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 C
11 giugno 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. Si condideri il seguente sottogruppo del gruppo $\mathbf{GL}_3(\ Z_3)$ delle matrici invertibili del terzo ordine ad elementi in $\mathbb{Z}_3$ (rispetto al prodotto righe per colonne);

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ ; \ a, b, c \in \mathbb{Z}_3 \right\}.$$

   (a) Verificare che ogni elemento diverso dall'elemento neutro ha ordine 3;

   (b) Trovare il centro di G;

   (c) Trovare l'ordine del gruppo $G/Z(G)$; stabilire se $G/Z(G)$ è abeliano e/o ciclico.

Soluzione

(a) Indicando con $[a,b,c]$ la matrice $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, risulta $[a,b,c]^2 = [2a, 2b+ac, 2c]$ e $[a,b,c]^3 = [3a, 3b+3ac, 3c] = [0,0,0]$.

(b) Il centro di G è costituito dalle matrici $[a,b,c]$ tali che $[a,b,c][d,e,f] = [d,e,f][a,b,c]$ per ogni $[d,e,f] \in G$, cioè tali che $af = dc$ per ogni $d, f \in \mathbb{Z}_3$; da cui $a = c = 0$; pertanto

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

(c) G ha ordine 27, $Z(G)$ ha ordine 3; pertanto l'ordine di $G/Z(G)$ è $9 = 3^2$, cioè il quadrato di un numero primo; da qui segue che $G/Z(G)$ è abeliano. $G/Z(G)$ non è ciclico poiché per il punto (a) si ha che $(gZ(G))^3 = Z(G)$ per ogni $g \in G$.

2. Siano X un insieme non vuoto e $\mathcal{P}(X)$ l'insieme delle sue parti. Si consideri l'anello commutativo unitario $(\mathcal{P}(X), \Delta, \cap)$ (Dove $A \Delta B = (A \cup B) \setminus (A \cap B)$ è la differenza simmetrica).

(a) Verificare che l'anello $\mathcal{P}(X)$ è booleano, cioè che per ogni $A \in \mathcal{P}(X)$ si ha che $A^2 = A$.

(b) Provare che $\mathcal{P}(X)$ è un dominio d'integrità se e solo se $|X| = 1$.

(c) Sia $x \in X$; sia

$$I_x = \{A \in \mathcal{P}(X) \quad | \quad x \notin A\}.$$

Provare che I_x è un ideale massimale di $\mathcal{P}(X)$.

(d) Provare che $\mathcal{P}(X)/I_x \cong \mathbb{Z}_2$.

(e) Se $|X| = 3$, determinare tutti gli ideali di $\mathcal{P}(X)$ e mostrare che ogni ideale massimale è del tipo I_x per qualche $x \in X$.

Soluzione

(a) Per ogni $A \in \mathcal{P}(X)$ si ha che $A^2 = A \cap A = A$.

(b) Se $|X| = 1$, $\mathcal{P}(X) = \{\emptyset, X\}$; allora $\mathcal{P}(X)$, essendo costituito solamente dall'elemento neutro additivo e dall'elemento neutro moltiplicativo, è un campo con due elementi. Se $|X| > 1$, sia a un elemento di X; allora $\{a\}$ e $X - \{a\}$ sono due elementi di $\mathcal{P}(X)$ entrambi diversi dall'insieme vuoto, cioè dallo zero di $\mathcal{P}(X)$, tali che il loro prodotto $\{a\} \cap (X - \{a\})$ è lo zero di $\mathcal{P}(X)$.

(c) Se $A, B \in I_x$, si ha che $x \notin A$ e $x \notin B$, da cui $x \notin (A - B) \cup (B - A) = A\Delta B = A\Delta(-B)$.

Se $A \in I_x$ e $C \in \mathcal{P}(X)$, allora $x \notin A \cap C$, cioè $A \cap C \in I_x$. Pertanto I_x è un ideale di $\mathcal{P}(X)$.

Sia J un ideale di $\mathcal{P}(X)$ contenente propriamente I_x; allora esiste $C \subseteq X$ tale che $C \in J - I_x$; poiché $x \in C$, $X - C \in I_x$ da cui $X = C\Delta(X - C) \in J$. Pertanto $J = \mathcal{P}(X)$ e l'ideale I_x è massimale.

(d) $\mathcal{P}(X)/I_x = \{I_x, \{x\}\Delta I_x\}$: sia $A \in \mathcal{P}(X)$; se $x \notin A$, allora $A\Delta I_x = I_x$; se $x \in A$, allora $A\Delta\{x\} = A - \{x\} \in I_x$, da cui $A\Delta I_x = \{x\}\Delta I_x$.

$\mathcal{P}(X)/I_x$, essendo un anello commutativo unitario con solo due elementi, è banalmente isomorfo a $\mathbb{Z}_2$. Da questo si può riottenere che l'ideale I_x è massimale.

(e) Sia $X = \{a, b, c\}$. Oltre ai due ideali banali, vi sono i 3 ideali con 2 elementi $(\{a\}) = \{\emptyset, \{a\}\}$, $(\{b\}) = \{\emptyset, \{b\}\}$, $(\{c\}) = \{\emptyset, \{c\}\}$ e i 3 ideali con 4 elementi $(\{a, b\}) = \{\emptyset, \{a, b\}, \{a\}, \{b\}\}$, $(\{a, c\}) = \{\emptyset, \{a, c\}, \{a\}, \{c\}\}$, $(\{b, c\}) = \{\emptyset, \{b, c\}, \{b\}, \{c\}\}$; questi ultimi tre sono massimali e sono rispettivamente I_c, I_b e I_a.

3. Si consideri l'anello $\mathbb{Z}[\sqrt{-5}]$.

(a) Provare che 3 e $1 - \sqrt{-5}$ sono elementi di $\mathbb{Z}[\sqrt{-5}]$ irriducibili e non primi;

(b) Sia $I = \left(3, 1 - \sqrt{-5}\right)$.

- Verificare che $I \neq \mathbb{Z}[\sqrt{-5}]$;
- Provare che I non è un ideale principale.

Soluzione

(a) In $\mathbb{Z}[\sqrt{-5}]$ non vi sono elementi di norma 3: se $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, la sua norma è $a^2 + 5b^2$; se $b = 0$, non c'è alcun numero intero a tale che $a^2 = 3$; se $b \neq 0$, $a^2 + 5b^2 \geqslant 5 > 3$.

Siano $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ tali che $3 = \alpha\beta$; passando alle norme si ha che $9 = N(\alpha)N(\beta)$, da cui non essendovi in $\mathbb{Z}[\sqrt{-5}]$ elementi di norma 3, si ha che $N(\alpha) = 1$ oppure $N(\beta) = 1$ da cui α oppure β è invertibile; da qui la irriducibilità di 3.

Inoltre $3 \cdot 2 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, cioé 3 divide $(1 - \sqrt{-5})(1 + \sqrt{-5})$; è immediato verificare che 3 non divide né $1 - \sqrt{-5}$ né $1 + \sqrt{-5}$.

Analogamente si prova che $1 - \sqrt{-5}$ è un elemento di $\mathbb{Z}[\sqrt{-5}]$ irriducibile e non primo.

(b)
- Se $I = \mathbb{Z}[\sqrt{-5}]$, allora esisterebbero $a + b\sqrt{-5}, c + d\sqrt{-5}, \in \mathbb{Z}[\sqrt{-5}]$ tali che $1 = 3(a + b\sqrt{-5}) + (1 - \sqrt{-5})(c + d\sqrt{-5})$ da cui $1 = 3a + c + 5d$ e $0 = 3b + d - c$; quindi si avrebbe che $1 = 3(a + b + 2d)$ con $a + b + 2d \in Z$, cioè 3 sarebbe invertibile in $\mathbb{Z}$.
- Si supponga che I sia principale; sia γ un suo generatore; per quanto provato nel punto precedente γ non sarebbe invertibile in $\mathbb{Z}[\sqrt{-5}]$; poiché $3 \in I$ ed è irriducibile, 3 sarebbe associato a γ così come lo sarebbe $1 - \sqrt{-5}$; quindi 3 e $1 - \sqrt{-5}$ sarebbero associati in contraddizione con il fatto che gli unici elementi invertibili di $\mathbb{Z}[\sqrt{-5}]$ sono 1 e -1; si può pertanto concludere che I non è principale.

4. Si consideri nell'anello $\mathbb{Z}_3[X]$ il polinomio $f(X) = X^4 + X + 2$ el'ideale $I = (f(X))$.

   (a) Stabilire se il polinomio $f(X)$ è irriducibile in $\mathbb{Z}_3[X]$.

   (b) Descrivere l'anello $\mathbb{Z}_3[X]/I$.

   (c) Stabilire se $(X^7 + 2X^5 + X^2 + 2) + I$ è invertibile in $\mathbb{Z}_3[X]/I$ e, nel caso lo sia, trovarne l'inverso.

Soluzione

(a) E' immediato verificare che $f(X)$ è privo di radici in $\mathbb{Z}_3$; ciò non basta per affermare che $f(X)$ è irriducibile in $\mathbb{Z}_3[X]$, essendo il polinomio di quarto grado. Se $f(X)$ fosse riducibile in $\mathbb{Z}_3[X]$, allora dovrebbero esistere $X^2+aX+b,\ X^2+cX+d \in \mathbb{Z}_3[X]$ tali che $f(X)=(X^2+aX+b)(X^2+cX+d)$; quindi dovrebbero esistere $a,b,c,d \in \mathbb{Z}_3[X]$ tali che

$$\begin{cases} a+c=0 \\ d+ac+b=0 \\ ad+bc=1 \\ bd=2 \end{cases} \text{ ; da cui } \begin{cases} c^2=0 \\ a^2=0 \\ ad+bc=1 \\ bd=2 \end{cases}$$

Da qui si avrebbe $1=0$. Pertanto $f(X)$ è irriducibile in $\mathbb{Z}_3[X]$.

(b) $\mathbb{Z}_3[X]/I$ è un campo con 3^4 elementi;

$$\mathbb{Z}_3[X]/I = \left\{(a_3X^3+a_2X^2+a_1X+a_0)+I \ \mid \ a_3,a_2,a_1,a_0 \in \mathbb{Z}_3\right\}.$$

(c) Dividendo $X^7+2X^5+X^2+2$ per X^4+X+2, si ottiene

$$X^7+2X^5+X^2+2=(X^3+2X+2)(X^4+X+2)+X^3+2X^2+1;$$

$(X^7+2X^5+X^2+2)+I=(X^3+2X^2+1)+I \neq I$ è pertanto invertibile.
Si ponga $t=X+I$; da $(t^3+2t^2+1)(a_3t^3+a_2t^2+a_1t+a_0)=1$, tenendo conto che $t^4=2t+1$, $t^5=2t^2+t$, $t^6=2t^3+t^2$, si ottiene che $a_0=a_1=a_2=1$ e $a_3=2$; pertanto l'inverso di t^3+2t^2+1 è $2t^3+t^2+t+1$.