Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica
a.a. 2007/2008
AL2 - Algebra 2, gruppi, anelli e campi
Seconda prova di valutazione intermedia
11 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 A un anello commutativo ed unitario; un elemento $a \in A$ si dice *nilpotente* se esiste $n > 0$ tale che $a^n = 0$. Sia $\mathcal{N}(A)$ l'insieme degli elementi nilpotenti di A.

   (a) Provare che $\mathcal{N}(A)$ è un ideale di A detto *nilradicale* o *radicale primo* dell'anello A.

   (b) Provare che $\mathcal{N}(A)$ è contenuto in ogni ideale primo di A.

   (c) Trovare $\mathcal{N}(\mathbb{Z}_{180})$.

   Soluzione

   (a) $\mathcal{N}(A) \neq \emptyset$ poiché almeno $0 \in \mathcal{N}(A)$. Siano $a, b \in \mathcal{N}(A)$; allora esistono $n, m > 0$ tali che $a^n = 0$ e $b^m = 0$. Si consideri

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

Per $k < m$ si ha che $n + m - 1 - k \geq n$; pertanto $a^{n+m-1-k} = 0$ e $a^{n+m-1-k}b^k = 0$. Se $k \geqslant m$ si ha che $b^k = 0$ e $a^{n+m-1-k}b^k = 0$. Quindi $(a-b)^{n+m-1} = 0$, da cui segue che $a - b \in \mathcal{N}(A)$.

Inoltre sia a un qualunque elemento di $\mathcal{N}(A)$ e sia $n > 0$ tale che $a^n = 0$; se x è un qualunque elemento di A si ha che $(xa)^n = x^n a^n = 0$.

Perciò $\mathcal{N}(A)$ è un ideale di A.

(b) Sia $a \in \mathcal{N}(A)$ e sia $n \geqslant 1$ tale che $a^n = 0$. Allora $a^n = 0 \in P$, per ogni ideale primo P di A, e per la definizione di ideale primo segue che $a \in P$. Cioè $\mathcal{N}(A) \subseteq P$, per ogni ideale primo di A.

(c) $180 = 2^2 \cdot 3^2 \cdot 5$. Qundi $[a]_{180} \in \mathcal{N}(\mathbb{Z}_{180})$ se e soltanto se $a^n \equiv 0 \mod 180$ se e soltanto se $2 \cdot 3 \cdot 5$ divide a. Pertanto $\mathcal{N}(\mathbb{Z}_{180}) = ([30]_{180})$.

In alternativa; dal punto (b) si ottiene che $N(\mathbb{Z}_{180}) \subseteq ([30]_{180})$. Poichè poi $[30]^2_{180} = 0$, si ha l'uguaglianza.

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

$$v(f(X)) := f(2 + 5i).$$

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

(b) Applicare a v il Teorema Fondamentale di omomorfismo.

Soluzione

(a) Il nucleo di v è l'ideale di $\mathbb{Q}[X]$ generato dal polinomio monico di grado minimo di $\mathbb{Q}[X]$ che ha $2+5i$ come radice, che risulta essere

$$m(X) := (X - 2 - 5i)(X - 2 + 5i) = X^2 - 4X + 29.$$

L'immagine di v è banalmente contenuta in $\mathbb{Q}(i)$; inoltre $i = v(-\frac{2}{5} + \frac{1}{5}X)$. Pertanto l'immagine di v è $\mathbb{Q}(i)$.

(b) Il teorema fondamentale di omomorfismo asserisce che l'applicazione

$$\overline{v} : \mathbb{Q}[X]/(m(X)) \longrightarrow \mathbb{Q}(i)$$

$$f(X) + (m(X)) \longmapsto f(2 + 5i)$$

è un isomorfismo di anelli.

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

$$I = (4 - 7i, 11 + 2i).$$

(a) Mostrare che I è principale e determinare un generatore di I.

(b) Mostrare che $\mathbb{Z}[i]/I$ è un campo. Inoltre determinare esplicitamente i suoi elementi e la sua caratteristica.

Soluzione

(a) L'anello degli interi di Gauss è un dominio euclideo e pertanto un dominio ad ideali principali. Allora l'ideale $I = (4 - 7i, 11 + 2i)$ è principale e generato da $\mathrm{MCD}(4 - 7i, 11 + 2i)$, che può essere calcolato con l'algoritmo delle divisioni successive oppure attraverso la fattorizzazione di $4 - 7i$ e $11 + 2i$ in fattori irriducibili.
$4 - 7i = (3 - 2i)(2 - i)$ con $3 - 2i$ e $2 - i$ irriducibili in quanto entrambi di norma un numero primo;
$11 + 2i = (1 + 2i)(2 - i)^2$ con $1 + 2i$ e $2 - i$ irriducibili in quanto entrambi di norma un numero primo;
pertanto $\mathrm{MCD}(4 - 7i, 11 + 2i) = 2 - i$ e $I = (2 - i)$.

(b) I è un ideale massimale di $\mathbb{Z}[i]$ poiché è generato da un elemento irriducibile di un dominio euclideo; pertanto $\mathbb{Z}[i]/I$ è un campo.
Essendo $\mathrm{N}(2 - i) = 5$, è immediato verificare che gli elementi distinti di $\mathbb{Z}[i]/I$ sono $I,\ 1 + I,\ i + I,\ (1 + i) + I,\ (1 - i) + I$; quindi $\mathbb{Z}[i]/I \simeq \mathbb{Z}_5$ e la caratteristica di $\mathbb{Z}[i]/I$ è banalmente 5.

4. Si consideri il dominio d'integrità $\mathbb{Z}[\sqrt{-7}]$.

(a) Verificare che in $\mathbb{Z}[\sqrt{-7}]$ non esistono elementi di norma uguale a 2.

(b) Verificare che 2 , $1+\sqrt{-7}$ e $1-\sqrt{-7}$ sono elementi irriducibili e non primi in $\mathbb{Z}[\sqrt{-7}]$.

(c) Utilizzando il punto precedente, trovare un elemento di $\mathbb{Z}[\sqrt{-7}]$ che ammette due fattorizzazioni in elementi irriducibili non associati.

(d) Dimostrare che in $\mathbb{Z}[\sqrt{-7}]$ si ha che $\mathrm{MCD}(2, 1 + \sqrt{-7}) = 1$ e non sussiste una identità di Bézout.

Soluzione

(a) Se $a + b\sqrt{-7} \in \mathbb{Z}[\sqrt{-7}]$, la sua norma è $a^2 + 7b^2$; se $b = 0$, l'equazione $X^2 = 2$ non ha soluzioni in $\mathbb{Z}$; se $|b| \geqslant 1$, allora $a^2 + 7b^2 \geqslant 7 > 2$; pertanto non esistono in $\mathbb{Z}[\sqrt{-7}]$ elementi di norma 2.

(b) 2 ha norma 4; $1 + \sqrt{-7}$ e $1 - \sqrt{-7}$ hanno norma 8. Poiché la norma è moltiplicativa e in $\mathbb{Z}[\sqrt{-7}]$ non ci sono elementi di norma 2, gli elementi 2 e $1 \pm \sqrt{-7}$ sono irriducibili.

Da

$$2 \cdot 4 = 8 = (1 + \sqrt{-7})(1 - \sqrt{-7})$$

segue che 2 divide $(1 + \sqrt{-7})(1 - \sqrt{-7})$; inoltre, banalmente, 2 non divive $1 + \sqrt{-7}$ né divide $1 - \sqrt{-7}$. Quindi 2 non è primo. Analogamente, $1+\sqrt{-7}$ e $1-\sqrt{-7}$ dividono 8, ma non dividono né 2 né 4.

(c) $8 = 2 \cdot 2 \cdot 2 = (1 + \sqrt{-7})(1 - \sqrt{-7})$ con 2, $1 + \sqrt{-7}$, $1 - \sqrt{-7}$ elementi irriducibili e non associati.

(d) Essendo 2 e $1 + \sqrt{-7}$ elementi irriducibili non associati, si ha che $\mathrm{MCD}(2, 1 + \sqrt{-7}) = 1$; se esistesse una identità di Bézout , da facili calcoli seguirebbe che 1 sarebbe pari.

5. Siano $f_a(X) = X^3 + X^2 + X + a \in \mathbb{Z}_3[X]$ ed $I_a = (f_a(X))$.

(a) Determinare per quali valori di a in $\mathbb{Z}_3$ l'anello quoziente $R_a = \mathbb{Z}_3[X]/I_a$ è un campo.

(b) Mostrare che $(X^5 - X^4) + I_2$ è invertibile in R_2 e calcolare il suo inverso.

Soluzione

(a) Essendo $f_a(X) = X^3 + X^2 + X + a \in \mathbb{Z}_3[X]$ un polinomio di terzo grado, $R_a = \mathbb{Z}_3[X]/I_a$ è un campo se e solo se $f_a(X)$ è privo di radici in $\mathbb{Z}_3$; è immediato verificare che soltanto per $a = 2$, $f_2(X)$ è privo di radici in $\mathbb{Z}_3$.

(b) Dividendo $X^5 - X^4$ per $X^3 + X^2 + X + 2$, si ottiene che

$$(X^5 - X^4) + I_2 = (2X^2 + 1) + I_2 \neq I_2;$$

pertanto $(X^5 - X^4) + I_2$ è invertibile in R_2. Da

$$\begin{array}{l} X^3 + X^2 + X + 2 = (2X^2 + 1)(2X + 2) - X \\ 2X^2 + 1 = -X(-2X) + 1 \end{array},$$

si ha

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

pertanto l'inverso di $(X^5 - X^4) + I_2 = (2X^2 + 1) + I_2$ è

$$(2X^2 + 2X + 1) + I_2.$$