SOLUZIONI DELLA SECONDA PROVA IN ITINERE DEL CORSO AL210
15 GENNAIO 2019

(1) (3 punti) Si consideri il sottoinsieme dei numeri complessi

$$\mathbb{Q}(\sqrt{-3}) := \{a + b\sqrt{-3} \ : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

Dimostrare che $\mathbb{Q}(\sqrt{-3})$ è un campo.

Soluzione:

Il sottoinsieme

$$\mathbb{Q}(\sqrt{-3}) := \{a + b\sqrt{-3} \ : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

di $\mathbb{C}$ è chiaramente un sottoanello unitario perché contiene 0 e 1 e vale che

$$\begin{cases} (a_1 + b_1\sqrt{-3}) + (a_2 + b_2\sqrt{-3}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-3}, \\ -(a + b\sqrt{-3}) = -a - b\sqrt{-3}, \\ (a_1 + b_1\sqrt{-3}) \cdot (a_2 + b_2\sqrt{-3}) = (a_1a_2 - 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-3}. \end{cases} \tag{0.1}$$

Inoltre è un sottocampo perché dato un elemento $0 \neq x = a + b\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$ allora il suo inverso moltiplicativo è dato da

$$x^{-1} = \frac{\overline{x}}{N(x)} = \frac{a - b\sqrt{-3}}{a^2 + 3b^2} \in \mathbb{Q}(\sqrt{-3}).$$

(2) (4 punti) Si consideri l'elemento

$$\omega := \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}). \tag{0.2}$$

Dimostrare che:

(i) ω è una radice del polinomio $X^2 + X + 1 \in \mathbb{C}[X]$;
(ii) $\overline{\omega} = \omega^2$;
(iii) le radici del polinomio $X^2 + X + 1$ sono ω e ω^2.
(iv) ω e ω^2 sono le due radici complesse terze non banali (cioè diverse da 1) dell'unità;

Soluzione:

Si verifica direttamente che l'elemento

$$\omega = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$$

è una radice del polinomio $X^2 + X + 1 \in \mathbb{C}[X]$. Siccome vale che $(X - 1)(X^2 + X + 1) = X^3 - 1$, allora ω è una radice terza dell'unità ed è chiaramente diversa dall'identità. Dunque, usando che ω ha norma quadrata $\omega\overline{\omega} = N(\omega) = 1$, otteniamo che

$$\omega^2 = \omega^{-1} = \overline{\omega}.$$

L'elemento ω^2 è anche esso una radice terza non banale dell'unità (diversa da ω), e dunque deve essere una radice del polinomio $X^2 + X + 1$ a causa della relazione $(X - 1)(X^2 + X + 1) = X^3 - 1$. Siccome $X^2 + X + 1$ ha grado due, le sue uniche radici sono ω e ω^2.

(3) (4 punti) Si considerino i due sottoinsiemi di $\mathbb{C}$:

$$\begin{cases} \mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \ : a, b \in \mathbb{Z}\}, \\ \mathbb{Z}[\omega] := \{a + b\omega \ : a, b \in \mathbb{Z}\}. \end{cases}$$

Dimostrare che $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega]$ sono due domini integrali (rispetto all'addizione e la moltiplicazione indotte da $\mathbb{C}$) con campo dei quozienti $\mathbb{Q}(\sqrt{-3})$.

Soluzione:

Il sottoinsieme $\mathbb{Z}[\sqrt{-3}]$ è un sottoanello unitario (e dunque un dominio) di $\mathbb{C}$ perché contiene 0, 1 e valgono le formule (0.1).

Il sottoinsieme $\mathbb{Z}[\omega]$ è un sottoanello unitario (e dunque un dominio) di $\mathbb{C}$ perché contiene 0, 1 e valgono le formule (usando che $\omega^2 = -\omega - 1$ per il punto (2)):

$$\begin{cases} (a_1 + b_1\omega) + (a_2 + b_2\omega) = (a_1 + a_2) + (b_1 + b_2)\omega, \\ -(a + b\omega) = -a - b\omega, \\ (a_1 + b_1\omega) \cdot (a_2 + b_2\omega) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1 - b_1b_2)\omega. \end{cases} \tag{0.3}$$

Vale l'inclusione $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega]$ perchè:

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\omega \ : b \text{ è pari}\}.$$

Siccome abbiamo delle inclusioni $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\omega] \subset \mathbb{Q}(\sqrt{-3})$ e $\mathbb{Q}(\sqrt{-3})$ è un campo per il punto (1), dalla proprietà universale del campo dei quozienti deduciamo che

$$Q(\mathbb{Z}[\sqrt{-3}]) \subseteq Q(\mathbb{Z}[\omega]) \subset \mathbb{Q}(\sqrt{-3}).$$

Per concludere che le inclusioni di sopra sono delle uguaglianze, basta mostrare che ogni elemento di $\mathbb{Q}(\sqrt{-3})$ si scrive come quoziente di due elementi di $\mathbb{Z}[\sqrt{-3}]$. Ma questo segue dal fatto che se $n_1/d_1 + n_2/d_2\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$ con $n_1, n_2, d_1, d_2 \in \mathbb{Z}$ e $d_1, d_2 \neq 0$ allora

$$\frac{n_1}{d_1} + \frac{n_2}{d_2}\sqrt{-3} = \frac{n_1d_2 + n_2d_1\sqrt{-3}}{d_1d_2}.$$

(4) (5 punti)

Si dimostri che un elemento di $\mathbb{Q}(\sqrt{-3})$ soddisfa un'equazione quadratica monica a coefficienti in $\mathbb{Z}$, cioè un'equazione della forma $X^2 + BX + C = 0$ con $B, C \in \mathbb{Z}$, se e solo se appartiene a $\mathbb{Z}[\omega]$.

Soluzione:

Fissiamo un elemento $z = a + b\sqrt{-3}$ con $a, b \in \mathbb{Q}$. Distinguiamo due casi:

Caso I: $z \in \mathbb{Q}$.

In questo caso, z è radice del polinomio $X^2 + BX + C$ con $B, C \in \mathbb{Z}$ se e solo se esiste $w \in \mathbb{Q}$ tale che

$$X^2 + BX + C = (X - z)(X - w) = X^2 - (z + w)X + zw. \tag{0.4}$$

Scriviamo $z = \frac{n}{m}$ con $n, m \in \mathbb{Z}$ coprimi e $w = \frac{h}{k}$ con $h, k \in \mathbb{Z}$ coprimi. Allora l'equazione (0.4) è soddisfatta per certi $B, C \in \mathbb{Z}$ se e solo se

$$mk|(nk + hm) \quad \text{e} \quad mk|nh. \tag{0.5}$$

Queste due condizioni implicano che

$$\begin{cases} m|k \quad \text{e} \quad m|h, \\ k|m \quad \text{e} \quad k|n. \end{cases}$$

Questo implica, usando che n e m sono coprimi e che h e k sono coprimi, che $m = \pm 1$ e $k = \pm 1$. Questo si traduce nel fatto che $z, w \in \mathbb{Z}$ e conclude la dimostrazione in questo caso.

Caso II: $z \notin \mathbb{Q}$.

Osserviamo che se z è radice del polinomio $X^2 + BX + C$ con $B, C \in \mathbb{Z}$ allora anche $\overline{z}$ è una radice dello stesso polinomio. Dunque, siccome $z \neq \overline{z}$, z è radice di un polinomio $X^2 + BX + C$ con $B, C \in \mathbb{Z}$ se e solo se

$$X^2 + BX + C = (X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + 3b^2),$$

e dunque se e solo se

$$2a \in \mathbb{Z}, \tag{0.6}$$

$$a^2 + 3b^2 \in \mathbb{Z}. \tag{0.7}$$

L'equazione (0.6) è soddisfatta se e solo se

$$a = \frac{\alpha}{2} \quad \text{con } \alpha \in \mathbb{Z}. \tag{0.8}$$

Usando questa condizione e scrivendo $b = n/m$ con $n, m \in \mathbb{Z}$ tali che $\mathrm{mcd}(n, m) = 1$, allora l'equazione (0.7) è soddisfatta se e solo se

$$\frac{\alpha^2}{4} + 3\frac{n^2}{m^2} \in \mathbb{Z}, \quad \text{o equivalentemente } 4m^2 | (\alpha^2 m^2 + 12n^2). \tag{0.9}$$

La condizione (0.9) implica che $m^2 | 12n^2$ e questo forza $m = 1$ o 2 (usando che n e m sono coprimi).

- Se $m = 1$, allora la condizione (0.9) si riduce a $4|\alpha^2$, e cioè α pari. Dunque in tal caso abbiamo che $a, b \in \mathbb{Z}$.
- Se invece $m = 2$, allora la condizione (0.9) si riduce a $4|(\alpha^2 + 3n^2)$, e questo è verificato, usando che n è dispari, se e solo se α è dispari. Dunque in tal caso abbiamo che $a = \alpha/2$ e $b = n/2$ con α e n dispari.

I due casi precedenti equivalgono a dire che $z = a + b\sqrt{-3} \in \mathbb{Z}[\omega]$, come segue dalla seguente descrizione

$$\mathbb{Z}[\omega] = \left\{ \frac{c + d\sqrt{-3}}{2} \ : c, d \in \mathbb{Z} \text{ e } \ c \equiv d \mod 2 \right\}.$$

(5) (5 punti) Dimostrare che $\mathbb{Z}[\sqrt{-3}]$ non è un dominio a fattorizzazione unica.

Soluzione:

Si consideri l'elemento $\omega \in \mathbb{Q}(\sqrt{-3})$. Siccome $\mathbb{Q}(\sqrt{-3})$ è il campo dei quozienti di $\mathbb{Z}[\sqrt{-3}]$ per il punto (3), allora possiamo scrivere $\omega = \frac{x}{y}$ con $x, y \in \mathbb{Z}[\sqrt{-3}])$. Siccome $\omega \notin \mathbb{Z}[\sqrt{-3}]$, allora y non è un'unità di $\mathbb{Z}[\sqrt{-3}]$. Inoltre, a meno di semplificare la frazione $\frac{x}{y}$, possiamo sempre supporre che $\mathrm{mcd}(x, y) \sim 1$ in $\mathbb{Z}[\sqrt{-3}]$. Sostituendo l'espressione $\omega = \frac{x}{y}$ nell' $X^2 + X + 1 = 0$, che è soddisfatta da ω per il punto (2), si deduce che $y|x^2$. Dunque $\mathrm{mcd}(x^2, y) = y \not\sim 1$. Ora questo implica che $\mathbb{Z}[\sqrt{-3}]$ non è un UFD perché in tali domini se $\mathrm{mcd}(x, y) \sim 1$ allora anche $\mathrm{mcd}(x, y^2) \sim 1$.

(6) (5 punti) Dimostrare che $\mathbb{Z}[\omega]$ è un dominio Euclideo rispetto alla funzione $N = ||.||^2$ che è esplicitamente data da:

$$\begin{aligned} N : \mathbb{Z}[\omega]^* &\longrightarrow \mathbb{N}_{>0}, \\ a + b\omega &\mapsto a^2 - ab + b^2. \end{aligned} \tag{0.10}$$

Soluzione:

Innanzitutto, usando che $\overline{\omega} = \omega^2 = -\omega - 1$ e $\omega^3 = 1$ per il punto (2), la funzione N è data da

$$N(a+b\omega) = (a+b\omega)(a+b\overline{\omega}) = (a+b\omega)(a+b\omega^2) = a^2 + ab\omega + ab\omega^2 + b^2\omega^3 = a^2 + b^2 - ab.$$

Si considerino ora due elementi $x, y \in \mathbb{Z}[\omega]$ con $y \neq 0$ e il loro quoziente $\frac{x}{y} = p + q\omega \in \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. Si scelgano due interi n e m tali che $|p-n| \leq 1/2$ e $|q-m| \leq 1/2$ e si ponga

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

La norma di r sarà data da

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

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

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

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

(7) (4 punti) Mostrare che le unità di $\mathbb{Z}[\omega]$ sono date da

$$U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}.$$

Soluzione:

Mostriamo innanzitutto che $z \in \mathbb{Z}[\omega]$ è un'unità se e solo se $N(z) = 1$. Infatti, se z è un'unità, allora esiste $w \in \mathbb{Z}[\omega]$ 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 $\mathbb{Q}(\sqrt{-3})$ è dato da

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

per il punto (1). Dunque tale inverso appartiene a $\mathbb{Z}[\omega]$ e quindi $z \in U(\mathbb{Z}[\omega])$.

Dunque, usando l'espressione (0.10), segue che $z = a + b\omega \in \mathbb{Z}[\omega]$ è un'unità di $\mathbb{Z}[\omega]$ se e solo se

$$N(a+b\omega) = a^2 - ab + b^2 = 1. \tag{0.11}$$

Ora cerchiamo le soluzioni di (0.11) distinguendo vari casi:

- Se $ab = 0$ allora (0.11) equivale a $1 = a^2 + b^2$ e dunque abbiamo le soluzioni $(a,b) = (0, \pm 1)$ o $(\pm 1, 0)$.
- Se $ab < 0$ allora (0.11) implica che $1 = a^2 - ab + b^2 > a^2 + b^2$ che forza $(a,b) = (0,0)$, il che dà origine ad un assurdo.
- Se $ab > 0$ allora (0.11) implica che $1 = a^2 - ab + b^2 > a^2 - 2ab + b^2 = (a-b)^2$, il che implica $a = b = \pm 1$.

Le 6 soluzioni cercate corrispondono (usando che $\omega^2 = -\omega - 1$) agli elementi $\{\pm 1, \pm\omega, \pm\omega^2 = \pm(\omega+1)\}$.

(8) (5 punti) Dimostrare che la mappa

$$\Phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\omega],$$
$$p(X) \mapsto p(\omega),$$

è un omomorfismo unitario di anelli che è suriettivo e il cui nucleo è l'ideale principale $(X^2 + X + 1)$.

Dedurre che Φ induce un isomorfismo unitario di anelli

$$\Phi : \frac{\mathbb{Z}[X]}{(X^2+X+1)} \xrightarrow{\cong} \mathbb{Z}[\omega],$$
$$[p(X)] \mapsto p(\omega),$$

Soluzione:

La seconda asserzione segue dalla prima e dal Teorema di fattorizzazione degli omomorfismi di anelli.

Dunque è sufficiente dimostrare la prima asserzione. La mappa Φ è la sostituzione della variabile X con il valore ω e dunque è chiaro che Φ è un omomorfimo unitario di anelli. Il fatto che Φ è suriettivo segue dalla definizione di $\mathbb{Z}[\omega]$.

Rimane da dimostrare che $\operatorname{Ker}\Phi = (X^2+X+1)$. Dal punto (2), segue che X^2+X+1 appartiene al nucleo di Φ. Viceversa, sia $p(X) \in \operatorname{Ker}\Phi$, cioè $p(\omega)=0$, e mostriamo che $p(X)$ é divisibile per X^2+X+1.

Daremo due dimostrazioni, la prima più elementare ma con più conti, la seconda più concettuale e con meno conti.

PRIMA DIMOSTRAZIONE

Scriviamo $p(X) = \sum_{h=0}^{N} a_h X^h$, con $N = \deg p \geq 0$. Dal punto (2) deduciamo che

$$\omega^h = \begin{cases} 1 & \text{se } h \equiv 0 \mod 3, \\ \omega & \text{se } h \equiv 1 \mod 3, \\ \omega^2 = -1-\omega & \text{se } h \equiv 2 \mod 3. \end{cases} \tag{0.12}$$

Dunque, distinguendo i coefficienti di $p(X)$ a seconda della loro congruenza modulo 3, calcoliamo l'elemento $p(\omega) \in \mathbb{Z}[\omega]$:

$$p(\omega) = \left(\sum_{i=0}^{\lfloor \frac{N}{3} \rfloor} a_{3i} - \sum_{k=0}^{\lfloor \frac{N-2}{3} \rfloor} a_{3k+2} \right) + \left(\sum_{j=0}^{\lfloor \frac{N-1}{3} \rfloor} a_{3j+1} - \sum_{k=0}^{\lfloor \frac{N-2}{3} \rfloor} a_{3k+2} \right) \omega$$

Dunque l'ipotesi $p(\omega)=0$ si traduce nelle due uguaglianze

$$\sum_{i=0}^{\lfloor \frac{N}{3} \rfloor} a_{3i} = \sum_{k=0}^{\lfloor \frac{N-2}{3} \rfloor} a_{3k+2} \quad \text{e} \quad \sum_{j=0}^{\lfloor \frac{N-1}{3} \rfloor} a_{3j+1} = \sum_{k=0}^{\lfloor \frac{N-2}{3} \rfloor} a_{3k+2}. \tag{0.13}$$

D'altra parte la tesi a cui vogliamo arrivare è che $p(X)$ è divisibile per X^2+X+1, e cioè che esista un polinomio $q(X) = \sum_{m=0}^{N} b_m X^m$ (necessariamente di grado minore o uguale a $N-2$) tale che

$$p(X) = (X^2+X+1)q(X).$$

Esplicitando questa equazione, otteniamo che i coefficienti b_m devono essere dati dalla formula

$$b_m = \sum_{s=0}^{\lfloor \frac{m}{3} \rfloor} a_{m-3s} - \sum_{t=0}^{\lfloor \frac{m-1}{3} \rfloor} a_{m-1-3t},$$

e devono valere le due condizioni che

$$0 = \sum_{s=0}^{\lfloor \frac{N}{3} \rfloor} a_{N-3s} - \sum_{t=0}^{\lfloor \frac{N-1}{3} \rfloor} a_{N-1-3t} \quad \text{e} \quad 0 = \sum_{s=0}^{\lfloor \frac{N-1}{3} \rfloor} a_{N-1-3s} - \sum_{t=0}^{\lfloor \frac{N-2}{3} \rfloor} a_{N-2-3t}. \tag{0.14}$$

Ora rimane da osservare che le condizioni (0.14) seguono dalle (e in realtà sono equivalenti alle) condizioni (0.13).

SECONDA DIMOSTRAZIONE

Si consideri l'omomorfismo unitario suriettivo di anelli

$$\overline{\Phi} : \mathbb{Q}[X] \longrightarrow \mathbb{Q}(\omega),$$
$$p(X) \mapsto p(\omega).$$

Mostriamo che

$$\operatorname{Ker} \overline{\Phi} = (X^2 + X + 1). \tag{0.15}$$

Infatti, siccome $\mathbb{Q}[X]$ è un PID, allora $\operatorname{Ker} \overline{\Phi} = (f(X))$. Il polinomio $X^2 + X + 1$ appartiene a $\operatorname{Ker} \overline{\Phi}$ e dunque $f(X)$ divide $X^2 + X + 1$. Questo implica che $\deg f(X) \leq 2$. Ma, siccome $\omega \notin \mathbb{Q}$, allora non esiste nessun polinomio non nullo di grado minore o uguale a uno a coefficienti in $\mathbb{Q}$ che annulla ω. Dunque $\deg f(X) = 2$ e, siccome $f(X)$ divide X^2+X+1, deduciamo che $f(X) \sim X^2+X+1$ in $\mathbb{Q}[X]$ e quindi che $\operatorname{Ker} \overline{\Phi} = (X^2 + X + 1)$.

Torniamo ora al nostro polinomio $p(X) \in \operatorname{Ker} \Phi$. Assumiamo che $p(X) \neq 0$, altrimenti non c'è niente da dimostrare. Se consideriamo $p(X)$ come un polinomio in $\mathbb{Q}[X]$, abbiamo che $p(X) \in \operatorname{Ker} \overline{\Phi}$. Dunque (0.15) implica che

$$p(X) = (X^2 + X + 1)q(X) \text{ per un certo } 0 \neq q(X) \in \mathbb{Q}[X].$$

Se scriviamo $q(X) = rh(X)$ con $r \in \mathbb{Q}^*$ e $0 \neq h(X)$ polinomio primitivo di $\mathbb{Z}[X]$, allora otteniamo

$$p(X) = r(X^2 + X + 1)h(X). \tag{0.16}$$

Prendendo il contenuto dell'uguaglianza di sopra e usando la sua moltiplicatività (Lemma di Gauss), otteniamo che

$$r = C(p) \in \mathbb{Z}.$$

Dunque la fattorizzazione in (0.16) vale in $\mathbb{Z}[X]$ e questo mostra che $p(X) \in \operatorname{Ker} \Phi$.

(9) (3 punti) Dimostrare che $1 - \omega$ è un elemento irriducibile tale che $\overline{1 - \omega} \sim 1 - \omega$ e $N(1 - \omega) = (1 - \omega)(\overline{1 - \omega}) = 3$.

Soluzione:

Usando la formula (0.10), otteniamo che

$$(1 - \omega)(\overline{1 - \omega}) = N(1 - \omega) = 3.$$

Consideriamo ora una fattorizzazione $1 - \omega = z_1 z_2$. Prendendo la norma e usando la sua moltiplicatività, otteniamo che $3 = N(1-\omega) = N(z_1)N(z_2)$. Questo implica che che $N(z_i) = 1$ per qualche $i = 1, 2$, e dunque che z_i è un'unità per quanto mostrato nel punto (7). Dunque ne deduciamo che $1 - \omega$ è irriducibile.

Infine, usando che $\omega^3 = 1$ per il punto (2), abbiamo che

$$\overline{1 - \omega} = 1 - \overline{\omega} = 1 - \omega^2 = -\omega^2(1 - \omega).$$

Siccome ω^2 è un un'unità, come mostrato nel punto (7), ne deduciamo che $\overline{1 - \omega}$ e $1 - \omega$ sono associati.

(10) (5 punti) Sia p un numero primo diverso da 3. Dimostrare che p è irriducibile in $\mathbb{Z}[\omega]$ se e solo se p non è norma di un elemento di $\mathbb{Z}[\omega]$ se e solo se $p \equiv 2 \mod 3$.

Soluzione:

La dimostrazione seguirà dalle seguenti asserzioni:

(a) p è riducibile se e solo se esiste un elemento di $\mathbb{Z}[\omega]$ di norma uguale a p.
Infatti, se esiste una fattorizzazione $p = xy$ con x e y che non sono unitá, allora prendendo la norma otteniamo

$$p^2 = N(p) = N(x)N(y).$$

Siccome $N(x), N(y) \neq 1$ per quanto mostrato nel punto (7), allora necessariamente dobbiamo avere che $N(x) = N(y) = p$.
Viceversa, sia $x \in \mathbb{Z}[\omega]$ tale che $N(x) = p$. Allora abbiamo che

$$p = N(x) = x \cdot \overline{x}$$

è una fattorizzazione non banale di p, visto che $N(x) = N(\overline{x}) \neq 1$.

(b) p è irriducibile se e solo se $\mathbb{Z}_p[X]/(X^2 + X + 1)$ è un dominio.
Infatti, siccome $\mathbb{Z}[\omega]$ è un UFD (essendo Euclideo per il punto (6)), allora p è irriducibile se e solo l'ideale (p) è primo. Ciò equivale a dire che il quoziente $\mathbb{Z}[\omega]/(p)$ è un dominio integrale. Ma usando il punto (8), abbiamo che

$$\frac{\mathbb{Z}[\omega]}{(p)} \cong \frac{\mathbb{Z}[X]}{(X^2 + X + 1, p)} \cong \frac{\mathbb{Z}_p[X]}{(X^2 + X + 1)},$$

e questo conclude la dimostrazione.

(c) $\mathbb{Z}_p[X]/(X^2 + X + 1)$ è un dominio se e solo se $\mathbb{Z}_p$ non contiene una radice terza non banale dell'unità.
Infatti, siccome $\mathbb{Z}_p[X]$ è UFD (essendo un PID visto che $\mathbb{Z}_p$ è un campo), allora è un dominio integrale se e solo se $X^2 + X + 1$ è irriducibile in $\mathbb{Z}_p[X]$. Siccome $X^2 + X + 1$ ha grado due, allora $X^2 + X + 1$ è irriducibile in $\mathbb{Z}_p[X]$ se e solo se non ha radici in $\mathbb{Z}_p[X]$. Siccome $(X^2 + X + 1)(X - 1) = X^3 - 1$, allora le radici di $X^2 + X + 1$ sono le radici di $X^3 - 1$ che non sono radici di $X - 1$. E queste sono esattamente le radici terze non banali dell'unità in $\mathbb{Z}_p$.

(d) $\mathbb{Z}_p$ contiene una radice terza non banale dell'unità se e solo se $p \equiv 1 \mod 3$.
Infatti, le radici terze non banali dell'unità in $\mathbb{Z}_p$ sono esattamente gli elementi di $(\mathbb{Z}_p)^*, .)$ che hanno ordine 3. Siccome sappiamo che $(\mathbb{Z}_p)^*, .)$ è un gruppo ciclico di ordine $p-1$, allora esistono elementi di ordine 3 se e solo se $3|(p-1)$, da cui la conclusione.

(11) (4 punti) Se p è un numero primo tale che $p \equiv 1 \mod 3$, allora la fattorizzazione di p in irriducibili $\mathbb{Z}[\omega]$ è:

$$p = \pi_p \overline{\pi}_p$$

con $\pi_p = a + b\omega \in \mathbb{Z}[\omega]$ tale che $N(a + b\omega) = p$. Inoltre π_p e $\overline{\pi}_p$ non sono associati.

Soluzione:

Per il punto (10), esiste $\pi_p = a + b\omega \in \mathbb{Z}[\omega]$ tale che $N(a + b\omega) = p$. Usando lo stesso argomento del punto (9), segue che π_p è irriducibile. Allo stesso modo, anche $\overline{\pi}_p$ è irriducibile visto che $N(\overline{\pi}_p) = p$. Dunque

$$p = \pi_p \overline{\pi}_p$$

è la decomposizione di p in irriducibili.

Supponiamo ora per assurdo che $\pi_p \sim \overline{\pi}_p$. Per la descrizione dell'unità si $\mathbb{Z}[\omega]$ nel punto (7), possiamo distinguere sei casi:

- Se $\pi_p = \overline{\pi}_p$ allora $b = 0$ e dunque $N(\pi_p) = a^2$,
- Se $\pi_p = -\overline{\pi}_p$ allora $b = 2a$ e dunque $N(\pi_p) = 3a^2$,
- Se $\pi_p = \omega\overline{\pi}_p$ allora $b = a$ e dunque $N(\pi_p) = a^2$,
- Se $\pi_p = -\omega\overline{\pi}_p$ allora $b = -a$ e dunque $N(\pi_p) = 3a^2$,
- Se $\pi_p = \omega^2\overline{\pi}_p$ allora $a = 0$ e dunque $N(\pi_p) = b^2$,

• Se $\pi_p = -\omega^2\overline{\pi}_p$ allora $a = 2b$ e dunque $N(\pi_p) = 3b^2$.

In ciascuno dei sei casi, la norma di π_p non può essere uguale al primo p perché si è supposto che $p \neq 3$, e questo mostra l'assurdo.

(12) (4 punti) Mostrare che gli irriducibili di $\mathbb{Z}[\omega]$ sono, a meno di associazione, tutti e soli gli elementi $1-\omega$, $\{p \ : p \equiv 2 \mod 3\}$, $\{\pi_p, \overline{\pi}_p \ : p \equiv 1 \mod 3\}$.

Soluzione:

Gli elementi indicati sono tutti irriducibili per quanto mostrato nei punti (9), (10) e (11). Inoltre, tali elementi sono non associati come si evince combinando il punto (11) al fatto che due elementi associati hanno la stessa norma per quanto mostrato nel punto (7).

Rimane da mostrare che gli elementi indicati sono tutti gli elementi irriducibili di $\mathbb{Z}[\omega]$. Sia dunque γ un elemento irriducibile di $\mathbb{Z}[\omega]$. Consideriamo l'intero positivo $n = N(\gamma) = \gamma \cdot \overline{\gamma}$. Allora γ è uno dei fattori irriducibili che appaiono nella fattorizzazione di n. Tuttavia i fattori irriducibili che appaiono nella fattorizzazione di n sono esattamente i fattori irriducibili che appaiono nella fattorizzazione in $\mathbb{Z}[\omega]$ dei numeri primi che dividono n. Dunque, per i punti (9), (10) e (11), γ deve essere uno degli elementi irriducibili che appaiono nella lista dell'enunciato.

(13) (4 punti) Dimostrare che dato un intero positivo n, esistono degli interi $a, b \in \mathbb{Z}$ tali che $a^2 - ab + b^2 = n$ se e solo se tutti i primi $p \equiv 2 \mod 3$ compaiono nella fattorizzazione di n con esponente pari.

Soluzione:

Dalla formula (0.10) segue che $n = a^2 - ab + b^2$ per certi interi $a, b \in \mathbb{Z}$ se e solo se esiste un elemento $x \in \mathbb{Z}[\omega]$ tale che $N(x) = n$. Mostriamo ora le due implicazioni.

Supponiamo prima che esista $x \in \mathbb{Z}[\omega]$ tale che $N(x) = n$. Per il punto (12), la decomposizione di x in irriducibili è della forma

$$x = u(1-\omega)^{e_3} \prod_{p \equiv 2 \mod 3} p^{e_p} \prod_{p \equiv 1 \mod 3} (\pi_p^{e_p^1} \overline{\pi}_p^{e_p^2}),$$

per un certo $u \in U(\mathbb{Z}[\omega])$, e per elementi $e_3, e_p, e_p^1, e_p^2 \in \mathbb{N}$ quasi tutti nulli. Prendendo la norma di x e usando i punti (7), (9) e (11), otteniamo che

$$N(x) = 3^{e_3} \prod_{p \equiv 2 \mod 3} p^{2e_p} \prod_{p \equiv 1 \mod 3} p^{e_p^1 + e_p^2}.$$

Da questo si evince che nella fattorizzazione di n in primi di $\mathbb{Z}$, i primi p che sono congrui a 2 modulo 3 compaiono con esponente pari.

Supponiamo ora che nella fattorizzazione di n in primi di $\mathbb{Z}$, i primi p che sono congrui a 2 modulo 3 compaiono con esponente pari. Dunque possiamo scrivere (usando che $n > 0$)

$$n = \prod_p p^{f_p} \quad \text{tale che } 2 | f_p \text{ se } p \equiv 2 \mod 3.$$

Siccome la norma è moltiplicativa, allora basta mostrare che ciascun fattore p^{f_p} è norma di un elemento di $\mathbb{Z}[\omega]$. Questo segue dai punti (9), (10) e (11).