SOLUZIONI DELL'APPELLO B DEL CORSO AL210 – ALGEBRA 2
18 FEBBRAIO 2019

(1) Si consideri il gruppo
$$G = \langle a, x | a^8 = 1, x^2 = 1, xax = a^5 \rangle.$$

(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
$$xa^k = a^{5k} x \quad \text{per ogni } k \in \mathbb{Z}_8, \tag{0.1}$$
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 le formule 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
$$\begin{cases} a^k a^l = a^{k+l}, \\ a^k (a^l x) = a^{k+l} x, \\ (a^k x) a^l = a^{k+5l} x, \\ (a^k x)(a^l x) = a^{k+5l} x^2 = a^{k+5l}. \end{cases} \tag{0.2}$$

(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
$$\begin{cases} (a^k)^{-1} = a^{-k}, \\ (a^k x)^{-1} = x^{-1} a^{-k} = x a^{-k} = a^{-5k} x = a^{3k} x. \end{cases} \tag{0.3}$$

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 innanzitutto che l'ordine deve dividere l'ordine del gruppo G che è 16 (per il teorema di Lagrange). Dunque calcoliamo (usando (0.2))

$$(a^k x)^2 = a^{6k}, \quad (a^k x)^4 = (a^{6k} x)^2 = a^{12k} = a^{4k}, \quad (a^k x)^8 = (a^{4k})^2 = 1, \tag{0.4}$$

il che implica che

$$o(a^k x) = \begin{cases} 2 & \text{se } k = 0, 4, \\ 4 & \text{se } k = 2, 6, \\ 8 & \text{se } k = 1, 3, 5, 7. \end{cases}$$

(D) (4 punti) Determinare le classi di coniugio di G.
Soluzione:
Calcoliamo gli automorfismi interni $I(a^k)$ e $I(a^k x)$ usando (0.3) e (0.2)

$$\begin{cases} I(a^k)(a^l) = a^{-k} a^l a^k = a^l, \\ I(a^k)(a^l x) = a^{-k} a^l x a^k = a^{l+4k} x. \end{cases}$$

$$\begin{cases} I(a^k x)(a^l) = a^{3k} x a^l a^k x = a^{3k} a^{5(k+l)} x^2 = a^{5l}, \\ I(a^k x)(a^l x) = a^{3k} x a^l x a^k x = a^{3k} a^{5l} x^2 a^k x = a^{5l+4k} x. \end{cases}$$

Come si vede dalle formule di sopra, la classe di coniugio di a^l è uguale a $\{a^l, a^{5l}\}$, mentre la classe di coniugio di $a^l x$ è uguale a $\{a^l x, a^{l+4} x, a^{5l} x, a^{5l+4} x\}$. Dunque deduciamo che le classi di coniugio sono:

$$\{1\}, \{a, a^5\}, \{a^2\}, \{a^3, a^7\}, \{a^4\}, \{a^6\}, \{x, a^4 x\}, \{ax, a^5 x\}, \{a^2 x, a^6 x\}, \{a^3 x, a^7 x\}. \tag{0.5}$$

(E) (4 punti) Determinare il sottogruppo commutatore $[G, G]$ di G e mostrare che il quoziente $G/[G, G]$ è isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$.
Soluzione:
Usando le formule (0.2) e (0.3) e la relazione (0.1), calcoliamo i commutatori di G:

$$\begin{cases} [a^k, a^l] = a^k a^l a^{-k} a^{-l} = 1, \\ [a^k, a^l x] = a^k a^l x a^{-k} a^{3l} x = a^{k+l} a^{5(-k+3l)} x^2 = a^{-4k}, \\ [a^k x, a^l x] = a^k x a^l x a^{3k} x a^{3l} x = a^{k+5l} x^2 a^{3k+5(3l)} x^2 = a^{4(k+5l)}. \end{cases} \tag{0.6}$$

Deduciamo che il sottogruppo commutatore di G è uguale a

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

Per la seconda parte ci sono due dimostrazioni:
<u>Prima dimostrazione:</u>

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

$$\begin{aligned} \Psi : G &\longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2, \\ a &\mapsto (1,0), \\ x &\mapsto (0,1), \end{aligned} \tag{0.7}$$

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 $\mathbb{Z}_4 \times \mathbb{Z}_2$. L'omomorfismo Ψ è suriettivo perché la sua immagine contiene i generatori $(1,0)$ e $(0,1)$ di $\mathbb{Z}_4 \times \mathbb{Z}_2$. Dunque, siccome $|G| = 16$ e $|\mathbb{Z}_4 \times \mathbb{Z}_2| = 8$, ne deduciamo che il nucleo di Ψ deve avere cardinalità uguale a 2. Siccome $\Psi(a^4) = 4(1,0) = (0,0)$, abbiamo che $[G,G] = \langle a^4 \rangle \subseteq \ker \Psi$ e dunque confrontando le loro cardinalità ne deduciamo che $[G,G] = \ker \Psi$. Ora il primo teorema di isomorfismo implica che

$$G/[G,G] \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

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

$$G/[G,G] = \langle a, x | a^8 = 1, x^2 = 1, xa = a^5 x, a^4 = 1 \rangle = \langle a, x | a^4 = 1, x^2 = 1, xa = ax \rangle.$$

Dunque $G/[G,G]$ è generato da due elementi che commutano tra di loro e hanno ordine 4 e 2. Quindi $G/[G,G]$ è isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$.

(F) (5 punti) Dimostrare che gli unici sottogruppi non normali di G sono $U_1 := \langle x \rangle$ e $U_2 := \langle a^4 x \rangle$.

<u>Soluzione:</u>
Osserviamo che tutti i sottogruppi di G che contengono $[G,G]$ sono normali per il Teorema di corrispondenza e il fatto che $G/[G,G]$ è abeliano e dunque tutti i suoi sottogruppi sono normali. Dunque se U è un sottogruppo non normale di G, U non può contenere a^4. Dalle formule (0.4) e dalle formule di moltiplicazione in $\langle a \rangle \cong \mathbb{Z}_8$, deduciamo che

$$U \subseteq \{1, x, a^4 x\}.$$

Siccome x e $a^4 x$ hanno ordine 2 per il punto (C), gli unici sottogruppi di G contenuti in $\{1, x, a^4 x\}$ sono $U_1 := \langle x \rangle$ e $U_2 := \langle a^4 x \rangle$. Siccome x e $a^4 x$ sono coniugati per il punto (D), allora ne deduciamo che U_1 e U_2 non sono normali.

(G) (5 punti) Dimostrare che gli unici sottogruppi di G di ordine 4 sono

$$\begin{cases} H_1 = \langle a^2 \rangle, \\ H_2 = \langle a^2 x \rangle, \\ H_3 = \langle a^4, x \rangle. \end{cases}$$

<u>Soluzione:</u>
Sappiamo che ogni sottogruppo sottogruppo di ordine 4 è isomorfo a $\mathbb{Z}_4$ oppure $\mathbb{Z}_2 \times \mathbb{Z}_2$. Dal punto (C), sappiamo che gli elementi di G di ordine 4 sono $\{a^2, a^6, a^2 x, a^6 x\}$ e quelli di ordine 2 sono $\{a^4, x, a^4 x\}$. Dunque, siccome $(a^2)^3 = a^6$ e $(a^2 x)^3 = a^6 x$, ne deduciamo che i sottogruppi di G isomorfi a $\mathbb{Z}_4$ sono

$$\begin{cases} H_1 = \langle a^2 \rangle = \langle a^6 \rangle, \\ H_2 = \langle a^2 x \rangle = \langle a^6 x \rangle. \end{cases}$$

D'altra parte, siccome gli elementi in $\{a^4, x, a^4x\}$ commutano a due a due, e il prodotto di due di loro è uguale al terzo, allora abbiamo che l'unico sottogruppo di G isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ è

$$H_3 = \langle a^4, x\rangle = \{1, a^4, x, a^4x\}.$$

(H) (5 punti) Per ciascuno dei sottogruppi H_i del punto precedente, si dica se G/H_i è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ oppure $\mathbb{Z}_4$ e si determini se l'estensione

$$0 \to H_i \to G \to G/H_i \to 0$$

spezza.

Soluzione:

Calcoliamo i quozienti G/H_i usando la presentazione di G:

$$\frac{G}{H_1} = \langle a, x | a^8 = 1, x^2 = 1, xa = a^5x, a^2 = 1\rangle = \langle a, x | a^2 = 1, x^2 = 1, xa = ax\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2,$$
$$\frac{G}{H_2} = \langle a, x | a^8 = 1, x^2 = 1, xa = a^5x, x = a^{-2}\rangle = \langle a | a^4 = 1\rangle \cong \mathbb{Z}_4,$$
$$\frac{G}{H_3} = \langle a, x | a^8 = 1, x^2 = 1, xa = a^5x, a^4 = 1, x\rangle = \langle a, x | a^4 = 1\rangle \cong \mathbb{Z}_4.$$

Ora sappiamo che l'estensione

$$0 \to H_i \to G \to G/H_i \to 0 \tag{0.8}$$

spezza se e solo se esiste un sottogruppo A_i di G che si mappa isomorficamente su G/H_i tramite la restrizione del quoziente $G \to G/H_i$ a A_i. Ciò accade se e solo se A_i è un sottogruppo isomorfo a G/H_i tale che $A_i \cap H_i = \{1\}$. Dalla classificazione dei sottogruppi di ordine 4 del punto (G), sappiamo che ogni tale A_i deve essere uguale ad un sottogruppo della forma H_j. Tuttavia tutti i sottogruppi H_i contengono a^4, e dunque non esiste nessuna coppia (H_i, H_j) di sottogruppi di ordine 4 tale che $H_i \cap H_j = \{1\}$. Ne deduciamo che l'estensione (0.8) non spezza in nessun caso.

(I) (5 punti) Dimostrare che gli unici sottogruppi di ordine 8 di G sono

$$\begin{cases} L_1 = \langle a\rangle, \\ L_2 = \langle ax\rangle, \\ L_3 = \langle a^2, x\rangle. \end{cases}$$

Soluzione:

Ogni sottogruppo di ordine 8 è normale (perchè ha indice 2) e con quoziente isomorfo a $\mathbb{Z}_2$ e dunque abeliano. Dunque, per il Teorema di corrispondenza, ogni tale sottogruppo è l'immagine inversa tramite l'omomorfismo $\Psi : G \twoheadrightarrow G/[G,G] \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ di (0.7) di un sottogruppo di $\mathbb{Z}_4 \times \mathbb{Z}_2$ di indice 2. I sottogruppi di indice 2 di $\mathbb{Z}_4 \times \mathbb{Z}_2$ sono

$$\begin{cases} M_1 = \langle (1,0)\rangle \cong \mathbb{Z}_4, \\ M_2 = \langle (1,1)\rangle \cong \mathbb{Z}_4, \\ M_3 = \langle (2,0), (0,1)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2. \end{cases}$$

Usando la formula (0.7) per l'omomorfismo Ψ, deduciamo che $\Psi^{-1}(M_i) = L_i$ per ogni $i = 1, 2, 3$.

(J) (5 punti) Per ciascuno dei sottogruppi L_i del punto precedente, si dica se G è isomorfo al prodotto semidiretto interno $G = L_i \rtimes S_i$ per un qualche sottogruppo S_i.

Soluzione:

Sappiamo che $G \cong L_i \rtimes S_i$ per un qualche sottogruppo S_i se e solo se S_i è un sottogruppo isomorfo a G/L_i tale che $S_i \cap L_i = \{1\}$. Siccome $G/L_i \cong \mathbb{Z}_2$, S_i deve essere un gruppo ciclico generato da un elemento di ordine 2. Dal punto (C), sappiamo che gli elementi di G di ordine 2 sono $\{a^4, x, a^4x\}$. Dunque abbiamo che:

- Se $i = 1, 2$, siccome l'unico elemento di ordine 2 contenuto in L_i è a^4, allora $G \cong L_i \rtimes S_i$ con $S_i = \langle x \rangle$ oppure $S_1 = \langle a^4x \rangle$.
- Siccome L_3 contiene tutti gli elementi in $\{a^4, x, a^4x\}$, allora non esiste nessun sottogruppo S_3 tale che $G \cong L_3 \rtimes S_3$.

(2) Sia R un dominio a ideali principali.

Avvertenza: C'erano alcune imprecisioni nel testo, e cioè:

- si doveva assumere che R non fosse un campo;
- nel punto (B), M si doveva assumere diverso da (0);
- nel punto (C), a si doveva assumere diverso da 0.

Correggerò l'esercizio assumendo queste condizioni. Chi si è accorto di queste imprecisioni, ha ricevuto un punteggio più alto.

(A) (4 punti) Sia M un ideale di R. Dimostrare che le seguenti condizioni su M sono equivalenti:

(i) M è massimale,
(ii) M è primo e diverso da (0),
(iii) $M = (p)$ con p elemento irriducibile.

Soluzione:

$(i) \Rightarrow (ii)$: sia M un ideale massimale di R. Allora M è anche primo (perchè ogni ideale massimale è primo in un qualsiasi anello). Se per assurdo $M = (0)$, allora per ogni $0 \neq x \in R$ si avrebbe che $(0) \subsetneq (x)$ e dunque per la massimalità di M avremmo che $(x) = R$. Questo implica che x è invertibile, e dunque che R è un campo, che invece è escluso per ipotesi. Siccome R non è un campo, allora esiste un elemento $x \in R$ non nullo e non invertibile. Questo implica che $(0) \neq (x) \neq R$.

$(ii) \Rightarrow (iii)$: siccome R è un dominio a ideali principali, abbiamo che $M = (p)$. Dato che $M \neq (0), R$, allora abbiamo $p \neq 0$ e p non è un'unità di R. Inoltre siccome $M = (p)$ è un ideale primo, allora p è un elemento primo e dunque irriducibile (usando che R è un dominio integrale).

$(iii) \Rightarrow (i)$: sia $M = (p)$ con p irriducibile. Siccome $p \neq 0$ e p non è un'unità, allora $M \neq (0)$ e $M \neq R$. Se per assurdo M non fosse massimale, allora esisterebbe un ideale $N \neq R$ che contiene strettamente M. Siccome R è un dominio a ideali principale, allora $N = (q)$ per un certo q. L'ipotesi $N = (q) \neq R$ si traduce nel fatto che q non è un unità, mentre l'ipotesi che $M = (p) \subsetneq N = (q)$ si traduce nel fatto che q è un fattore proprio di p. Questo implicherebbe che p non è irriducibile, il che contraddice le ipotesi.

(B) (4 punti) Dimostrare che ogni ideale proprio di R si scrive come prodotto $M_1 \cdots M_n$ di ideali massimali, che sono univocamente determinati a meno dell'ordine.

Soluzione:

Sia M un ideale proprio di R e diverso da (0). Siccome R è un dominio a ideali principali, allora $M = (x)$ per un certo $x \in R$ non nullo e non un'unità di R. Siccome R è un dominio a fattorizzazione unica (essendo un dominio a ideali principali), x ammette una fattorizzazione in irriducibili

$$x \sim p_1 \dots p_n.$$

Ponendo $M_i = (p_i)$, la fattorizzazione di sopra si traduce in un'uguaglianza di ideali

$$M = M_1 \dots M_n,$$

e ciascun M_i è un ideale massimale per il punto (A).

(C) (4 punti) Sia $a \in R$. Dimostrare che:
- $R/(a)$ è un campo se a è un elemento primo.
- $R/(a)$ non è un dominio se a non è un elemento primo.

<u>Soluzione:</u>
Dalla teoria, sappiamo che:
- $R/(a)$ è un campo se e solo se (a) è un ideale massimale;
- $R/(a)$ non è un dominio se e solo se (a) non è un ideale primo.

Dunque concludiamo usando il punto (A) che implica che, siccome $a \neq 0$, allora (a) è massimale se e solo se (a) è primo se e solo se a è irriducibile se e solo se a è un elemento primo (per quest'ultima implicazione abbiamo usato che R è un dominio a fattorizzazione unica).

(3) Si consideri il seguente sottoanello unitario di $\mathbb{C}$

$$\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \ : a, b \in \mathbb{Z}\} \subseteq \mathbb{C},$$

e il suo campo dei quozienti

$$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \ : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

(A) (3 punti) Dimostrare che la funzione

$$\begin{aligned} \sigma : \mathbb{Z}[\sqrt{2}] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ a + b\sqrt{2} &\mapsto a - b\sqrt{2} \end{aligned}$$

è un isomorfismo unitario di anelli. Dedurre che la funzione

$$\begin{aligned} N : \mathbb{Z}[\sqrt{2}] &\longrightarrow \mathbb{Z} \\ x &\mapsto x \cdot \sigma(x) \end{aligned}$$

è moltiplicativa, cioè soddisfa $N(xy) = N(x)N(y)$ per ogni $x, y \in \mathbb{Z}[\sqrt{2}]$.

<u>Soluzione:</u>
La funzione σ è un omomorfismo unitario di anelli perché:

$$\begin{cases} \sigma((a + b\sqrt{2}) + (c + d\sqrt{2})) = (a + c) - (b + d)\sqrt{2} = \sigma(a + b\sqrt{2}) + \sigma(c + d\sqrt{2})), \\ \sigma((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) = \sigma((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = \\ = (a - b\sqrt{2}) \cdot (c - d\sqrt{2}) = \sigma(a + b\sqrt{2}) \cdot \sigma(c + d\sqrt{2}), \\ \sigma(1) = 1, \end{cases}$$

Inoltre σ è chiaramente iniettiva e suriettiva, e dunque è un isomorfismo unitario di anelli.
La funzione N è moltiplicativa perché

$$N(xy) = xy\sigma(xy) = xy\sigma(x)\sigma(y) = x\sigma(x)y\sigma(y) = N(x)N(y),$$

usando che σ è moltiplicativa e che l'anello $\mathbb{Z}[\sqrt{2}]$ è commutativo.

(B) (5 punti) Dimostrare che $\mathbb{Z}[\sqrt{2}]$ è un dominio Euclideo rispetto alla funzione

$$|N| : \mathbb{Z}[\sqrt{2}]^* \longrightarrow \mathbb{N}_{>0},$$
$$a + b\sqrt{2} \mapsto |N(a + b\sqrt{2})| = |a^2 - 2b^2|.$$

Soluzione:
Si considerino ora due elementi $x, y \in \mathbb{Z}[\sqrt{2}]$ con $y \neq 0$ e il loro quoziente $\frac{x}{y} = p + q\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Si scelgano due interi n e m tali che $|p - n| \leq 1/2$ e $|q - m| \leq 1/2$ e si ponga

$$r := x - y(n + m\sqrt{2}) = y\left[(p - n) + (q - m)\sqrt{2}\right] \in \mathbb{Z}[\sqrt{2}].$$

Ora calcoliamo la funzione $|N|$ applicata a r:

$$|N(r)| = \left|N(y)\left[(p - n)^2 - 2(q - m)^2\right]\right| \leq |N(y)|\left[|(p - n)^2| + |2(q - m)^2|\right] \leq$$
$$\leq |N(y)|\left[\frac{1}{4} + \frac{1}{2}\right] < N(y).$$

Dunque abbiamo ottenuto in $\mathbb{Z}[\sqrt{2}]$ una scrittura della forma

$$x = y(n + m\sqrt{2}) + r \quad \text{con } |N(r)| < |N(y)|,$$

e ciò mostra che $\mathbb{Z}[\sqrt{2}]$ è un dominio Euclideo rispetto a $|N|$.

(C) (5 punti) Mostrare che 2 è il prodotto di due irriducibili associati di $\mathbb{Z}[\sqrt{2}]$.

Soluzione:
Osserviamo innanzitutto che un elemento x di $\mathbb{Z}[\sqrt{2}]$ è un'unità se e solo se $N(x) = \pm 1$, come segue dalla moltiplicatività di N e dalla formula

$$x^{-1} = \frac{\sigma(x)}{N(x)} \in \mathbb{Q}(\sqrt{2}) \quad \text{se } x \neq 0. \tag{0.9}$$

Questo implica che ogni elemento di $\mathbb{Z}[\sqrt{2}]$ che ha norma uguale a $\pm p$, con p numero primo, è irriducibile.
Ora vale che

$$2 = (\sqrt{2})^2 \quad \text{e} \quad N(\sqrt{2}) = 2.$$

Dunque $\sqrt{2}$ è irriducibile e $2 = (\sqrt{2})^2$ è la fattorizzazione in irriducibili.

(D) (5 punti) Mostrare che 7 è il prodotto di due irriducibili non associati di $\mathbb{Z}[\sqrt{2}]$.

Soluzione:
Osserviamo che

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}) \quad \text{e } N(3 + \sqrt{2}) = N(3 - \sqrt{2}) = 7.$$

Dunque, per quanto osservato nel punto (B), gli elementi $3+\sqrt{2}$ e $3-\sqrt{2}$ sono irriducibili. Rimane da dimostrare che essi non sono associati. Per assurdo, supponiamo che $3 + \sqrt{2}$ e $3 - \sqrt{2}$ siano associati, cioè

$$3 + \sqrt{2} = u(3 - \sqrt{2}),$$

con u unità di $\mathbb{Z}[\sqrt{2}]$. Dunque usando la formula (0.9), abbiamo che

$$u = (3 + \sqrt{2})\frac{\sigma(3 - \sqrt{2})}{N(3 - \sqrt{2})} = (3 + \sqrt{2})\frac{3 + \sqrt{2}}{7} = \frac{11 + 6\sqrt{2}}{7} \in \mathbb{Q}(\sqrt{2}).$$

Chiaramente tale elemento u non appartiene a $\mathbb{Z}[\sqrt{2}]$ e questo è assurdo.

(E) (5 punti) Dimostrare che 3 è irriducibile in $\mathbb{Z}[\sqrt{2}]$.

Soluzione:

Supponiamo per assurdo che 3 non sia irriducibile. Allora 3 ammette un fattore non banale $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Siccome $N(3) = 9$, per quanto detto nel punto (B) dobbiamo avere che

$$N(x) = a^2 - 2b^2 = \pm 3.$$

Prendendo la congruenza modulo 3, abbiamo che

$$a^2 \equiv 2b^2 \mod 3 \tag{0.10}$$

Ora distinguiamo due casi:

- Se $b \not\equiv 0 \mod 3$ (e dunque $b \equiv \pm 1 \mod 3$), allora $b^2 \equiv 1 \mod 3$. L'equazione (0.10) implica che $a \not\equiv 0 \mod 3$, che similmente implica che $a^2 \equiv 1 \mod 3$. Ma allora l'equazione (0.10) non è soddisfatta, il che è assurdo.
- Se $b \equiv 0 \mod 3$, allora (0.10) implica che $a \equiv 0 \mod 3$. Dunque a e b sono entrambi divisibili per 3, il che implica che $N(x) = a^2 - 2b^2$ è divisibile per 9. Ma allora $N(x) \neq \pm 3$, il che è un assurdo.