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 B
7 febbraio 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 $n \geq 3$ un numero naturale. Nel prodotto cartesiano $\mathbb{Z}_n \times \mathbb{Z}_2$ si consideri l'operazione $*$ definita nel seguente modo:

$$([x]_n, [0]_2) * ([y]_n, [0]_2) = ([x+y]_n, [0]_2)$$

$$([x]_n, [0]_2) * ([y]_n, [1]_2) = ([x+y]_n, [1]_2)$$

$$([x]_n, [1]_2) * ([y]_n, [0]_2) = ([x-y]_n, [1]_2)$$

$$([x]_n, [1]_2) * ([y]_n, [1]_2) = ([x-y]_n, [0]_2)$$

   (a) Sapendo che l'operazione $*$ è associativa, provare che $(\mathbb{Z}_n \times \mathbb{Z}_2, *)$ è un gruppo non abeliano.

   (b) Posto $\sigma = ([1]_n, [0]_2)$ e $\rho = ([0]_n, [1]_2)$, provare che σ genera un sottogruppo di $(\mathbb{Z}_n \times \mathbb{Z}_2, *)$ isomorfo a $(\mathbb{Z}_n, +)$ e ρ un sottogruppo di $(\mathbb{Z}_n \times \mathbb{Z}_2, *)$ isomorfo a $(\mathbb{Z}_2, +)$.

   (c) Stabilire se $(\mathbb{Z}_4 \times \mathbb{Z}_2, *)$ è isomorfo a D_4 oppure al gruppo (moltiplicativo) delle unità dei quaternioni.

Soluzione

(a) E' immediato verificare che in $(\mathbb{Z}_n \times \mathbb{Z}_2, *)$ $([0]_n, [0]_2)$ è l'elemento neutro e che per ogni $[x]_n \in \mathbb{Z}_n$ l'inverso di $([x]_n, [0]_2)$ è $([-x]_n, [0]_2)$ e l'inverso di $([x]_n, [1]_2)$ è $([x]_n, [1]_2)$.

Inoltre l'operazione non è commutativa, in quanto

$$([1]_n, [0]_2) * ([1]_n, [1]_2) = ([2]_n, [1]_2) \;\; e \;\; ([1]_n, [1]_2) * ([1]_n, [0]_2) = ([0]_n, [1]_2)$$

con $[2]_n \neq [0]_n$, poiché $n \geq 3$.

(b) L'ordine di σ è n; pertanto σ genera un gruppo ciclico di ordine n che è isomorfo a $(\mathbb{Z}_n, +)$; l'ordine di ρ è 2; pertanto ρ genera un sottogruppo ciclico isomorfo a $(\mathbb{Z}_2, +)$.

(c) $(\mathbb{Z}_4 \times \mathbb{Z}_2, *)$ è un gruppo non abeliano con 8 elementi; si vede facilmente che

$$\mathbb{Z}_4 \times \mathbb{Z}_2 = \{\sigma, \sigma^2, \sigma^3, \sigma^4 = ([0]_n, [0]_2), \rho, \sigma\rho, \sigma^2\rho, \sigma^3\rho\}.$$

$(\mathbb{Z}_4 \times \mathbb{Z}_2, *)$ è pertanto isomorfo a D_4

2. Sia $\varphi : \mathbb{Q}[X] \longrightarrow \mathbb{C} \times \mathbb{C}$ l'omomorfismo di anelli definito nel seguente modo: se $f(X) \in \mathbb{Q}[X]$

$$\varphi(f(X)) := (f(2), f(-3))$$

(a) Trovare il nucleo e l'immagine di φ.

(b) Stabilire se l'anello quoziente $\mathbb{Q}[X]/\mathtt{Ker}(\varphi)$ è integro.

(c) Applicare a φ il Teorema Fondamentale di omomorfismo.

Soluzione

(a) Poiché $\mathbb{Q}[X]$ è un dominio euclideo,

$$\begin{aligned} \mathtt{Ker}(\varphi) &= \{f(X) \in \mathbb{Q}[X] \;\; ; \;\; (f(2), f(-3)) = (0,0)\} \\ &= \{f(X) \in \mathbb{Q}[X] \;\; ; \;\; f(2) = f(-3) = 0\} \end{aligned}$$

è un ideale principale generato dal polinomio monico di grado minimo che ha 2 e -3 come radici, cioè dal polinomio $(X-2)(X+3) = (X^2-5X+6)$. (Oppure $\texttt{Ker}(\varphi) = (X-2) \cap (X+3) = (X-2)\cdot(X+3) = (X^2-5X+6)$).

Inoltre $\texttt{Im}(\varphi) = \{(f(2), f(-3)) \quad ; \quad f(X) \in \mathbb{Q}[X]\}$; banalmente, per ogni $f(X) \in \mathbb{Q}[X]$ si ha che $(f(2), f(-3)) \in \mathbb{Q} \times \mathbb{Q}$,da cui $\texttt{Im}(\varphi) \subseteq \mathbb{Q} \times \mathbb{Q}$; d'altra parte, presi comunque $u, v \in \mathbb{Q}$, è immediato verificare che $\varphi\left(\frac{u-v}{5}X + \frac{3u+2v}{5}\right) = (u, v)$, da cui $\mathbb{Q} \times \mathbb{Q} \subseteq \texttt{Im}(\varphi)$; in conclusione $\texttt{Im}(\varphi) = \mathbb{Q} \times \mathbb{Q}$:

(b) L'anello quoziente $\mathbb{Q}[X]/\texttt{Ker}(\varphi)$ non è integro, poiché il polinomio X^2-5X+6 è riducibile. (Oppure, per il Teorema Fondamentale di Omomorfismo si ha che $\mathbb{Q}[X]/\texttt{Ker}(\varphi) \cong \texttt{Im}(\varphi) = \mathbb{Q}\times\mathbb{Q}$ e $\mathbb{Q}\times\mathbb{Q}$ non è integro, poiché, ad esempio, $(1,0)$ e $(0,1)$ sono zero-divisori.)

(c) Il teorema Fondamentale di Omomorfismo asserisce che l'applicazione

$$\begin{aligned}\overline{\varphi} :&\mathbb{Q}[X]/(X^2-5X+6) \longrightarrow \mathbb{Q}\times\mathbb{Q}\\ &f(X)+(X^2-4X+29) \longmapsto \varphi(f(X)) = (f(2), f(-3))\end{aligned}$$

è un isomorfismo di anelli.

3. Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ siano $\alpha = 7+17i$ e $\beta = -5+12i$.

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

(b) Stabilire se le classi modulo I degli elementi $\gamma = -10+11i$ e $\delta = 3-5i$ sono invertibili nell'anello quoziente $A := \mathbb{Z}[i]/I$;

(c) Mostrare che A ha un unico ideale proprio non nullo M;

(d) Stabilire se A/M è un campo.

Soluzione

(a) Poichè $\mathbb{Z}[i]$ è un dominio euclideo, l'ideale I è principale ed un suo generatore è un MCD(α, β). Notiamo che α ha norma 338 e β ha norma 169. Da $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{169} = 1-i$, si ha che MCD$(\alpha, \beta) = \beta$. Pertanto $I := \langle \beta \rangle = \langle -5+12i \rangle$.

Un elemento $a+ib$ di $\mathbb{Z}[i]$ con $a \neq 0$ e $b \neq 0$ è irriducibile se e solo se la sua norma è un numero primo. Pertanto β è riducibile. Inoltre è immediato vedere che $\beta = (2+3i)^2$ e che $2+3i$ è irriducibile.

(b) Se $\eta \in \mathbb{Z}[i]$, $\eta + I \neq I$ è invertibile in $A := \mathbb{Z}[i]/I$ se e solo se $\mathrm{MCD}(\eta, (2+3i)^2) = 1$ (se e solo se $\mathrm{MCD}(\eta, 2+3i) = 1$).

$\gamma = -10 + 11i$ ha norma $221 = 13 \cdot 17$; pertanto $\gamma \notin I$. Inoltre, dividendo γ per $2+3i$ si ottiene $\gamma = (2+3i)(1+4i)$ con $(1+4i)$ irriducibile; dunque $\mathrm{MCD}(\gamma, \beta) = (2+3i)$, da cui $\gamma + I$ non solo non è invertibile in A, ma è uno zero-divisore in A.

$\delta = 3-5i$ ha norma $34 = 2 \cdot 17$; pertanto $\delta \notin I$; δ si decompone in fattori irriducibili in $(1+4i)(1+i)$; pertanto $\mathrm{MCD}(\delta, (2+3i)^2) = 1$ da cui segue che $\delta + I$ è invertibile in A.

(c) C'è una corrispondenza biunivoca che conserva le inclusioni tra gli ideali di A e gli ideali di $\mathbb{Z}[i]$ che contengono I. Poiché $I = ((2+3i)^2)$ con $2+3i$ irriducibile, gli unici ideali di $\mathbb{Z}[i]$ che contengono I sono I, $(2+3i)$ e $\mathbb{Z}[i]$. Passando al quoziente, si ottengono l'ideale nullo, l'ideale $(2+3i)/I$ e tutto l'anello A; pertanto A ha un solo ideale proprio non nullo $M = (2+3i)/I$.

(d) M, essendo l'unico ideale proprio non nullo di A, banalmente un ideale massimale di A;, pertanto A/M è un campo.

4. Siano $f(X) = X^2 + 1 \in \mathbb{Z}_3[X]$ e $I := (f(X))$.

(a) Mostrare che $K := \mathbb{Z}_3[X]/I$ è un campo e, posto $\alpha = X + I$, esplicitare i suoi elementi in funzione di α.

(b) Determinare il sottogruppo ciclico di $(K^*, \cdot)$ generato da $\alpha + 1$ ed elencare i suoi generatori.

Soluzione

(a) Poiché $f(X)$ è un polinomio di secondo grado a coefficienti in un campo privo di radici, $f(X)$ è irriducibile in $\mathbb{Z}_3[X]$. Pertanto I è un ideale massimale in $\mathbb{Z}_3[X]$, da cui segue che $K := \mathbb{Z}_3[X]/I$ è un campo. Da $\alpha = X + I$, segue che $\alpha^2 = 2$.

$$\begin{aligned}\mathbb{Z}_3[X]/I &= \{g(X) + I;\ ;\quad g(X) \in \mathbb{Z}_3[X]\} \\ &= \{(a + bX) + I\ \ ;\ \ a, b \in \mathbb{Z}_3\} \\ &= \{a + b\alpha\ \ ;\ \ a, b \in \mathbb{Z}_3\} \\ &= \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}\end{aligned}$$

(b) $(K^*, \cdot)$ è un gruppo abeliano con 8 elementi. Da $(\alpha+1)^2 = 2\alpha$ e $(\alpha+1)^4 = 2$ segue che $\alpha+1$ ha ordine 8; dunque $\langle \alpha+1 \rangle = K^*$. I generatori di $\langle \alpha+1 \rangle$ sono 4 e della forma $(\alpha+1)^t$ con $1 \leqslant t \leqslant 8$ e primo con 4. Allora i generatori di $\langle \alpha+1 \rangle$ sono:

$$\alpha+1, \;\; (\alpha+1)^3 = 2\alpha+1, \;\; (\alpha+1)^5 = 2\alpha+2, \;\; (\alpha+1)^7 = \alpha+2.$$