Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2002/2003
AL2 - Algebra 2, gruppi, anelli e campi
Seconda prova di valutazione intermedia
12 gennaio 2004
Soluzioni

1. (10 pt) Siano p un numero primo e $A = \mathcal{M}_3(\mathbb{Z}_p)$, con l'usuale somma e prodotto righe per colonne.

1. Trovare la cardinalità di A.
2. Sia
$$B = \{M = (m_{ij}) \in A : m_{ij} = 0, i \leq j\}$$
Verificare se
   (a) B è un sottoanello di A.
   (b) B è un ideale destro o sinistro.
   (c) $\forall\ M \in B$ esiste $n \in \mathbb{N}$ tale che $M^n = 0$.
3. Definiamo un nuovo prodotto su A: $\forall\ M$ e $N \in A$ poniamo
$$M * N = M \cdot N - N \cdot M.$$
Verificare se $*$ gode delle proprietà
   (a) associativa.
   (b) distributiva.

   Dire se $(A, +, *)$, con $+$ l'usuale somma sulle matrici, è un anello.

Soluzione 1.

1. $|A| = p^9$.

2.

(a) B è un sottoanello. Infatti si verifica facilmente che se M e $N \in B$ allora:
$$M - N \in B.$$
$$MN \in B$$

(b) B non è un ideale né destro né sinistro. Infatti, per esempio:
$$\begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & c & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & 0 \\ 0 & b & 0 \end{pmatrix} \notin B.$$
$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & c & 0 \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin B.$$

(c) $\forall\ M \in B$ *si verifica subito che* $M^3 = 0$.

3. *(a)* $*$ *non è associativo, infatti:*

$$M * (N * P) = MNP - NPM - MPN + PNM$$
$$(M * N) * P = MNP - PNM - NMP + PNM.$$

Quindi

$$M * (N * P) - (M * N) * P = PNM + NMP - NPM - MPN.$$

(b) $*$ *è distributivo*

Poiché $*$ *non è associativo* $(A, +, *)$ *non è un anello.*

2. (9 pt) Stabilire se i seguenti ideali di $\mathbb{Z}[X]$ sono primi e/o massimali:

1. $(3, X)$;
2. $(X^2 - 3X + 2)$
3. $(X^2 - 3)$;
4. $(7, X^2 - 3)$.

Soluzione 2. *Usiamo il seguente criterio per stabilire se gli ideali sono primi o massimali.*

$$I \text{ è primo (massimale)} \Leftrightarrow R/I \text{ è un dominio (campo).}$$

1. $\mathbb{Z}[X] / (3, X) \cong \mathbb{Z}_3$, *dunque* $(3, X)$ *è massimale*
2. $\mathbb{Z}[X] / \left(X^2 - 3X + 2\right)$ *non è un dominio, infatti*

$$X^2 - 3X + 2 = (X - 1)(X - 2).$$

Dunque nel quoziente $\overline{X - 1}$ *è uno zero divisore non nullo.Quindi* $\left(X^2 - 3X + 2\right)$ *non è primo.*

3. $\mathbb{Z}[X] / \left(X^2 - 3\right) = \mathbb{Z}\left[\sqrt{3}\right]$, *dunque* $\left(X^2 - 3\right)$ *è primo ma non massimale. Infatti* $\mathbb{Z}\left[\sqrt{3}\right]$ *è un dominio ma non un campo.*
4. *Osserviamo che*

$$\mathbb{Z}[X] / \left(7, X^2 - 3\right) \cong \mathbb{Z}\left[\sqrt{3}\right] / (7).$$

Ricordiamo che $\mathbb{Z}\left[\sqrt{3}\right]$ *è un dominio euclideo e che 7 è irriducibile in* $\mathbb{Z}\left[\sqrt{3}\right]$, *dunque* $\mathbb{Z}\left[\sqrt{3}\right] / (7)$ *è un campo. Quindi* $\left(7, X^2 - 3\right)$ *è massimale.*

3. (8 pt) Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ si consideri l'ideale

$$I = (3 - i, 5 + 10i).$$

1. Stabilire se I è principale ed eventualmente determinarne un generatore.
2. Stabilire se I è primo e/o massimale.

3. Descrivere l'anello quoziente $\mathbb{Z}[i]/I$.(Sugg. Si consideri l'omomorfismo anulare $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/I$ definito da $\varphi(n) = n + I$ per ogni $n \in \mathbb{Z}$).

Soluzione 3. *Osserviamo che l'anello degli interi Gauss è un dominio euclideo, dunque, in particolare, $\mathbb{Z}[i]$ è un PID.*

1. *Per l'osservazione precedente I è principale e il suo generatore è il massimo comun divisore fra $3-i$ e $5+10i$. Per calcolare il massimo comun divisore applichiamo l'algoritmo euclideo.*

$$\begin{aligned} 5+10i &= 3i\,(3-i)+2+i \\ 3-i &= (i-i)\,(2+i)+0. \end{aligned}$$

   Dunque $I = (MCD(3-i, 5+10i)) = (2+i)$.

2. *Osserviamo che $N(2+i) = 4+1 = 5$, dunque $2+i$ è irriducibile e I è massimale.*

3. *Cosideriamo l'omomorfismo $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}[i]/I$ definito da $\varphi(n) = n + I$ per ogni $n \in \mathbb{Z}$. Allora è facile vedere che $\ker\varphi = 5\mathbb{Z}$. Vediamo che è suriettiva. Dimostriamo che per ogni $x \in \mathbb{Z}\,[i]$, esiste $n \in \mathbb{Z}$ tale che $x - n \in I$, cioè*

$$2+i|x-n.$$

   Sia $w = a+ib \in \mathbb{Z}\,[i]$, poniamo $x = \alpha + i\beta$ allora

$$\begin{aligned} 2+i|x-n \quad &\Leftrightarrow \quad x-n = w\,(2+i) \\ &\Leftrightarrow \quad \alpha - n + i\beta = a+ib\,(2+i) = 2a-b+i\,(a+2b)\,. \end{aligned}$$

   Da cui

$$\begin{aligned} 2a-b+n &= \alpha \qquad (1) \\ a+2b &= \beta \qquad (2) \end{aligned}$$

   Dunque, $a = \beta - 2b$, $n = \alpha - 2\beta + 5b$ e b qualsiasi. Da cui φ è suriettiva e per il teorema di omomorfismo si ha

$$\mathbb{Z}[i]/I \cong \mathbb{Z}_5.$$

4. (9 pt) Si consideri nell'anello $\mathbb{Z}_3[X]$ il polinomio $f(X) = X^3 + 2X^2 + 1$; sia $I = (X^3 + 2X^2 + 1)$.

1. Verificare che il polinomio $f(X)$ è irriducibile in $\mathbb{Z}_3[X]$.
2. Descrivere il campo $K = \mathbb{Z}_3[X]/I$.
3. Trovare in K l'inverso dell'elemento $(X^4 + X) + I$.
4. Provare che $t = X + I$ è un generatore del gruppo moltiplicativo $K - \{0\}$.

Soluzione 4.

1. *Osserviamo che $f(0) = 1$, $f(1) = 1$ e $f(2) = 2$, dunque essendo di 3° grado f è irriducibile.*

2. $$K=\left\{a+bX+cX^2 : a,b,c\in\mathbb{Z}_3 \text{ e } X^3=X^2+2\right\}.$$

   e ha $3^3=27$ *elementi.*

3. *Per trovare l'inverso si* X^4+X+I *dobbiamo risolvere*

$$\left(X^4+X\right)\left(a+bX+cX^2\right)=1+I.$$

   Risolvendo otteniamo $a=2$, $b=1$ *e* $c=2$.

4. *Osserviamo che* $K-\{0\}$ *è un gruppo ciclico con 26 elementi. Per dimostrare che* t *è un generatore facciamo vedere che* $n=Ord(t)=26$. *Sappiamo dalla teoria che* $n|26$, *dunque* $n=2$, 13 *o* 26.

$$\begin{aligned} t^2 &= X^2+I\neq 1+I. \\ t^{13} &= X^{13}+I=2\neq 1+I. \end{aligned}$$

   Da cui $Ord(t)=26$ *e* t *è un generatore di* $K-\{0\}$.