathbb{Z}[i]/(10)$ è sicuramente un anello finito perché possiamo rappresentare i laterali $a+ib+(10)$ mediante i resti modulo 10 ovvero

$$a+ib = 0 \text{ oppure } \nu(a+ib) = a^2+b^2 < 100 = \nu(10).$$

Chiaramente abbiamo solo un numero finito di punti a coordinate intere

contenuti all'interno della circonferenza di equazione $x^2 + y^2 = 100$ (raggio 10). Se eseguiamo la divisione in $\mathbb{Z}[i]$ nel modo che abbiamo visto, si hanno resti del tipo

$$a + ib = (c + id) \cdot 10 \text{ dove } |c| \leq \frac{1}{2}, |d| \leq \frac{1}{2}$$

ovvero $|a| \leq 5$, $|b| \leq 5$, cioè i resti sono punti a coordinate intere contenuti nel quadrato di lato 10 con centro nell'origine. Il problema con la divisione di $\mathbb{Z}[i]$ è che essa non ha resto unico. Ad esempio

$$15 = 1 \cdot 10 + 5 \ |5| \leq 5$$

$$15 = 2 \cdot 10 - 5 \ | -5| \leq 5$$

ovvero 5 e -5 sono entrambi resti di 15 nella divisione modulo 10 in $\mathbb{Z}[i]$. Notiamo esplicitamente che questa divisione è diversa da quella di $\mathbb{Z}$. La non unicità dei resti implica che due resti distinti possono essere congrui fra loro ed infatti abbiamo

$$-5 = (-1) \cdot 10 + 5$$

cioè 5 e -5 sono congrui modulo 10 in $\mathbb{Z}[i]$ (oltre ad esserlo in $\mathbb{Z}$). Allora

$$|\{\text{resti}\}| \geq |\{\text{classi laterali}\}|.$$

Poiché $n \in \mathbb{Z} \subset \mathbb{R}$ abbiamo un modo semplice per determinare un sistema completo ed univoco di rappresentanti per le classi laterali $a + ib + (n) \in \mathbb{Z}[i] \subset \mathbb{C}$. Guardiamo più da vicino le congruenze modulo n in $\mathbb{Z}[i]$.

$$a + ib \equiv 0 \text{ mod } n \text{ in } \mathbb{Z}[i] \Leftrightarrow$$

$$a + ib = (\alpha + i\beta)n \text{ con } \alpha + i\beta \in \mathbb{Z}[i] \Leftrightarrow$$

$$a + ib = \alpha n + i\beta n \Leftrightarrow a = \alpha n, b = \beta n \Leftrightarrow$$

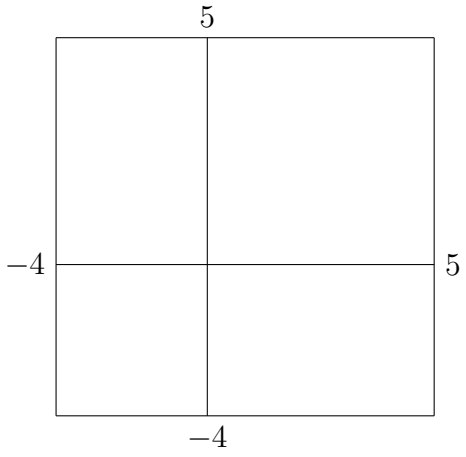
$$a \equiv 0 \text{ mod } n, b \equiv 0 \text{ mod } n \text{ in } \mathbb{Z}.$$

Dunque gli elementi distinti di $\mathbb{Z}[i]/(n)$ sono tutti e soli i laterali $a + ib + (n)$

dove a e b sono resti modulo n, ovvero $\mathbb{Z}[i]/(n)$ è un anello con n^2 elementi. Notiamo esplicitamente che $\mathbb{Z}[i]/(n)$ non è isomorfo all'anello $\mathbb{Z}_n \times \mathbb{Z}_n$, poiché la moltiplicazione

$$(a + ib)(\alpha + i\beta) = (a\alpha - b\beta) + i(a\beta + b\alpha)$$

è definita in modo diverso. Il nostro anello $\mathbb{Z}[i]/(10)$ è costituito quindi da 100 laterali $a + ib + (10)$ con $a, b \in \{-4, -3, \ldots, -1, 0, 1, \ldots 5\}$ resti modulo 10.



Essendo un anello commutativo finito, abbiamo che $\mathbb{Z}[i]/(10)$ è unione disgiunta

$$\{0\} \cup \{ \text{ elementi unitari } \} \cup \{ \text{ divisori dello zero } \}.$$

Inoltre, poiché $\mathbb{Z}[i]$ è un dominio euclideo, possiamo identificare questi insiemi come

$$\{ \text{ elementi unitari } \} = \{a + ib + (10) \mid GCD(a + ib, 10) = 1\}$$

$$\{ \text{ divisori dello zero } \} = \{a + ib + (10) \mid GCD(a + ib, 10) \neq 1\}.$$

A conti fatti ci sono 67 divisori dello zero che sono i laterali $a + ib + (10)$ con a e b resti ed $a + ib$ divisibile da uno dei fattori primi di 10, cioè $1 + i$,

$1+2i$, $1-2i$. Abbiamo quindi $100-67-1=32$ elementi unitari. per quanto riguarda gli elementi nilpotenti abbiamo

$$(z+(10))^k=(10)\Leftrightarrow z^k+(10)=(10)\Leftrightarrow$$

$$10 \text{ divide } z^k \Leftrightarrow \text{ ogni primo di 10 divide } z,$$

ovvero $1+i$, $1+2i$, $1-2i$ dividono tutti il numero $z=a+ib$. Il prodotto di questi fattori primi è chiaramente

$$(1+i)(1+2i)(1-2i)=5(1+i).$$

Gli altri elementi nilpotenti non possono che essere elementi associati a $5(1+i)$ in quanto $|a|\leq 5$ e $|b|\leq 5$.

Esercizio 9. *Dimostrare che sussiste un isomorfismo di anelli (unitari)*

$$\mathbb{Z}_n[x]\simeq \mathbb{Z}[x]/(n)_{\mathbb{Z}[x]}$$

Descrivere inoltre l'anello quoziente

$$\mathbb{Z}[x]/(5,x^2+3)$$

Svolgimento

Con $(n)_{\mathbb{Z}[x]}=\mathbb{Z}[x]\cdot(n)$ indichiamo l'ideale principale generato da n in $\mathbb{Z}[x]$. Ricordiamo che $\mathbb{Z}[x]$ è un UFD ma non un PID. Resta indotta una mappa da $\mathbb{Z}\to\mathbb{Z}_n$

$$\phi:\mathbb{Z}[x]\to\mathbb{Z}_n[x]$$

$$\sum_i \alpha_i x^i \to \sum_i \bar{\alpha}_i x^i$$

dove con $\bar{\alpha}_i$ indichiamo la riduzione modulo n di α_i. Facciamo vedere che ϕ è omomorfismo di anelli.

$$\sum \alpha_i x^i+\sum \beta_i x^i=\sum(\alpha_i+\beta_i)x^i\to\sum(\overline{\alpha_i+\beta_i})x^i=$$

$$\sum(\bar{\alpha}_i + \bar{\beta}_i)x^i = \sum \bar{\alpha}_i x^i + \sum \bar{\beta}_i x^i$$

e

$$\sum \alpha_i x^i \cdot \sum \beta_i x^i = \sum_k \sum_{i+j=k} \alpha_i \beta_j x^k \to \sum_k \overline{\sum_{i+j=k} \alpha_i \beta_j} x^k =$$

$$\sum_k \sum_{i+j=k} \bar{\alpha}_i \bar{\beta}_j x^k = \sum \bar{\alpha}_i x^i \cdot \sum \bar{\beta}_i x^i$$

ed inoltre $\phi(1) = \bar{1}$. Calcoliamo il nucleo di ϕ. Abbiamo dal principio di identità dei polinomi

$$\sum \bar{\alpha}_i x^i = 0 \Leftrightarrow \bar{\alpha}_i = 0 \ \forall i$$

ovvero n divide α_i per ogni i e quindi n divide $\sum \alpha_i x^i$. In altri termini abbiamo $ker(\phi) = (n)_{\mathbb{Z}[x]}$ e quindi è dato l'isomorfismo

$$\mathbb{Z}[x]/(n) \to \mathbb{Z}_n[x]$$

$$\sum \alpha_i x^i + (n) \to \sum \bar{\alpha}_i x^i.$$

Notiamo che se $n = p$ è primo (quindi irriducibile) in $\mathbb{Z}$ tale è pure come elemento di $\mathbb{Z}[x]$ ovvero $(p)_{\mathbb{Z}[x]}$ è un ideale primo e quindi $\mathbb{Z}_p[x]$ è un dominio (anello di polinomi a coefficienti in un campo). Inoltre poiché $\mathbb{Z}[x]$ è un UFD, ma non un PID, non possiamo concludere che $(p)_{\mathbb{Z}[x]}$ è un ideale massimale, infatti ciò è falso essendo $(p) \subset (p, x)$. Abbiamo che l'ideale (p, x) è massimale in quanto

$$\mathbb{Z}[x]/(p, x) \simeq \mathbb{Z}_p.$$

Studiamo ora l'anello $\mathbb{Z}[x]/(5, x^2 + 3)$. Poiché $I = (5, x^2 + 3)$ si ha che $(5) \subset I = (5) + (x^2 + 3)$, allora dal secondo teorema di isomorfismo segue che

$$\mathbb{Z}[x]/I \simeq \mathbb{Z}[x]/(5) \ / \ I/(5)$$

Abbiamo provato che $\mathbb{Z}[x]/(5) \simeq \mathbb{Z}_5[x]$ e quindi

$$I/(5) = (5, x^2 + 3)/(5) = (\bar{5}, x^2 + \bar{3}) = (x^2 + \bar{3})_{\mathbb{Z}_5[x]}.$$

L'anello da studiare è quindi

$$A = \mathbb{Z}_5[x]/(x^2 + \bar{3})$$

dove $\mathbb{Z}_5[x]$ è l'anello dei polinomi a coefficienti nel campo finito $\mathbb{Z}_5$. Facile provare che $x^2 + \bar{3}$ non ha radici in $\mathbb{Z}_5$ e quindi risulta essere irriducibile (perché di grado 2) in $\mathbb{Z}_5[x]$. Poiché $\mathbb{Z}_5[x]$ è un dominio euclideo (quindi un PID) abbiamo che $(x^2 + \bar{3})$ è massimale ovvero $A = \mathbb{Z}_5[x]/(x^2 + \bar{3})$ è un campo. Chiaramente si tratta del campo finito con $5^2 = 25$ elementi.

Teoria dei campi

Esercizio 10. *Determinare il grado* $[\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}]$ *dove* ξ_3 *e* ξ_4 *sono rispettivamente radici primitive terza e quarta dell'unità.*
Svolgimento

Ricordiamo che il polinomio minimo di una radice primitiva n-esima dell'unità è dato sul campo $\mathbb{Q}$ dall'n-esimo polinomio ciclotomico ϕ_n. Abbiamo

$$\phi_3 = x^2 + x + 1,\ \phi_4 = x^2 + 1$$

e quindi

$$[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2,\ [\mathbb{Q}(\xi_4) : \mathbb{Q}] = 2.$$

Dalla regola di moltiplicazione dei gradi sappiamo che

$$[\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}] = [\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}(\xi_4)] \cdot [\mathbb{Q}(\xi_4) : \mathbb{Q}]$$

e quindi dobbiamo calcolare il grado di ξ_3 sull'estensione $\mathbb{Q}(\xi_4)$. Poiché $[\mathbb{Q}(\xi_3) : \mathbb{Q}] = 2$, abbiamo che $[\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}(\xi_4)] \leq 2$. Se il grado di ξ_3 su $\mathbb{Q}(\xi_4)$ fosse uguale ad 1, allora $\xi_3 \in \mathbb{Q}(\xi_4)$. Diciamo

$$\xi_3 = \frac{-1 + i\sqrt{3}}{2} \text{ e } \xi_4 = i$$

quindi

$$\frac{-1 + i\sqrt{3}}{2} = a + ib \text{ con } a, b \in \mathbb{Q}.$$

Ma questo significa che $\frac{\sqrt{3}}{2}$ deve stare in $\mathbb{Q}$ e quindi $\sqrt{3} \in \mathbb{Q}$, ma questo è assurdo. Allora

$$[\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}(\xi_4)] = 2$$

e quindi dalla regola di moltiplicazione dei gradi concludiamo che

$$[\mathbb{Q}(\xi_3, \xi_4) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Una base di $\mathbb{Q}(\xi_3, \xi_4)$ come spazio vettoriale su $\mathbb{Q}$ è data dal prodotto delle

basi 1, ξ_3 di $\mathbb{Q}(\xi_3)$ e 1, ξ_4 di $\mathbb{Q}(\xi_4)$ ovvero

$$\{1, \xi_2, \xi_4, \xi_3\xi_4\} = \left\{1, \frac{-1+i\sqrt{3}}{2}, i, \frac{-\sqrt{3}-i}{2}\right\}.$$

Prima di procedere con il prossimo esercizio è utile ricordare che una condizione necessaria (ma non sufficiente) alla irriducibilità di un polinomio in $\mathbb{Z}_p[x]$ (p primo) è la seguente

Proposizione 1. *Sia $g(x) \in \mathbb{Z}_p[x]$ un polinomio di grado d. Se $g(x)$ è irriducibile allora $g(x)$ divide $x^{p^d} - x$.*

La condizione non è purtroppo sufficiente. Per esempio il polinomio $x^2 + x = (x+1)x$ divide $x^4 - x$ in $\mathbb{Z}_2[x]$, ma chiaramente non è irriducibile.
D'altra parte come condizione necessaria è pratica solo se il grado p^d di $x^{p^d} - x$ non è troppo alto. Più importante è il risultato dal quale questa condizione deriva.

Proposizione 2. *Sia $g(x) \in \mathbb{Z}_p[x]$ un polinomio irriducibile (monico) di grado d. Se d divide n, allora $g(x)$ compare con molteplicità 1 nella fattorizzazione unica del polinomio $x^{p^n} - x \in \mathbb{Z}_p[x]$.*

Per una dimostrazione si veda J. Milne, Fields and Galois Theory, Corollary 4.20.

Consideriamo ora il campo di spezzamento di $f(x)$ sul campo $\mathbb{Z}_p$. Una importante conseguenza della precedente Proposizione è il seguente

Corollario 1. *Sia $g(x) \in \mathbb{Z}_p[x]$ un polinomio irriducibile. Allora il campo di spezzamento di $g(x)$ su $\mathbb{Z}_p$ è l'estensione semplice $\mathbb{Z}_p(\alpha)$ dove α è una qualunque radice di $g(x)$.*

Dimostrazione. Il polinomio $g(x)$ divide $x^{p^d} - x$ con $d = deg(g)$. Allora $g(x)$ si spezza sul campo di spezzamento di $x^{p^d} - x$ su $\mathbb{Z}_p$ ovvero $GF(p^d)$ che ha grado d su $\mathbb{Z}_p$. Dunque il campo di spezzamento E di $g(x)$ su $\mathbb{Z}_p$ ha grado $\leq d$, in quanto $E \subset GF(p^d)$. D'altra parte $\mathbb{Z}_p(\alpha) \subset E$ con α radice di $g(x)$ e $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = d$. Dunque concludiamo che $E = \mathbb{Z}_p(\alpha) = GF(p^d)$. □

Data quindi una radice α di $g(x)$ come possiamo calcolare tutte le altre radici che sono nel campo $E = \mathbb{Z}_p(\alpha)$ e quindi che hanno la forma

$$\sum_{i=o}^{d-1} a_i \alpha_i, \quad a_i \in \mathbb{Z}_p, d = deg(g)?$$

Sappiamo che se $\phi : E \to E$ è $\mathbb{Z}_p$-automorfismo di E, allora

$$g(\alpha) = 0 \ (\alpha \in E) \Rightarrow g(\phi(\alpha)) = \phi(g(\alpha)) = \phi(0) = 0$$

quindi ϕ manda una radice di $g(x)$ ancora in una radice. Poiché E è un campo finito di caratteristica p, è dato lo $\mathbb{Z}_p$-automorfismo di Frobenius

$$\phi : E \to E$$

$$\xi \to \xi^p$$

Notiamo che essendo $E = GF(p^d)$ abbiamo che ϕ ha periodo d (infatti $\xi^{p^d} = \xi$) e quindi ogni $\mathbb{Z}_p$-automorfismo di E è una potenza di ϕ. Dunque se α è una radice, allora tutte le radici (distinte) di $g(x)$ (irriducibile) sono:

$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$$

Notiamo che se $p^i \geq d$, allora dovremo normalizzare α^{p^i} rispetto alla relazione $g(\alpha) = 0$, ovvero eseguire la divisione di x^{p^i} modulo $g(x)$.

Esercizio 11. *Si consideri il seguente polinomio di* $\mathbb{Z}_3[x]$

$$f(x) = x^4 + 2x^3 + 2$$

(a) Calcolare il campo di spezzamento E di $f(x)$ su $\mathbb{Z}_3$ e determinare il numero di elementi di E.
(b) Determinare un generatore del gruppo $U(E)$.
Svolgimento

Verifichiamo che $f(x)$ non ha nessuna radice in $\mathbb{Z}_3$. Infatti

$$f(0) = 2,\ f(1) = 5 \equiv 2,\ f(2) = 34 \equiv 1.$$

Ma il polinomio potrebbe però essere prodotto di due fattori quadratici. Eseguiamo allora la divisione in $\mathbb{Z}_3[x]$ di $f(x)$ per un generico polinomio quadratico (monico). Abbiamo dunque

$$f(x) = (x^2 + ax + b)(x^2 + (2 - a)x + (-b - 2a + a^2))+$$

$$[(2a^2 - a^3 + 2ab - 2b)x + (2 + b^2 + 2ab - a^2b)]$$

devo quindi imporre che il resto sia uguale a zero (in questo modo avrò la divisibilità). Allora devo risolvere un sistema di due equazioni nelle incognite a e b in $\mathbb{Z}_3$.

$$\begin{cases} 2a^2 - a^3 + 2ab - 2b = 0 \\ 2 + b^2 + 2ab - a^2b = 0 \end{cases}$$

Facile verificare che questo sistema non ammette soluzione in $\mathbb{Z}_3$. Pertanto possiamo concludere che $f(x)$ è un polinomio irriducibile. Se α è una radice qualsiasi di $f(x)$ allora il campo di spezzamento di $f(x)$ su $\mathbb{Z}_3$ è $E = \mathbb{Z}_3(\alpha)$. Applicando l'automorfismo di Frobenius abbiamo che tutte le radici di $f(x)$ sono

$$\alpha, \alpha^3, \alpha^9, \alpha^{27}.$$

Poiché $deg(f) = 4$ dobbiamo normalizzare α^9 e α^{27}. Abbiamo quindi

$$x^9 = (x^4 + 2x^3 + 2)(x^5 + x^4 + x^3 + x^2 + 2x) + (x^3 + x^2 + 2x)$$

Dunque $\alpha^9 = 2\alpha + \alpha^2 + \alpha^3$. L'ultima radice invece la ricaviamo usando le formule di Viete

$$\alpha + \alpha^3 + (2\alpha + \alpha^2 + \alpha^3) + \alpha^{27} = -2 = 1$$

da cui concludiamo che

$$\alpha^{27} = 1 - \alpha^2 - 2\alpha^3 = 1 + 2\alpha^2 + \alpha^3.$$

Per quanto riguarda i generatori del gruppo $U(E)$, ricordiamo che $E = \mathbb{Z}_3(\alpha) = \mathbb{Z}_3[x]/(f)$, pertanto $|U(E)| = |E| - 1 = 3^4 - 1 = 80 = 2^4 \cdot 5$ elementi. I possibili periodi sono quindi:

$$1, 2, 4, 5, 8, 10, 16, 20, 40, 80.$$

Verifichiamo se x è un generatore di $U(E)$. Dobbiamo calcolare i resti di x^n modulo $f(x)$ in $\mathbb{Z}_3[x]$ per ogni intero n divisore di 80. Si ha
$x = 0 \cdot f(x) + x$ (in quanto il grado del resto deve essere strettamente inferiore del divisore, che in questo caso è 4);
$x^2 = 0 \cdot f(x) + x^2$;
$x^4 = (1)(x^4 + 2x^3 + 2) + (x^3 + 1)$;
$x^5 = (x + 1)f(x) + (x^3 + x + 1)$;
$x^8 = (x^4 + x^3 + x^2 + x + 2)f(x) + (x^2 + x + 2)$;
$x^{10} = (x^6 + x^5 + x^4 + x^3 + 2x^2 + 1)f(x) + (2x^3 + 2x^2 + 1)$;
$x^{16} = q(x)f(x) + (2x^2 + x + 2)$;
$x^{20} = q(x)f(x) + (2x^3 + 2x^2 + 2)$;
$x^{40} = q(x)f(x) + 2$;
$x^{80} = q(x)f(x) + 1$,
allora $U(E) = \langle\alpha\rangle$.

Esercizio 12. *Verificare che gli anelli* $K_1 = \mathbb{Z}_3[x]/(x^2+1)$ *e* $K_2 = \mathbb{Z}_3[x]/(x^2+x+2)$ *sono campi e costruire uno* $\mathbb{Z}_3$*-isomorfismo* $\phi : K_1 \to K_2$.
Svolgimento

I polinomi quadratici $x^2 + 1$, $x^2 + x + 2$ sono chiaramente irriducibili su $\mathbb{Z}_3$, in quanto non hanno radici. Pertanto K_1 e K_2 sono campi. Poiché $[K_1 : \mathbb{Z}_3] = [K_2 : \mathbb{Z}_3] = 2$, abbiamo $K_1 \simeq K_2 \simeq GF(3^2)$. Sappiamo che $K_1 = \mathbb{Z}_3(\alpha)$ dove α è una radice del polinomio $x^2 + 1$ e $K_2 = \mathbb{Z}_3(\beta)$ dove β è una radice del polinomio $x^2 + x + 2$. Per costruire esplicitamente uno $\mathbb{Z}_3$-isomorfismo $\phi : K_1 \to K_2$ è sufficiente definire in maniera opportuna

$\gamma = \phi(\alpha) \in K_2$ e porre

$$\phi(p(\alpha)) = p(\gamma),$$

$$\phi(a + b\alpha) = a + b\gamma \text{ per ogni } a, b \in \mathbb{Z}_3.$$

L'elemento $\gamma \in K_2 = \mathbb{Z}_3(\beta)$ deve avere lo stesso polinomio minimo di α su $\mathbb{Z}_3$, ovvero

$$\gamma^2 = -1 = 2,$$

allora sia $\gamma = a + b\beta \in \mathbb{Z}_3(\beta)$ ed imponiamo questa relazione

$$2 = (a+b\beta)^2 = a^2+2ab\beta+b^2\beta^2 = a^2+2ab\beta+b^2(-\beta-2) = a^2+b^2+2b(a+b)\beta.$$

Dall'unicità della scrittura abbiamo quindi

$$\begin{cases} a^2 + b^2 = 2 \\ b(a + b) = 0 \end{cases}$$

Le uniche coppie $(a, b) \in {\mathbb{Z}_3}^2$ che soddisfano questo sistema sono $(1, 2)$ e $(2, 1)$. Scegliamo la prima coppia e poniamo

$$\phi(\alpha) = 1 + 2\beta,$$

allora esplicitamente lo $\mathbb{Z}_3$-isomorfismo $\phi : K_1 \to K_2$ è dato da

$$0 \to 0, \;\; \alpha \to 1 + 2\beta, \;\; 2\alpha \to 2 + \beta$$

$$1 \to 1, \;\; 1 + \alpha \to 2 + 2\beta, \;\; 2\alpha + 1 \to \beta$$

$$2 \to 2, \;\; 2 + \alpha \to 2\beta, \;\; 2\alpha + 2 \to 1 + \beta$$

Esercizio 13. *Si consideri l'elemento* $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.
(a) Calcolare il polinomio minimo $f(x)$ *di* α *sul campo* $\mathbb{Q}$.
(b) Determinare il campo di spezzamento E *di* $f(x)$ *su* $\mathbb{Q}$.
Svolgimento

Essendo $\alpha = \sqrt{2+\sqrt{2}}$ abbiamo

$$\alpha^2 = 2 + \sqrt{2} \Rightarrow \alpha^2 - 2 = \sqrt{2} \in \mathbb{Q}(\alpha)$$

da cui, elevando ancora al quadrato, abbiamo

$$\alpha^4 - 4\alpha^2 + 2 = 0.$$

Sicuramente il polinomio $f(x) = x^4 - 4x^2 + 2$ ammette α come radice, ma non possiamo ancora dire che si tratta del polinomio minimo. Infatti dobbiamo provare l'irriducibilità. Dal criterio di Eisenstein (per $p = 2$) segue che $f(x)$ è irriducibile sul campo $\mathbb{Q}$ e quindi $f(x)$ è il polinomio minimo di α su $\mathbb{Q}$.
In generale se abbiamo un polinomio biquadratico $x^4 + bx^2 + c$, le sue radici sono chiaramente del tipo

$$\pm\sqrt{\frac{-b \pm \sqrt{\Delta}}{2}}$$

ovvero dei cosiddetti *radicali doppi*.
Indichiamo brevemente con $\pm\alpha$, $\pm\beta$ queste radici, pertanto il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è $\mathbb{Q}(\alpha, \beta)$. Inoltre

$$x^4 + bx^2 + c = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta)$$

e quindi

$$c = \alpha^2\beta^2$$

ovvero $\alpha\beta = \sqrt{c}$. Allora abbiamo che

$$\beta \in \mathbb{Q}(\alpha) \Leftrightarrow \sqrt{c} \in \mathbb{Q}(\alpha),$$

quindi nel nostro caso

$$\sqrt{c} = \sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$$

e dunque

$$\beta = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha)$$

da cui concludiamo che il campo di spezzamento di $f(x)$ su $\mathbb{Q}$ è semplicemente $\mathbb{Q}(\alpha)$ che ha grado $4 = deg(f)$.
Se vogliamo portare β in forma normale rispetto alla base di $\mathbb{Q}(\alpha)$ $(1, \alpha, \alpha^2, \alpha^3)$, dobbiamo semplicemente calcolare

$$\frac{x^2 - 2}{x}$$

modulo $x^4 - 4x^2 + 2$. Applicando l'algoritmo di Euclide esteso otteniamo

$$1 = GCD(x^4 - 4x^2 + 2, x) = s(x^4 - 4x^2 + 2) + tx.$$

In particolare s sarà un elemento di $\mathbb{Q}$ e t un polinomio di grado 3, ovvero

$$s(x^4 - 4x^2 + 2) + (ax^3 + bx^2 + cx + d)x.$$

Per il principio di identità dei polinomi abbiamo

$$s = \frac{1}{2} \text{ e } t = \frac{x^3}{2} + 2x$$

e quindi

$$\frac{1}{\alpha} = \frac{\alpha^3}{2} + 2\alpha.$$

Moltiplicando per $x^2 - 2$ otteniamo

$$\frac{x^2 - 2}{x} = (\frac{x^3}{2} + 2x)(x^2 - 2) = \frac{x^5}{2} + 3x^3 - 4x$$

il cui resto modulo $x^4 - 4x^2 + 2$ è $x^3 - 3x$, ovvero

$$\beta = \alpha^3 - 3\alpha.$$

Prove d'esame svolte

Esercizio 14. *Nel gruppo $GL_2(\mathbb{C})$ si considerino i seguenti sottogruppi ciclici*

$$H = \langle A \rangle, \quad K = \langle B \rangle$$

dove

$$A = \begin{bmatrix} -\xi & 0 \\ -\xi - 1 & \xi^2 \end{bmatrix} \text{ e } B = \begin{bmatrix} -1 & \xi \\ 2\xi^2 & 1 \end{bmatrix}$$

e ξ è una radice primitiva sesta dell'unità.
(a) Provare che l'insieme $G = HK$ è un sottogruppo di $GL_2(\mathbb{C})$.
(b) Descrivere gli elementi di G e calcolarne il periodo.
(c) Classificare, a meno di isomorfismi, il gruppo G.
(d) Calcolare tutti gli omomorfismi $D_6 \to G$.
Svolgimento

(a) Sappiamo che un prodotto di sottogruppi è ancora un sottogruppo se uno tra H e K è sottogruppo normale.
Osserviamo prima di tutto che dire che ξ è radice primitiva sesta dell'unità significa che è una radice del polinomio ciclotomico di ordine 6. Abbiamo

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

pertanto il polinomio ciclotomico di ordine 6 è $x^2 - x + 1$. Pertanto poiché ξ è radice di quest'ultimo polinomio, si ha che essa soddisfa la relazione

$$\xi^2 - \xi + 1 = 0$$

da cui

$$\xi^2 = \xi - 1.$$

Useremo quindi questa espressione per poter semplificare i calcoli nelle matrici. Prima di tutto calcoliamo l'ordine dei sottogruppi ciclici H e K, quindi

le potenze delle matrici A e B. Abbiamo dunque

$$A^2 = \begin{bmatrix} -\xi & 0 \\ -\xi - 1 & \xi^2 \end{bmatrix} \begin{bmatrix} -\xi & 0 \\ -\xi - 1 & \xi^2 \end{bmatrix} = \begin{bmatrix} \xi^2 & 0 \\ \xi - \xi^3 & \xi^4 \end{bmatrix} = \begin{bmatrix} \xi - 1 & 0 \\ \xi + 1 & -\xi \end{bmatrix}$$

$$A^3 = \begin{bmatrix} -\xi & 0 \\ -\xi - 1 & \xi^2 \end{bmatrix} \begin{bmatrix} \xi - 1 & 0 \\ \xi + 1 & -\xi \end{bmatrix} = \begin{bmatrix} -\xi^2 + \xi & 0 \\ \xi^3 + 1 & -\xi^3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$B^2 = \begin{bmatrix} -1 & \xi \\ 2\xi^2 & 1 \end{bmatrix} \begin{bmatrix} -1 & \xi \\ 2\xi^2 & 1 \end{bmatrix} = \begin{bmatrix} 1 + 2\xi & 0 \\ 0 & 1 + 2\xi^3 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$B^3 = \begin{bmatrix} -1 & \xi \\ 2\xi^2 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -\xi \\ -2\xi^2 & 1 \end{bmatrix}$$

$$B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

quindi $|H| = 3$ e $|K| = 4$. Vogliamo provare che uno dei sottogruppi è normale. Facciamo vedere che per ogni $h \in H$ e per ogni $k \in K$ risulta

$$hkh^{-1} \in K.$$

Calcoliamo

$$BAB^{-1} = BAB^3 = \begin{bmatrix} -1 & \xi \\ 2\xi^2 & 1 \end{bmatrix} \begin{bmatrix} -\xi & 0 \\ -\xi - 1 & \xi^2 \end{bmatrix} \begin{bmatrix} 1 & -\xi \\ -2\xi^2 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} \xi^2 & \xi^3 + 1 \\ -\xi + 1 - 2\xi^4 & -\xi \end{bmatrix} = A^2 \in H$$

ed è chiaro che da questa relazione segue

$$B^{-1}A^2B = A \in H$$

pertanto abbiamo che H è un sottogruppo normale, dunque HK risulta essere effettivamente un sottogruppo di $GL_2(\mathbb{C})$.
(b) Osserviamo che $H \cap K = \{I_2\}$, pertanto possiamo conlcudere che il gruppo

G non è altro che un prodotto semidiretto di H e K, ovvero $G = H \rtimes K$. Abbiamo dunque che $|G| = |H||K| = 3 \cdot 4 = 12$. Pertanto G è costituito da

$$G = \{I_2, A, A^2, B, B^2, B^3, AB, AB^2, AB^3, A^2B, A^2B^2, A^2B^3\}.$$

Cominciamo calcolando l'ordine degli elementi di H e K. Abbiamo chiaramente $o(A) = o(A^2) = 3$, $o(B) = o(B^3) = 4$ e $o(B^2) = 2$. Per calcolare i periodi delle matrici prodotto non è necessario svolgere esplicitamente i prodotti, ma è sufficiente sfruttare le relazioni trovate, ovvero $BAB^{-1} = A^2$ e $B^{-1}A^2B = A$.

$$(AB)^2 = (AB)(AB) = (AB)(B^{-1}A^2B)B = AIA^2B^2 = B^2$$

pertanto $(AB)^4 = B^4 = I$ e quindi AB ha periodo 4.

$$(A^2B)^2 = (A^2B)(A^2B) = (A^2B)(BAB^{-1}B) = A^2B^2A$$

$$= A^2(-I)A = (-I)(A^2)A = -I$$

da cui deduciamo che A^2B ha periodo 4.
Utilizzando lo stesso metodo abbiamo

- AB^2 ha periodo 6;
- AB^3 ha periodo 4;
- A^2B^2 ha periodo 6;
- A^2B^3 ha periodo 4.

(c) Chiaramente G non è un gruppo abeliano. Ad ordine 12 i gruppi non abeliani sono

$$D_6,\ A_4 \text{ e } T = \mathbb{Z}_3 \rtimes \mathbb{Z}_4,$$

allora è chiaro che G è isomorfo a T.
(d) Ricordiamo che il gruppo diedrale D_6 (in generale D_n) è un gruppo

presentato, ovvero può essere descritto come segue

$$D_n = \langle \sigma, \tau \mid \sigma^6 = \tau^2 = id,\, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle.$$

Pertanto per determinare gli omomorfismi da D_6 in G basterà assegnare in maniera opportuna le immagini dei generatori σ e τ. Queste assegnazioni devono essere coerenti con la definizione di omomorfismo, pertanto i periodi delle immagini devono essere divisori dei periodi di σ e τ rispettivamente. Devono inoltre essere ancora soddisfatte le identità verificate da σ e τ, ovvero

$$\phi(\tau)\phi(\sigma)\phi(\tau)^{-1} = \phi(\tau\sigma\tau^{-1}) = \phi(\sigma^{-1}) = \phi(\sigma)^{-1}.$$

Sappiamo che σ ha periodo 6 e quindi le possibili immagini sono date dagli elementi di G che hanno periodo divisore di 6. Allo stesso modo, essendo τ di periodo 2, le possibili immagini sono date dagli elementi di periodo divisore di 2. Dunque abbiamo le possibili assegnazioni

$$\sigma \to I, A, A^2, B^2 = -I, AB^2 = -A, A^2B^2 = -A^2$$

$$\tau \to I, B^2 = -I$$

ma chiaramente non possiamo fermarci qui, in quanto dobbiamo verificare la consistenza di questi possibili omomorfismi. Sappiamo che l'omomorfismo banale c'è sempre ed è quella mappa che manda tutti gli elementi nella matrice identica. Restano da considerare gli altri casi. Supponiamo $\phi(\tau) = I$, allora

- se $\phi(\sigma) = A$, allora $\phi(\tau\sigma\tau) = IAI = A \neq A^2 = A^{-1} = \phi(\sigma)^{-1}$, quindi questo non è un omomorfismo;
- se $\phi(\sigma) = A^2$, allora $\phi(\tau\sigma\tau) = IA^2I = A \neq A = (A^2)-1 = \phi(\sigma)^{-1}$, quindi non va bene;
- se $\phi(\sigma) = B^2 = -I$, allora $\phi(\tau\sigma\tau) = IB^2I = B^2 = (B^2)-1 = \phi(\sigma)^{-1}$, quindi si tratta di un omomorfismo;

- se $\phi(\sigma) = AB^2 = -A$, allora $\phi(\tau\sigma\tau) = IAB^2I = AB^2 = -A \neq (-A^2) = (AB^2)^{-1} = \phi(\sigma)^{-1}$, quindi questo non va bene;
- se $\phi(\sigma) = A^2B^2 = -A^2$, allora $\phi(\tau\sigma\tau) = IA^2B^2I = A^2B^2 = -A^2 \neq -A = (A^2B^2)^{-1} = \phi(\sigma)^{-1}$, quindi questo non va bene.

Supponiamo invece che $\phi(\tau) = -I$, allora

- se $\phi(\sigma) = A$, allora $\phi(\tau\sigma\tau) = (-I)A(-I) = A \neq A^2 = A^{-1} = \phi(\sigma)^{-1}$, quindi questo non è un omomorfismo;
- se $\phi(\sigma) = A^2$, allora $\phi(\tau\sigma\tau) = (-I)A^2(-I) = A \neq A = (A^2)-1 = \phi(\sigma)^{-1}$, quindi non va bene;
- se $\phi(\sigma) = B^2 = -I$, allora $\phi(\tau\sigma\tau) = (-I)B^2(-I) = B^2 = (B^2)-1 = \phi(\sigma)^{-1}$, quindi si tratta di un omomorfismo;
- se $\phi(\sigma) = AB^2 = -A$, allora $\phi(\tau\sigma\tau) = (-I)AB^2(-I) = AB^2 = -A \neq (-A^2) = (AB^2)^{-1} = \phi(\sigma)^{-1}$, quindi questo non va bene;
- se $\phi(\sigma) = A^2B^2 = -A^2$, allora $\phi(\tau\sigma\tau) = (-I)A^2B^2(-I) = A^2B^2 = -A^2 \neq -A = (A^2B^2)^{-1} = \phi(\sigma)^{-1}$, quindi questo non va bene.

Abbiamo in totale 3 omomorfismi da D_6 in G.

Esercizio 15. *Sia $G \subset \mathbb{S}_5$ il sottogruppo generato dalle permutazioni $\alpha = (13)(24)$ e $\beta = (45)$.*
(a) Calcolare l'ordine e gli elementi del sottogruppo G.
(b) Classificare il gruppo G a meno di isomorfismi.
(c) Calcolare le classi di coniugazione di G.
(d) Determinare l'ordine e gli elementi dei sottogruppi centralizzanti $C(\alpha)$, $C(\beta)$.
Svolgimento

(a) Per calcolare gli elementi del sottogruppo G devo iniziare facendo i prodotti tra α e β. Abbiamo quindi

- $\alpha\beta = (13)(24)(45) = (13)(245)$;

- $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \beta\alpha = (13)(254)$;
  Posto $\gamma = \alpha\beta$ è chiaro che in G troviamo tutte le sue potenze
- $\gamma^2 = (13)(245)(13)(245) = (245)^2 = (254)$;
- $(\gamma^2)^{-1} = (254)^{-1} = (245)$;
- $\gamma^3 = (13)(245)(254) = (13)$.

Restano da fare i prodotti del tipo $\alpha\gamma^i$, allora otteniamo

$$G = \big\{id, (13)(24), (45), (13)(245), (254), (13), (245), (13)(254), (13)(25),$$

$$(24), (13)(45), (25)\big\}$$

pertanto $|G|$=12. Per quanto riguarda i periodi degli elementi sappiamo che i cicli di lunghezza n hanno periodo n, quindi per esempio (13) ha periodo 2 e (254) ha periodo 3. Se invece abbiamo permutazioni scritte come prodotto di cicli disgiunti, allora il periodo è dato facendo il minimo comune multiplo dei periodi di ogni fattore. Per esempio (13)(24) ha periodo $2 = mcm(2, 2)$ e (13)(254) ha periodo $6 = mcm(2, 3)$.
(b) Chiaramente G non è un gruppo abeliano e sappiamo che, ad ordine 12, i gruppi non abeliani sono

$$D_6,\ A_4 \text{ e } T = \langle a, b \mid a^4 = b^3 = 1, aba^{-1} = b^{-1}\rangle.$$

Nel nostro gruppo G non ci sono elementi di periodo 4, pertanto possiamo escludere che sia isomorfo a T (in T l'elemento a ha periodo 4). Analogamente G non può essere isomorfo ad A_4 in quanto in A_4 non ci sono elementi di periodo 6. Allora $G \simeq D_6$.
(c) Poiché $G \subset \mathbb{S}_5$ le classi di coniugio sono contenute nei sottoinsiemi di elementi che hanno la stessa struttura ciclica. Prima di tutto suddividiamo gli elementi per struttura ciclica.

$$G = \{id, \Big/ (13), (24), (25), (45), \Big/ (245), (254), \Big/ (13)(24), (13)(25), (13)(45) \Big/$$

$$(13)(245), (13)(254)\}.$$

Dobbiamo ricordare che il numero di elementi di un'orbita (quindi di una classe di coniugio) divide l'ordine del gruppo. Inoltre gli elementi del centro hanno classi di coniugio ridotte ad un singolo elemento. Cerchiamo di capire quali sono gli elementi di $Z(G)$. Se guardiamo gli elementi di G è chiaro che (13) commuta con tutti quanti, pertanto $\{(13)\}$ è una classe di coniugazione. In questo caso potevamo anche utilizzare l'isomorfismo con D_6 e quindi $Z(G) \simeq Z(D_6) = \{id, (\sigma^{\frac{n}{2}})\}$, come già visto nell'esercizio 5. Allora le classi di coniugio di G sono:

- $\{id\}$
- $\{(13)\}$
- $\{(24), (25), (45)\}$
- $\{(245), (254)\}$
- $\{(13)(24), (13)(25), (13)(45)\}$
- $\{(13)(245), (13)(254)\}$.

(d) Ricordiamo che $C(\alpha) = \{g \in G \mid g\alpha g^{-1} = \alpha\}$ ed inoltre

$$|Co(\alpha)| = (G : C(\alpha))$$

ovvero il numero di elementi di una classe di coniugio è uguale all'indice del centralizzante. Allora abbiamo che

$$3 = |Co(\alpha)| = \frac{12}{|C(\alpha)|}$$

quindi $|C(\alpha)| = 4$. Analogamente per il centralizzante di β. Si ottiene dunque

$$C(\alpha) = \{id, (13)(24), (13), (24)\}$$

e

$$C(\beta) = \{id, (45), (13), (13)(45)\}.$$

Esercizio 16. *Si consideri il gruppo alterno $\mathbb{A}_4 \subset \mathbb{S}_4$ e la sua azione naturale sull'anello dei polinomi $P = \mathbb{K}[x_1, \ldots, x_4]$ tale che*

$$\sigma \cdot x_i = x_{\sigma(i)}$$

per ogni permutazione $\sigma \in \mathbb{A}_4$ ed ogni variabile x_i con $i = 1, \ldots, 4$. Si considerino inoltre i polinomi $f = x_1x_3 + x_2x_4$ e $g = x_1x_2x_4 + x_3^3$.
(a) Calcolare orbita e stabilizzatori dei polinomi f e g sotto l'azione di $\mathbb{A}_4$ sull'insieme P.
(b) Posto $H = Stab(f)$ e $K = Stab(g)$, provare che $\mathbb{A}_4$ è prodotto semidiretto dei sottogruppi H e K.
Svolgimento

(a) Ricordiamo che

$$\mathbb{A}_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243),$$

$$(12)(34), (13)(24), (14)(23)\}$$

Sappiamo inoltre che $Stab(f) = \{\sigma \in \mathbb{A}_4 \mid \sigma \cdot f = f\}$, allora

$$Stab(f) = \{id, (12)(34), (13)(24), (14)(23)\}$$

e

$$Stab(g) = \{id, (124), (142)\}.$$

(b) Per provare che $\mathbb{A}_4$ è prodotto semidiretto dei sottogruppi H e K dobbiamo provare che

- $\mathbb{A}_4 = HK$;
- $H \cap K = \{id\}$;
- Uno dei sottogruppi tra H e K è normale.

Ovviamente $\mathbb{A}_4 = HK$ ed inoltre $H \cap K = \{id\}$. Resta dunque da provare la normalità di uno dei due. Chiaro anche che H è normale, in quanto unione di classi di coniugazione.

Esercizio 17. *Si consideri l'ideale $I = (6 - 8i)$ nell'anello $\mathbb{Z}[i]$ degli interi di Gauss. Poniamo $A = \mathbb{Z}[i]/I$.*
(a) Stabilire se l'anello A è un dominio.
(b) Descrivere il reticolo degli ideali di A, specificando quali tra essi sono primi o massimali.
(c) Posto $J = (1 - 3i)$ e $B = \mathbb{Z}[i]/J$, costruire un omomorfismo di anelli $\phi : A \to B$.
(d) Stabilire se ϕ è surgettivo e calcolare il nucleo.
Svolgimento

(a) Poiché A è un anello quoziente, sappiamo che

$$A = \mathbb{Z}[i]/I \text{ è un dominio } \Leftrightarrow I \text{ è primo}$$

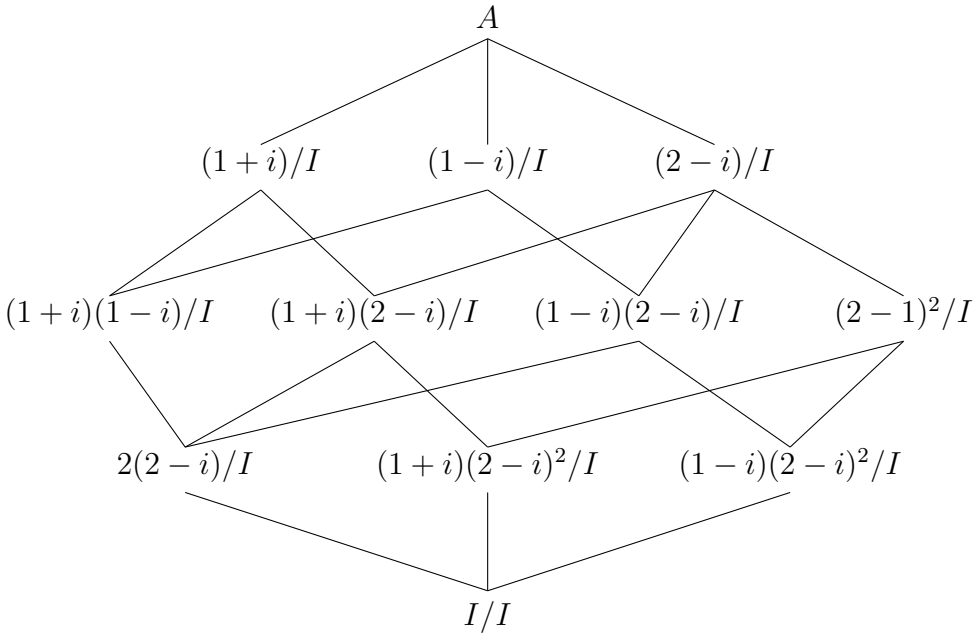
Osserviamo che $6 - 8i$ è fattorizzabile

$$6 - 8i = 2(3 - 4i) = (1 + i)(1 - i)(2 - i)^2$$

pertanto I non può essere primo. Allora A non è un dominio.
(b) Vogliamo ora descrivere gli ideali di A. Per il teorema di corrispondenza, gli ideali di $A = \mathbb{Z}[i]/I$ sono tutti e soli del tipo J/I dove J è un ideale di $\mathbb{Z}[i]$ tale che $I \subset J$. Ricordiamo che $\mathbb{Z}[i]$ è un dominio ad ideali principali (PID), pertanto ogni ideale J è generato da un elemento $a+ib \in \mathbb{Z}[i]$. Inoltre dobbiamo osservare che

$$I \subset J \Leftrightarrow a + ib \text{ divide } 6 - 8i$$

allora il reticolo degli ideali di A è il seguente



Sempre dal teorema di corrispondenza abbiamo che gli ideali primi sono

$$(1+i)/I,\ (1-i)/I \text{ e } (2-i)/I$$

ed è chiaro, dal reticolo, che questi ultimi sono pure massimali.
(c) Sia ora $J = (1-3i)$ e $B = \mathbb{Z}[i]/J$. Dobbiamo prima di tutto fattorizzare $1-3i$. Abbiamo quindi

$$1-3i = (1-i)(2-i)$$

allora, poiché $1-3i$ divide $6-8i$, risulta $I \subset J$. Sappiamo dai teoremi di isomorfismo che

$$A/J/I = \mathbb{Z}[i]/I \Big/ J/I \simeq \mathbb{Z}[i]/J = B$$

allora l'omomorfismo $\phi : A \to B$ è dato assegnando

$$a + ib + I \to a + ib + J$$

così come dal teorema.

(d) Chiaro che ϕ è surgettivo ma non ingettivo. Abbiamo quindi

$$ker(\phi) = \{a+ib+I \in A \mid a+ib+J = J\} = \{a+ib+I \mid a+ib \in J\} = J/I.$$

Esercizio 18. *Nell'anello $A = \mathbb{Z}[x]$ si consideri il seguente ideale*

$$I = (x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1, 3)$$

(a) Stabilire se l'ideale I è primo oppure massimale in A.
(b) Verificare che A/I è un anello finito e determinare il numero dei suoi elementi.
(c) Calcolare gli elementi nilpotenti di A/I.
(d) Stabilire se l'elemento $(x^2 - x - 1) + I$ è invertibile in A/I ed in tal caso calcolarne l'inverso.
Svolgimento

(a) Osserviamo che

$$I = (x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1, 3) = (x^5 + x^4 - x^3 - 1) + (x^4 + x^2 + 1) + (3)$$

pertanto $(3) \subset I$. Allora, per i teoremi di isomorfismo, sappiamo che

$$A/I = \mathbb{Z}[x]/I \simeq \mathbb{Z}[x]/(3) \Big/ I/(3).$$

Inoltre $I/(3) = (x^5+x^4-x^3-1, x^4+x^2+1, 3)/(3) = (x^5+x^4-x^3-1, x^4+x^2+1)$ (ideale in $\mathbb{Z}_3[x]$). Quindi poiché

$$A/I \simeq \mathbb{Z}_3[x]/(x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1)$$

possiamo ricondurre il nostro studio a quest'ultimo anello quoziente.
In generale in un PID abbiamo

$$(a_1, \ldots, a_m) = (a_1) + \cdots + (a_m) = (MCD(a_1, \ldots, a_m))$$

e

$$(a_1) \cap \cdots \cap (a_m) = (mcm(a_1, \ldots, a_m)).$$

Poiché $\mathbb{Z}_3[x]$ è un dominio ad ideali principali, possiamo dire che

$$J = (x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1) = \big(MCD(x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1)\big).$$

Per prima cosa dobbiamo fattorizzare i polinomi. Consideriamo $x^5 + x^4 - x^3 - 1 \in \mathbb{Z}_3[x]$. Chiaramente 1 è radice, allora abbiamo

	1	1	−1	0	0	−1
1		1	2	1	1	1
	1	2	1	1	1	0

da cui $x^5 + x^4 - x^3 - 1 = (x-1)(x^4 + 2x^3 + x^2 + x + 1)$. Quest'ultimo fattore ammette 1 come radice, allora

	1	2	1	1	1
1		1	0	1	2
	1	0	1	2	0

quindi $x^5 + x^4 - x^3 - 1 = (x-1)^2(x^3 + x + 2)$. L'ultimo fattore ammette 2 come radice

	1	0	1	2
2		2	4	4
	1	2	2	0

Quindi

$$x^5 + x^4 - x^3 - 1 = (x-1)^2(x+1)(x^2 + 2x + 2)$$

è la fattorizzazione in polinomi irriducibili del primo generatore. Per quanto riguarda il secondo generatore si ha

$$x^4 + x^2 + 1 = (x-1)^2(x+1)^2$$

allora $MCD(x^5 + x^4 - x^3 - 1, x^4 + x^2 + 1) = (x-1)^2(x+1)$. Pertanto l'ideale J è generato da un elemento non irriducibile e questo ci dice che

$\mathbb{Z}_3[x]/J$ non è un dominio di integrità. Ma allora, per isomorfismo, A/I non è un dominio di integrità e quindi I non può essere un ideale primo (né tantomeno massimale).
(b) Per dare una risposta al quesito (b) sfruttiamo l'isomorfismo

$$A/I \simeq \mathbb{Z}_3[x]/J.$$

Il quoziente $\mathbb{Z}_3[x]/J$ è costituito dalle classi laterali (modulo J) di polinomi in $\mathbb{Z}_3[x]$ che sono resti rispetto alla divisione per J $\big($ovvero per $f(x) = (x-1)^2(x+1)\big)$. Ma allora il grado di questi polinomi deve essere strettamente inferiore di $deg(f) = 3$. Dunque

$$\mathbb{Z}_3[x]/J = \{a + bx + cx^2 + J \mid a, b, c \in \mathbb{Z}_3\}.$$

Avendo un numero finito di scelte sui coefficienti a, b e c, è chiaro che A/I è un anello finito. Inoltre risulta

$$|A/I| = 3^3 = 27.$$

(c) Gli elementi nilpotenti di A/I non sono altro che gli elementi nilpotenti di $\mathbb{Z}_3[x]/J$ (per l'isomorfismo visto in precedenza). Allora $g(x) + (f(x)) \in \mathbb{Z}_3[x]/J$ è nilpotente se esiste $k \in \mathbb{N}$ tale che

$$(g(x))^k + (f(x)) = (f(x)) \Leftrightarrow (g(x))^k \in (f(x))$$

e questo equivale a dire che $f(x)$ divide una potenza di $g(x)$. Questo accade se ogni fattore irriducibile di $f(x)$ divide $g(x)$. Questo significa che gli elementi nilpotenti sono del tipo

$$(x-1)(x+1)q(x) + J,$$

ma poiché i rappresentanti hanno grado minore o uguale a 2, possiamo concludere che gli elementi nilpotenti sono

$$a(x-1)(x+1) + J.$$

(d) Per stabilire se l'elemento $(x^2-x-1)+I$ è invertibile in A/I, lo guardiamo come $(x^2-x-1)+J \in \mathbb{Z}_3[x]/J$. Sappiamo che

$$g(x)+(f(x)) \text{ è invertibile se } MCD(g(x),f(x))=1$$

allora basta calcolare il massimo comune divisore. Il polinomio x^2-x-1 ha grado 2 e non ha radici in $\mathbb{Z}_3$, pertanto è irriducibile. Allora è chiaro che $MCD(x^2-x-1,f(x))=1$, dunque

$$(x^2-x-1)+J$$

risulta essere invertibile in $\mathbb{Z}_3[x]/J$. Per calcolare il suo inverso dobbiamo scrivere l'identità di Bezout. Si ha che

$$f(x)-x(x^2-x-1)=1$$

da cui deduciamo che $-x+J$ risulta essere l'inverso di $x^2-x-1+J$.

Esercizio 19. *Nell'algebra $M_3(\mathbb{Q})$ si consideri la seguente matrice*

$$A=\begin{bmatrix}0 & 2 & 0\\ 1 & -1 & 0\\ 2 & 2 & -2\end{bmatrix}$$

e si consideri inoltre il seguente omomorfismo di $\mathbb{Q}$-algebre

$$\rho : \mathbb{Q}[x] \to M_3(\mathbb{Q})$$

$$x \to A$$

(a) Provare che ρ non è un omomorfismo ingettivo.
(b) Determinare il nucleo di ρ.
(c) Calcolare la $\mathbb{Q}$-dimensione della sottoalgebra $Im(\rho)=\mathbb{Q}[A] \subset M_3(\mathbb{Q})$ e descriverne una base.
(d) Stabilire se l'anello $\mathbb{Q}[A]$ è un dominio.
(e) Verificare se $\mathbb{Q}[A]$ contiene elementi nilpotenti.

Svolgimento

(a) Consideriamo il polinomio caratteristico della matrice A

$$p(x) = det(A - xI).$$

Il teorema di Cayley-Hamilton dice che ogni matrice quadrata è radice del suo polinomio caratteristico, ovvero

$$p(A) = 0,$$

allora $\rho(p(x)) = p(A) = 0$. Essendo $p(x) \neq 0$, si ha che $ker(\rho) \neq \{0\}$, quindi ρ non è ingettiva.
(b) Vogliamo ora determinare il nucleo di ρ. Poiché $\mathbb{Q}[x]$ è un dominio ad ideali principali, dobbiamo cercare un polinomio che sia generatore del nucleo, che ovviamente è un ideale. Per definizione il polinomio minimo $p_m(x)$ della matrice A è il polinomio monico di grado minimo, tale che $p_m(A) = 0$. Pertanto il polinomio minimo è proprio il generatore del nucleo di ρ. Calcoliamo il polinomio caratteristico di A ed in seguito il polinomio minimo.

$$p(x) = det(A - xI) = \begin{bmatrix} -x & 2 & 0 \\ 1 & -1-x & 0 \\ 2 & 2 & -2-x \end{bmatrix} =$$

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

Sappiamo che il polinomio minimo è un divisore, monico, di cui A è radice. Segue che

$$p_m(x) = (x+2)(x-1)$$

quindi $ker(\rho) = \big((x+2)(x-1)\big)$.
(c) Sappiamo dai teoremi di isomorfismo che

$$\mathbb{Q}[x]/ker(\rho) \simeq Im(\rho) = \mathbb{Q}[A]$$

pertanto la $\mathbb{Q}$-dimensione di $\mathbb{Q}[A]$ non è altro che la dimensione di $\mathbb{Q}[x]/ker(\rho)$

come spazio vettoriale su $\mathbb{Q}$. Osserviamo che $p_m(x)$ è un polinomio di grado 2 ed inoltre gli elementi di $\mathbb{Q}[x]/\big(p_m(x)\big)$ sono classi laterali, i cui rappresentanti sono resti della divisione per il polinomio $p_m(x)$. Allora

$$\mathbb{Q}[x]/\big(p_m(x)\big) = \{a + bx + (p_m(x)) \mid a, b \in \mathbb{Q}\}$$

da cui possiamo concludere che $dim_{\mathbb{Q}}\mathbb{Q}[A] = 2$. Chiaro che una base è data da $\{I, A\}$.
(d) Per stabilire se $\mathbb{Q}[A]$ è un dominio utilizziamo l'isomorfismo noto

$$\mathbb{Q}[A] \simeq \mathbb{Q}[x]/ker(\rho).$$

Sappiamo infatti che se R è un anello e I un suo ideale allora R/I è un dominio se, e solo se, I è un ideale primo. Chiaro che $ker(\rho)$ non può essere un ideale primo, in quanto generato da un polinomio non irriducibile. Allora $\mathbb{Q}[A]$ non è un dominio.
(e) Per stabilire se $\mathbb{Q}[A]$ contiene elementi nilpotenti possiamo considerare, per l'isomorfismo, gli elementi di

$$\mathbb{Q}[x]/\big(p_m(x)\big).$$

Un elemento $g(x) + (p_m(x))$ è nilpotente se esiste $n \in \mathbb{N}$ tale che $\big(g(x) + (p_m(x))\big)^n = (p_m(x))$, ovvero $g(x)^n \in (p_m(x))$. Questo accade se $p_m(x)$ divide una potenza opportuna di $g(x)$, ma allora ogni fattore irriducibile di $p_m(x)$ deve dividere $g(x)$. Allora gli elementi nilpotenti sono

$$(x + 2)(x - 1)q(x) + (p_m(x)),$$

ma $(x+2)(x-1)q(x) \in (p_m(x))$ e quindi otteniamo lo zero in $\mathbb{Q}[x]/\big(p_m(x)\big)$. Pertanto non ci sono elementi nilpotenti in $\mathbb{Q}[A]$.

Esercizio 20. *Sia R un anello commutativo unitario e siano I, $J \subset R$ due suoi ideali. Si ricordi che per definizione*

$$IJ = \langle fg \mid f \in I, g \in J\rangle \subset I \cap J.$$

Assumendo che $I + J = R$, dimostrare quanto segue.
(a) $IJ = I \cap J$.
(b) Per ogni b_1, $b_2 \in R$, il sistema di congruenze

$$\begin{cases} x \equiv b_1 \ mod \ I \\ x \equiv b_2 \ mod \ J \end{cases}$$

ammette sempre soluzione.
(c) L'omomorfismo di anelli

$$R \to R/I \times R/J$$

$$x \to (x + I, x + J)$$

è surgettivo.
(d) L'anello R/IJ è isomorfo a $R/I \times R/J$.
Svolgimento

(a) Dobbiamo provare $I \cap J \subset IJ$. Consideriamo $f \in I \cap J$, allora $f \in I$ e $f \in J$. Per ipotesi $I + J = R$ ed inoltre R è unitario, allora esitono $g \in I$ e $p \in J$ tali che $1 = g + p$. Ma allora

$$f = f \cdot 1 = f(g + p) = fg + fp \in IJ.$$

(b) Osserviamo che ciò che vogliamo provare non è altro che una generalizzazione del sistema di congruenze

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$

dove $MCD(m_1, m_2) = 1$. In questo caso a noi noto scriviamo l'identità di Bezout

$$1 = sm_1 + tm_2$$

ed otteniamo la soluzione

$$x = a_2 sm_1 + a_1 tm_2.$$

Nel nostro caso non abbiamo l'identità di Bezout, ma sappiamo che $I+J = R$, allora possiamo scrivere

$$1 = f + g$$

con $f \in I$ e $g \in J$, e quindi

$$x = b_2 f + b_1 g$$

è la soluzione del nostro sistema di congruenze.
(c) Consideriamo l'omomorfismo di anelli

$$\phi : R \to R/I \times R/J$$

$$x \to (x + I, x + J).$$

Vogliamo provare che è surgettivo, ovvero che per ogni $(a + I, b + J) \in R/I \times R/J$ esiste $x \in R$ tale che

$$\phi(x) = (a + I, b + J) \Leftrightarrow (x + I, x + J) = (a + I, b + J)$$

ovvero

$$\begin{cases} x \equiv a \bmod I \\ x \equiv b \bmod J \end{cases}$$

e dal punto (b) sappiamo che tale x esiste sempre. Pertanto ϕ è surgettivo.
(d) Consideriamo l'omomorfismo surgettivo

$$R/IJ \simeq R/I \times R/J$$

e calcoliamo il nucleo

$$ker(\phi) = \{x \in R \mid (x + I, x + J) = (I, J)\} = \{x \in R \mid x \in I \cap J\} = I \cap J.$$

Allora $ker(\phi) = I \cap J = IJ$ e, per i teoremi di isomorfismo, si ha

$$R/IJ \simeq R/I \times R/J.$$

Esercizio 21. *Sia A un anello commutativo unitario.*
(a) Sia $I \subsetneq A$ un ideale tale che $A - I \subset U(A)$. Provare che I è l'unico ideale massimale di A.
(b) Sia M un ideale massimale tale che $1 + x \in U(A)$ per ogni $x \in M$. Provare che M è l'unico ideale massimale di A.
Svolgimento

(a) Prima di tutto proviamo la massimalità di I. Sia dunque J un ideale di A tale che $I \subsetneq J$. Vogliamo provare che $J = A$. Poiché $I \subsetneq J$, possiamo dire che esiste $x \in J$ tale che $x \notin I$. Per ipotesi allora $x \in U(A)$, ovvero esiste $y \in A$ tale che $xy = 1$. D'altra parte, per definizione di ideale, $xy \in J$ e quindi $1 \in J$. Allora necessariamente $J = A$.
Proviamo ora l'unicità di I. Supponiamo per assurdo che esista un altro ideale massimale M diverso da I. Ma allora, essendo diversi, differiscono per almeno un elemento, quindi esiste $z \in M$ tale che $z \notin I$. Ma allora z è invertibile (in quanto $A - I \subset U(A)$) e quindi $M = A$. Ma questo è in contraddizione con l'ipotesi che M sia massimale.
(b) Per provare che M è l'unico ideale massimale di A cerchiamo di ricondurci al punto (a) appena provato. Allora vogliamo provare che

$$A - M \subset U(A).$$

Consideriamo dunque $y \notin M$, allora $M + (y)$ è un ideale di A ed inoltre

$$M \subsetneq M + (y).$$

Poiché M è massimale per ipotesi, abbiamo che

$$A = M + (y)$$

pertanto esitono $x \in M$ ed $s \in A$ tali che

$$1 = x + sy$$

da cui

$$sy = 1 - x \in U(A)$$

ma allora $y \in U(A)$. Allora la tesi segue dal punto (a).

Esercizio 22. *Sia A un anello commutativo unitario.*
(a) Siano I e J due ideali di A tali che $I \not\subset J$ e $J \not\subset I$. Provare che $I \cap J$ non è un ideale primo.
(b) Sia $I \subsetneq A$ un ideale. Provare che I è massimale se, e solo se, $I+(a) = A$ per ogni $a \in A$ e $a \notin I$.
Svolgimento

(a) Per definizione un ideale H è primo se

$$xy \in H \Rightarrow x \in H \text{ oppure } y \in H.$$

Noi vogliamo provare che $I \cap J$ non è primo. Siano $x \in I$ (quindi $x \notin J$) ed $y \in J$ (quindi $y \notin I$). Chiaro che $xy \in I \cap J$ (per le proprietà di ideale), ma nessuno tra x ed y appartiene ad $I \cap J$.
(b) Supponiamo che I sia massimale e consideriamo $a \in A - I$, allora $I + (a)$ è ideale di A ed inoltre

$$I \subsetneq I + (a).$$

Per la massimalità di I segue che $I + (a) = A$.
Supponiamo ora che $I + (a) = A$ per ogni $a \in A$, $a \notin I$. Se per assurdo I non è massimale, allora esiste $J \subsetneq A$ ideale tale che

$$I \subsetneq J \subsetneq A.$$

Allora è chiaro che esite $b \in J$ tale che $b \notin I$. Quindi

$$I \subsetneq I + (b) \subset J,$$

ma poiché $b \notin I$ dall'ipotesi abbiamo $I + (b) = A$ e quindi $J = A$. Ma questo è in contraddizione con l'ipotesi $J \subsetneq A$.

Esercizio 23. *Si consideri il polinomio* $f(x) = x^6 + 4x^4 + 16x^2 + 64 \in \mathbb{Q}[x]$.
(a) Calcolare il campo di spezzamento E *di* f *su* $\mathbb{Q}$.
(b) Descrivere una base di E *sul campo* $\mathbb{Q}$ *e calcolare la corrispondente tavola di moltiplicazione.*
(c) Determinare un elemento primitivo per l'estensione E.
Svolgimento

(a) Osserviamo che f non ha radici in $\mathbb{Q}$, infatti $f(x) > 0$ per ogni $x \in \mathbb{Q}$. Poniamo $y = x^2$ riconducendoci ad un polinomio di terzo grado

$$f(y) = y^3 + 4y^2 + 16y + 64$$

di cui calcoliamo le radici. Sappiamo che le radici sono da cercare tra gli elementi $\frac{r}{s}$ dove $r|64$ e $s|1$. Inoltre è chiaro che dobbiamo cercare tra quelle negative. Si ha che $f(-4) = -64 + 64 - 16 \cdot 4 + 64 = 0$, pertanto con il metodo di Ruffini abbiamo

	1	4	16	64
-4		-4	0	-64
	1	0	16	0

quindi la fattorizzazione di $f(x)$ è

$$f(x) = (x^2 + 4)(x^4 + 16)$$

dove $x^2 + 4$ ed $x^4 + 16$ sono polinomi irriducibili su $\mathbb{Q}$. Le radici di $x^2 + 4 = 0$ sono $\pm 2i$. Per quanto riguarda l'altro fattore irriducibile osserviamo che risolvere $x^4 + 16 = 0$ equivale a risolvere $x^4 + 1 = 0$ e successivamente moltiplicare le radici di quest'ultima per $\sqrt[4]{16} = 2$. Ma $x^4 + 1 = 0$ è il polinomio ciclotomico di ordine 8, allora indichiamo con ξ una radice primitiva ottava dell'unità, ovvero una radice di $x^4 + 1 = 0$.
Allora il campo di spezzamento di f su $\mathbb{Q}$ sarà dato estendendo $\mathbb{Q}$ con i e ξ, ovvero

$$E = \mathbb{Q}(i, \xi).$$

Possiamo però ricordare che le radici primitive ottave dell'unità sono

$$\left\{ \pm \frac{1+i}{\sqrt{2}}, \pm \frac{1-i}{\sqrt{2}} \right\}$$

ed ognuna di esse appartiene all'estensione $\mathbb{Q}(\xi)$. Ma allora anche

$$\frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} = \frac{2}{\sqrt{2}} = \sqrt{2} \in \mathbb{Q}(\xi)$$

e

$$\frac{1+i}{\sqrt{2}} - \frac{1-i}{\sqrt{2}} = \sqrt{2}i \in \mathbb{Q}(\xi)$$

da cui deduciamo che $i \in \mathbb{Q}(\xi)$. Questo quindi ci dice che il campo di spezzamento di f su $\mathbb{Q}$ è un'estensione semplice, ovvero

$$E = \mathbb{Q}(\xi).$$

(b) Per trovare una base di E sul campo $\mathbb{Q}$ dobbiamo valutare la dimensione dello spazio vettoriale $E = \mathbb{Q}(\xi)$. Sappiamo che

$$dim_{\mathbb{Q}} E = [E : \mathbb{Q}]$$

è data dal grado del polinomio minimo di ξ su $\mathbb{Q}$, quindi è uguale a 4. Allora una base di E su $\mathbb{Q}$ è data da

$$\left\{1, \xi, \xi^2, \xi^3\right\}$$

e la tavola di moltiplicazione è la seguente

	1	ξ	ξ^2	ξ^3
1	1	ξ	ξ^2	ξ^3
ξ	ξ	ξ^2	ξ^3	ξ^4
ξ^2	ξ^2	ξ^3	ξ^4	ξ^5
ξ^3	ξ^3	ξ^4	ξ^5	ξ^6

dove però dobbiamo normalizzare ξ^4, ξ^5, ξ^6, ovvero scriverle rispetto alla

base. Ricordando che ξ è radice primitiva ottava dell'unità abbiamo che $\xi^4 = -1$ e quindi $\xi^5 = -\xi$ e $\xi^6 = -\xi^2$.
(c) Nel punto precedente abbiamo già determinato un elemento primitivo, ovvero ξ.

Esercizio 24. *Si consideri il polinomio* $f(x) = x^5 - x^3 - x - 1 \in \mathbb{Z}_3[x]$.
(a) Calcolare il campo di spezzamento E *di* f *su* $\mathbb{Z}_3$.
(b) Determinare una base di E *sul campo* $\mathbb{Z}_3$.
(c) Calcolare la tavola di moltiplicazione di tale base.
(d) Esprimere le radici di f *come combinazioni lineari di tale base.*
Svolgimento

(a) Osserviamo che $f(x)$ ammette 2 come radice allora

	1	0	−1	0	−1	−1
2		2	4	0	0	−2
	1	2	0	0	−1	0

da cui

$$f(x) = (x-2)(x^4 + 2x^3 - 1).$$

Il polinomio $x^4 + 2x^3 - 1$ non ha radici in $\mathbb{Z}_3$, ma potrebbe fattorizzare come prodotto di due polinomi di secondo grado. Eseguiamo dunque la divisione in $\mathbb{Z}_3[x]$ di x^4+2x^3-1 per un generico polinomio monico di grado 2. Otteniamo

$$x^4 + 2x^3 - 1 = (x^2 + ax + b)\big(x^2 + (2-a)x + (2b + a + a^2)\big) +$$

$$(2ab + b + 2a^2 + 2a^3)x + (2 + b^2 + 2ab + 2a^2b)$$

ed imponiamo che il resto sia uguale a zero (in questo modo avremo la divisibilità). Allora dobbiamo risolvere un sistema di due equazioni nelle incognite a e b in $\mathbb{Z}_3$.

$$\begin{cases} 2ab + b + 2a^2 + 2a^3 = 0 \\ 2 + b^2 + 2ab + 2a^2b = 0 \end{cases}$$

Chiaramente questo sistema non ammette soluzione in $\mathbb{Z}_3$, pertanto x^4+2x^3-1 è un polinomio irriducibile. Ma allora il campo di spezzamento E non è altro che il campo di spezzamento di $g(x) = x^4+2x^3-1$, che essendo irriducibile in $\mathbb{Z}_3[x]$, può essere ottenuto estendendo $\mathbb{Z}_3$ con una radice qualunque di $g(x)$. Indichiamo quest'ultima con α, allora $E = \mathbb{Z}_(\alpha)$.
(b) Per determinare una base di E sul campo $\mathbb{Z}_3$ dobbiamo conoscere la dimensione di E come spazio vettoriale su $\mathbb{Z}_3$. Abbiamo

$$dim_{\mathbb{Z}_3} E = [E : \mathbb{Z}_3] = deg(g(x)) = 4$$

infatti $g(x)$ è il polinomio minimo di α su $\mathbb{Z}_3$. Allora una base di E su $\mathbb{Z}_3$ è data da

$$\{1, \alpha, \alpha^2, \alpha^3\}.$$

(c) La tavola di moltiplicazione di tale base è

	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	α^4
α^2	α^2	α^3	α^4	α^5
α^3	α^3	α^4	α^5	α^6

dove però dobbiamo normalizzare α^4, α^5, α^6, ovvero scriverle rispetto alla base. Per fare ciò dobbiamo effettuare la divisione dei polinomi x^4, x^5 ed x^6 rispetto a $g(x)$. Abbiamo dunque

$$x^4 = g(x)(1) + (-2x^3 + 1)$$

$$x^5 = g(x)(x-2) + (x^3 + x + 1)$$

$$x^6 = g(x)(x^2) + (x^2 - 2x + 1)(x^3 + x^2 - 2x + 1)$$

da cui

$$\alpha^4 = -2\alpha^3 + 1 = \alpha^3 + 1$$

$$\alpha^5 = \alpha^3 + \alpha + 1$$

$$\alpha^6 = \alpha^3 + \alpha^2 - 2\alpha + 1 = \alpha^3 + \alpha^2 + \alpha + 1.$$

(d) Esprimere le radici di f come combinazione lineare di tale base. Chiaramente 2 è una radice di $f(x)$ e le altre sono le radici di $g(x)$. Applicando l'automorfismo di Frobenius abbiamo che tutte le radici di $g(x)$ sono

$$\alpha, \alpha^3, \alpha^{3^2} = \alpha^9, \alpha^{3^3} = \alpha^{27},$$

quindi dobbiamo normalizzare α^9 e α^{27}. Dobbiamo dunque effettuare la divisione di x^9 per il polinomio $g(x)$

$$x^9 = g(x)(x^5 + x^4 + x^3 + x^2 + 2x) + (x^3 + x^2 + 2x)$$

da cui

$$\alpha^9 = \alpha^3 + \alpha^2 + 2\alpha.$$

Per ottenere α^{27} possiamo invece utilizzare le formule di Viete che riguardano la somma delle radici di un polinomio. Allora

$$\alpha + \alpha^3 + \alpha^9 + \alpha^{27} = 1$$

e quindi

$$\alpha^{27} = 1 - \alpha - \alpha^3 - \alpha^9 = \alpha^3 + 2\alpha^2 + 1.$$