Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2007/2008
AL2 - Algebra 2 - gruppi, anelli e campi
Prova di Esame - Appello A
21 gennaio 2008

*Cognome*_____ *Nome*_____

*Numero di matricola*_____

Avvertenza: Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e **giustificando tutte le affermazioni fatte**. Non è consentito l'uso di libri, appunti e calcolatrici

1. Sia

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \; ; \; a, b, c \in \mathbb{Z}_2 \right\}.$$

   (a) Verificare che H è un sottogruppo del gruppo $\mathbf{GL}_3(\mathbb{Z}_2)$ delle matrici invertibili del terzo ordine ad elementi in $\mathbb{Z}_2$ (rispetto al prodotto righe per colonne);

   (b) Dimostrare che H è isomorfo al gruppo diedrale D_4 delle isometrie del quadrato, costruendo esplicitamente un isomorfismo $\varphi : H \longrightarrow D_4$.

Soluzione: (a) Indicando con $[a, b, c]$ la matrice $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, risulta $[a, b, c][d, e, f] = [a + d, b + e + af, c + f]$ quindi H è chiuso rispetto all'operazione. Inoltre l'elemento neutro di $\mathbf{GL}_3(\mathbb{Z}_2)$ è $I_3 = [0, 0, 0]$ e

appartiene ad H. Infine $[a,b,c]^{-1} = [a, ac+b, c]$ e quindi l'inverso di ogni elemento di H appartiene ancora ad H.

(b) D_4 è un gruppo con 8 elementi e, se ρ è la rotazione di $2\pi/4$ e τ è una riflessione, risulta $D_4 = \{id, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$ con $\rho^i\tau = \tau\rho^{4-i}$.

Notiamo che H ha $2^3 = 8$ elementi ed è non commutativo. Inoltre la matrice $R := [1,1,1]$ ha ordine 4 e la matrice $T := [1,0,0]$ ha ordine 2. Si verifica subito che $H := \{I_3, R, R^2, R^3, T, RT, R^2T, R^3T\}$ e che la corrispondenza

$$H \longrightarrow D_4\,; \quad R^iT^j \mapsto \rho^i\tau^j$$

è un isomorfismo di gruppi.

2. Si consideri l'applicazione

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_6 \times \mathbb{Z}_{10}\,; \quad a \mapsto ([a]_6, [a]_{10}).$$

   (a) Mostrare che φ è un omomorfismo di gruppi;

   (b) Determinare il nucleo e l'immagine di φ;

   (c) Definire l'omomorfismo canonico indotto da φ per il Teorema Fondamentale di Omomorfismo.

Soluzione: (a) Siano $a, b \in \mathbb{Z}$; allora $\varphi(a+b) = ([a+b]_6, [a+b]_{10}) = ([a]_6, [a]_{10}) + ([b]_6, [b]_{10}) = \varphi(a) + \varphi(b)$. Pertanto φ è un omomorfismo di gruppi.

(b) Il nucleo di φ è costituito dagli interi $a \in \mathbb{Z}$ tali che $a \equiv 0 \mod 6$ e $a \equiv 0 \mod 10$, cioè dagli interi a multipli di $\mathrm{mcm}(6,10) = 30$; pertanto $\mathrm{Ker}(\varphi) = 30\mathbb{Z}$.

Poiché $\mathbb{Z}$ è ciclico, generato da 1, l'immagine di φ è il sottogruppo ciclico di $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ generato da $\varphi(1) = ([1]_6, [1]_{10})$. Per il Teorema Fondamentale di Omomorfismo $\mathrm{Im}(\varphi) \simeq \mathbb{Z}/30\mathbb{Z}$ ha ordine 30;

(c) L'omomorfismo canonico indotto da φ per il Teorema Fondamentale di Omomorfismo è definito da:

$$\overline{\varphi} : \mathbb{Z}/30\mathbb{Z} \longrightarrow \mathrm{Im}(\varphi) \subseteq \mathbb{Z}_6 \times \mathbb{Z}_{10}\,; \quad a + 30\mathbb{Z} \mapsto \varphi(a) = ([a]_6, [a]_{10}).$$

3. Sia A un anello commutativo unitario. Per ogni ideale I di A, definiamo il *radicale di* I come

$$\sqrt{I} := \{a \in A\,;\ \text{ esiste } n \geq 1 \text{ tale che } a^n \in I\}.$$

$\sqrt{(0)} := Nil(A)$ si chiama il *nilradicale di* A. Mostrare che

(a) $\sqrt{I}$ è un ideale di A contenente I;

(b) $a \in \sqrt{I}$ se e soltanto se $a + I \in Nil(A/I)$;

(c) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Calcolare inoltre il radicale dell'ideale $12\mathbb{Z}$ di $\mathbb{Z}$.

Soluzione: (a) I è contenuto in $\sqrt{I}$; infatti per ogni $x \in I$ si ha che $x = x^1 \in I$. Se $a, b \in \sqrt{I}$, esistono $n, m > 0$ tali che $a^n \in I$ e $b^m \in I$. Allora $(a-b)^t \in I$ per $t \geq n + m - 1$, da cui segue che $a - b \in \sqrt{I}$. Infatti, per la formula del binomio,

$$(a-b)^{n+m-1} = \sum_{k=0}^{n+m-1} (-1)^k \left(\begin{array}{c} n+m-1 \\ k \end{array} \right) a^{n+m-(k+1)} b^k.$$

Per $k < m$ si ha che $n + m - (k+1) \geq n$; pertanto $a^{n+m-(k+1)} b^k \in I$ (poiché $a^{n+m-(k+1)} \in I$). Se $k \geq m$ si ha che $a^{n+m-(k+1)} b^k \in I$ (poiché $b^k \in I$). Dunque $(a-b)^{n+m-1} \in I$.

Inoltre, sia a un qualunque elemento di $\sqrt{I}$ e sia $n > 0$ tale che $a^n \in I$; se x è un qualunque elemento di A si ha che $(xa)^n = x^n a^n \in I$, da cui segue che $xa \in \sqrt{I}$.

Perciò $\sqrt{I}$ è un ideale di A.

(b) $a \in \sqrt{I} \ \Leftrightarrow$ (per definizione) esiste $n \geq 1$ tale che $a^n \in I \ \Leftrightarrow$ esiste $n \geq 1$ tale che $I = a^n + I = (a + I)^n \ \Leftrightarrow a + I \in Nil(A/I)$.

(c) $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$: se $a \in \sqrt{I \cap J}$, allora esiste $n \geq 1$ tale che $a^n \in I \cap J$ da segue che $a^n \in I$ e $a^n \in J$; pertanto $a \in \sqrt{I} \cap \sqrt{J}$;

$\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I \cap J}$: se $a \in \sqrt{I} \cap \sqrt{J}$, allora esistono $n,\ m \geqslant 1$ tali che $a^n \in I$ e $a^m \in J$; per $l = \max\{n, m\}$ si ha che $a^l \in I \cap J$ da cui segue che $a \in \sqrt{I \cap J}$.

Infine, $a \in \sqrt{12\mathbb{Z}} \ \Leftrightarrow$ esiste $n \geqslant 1$ tale che $a^n \in 12\mathbb{Z} \Leftrightarrow$ esiste $n \geqslant 1$ tale che 12 divide $a^n \Leftrightarrow 6$ divide a; pertanto $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$.

4. Si consideri il sottoinsieme di $\mathbb{C}$

$$A := \left\{ \frac{m + n\sqrt{-3}}{2} \,;\; m, n \in \mathbb{Z}, m \equiv n \mod 2 \right\}.$$

(a) Verificare che A è un sottoanello di $\mathbb{C}$ contenente $\mathbb{Z}[\sqrt{-3}]$;

(b) Determinare il gruppo moltiplicativo $\mathcal{U}(A)$ degli elementi invertibili di A;

(c) Verificare che $\mathcal{U}(A)$ è un gruppo ciclico finito e determinare i suoi generatori.

Soluzione: (a) Se $a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, $a + b\sqrt{-3} = \dfrac{2a + 2b\sqrt{-3}}{2}$ con $2a \equiv 2b \mod 2$; pertanto $Z[\sqrt{-3}] \subseteq A \subseteq \mathbb{C}$.

Siano $\alpha = \dfrac{m + n\sqrt{-3}}{2}$ e $\beta = \dfrac{s + t\sqrt{-3}}{2}$ elementi di A, con $m \equiv n \mod 2$ e $s \equiv t \mod 2$. Allora

$$\alpha - \beta = \frac{(m - s) + (n - t)\sqrt{-3}}{2}$$

è tale che $m - s \equiv n - t \mod 2$; pertanto $\alpha - \beta \in A$. Inoltre

$$\alpha\beta = \frac{ms - 3nt + (mt + ns)\sqrt{-3}}{4}.$$

Poiché $ms \equiv nt \mod 2$, è immediato verificare che $ms - 3nt$ e $mt + ns$ sono entrambi pari e congrui $\mod 4$; pertanto $\alpha\beta \in A$.

(b) Un elemento $\alpha = \dfrac{m + n\sqrt{-3}}{2}$ di A è invertibile se e solo se $N(\alpha) = 1$, cioè se e solo se $m^2 + 3n^2 = 4$ con $m, n \in \mathbb{Z}$. Si ha pertanto che

$$\mathcal{U}(A) = \left\{ \pm 1,\; \frac{\pm 1 \pm \sqrt{-3}}{2} \right\}$$

ha 6 elementi ed è il gruppo moltiplicativo delle radici complesse seste dell'unità.

(c) $\mathcal{U}(A)$ è ciclico (di ordine 6) generato dalla radice sesta primitiva $\xi := \cos(\pi/3) + i\sin(\pi/3) = \dfrac{1 + \sqrt{-3}}{2}$. Infatti $\xi^2 = \dfrac{-1 + \sqrt{-3}}{2}$ e

$\xi^3 = -1$. Dunque ξ ha ordine 6. $\mathcal{U}(A)$ ha $\varphi(6) = 2$ generatori e l'altro suo generatore è $\xi^5 = \xi^{-1} = \overline{\xi} = \dfrac{1-\sqrt{-3}}{2}$.

5. Siano $f(X) := X^4 + 2X^3 + X^2 + X + 1$, $g(X) := X^3 + X^2 + 2X + 2 \in \mathbb{Z}_3[X]$.

   (a) Mostrare che l'ideale $I := \langle f(X), g(X)\rangle$ è principale e determinare un suo generatore;

   (b) Stabilire se le classi modulo I dei polinomi $h(X) := X^3 + X$ e $k(X) := X^2 + 2X$ sono invertibili nell'anello quoziente $\mathbb{Z}_3[X]/I$;

   (c) Determinare gli ideali primi e massimali dell'anello $\mathbb{Z}_3[X]/I$.

   Soluzione: (a) Osservando che entrambi i polinomi $f(X)$ e $g(X)$ hanno radici $1, 2 \in \mathbb{Z}_3$, si ottiene che essi si fattorizzano in polinomi monici irriducibili come

   $$f(X) = (X+1)(X+2)(X^2+2X+2)\,; \quad g(X) = (X+1)^2(X+2).$$

   Poiché $\mathbb{Z}_3[X]$ è euclideo, l'ideale I è principale generato

   $$d(X) := MCD(f, g) = (X+1)(X+2) = X^2 + 2.$$

   (b) Poiché $h(X) = X(X^2+1)$ è coprimo con $d(X)$, la sua classe modulo I è invertibile. Invece $k(X) = X(X+2)$ non è coprimo con $d(X)$; quindi la sua classe è uno zerodivisore e non è invertibile.

   (c) Gli ideali primi non nulli e gli ideali massimali di $\mathbb{Z}_3[X]$ coincidono e sono quelli generati da polinomi irriducibili. Allora gli ideali primi non nulli (e massimali) di $\mathbb{Z}_3[X]/I$ sono quelli generati dalle classi dei divisori irriducibili di $d(X)$. Essi sono quindi $P := \langle (X+1) + I\rangle$, $Q := \langle (X+2) + I\rangle$.