SOLUZIONI DELL'APPELLO A DEL CORSO AL210 – ALGEBRA 2
1 FEBBRAIO 2019

(1) Si consideri il gruppo

$$G = \langle a, x | a^8 = 1, x^2 = 1, xa = a^3x \rangle.$$

(A) (3 punti) Dimostrare che ogni elemento di G si scrive in maniera unica nella forma (chiamata in seguito forma canonica)

$$a^k \text{ oppure } a^k x \text{ con } k \in \mathbb{Z}_8,$$

con la solita convenzione che $a^0 = 1$ è l'identità di G.
Soluzione:
Ogni elemento di G si scrive come una parola con lettere a, a^{-1}, x e x^{-1}, e dunque si scriverà nella forma

$$g = a^{i_1}x^{j_1}a^{i_2}x^{j_2}\dots a^{i_k}x^{j_k},$$

per un certo $k \in \mathbb{N}$ e certi elementi $i_1, j_1, \dots, i_k, j_k \in \mathbb{Z}$.
La prima relazione mi dice che posso considerare gli indici $i_1, \dots, i_k$ come elementi di $\mathbb{Z}_8$. La seconda relazione mi dice che posso semplificare l'espressione di g fino a ridurmi al caso $j_1, \dots, j_k \in \{0, 1\}$. Infine l'ultima relazione implica che

$$xa^k = a^{3k}x \quad \text{per ogni } k \in \mathbb{Z}_8, \tag{0.1}$$

e questo mi consente di semplificare l'espressione di g fino a ridurmi all'espressione in forma canonica $g = a^k$ oppure $g = a^k x$ con $k \in \mathbb{Z}_8$.
Osserviamo anche che l'espressione in forma canonica non si può ulteriormente semplificare perché non contiene sottoparole della forma a^8 oppure x^2 oppure xa.

(B) (3 punti) Determinare la tabella di moltiplicazione del gruppo G, cioè scrivere $(a^k x^i) \cdot (a^l x^j)$ (per $k, l \in \mathbb{Z}_8$ e $i, j = 0, 1$) in forma canonica.
Soluzione:
Usando l'equazione (0.1) e la relazione $x^2 = 1$, otteniamo che

$$\begin{cases} a^k a^l = a^{k+l}, \\ a^k(a^l x) = a^{k+l}x, \\ (a^k x)a^l = a^{k+3l}x, \\ (a^k x)(a^l x) = a^{k+3l}x^2 = a^{k+3l}. \end{cases} \tag{0.2}$$

(C) (3 punti) Calcolare l'ordine di ciascun elemento di G e scrivere il suo inverso in forma canonica.
Soluzione:
Usando (0.1) e la relazione $x^2 = 1$, l'inverso si calcola nel seguente modo

$$\begin{cases} (a^k)^{-1} = a^{-k}, \\ (a^k x)^{-1} = x^{-1}a^{-k} = xa^{-k} = a^{-3k}x. \end{cases} \tag{0.3}$$

Per calcolare l'ordine degli elementi della forma a^k, osserviamo che $\langle a\rangle$ è un sottogruppo di G isomorfo a $\mathbb{Z}_8$. Dunque l'ordine di a^k in G è come l'ordine di k in $\mathbb{Z}_8$ e dunque

$$o(a^k) = \frac{8}{\mathrm{mcd}\{8,k\}}.$$

Per calcolare l'ordine degli elementi $a^k x$, osserviamo che (usando (0.2))

$$(a^k x)^2 = a^{4k}, \quad (a^k x)^3 = a^{4k} a x = a^{5k} x, \quad (a^k x)^4 = (a^{4k})^2 = 1,$$

il che implica che

$$o(a^k x) = \begin{cases} 2 & \text{se } k \text{ è pari,} \\ 4 & \text{se } k \text{ è dispari.} \end{cases}$$

(D) (3 punti) Dimostrare che le classi di coniugio di G sono

$$\{1\}, \{a, a^3\}, \{a^2, a^6\}, \{a^5, a^7\}, \{a^4\}, \{a^k x \ : k \text{ è pari}\}, \{a^k x \ : k \text{ è dispari}\}.$$

Soluzione:

Calcoliamo gli automorfismi interni $I(a^k)$ e $I(a^k x)$ usando (0.3) e (0.2)

$$\begin{cases} I(a^k)(a^l) = a^{-k} a^l a^k = a^l, \\ I(a^k)(a^l x) = a^{-k} a^l x a^k = a^{l+2k} x. \end{cases}$$

$$\begin{cases} I(a^k x)(a^l) = a^{-3k} x a^l a^k x = a^{-3k} a^{3(k+l)} x^2 = a^{3l}, \\ I(a^k x)(a^l x) = a^{-3k} x a^l x a^k x = a^{-3k} a^{3l} x^2 a^k x = a^{3l-2k} x. \end{cases}$$

Come si vede dalle formule di sopra, la classe di coniugio di a^l è uguale a $\{a^l, a^{3l}\}$, mentre la classe di coniugio di $a^l x$ consiste di tutti gli elementi della forma $a^{l'} x$ con l ed l' che hanno la stessa parità. Ne segue che le classi di coniugio di G sono quelle dell'enunciato.

(E) (4 punti) Dimostrare che il centro di G è uguale a

$$Z(G) = \langle a^4 \rangle,$$

e che il quoziente $G/Z(G)$ è isomorfo a D_4.

Soluzione:

Il centro $Z(G)$ è costituito da tutti gli elementi di G che commutano con qualsiasi altro elemento o, equivalentemente, da tutti gli elementi $g \in G$ la cui classe di coniugio è $\{g\}$. Dal punto precedente si vede dunque che

$$Z(G) = \{1, a^4\} = \langle a^4 \rangle \cong \mathbb{Z}_2.$$

Per la seconda parte ci sono due dimostrazioni:

Prima dimostrazione:

Usando la proprietà universale dei gruppi definiti da generatori e relazioni, possiamo definire l'omomorfismo di gruppi

$$\begin{aligned} \Phi : G &\longrightarrow D_4 = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle, \\ a &\mapsto \sigma, \\ x &\mapsto \tau, \end{aligned}$$

che è ben definito siccome tutte le relazioni soddisfatte da a e x in G sono anche soddisfatte da σ e τ in D_4. L'omomorfismo Φ è suriettivo perché la sua immagine contiene i generatori σ e τ di D_4. Dunque, siccome $|G| = 16$ e $|D_4| = 8$, ne deduciamo che il nucleo di Φ deve avere cardinalità uguale a

2. Siccome $\Phi(a^4) = \sigma^4 = 1$, abbiamo che $Z(G) = \langle a^4 \rangle \subseteq \ker \Phi$ e dunque confrontando le loro cardinalità ne deduciamo che $Z(G) = \ker \Phi$. Ora il primo teorema di isomorfismo implica che

$$G/Z(G) \cong D_4.$$

Seconda dimostrazione:
Il quoziente $G/Z(G)$ ammette la seguente presentazione:

$$G/Z(G) = \langle a, x | a^8 = 1, x^2 = 1, xa = a^3x, a^4 = 1 \rangle = \langle a, x | a^4 = 1, x^2 = 1, xa = a^{-1}x \rangle.$$

Siccome tale presentazione è la stessa del gruppo D_4, si conclude che $G/Z(G) \cong D_4$.

(F) (4 punti) Dimostrare che il sottogruppo commutatore di G è uguale a

$$[G, G] = \langle a^2 \rangle,$$

e che il quoziente $G/[G, G]$ è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Soluzione:
Usando le formule (0.2) e (0.3) e la relazione (0.1), calcoliamo i commutatori di G:

$$\begin{cases} [a^k, a^l] = a^k a^l a^{-k} a^{-l} = 1, \\ [a^k, a^l x] = a^k a^l x a^{-k} a^{-3l} x = a^{k+l} a^{3(-k-3l)} x^2 = a^{-2k}, \\ [a^k x, a^l x] = a^k x a^l x a^{-3k} x a^{-3l} x = a^{k+3l} x^2 a^{-3k+3(-3l)} x^2 = a^{2(l-k)}. \end{cases} \tag{0.4}$$

Deduciamo che il sottogruppo commutatore di G è uguale a

$$[G, G] = \{1, a^2, a^4, a^6\} = \langle a^2 \rangle.$$

Per la seconda parte ci sono due dimostrazioni:
Prima dimostrazione:
Usando la proprietà universale dei gruppi definiti da generatori e relazioni, possiamo definire l'omomorfismo di gruppi

$$\begin{aligned} \Psi : G &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2, \\ a &\mapsto (1, 0), \\ x &\mapsto (0, 1), \end{aligned} \tag{0.5}$$

che è ben definito siccome tutte le relazioni soddisfatte da a e x in G sono anche soddisfatte da $(1, 0)$ e $(0, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$. L'omomorfismo Ψ è suriettivo perché la sua immagine contiene i generatori $(1, 0)$ e $(0, 1)$ di $\mathbb{Z}_2 \times \mathbb{Z}_2$. Dunque, siccome $|G| = 16$ e $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, ne deduciamo che il nucleo di Ψ deve avere cardinalità uguale a 4. Siccome $\Psi(a^2) = 2(1, 0) = (0, 0)$, abbiamo che $[G, G] = \langle a^2 \rangle \subseteq \ker \Psi$ e dunque confrontando le loro cardinalità ne deduciamo che $[G, G] = \ker \Psi$. Ora il primo teorema di isomorfismo implica che

$$G/[G, G] \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Seconda dimostrazione:
Il quoziente $G/[G, G]$ ammette la seguente presentazione:

$$G/[G, G] = \langle a, x | a^8 = 1, x^2 = 1, xa = a^3x, a^2 = 1 \rangle = \langle a, x | a^2 = 1, x^2 = 1, xa = ax \rangle.$$

Dunque $G/[G, G]$ è generato da due elementi di ordine 2 che commutano tra di loro. Quindi $G/[G, G]$ è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(G) (4 punti) Dimostrare che $[G,G]$ è l'unico sottogruppo normale di G di ordine 4.

Soluzione:

Sia H un sottogruppo normale di ordine 4. Allora il quoziente G/H è un gruppo di ordine 4 che è dunque abeliano per la classificazione dei gruppi finiti di ordine 4. Dunque per la proprietà universale del sottogruppo commutatore, abbiamo che $[G,G] \subseteq H$. Siccome $[G,G]$ ha ordine 4, deduciamo che $H = [G,G]$.

(H) (4 punti) Dimostrare che gli unici sottogruppi di G di ordine 8 sono

$$\begin{cases} H_1 = \langle a \rangle, \\ H_2 = \langle a^2, x \rangle, \\ H_3 = \langle a^2, ax \rangle. \end{cases}$$

Soluzione:

Sia H un sottogruppo di ordine 8. Siccome H ha indice 2 in G, allora H è un sottogruppo normale il cui quoziente è abeliano (in quanto isomorfo a $\mathbb{Z}_2$). Dunque H contiene $[G,G]$ per la proprietà universale del sottogruppo commutatore. Per il Teorema di Corrispondenza, H è l'immagine inversa di un unico sottogruppo di ordine 2 (automaticamente normale) di $G/[G,G]$ tramite la mappa quoziente $G \to G/[G,G]$. Tale mappa quoziente si identifica con la mappa Ψ in (0.5) per il punto (F). I sottogruppi di indice 2 di $\mathbb{Z}_2 \times \mathbb{Z}_2$ sono $\langle (1,0) \rangle$, $\langle (0,1) \rangle$ e $\langle (1,1) \rangle$, la cui immagini inverse tramite Ψ sono, rispettivamente, i sottogruppi H_1, H_2 e H_3.

(I) (5 punti) Per ciascuno dei sottogruppi H_i del punto precedente, si trovino tutti i sottogruppi (qualora esistano) S di G tali che G è isomorfo al prodotto semidiretto interno $H_i \rtimes S$.

Soluzione:

Siccome H_i ha indice 2, allora $G/H_i \cong \mathbb{Z}_2$. Dunque, per la caratterizzazione del prodotto semidiretto interno, avremo che $G = H_i \rtimes S$ se e solo se $S = \langle g \rangle$ con $g \in G$ di ordine 2 che non appartiene a H_i.

Gli elementi di ordine 2 di G sono $\{a^4, x, a^2x, a^4x, a^6x\}$ per il punto (C). Notiamo che H_2 contiene tutti questi elementi mentre H_1 e H_3 contengono solo a^4. Dunque abbiamo che

$$G \cong H_i \rtimes S \Leftrightarrow i = 1,3 \quad \text{e} \quad S = \langle g \rangle \ \text{ con } \ g = x, a^2x, a^4x, a^6x.$$

(J) (5 punti) Dimostrare che gli automorfismi di G sono della forma

$$\phi_{s,t}(a) = a^s \text{ e } \phi_{s,t}(x) = a^{2t}x$$

con $s \in (\mathbb{Z}_8)^*$ e $t \in \mathbb{Z}_4$. Dedurre che $|\operatorname{Aut}(G)| = 16$.

Soluzione:

Osserviamo prima che, per ogni $s \in \mathbb{Z}_8^*$ e $t \in \mathbb{Z}_4$, gli elementi a^s e $a^{2t}x$ generano G (perchè a^s genera $\langle a \rangle$ per le ipotesi su s) e soddisfano le relazioni

$$\begin{cases} (a^s)^8 = a^{8s} = 1, \\ (a^{2t}x)^2 = a^{2t}xa^{2t}x = a^{2t+6t}x^2 = 1, \\ (a^{2t}x)a^s = a^{2t+3s}x = (a^s)^3(a^{2t}x). \end{cases}$$

Dunque, per la proprietá universale delle presentazioni, per ogni $s \in \mathbb{Z}_8^*$ e $t \in \mathbb{Z}_4$ risulta ben definito un unico automorfismo $\phi_{s,t} \in \mathrm{Aut}(G)$ tale che

$$\phi_{s,t}(a) = a^s \text{ e } \phi_{s,t}(x) = a^{2t}x.$$

Mostriamo ora che gli automorfismi di cui sopra sono tutti e soli gli automorfismi di G. Sia $\phi \in \mathrm{Aut}(G)$. Osserviamo che $\phi(a)$ ha ordine 8, $\phi(x)$ ha ordine 2 e che $\phi(a)$ e $\phi(x)$ generano G perchè un automorfismo manda generatori in generatori e preserva l'ordine degli elementi. Dal punto (C) deduciamo che $\phi(a) = a^s$ con $s \in (\mathbb{Z}_8)^* = \{1, 3, 5, 7\}$. Inoltre $\phi(x)$ non può appartenere al sottogruppo $\langle \phi(a) \rangle = \langle a \rangle$ altrimenti $\phi(a)$ e $\phi(x)$ non sarebbero generatori di G. Dunque, sempre dal punto (C) deduciamo che $\phi(x) = a^{2t}x$ per un certo $t \in \mathbb{Z}_4$. Deduciamo che $\phi = \phi_{s,t}$ perché i due automorfismi assumono gli stessi valori sui generatori a e x di G.

(K) (5 punti) Dimostrare che $\mathrm{Aut}(G) \cong \mathbb{Z}_4 \rtimes_\theta (\mathbb{Z}_8)^*$, con $\theta : \mathbb{Z}_8^* \twoheadrightarrow (\mathbb{Z}_4)^* \cong \mathrm{Aut}(\mathbb{Z}_4)$ dove il primo omomorfismo è indotto dalla riduzione modulo 4 e il secondo isomorfismo è indotto dalla moltiplicazione degli elementi in $\mathbb{Z}_4$.

Soluzione:

Gli automorfismi di G sono tutti della forma $\phi_{s,t}$ come nel punto (J). La composizione di due tali automorfismi soddisfa

$$\begin{cases} (\phi_{s_1,t_1} \circ \phi_{s_2,t_2})(a) = \phi_{s_1,t_1}(a^{s_2}) = a^{s_1 s_2}, \\ (\phi_{s_1,t_1} \circ \phi_{s_2,t_2})(x) = \phi_{s_1,t_1}(a^{2t_2}x) = a^{2t_2 s_1} a^{2t_1} x = a^{2(s_1 t_2 + t_1)}x. \end{cases}$$

Dunque abbiamo che

$$\phi_{s_1,t_1} \circ \phi_{s_2,t_2} = \phi_{s_1 s_2, s_1 t_2 + t_1}, \tag{0.6}$$

da cui si deduce che

$$\mathrm{Aut}(G) = \mathbb{Z}_4 \rtimes_\theta (\mathbb{Z}_8)^*,$$

dove $\theta : \mathbb{Z}_8^* \twoheadrightarrow (\mathbb{Z}_4)^* \cong \mathrm{Aut}(\mathbb{Z}_4)$ è la composizione della riduzione modulo 4 con isomorfismo canonico indotto dalla moltiplicazione degli elementi in $\mathbb{Z}_4$.

(L) (5 punti) Dimostrare che tutti i sottogruppi normali di G sono anche caratteristici.

Soluzione:

Analizziamo l'azione degli automorfismi di G, descritti nel punto (J), sulle classi di coniugio di G, descritte nel punto (D), si deduce facilmente che:

- un automorfismo $\phi_{s,t}$ con $s = 1, 3$ fissa tutte la classi di coniugio;
- un automorfismo $\phi_{s,t}$ con $s = 5, , 7$ scambia $\{a, a^3\}$ con $\{a^5, a^7\}$, mentre fissa tutte la altri classi di coniugio.

Sia ora H un sottogruppo normale di G. Dunque H è unione di classi di coniugio. Notiamo che H contiene la classe $\{a, a^3\}$ se e solo se contiene la classe $\{a^5, a^7\}$, perchè $\langle a \rangle = \langle a^5 \rangle$. Dunque, per quanto detto sopra, se $\phi_{s,t} \in \mathrm{Aut}(G)$, allora $\phi_{s,t}(H) = H$, e dunque H è un sottogruppo caratteristico di G.

(2) Siano H un gruppo abeliano finito e sia $F = (F, +, \cdot, 0, 1)$ un campo.

(A) (4 punti) Dimostrare che H non è ciclico se e solo se H contiene un sottogruppo isomorfo a $\mathbb{Z}_p \oplus \mathbb{Z}_p$ per qualche primo p.

Soluzione:

Dimostriamo le due implicazioni separatamente.

- Assumiamo che H sia ciclico. Dalla struttura dei gruppi ciclici, sappiamo che allora ogni suo sottogruppo è ciclico. Dunque H non può contenere un sottogruppo isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$, che invece non è ciclico.
- Assumiamo che H non sia ciclico. Per il teorema di struttura dei gruppi abeliani finiti, sappiamo che H ammette una decomposizione della forma

$$H = \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}, \tag{0.7}$$

per certi numeri naturali unici $2 \leq n_1 | n_2 | \ldots | n_k$ (i fattori invarianti di H). Siccome H non è ciclico abbiamo che $k \geq 2$ e dunque, usando la decomposizione (0.7), segue che H contiene un sottogruppo isomorfo a $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. Sia p un primo che divide n_1, e dunque che divide anche n_2. Dalla struttura dei gruppi ciclici, sappiamo che $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ contiene un sottogruppo isomorfo a $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Dunque anche H conterrà un tale sottogruppo.

(B) (4 punti) Dimostrare che H è ciclico se e solo se, per ogni $n \in \mathbb{N}_{>0}$, H contiene al più n elementi di ordine che divide n.
Soluzione:
Dimostriamo le due implicazioni separatamente.
- Assumiamo che H sia ciclico, cioè $H \cong \mathbb{Z}_m$ per un certo $m \geq 1$. Per ogni $n \geq 1$, gli elementi di ordine che divide n sono tutti e soli gli elementi che appartengono al sottogruppo $\langle \frac{m}{\text{mcd}\{n.m\}} \rangle \subseteq \mathbb{Z}_m$. Dunque ci sono esattamente $\text{mcd}\{n, m\}$ tali elementi, e chiaramente $\text{mcd}\{n, m\} \leq n$, q.e.d.
- Assumiamo che H non sia ciclico. Per il punto (A), esiste un primo p tale che H contiene un sottogruppo L isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$. Osserviamo che L ha p^2 elementi e tutti hanno ordine che divide p. Dunque in H ci sono almeno p^2 elementi di ordine che divide p, q.e.d.

(C) (4 punti) Dimostrare che ogni sottogruppo finito di $(F^*, \cdot, 1)$ è ciclico.
Soluzione:
Sia G un sottogruppo finito di $(F^*, \cdot, 1)$. Per mostrare che G è ciclico, basta mostrare per il punto (B) che, per ogni $n \geq 1$, ci sono al più n elementi di ordine che divide n. Gli elementi di G di ordine che divide n sono radici del polinomio $X^n - 1 \in F[X]$, e ci sono al più n radici perché il polinomio ha grado n.

(3) Si considerino i seguenti sottoinsiemi di $\mathbb{C}$:

$$\begin{cases} \mathbb{Q}(\sqrt{-5}) := \{a + b\sqrt{-5} \ : a, b \in \mathbb{Q}\}, \\ \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \ : a, b \in \mathbb{Z}\}, \end{cases}$$

(A) (4 punti) Dimostrare che, rispetto alle operazioni $+$ e $\cdot$ indotte da $\mathbb{C}$, $\mathbb{Z}[\sqrt{-5}]$ è un dominio integrale con campo dei quozienti $\mathbb{Q}(\sqrt{-5})$.
Soluzione:
I sottoinsiemi $\mathbb{Z}[\sqrt{-5}]$ e $\mathbb{Q}(\sqrt{-5})$ di $\mathbb{C}$ sono sottoanelli unitari perché contengono 0 e 1 e vale che

$$\begin{cases} (a_1 + b_1\sqrt{-5}) + (a_2 + b_2\sqrt{-5}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-5}, \\ -(a + b\sqrt{-5}) = -a - b\sqrt{-5}, \\ (a_1 + b_1\sqrt{-5}) \cdot (a_2 + b_2\sqrt{-5}) = (a_1a_2 - 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-5}, \end{cases} \tag{0.8}$$

per ogni $a_1, b_1, a_2, b_2 \in \mathbb{Q}$. Dunque $\mathbb{Z}[\sqrt{-5}]$ è un dominio integrale, cioè non ha divisori non banali dello zero, perché tale proprietà è vera per $\mathbb{C}$.
Inoltre $\mathbb{Q}(\sqrt{-5})$ è un sottocampo di $\mathbb{C}$ perché dato un elemento $0 \neq x = a + b\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$ allora il suo inverso moltiplicativo è dato da

$$x^{-1} = \frac{\overline{x}}{N(x)} = \frac{a - b\sqrt{-5}}{a^2 + 5b^2} \in \mathbb{Q}(\sqrt{-5}),$$

dove $\overline{x}$ è il coniugio complesso di x e $N = ||.||^2 : \mathbb{C} \to \mathbb{R}_{\geq 0}$ è il quadrato della norma usuale $||.||$
Siccome abbiamo l'inclusione $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{Q}(\sqrt{-5})$ e $\mathbb{Q}(\sqrt{-5})$ è un campo per quanto mostrato prima, dalla proprietà universale del campo dei quozienti deduciamo che

$$Q(\mathbb{Z}[\sqrt{-5}]) \subseteq \mathbb{Q}(\sqrt{-5}).$$

Per concludere che l'inclusione di sopra è un'uguaglianza, basta mostrare che ogni elemento di $\mathbb{Q}(\sqrt{-5})$ si scrive come quoziente di due elementi di $\mathbb{Z}[\sqrt{-5}]$. Ma questo segue dal fatto che se $n_1/d_1 + n_2/d_2\sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$ con $n_1, n_2, d_1, d_2 \in \mathbb{Z}$ e $d_1, d_2 \neq 0$ allora

$$\frac{n_1}{d_1} + \frac{n_2}{d_2}\sqrt{-5} = \frac{n_1 d_2 + n_2 d_1\sqrt{-5}}{d_1 d_2},$$

e chiaramente $n_1 d_2 + n_2 d_1\sqrt{-5}, d_1 d_2 \in \mathbb{Z}[\sqrt{-5}]$.

(B) (4 punti) Mostrare che le unità di $\mathbb{Z}[\sqrt{-5}]$ sono date da

$$U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\}.$$

Soluzione:
Mostriamo innanzitutto che $z \in \mathbb{Z}[\sqrt{-5}]$ è un'unità se e solo se $N(z) = 1$. Infatti, se z è un'unità, allora esiste $w \in \mathbb{Z}[\sqrt{-5}]$ tale che $zw = 1$. Applicando la funzione N a questa equazione e usando la moltiplicatività di N, abbiamo la relazione $N(z) \cdot N(w) = N(1) = 1$ in $\mathbb{Z}$, da cui deduciamo che $N(z) = 1$ (usando che $N(z) \geq 0$). Viceversa, se $N(z) = 1$ allora l'inverso di z in $\mathbb{Q}(\sqrt{-5})$ è dato da

$$z^{-1} = \frac{\overline{z}}{N(z)} = \overline{z}$$

per il punto (A). Dunque tale inverso appartiene a $\mathbb{Z}[\sqrt{-5}]$ e quindi $z \in U(\mathbb{Z}[\sqrt{-5}])$.
Dunque, $z = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ è un'unità di $\mathbb{Z}[\sqrt{-5}]$ se e solo se

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1. \tag{0.9}$$

Le uniche soluzioni intere della equazione (0.9) sono $(a, b) = (\pm 1, 0)$, e dunque le uniche unità di $\mathbb{Z}[\sqrt{-5}]$ sono ± 1.

(C) (4 punti) Dimostrare che $\mathbb{Z}[\sqrt{-5}]$ non è un dominio a fattorizzazione unica.
Soluzione:
Si considerino le due fattorizzazioni di 6

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \tag{0.10}$$

e mostriamo che esse sono due fattorizzazioni in irriducibili non equivalenti.
Osserviamo che $N(2) = 4$, $N(3) = 9$ e $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. In $\mathbb{Z}[\sqrt{-5}]$ non esistono elementi di norma 2 o 3, perché le equazioni

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 2 \quad \text{e} \quad N(a + b\sqrt{-5}) = a^2 + 5b^2 = 3$$

non hanno soluzioni intere. Questo mostra che gli elementi 2, 3 e $1 \pm \sqrt{-5}$ sono irriducibili in $\mathbb{Z}[\sqrt{-5}]$, perchè se avessero dei divisori propri allora tali divisori avrebbero norma 2 o 3 (usando anche che $N(z) = 1$ se e solo se z è un'unità di $\mathbb{Z}[\sqrt{-5}]$, come mostrato nel punto (B).
Inoltre, nessuna coppia di elementi in $\{2, 3, 1 \pm \sqrt{-5}\}$ è associata perché le unità di $\mathbb{Z}[\sqrt{-5}]$ sono ± 1 per il punto (B).
Dunque, l'elemento 6 ammette due fattorizzazioni in irriducibili non equivalenti come in (0.10).