Nome candidato:
Numero di matricola:

SECONDA PROVA IN ITINERE DEL CORSO AL210 – ALGEBRA 2
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.

[Suggerimento: per trovare l'inverso moltiplicativo di un elemento non nullo, si usi la formula $N(x) = x \cdot \overline{x}$, 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 $||.||$.]

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

$$\omega := \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}). \tag{0.1}$$

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;

[Suggerimento: si usi l'uguaglianza $(X - 1)(X^2 + X + 1) = X^3 - 1$.]

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

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

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 $\mathbb{Q}(\sqrt{-3})$.

(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 $\mathbb{Z}[\omega]$.

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

[Suggerimento: si consideri l'elemento ω. Argomentare che ω si può scrivere come $\omega = \frac{x}{y}$ con $x, y \in \mathbb{Z}[\sqrt{-3}]$) tali che $y \notin U(\mathbb{Z}[\sqrt{-3}]$ e $\mathrm{mcd}(x, y) \sim 1$ in $\mathbb{Z}[\sqrt{-3}]$. Sostituendo nell'equazione $x^2 + x + 1 = 0$, dedurre che $y | x^2$. Concludere che l'esistenza di due elementi $x, y \in \mathbb{Z}[\sqrt{-3}]$ che soddisfano le suddette proprietà implica che $\mathbb{Z}[\sqrt{-3}]$ non è un UFD.]

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

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

[Suggerimento: dati $x, y \in \mathbb{Z}[\omega]$ con $y \neq 0$, si consideri il quoziente $\frac{x}{y} = p + q\omega \in \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ e si approssimino i numeri razionali p e q con due interi n e m tali che $|p - n| \leq 1/2$ e $|q - m| \leq 1/2$. Poi si stimi la norma di $r := x - y(n + m\omega)$.]

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

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

[Suggerimento: mostrare che $z \in \mathbb{Z}[\omega]$ è un'unità se e solo se $N(z) = 1$.]

(8) (5 punti) Dimostrare che la mappa

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

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

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

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

(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 $p \equiv 2 \mod 3$.

[Suggerimento: usare le seguenti due condizioni
- p è riducibile se e solo se esiste un elemento di $\mathbb{Z}[\omega]$ di norma uguale a p.
- p è irriducibile se e solo se $\mathbb{Z}_p[X]/(X^2 + X + 1)$ è un dominio se e solo se $((\mathbb{Z}_p)^*, .)$ non contiene una radice terza non banale dell'unità.]

(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.

[Suggerimento: usare il punto (10) per la prima parte e il punto (7) per la seconda parte.]

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

(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.

[Suggerimento: reinterpretare la condizione su n in termini di norma di elementi di $\mathbb{Z}[\omega]$ e poi usare i punti (9), (10), (11).]