Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2004/2005
AL2 - Algebra 2, gruppi, anelli e campi
Seconda prova di valutazione intermedia
11 gennaio 2005

Soluzione

1. Sia $A = \left\{ \frac{a}{b} : \ a, \ b \in \mathbb{Z}, \ b \neq 0 \text{ e } 5 \not| b \right\}$

   (a) Dimostrare che A è un sottoanello di $\mathbb{Q}$.

   (b) Determinare gli elementi invertibili di A.

   (c) Sia $\phi : A \to \mathbb{Z}_5$ definita da

   $$\phi\left(\frac{a}{b}\right) = \overline{a}\overline{b}^{-1}.$$

   Dimostrare che ϕ è un omomorfismo di anelli e applicare il teorema di omomorfismo.

   (d) (*facoltativo*) Usando il punto 1b, mostrare che $\ker \phi$ è l'unico ideale massimale di A

Soluzione

(a) A è un sottoanello di $\mathbb{Q}$, se per ogni $\frac{a}{b}$ e $\frac{c}{d} \in A$ si ha

- $\frac{a}{b} - \frac{c}{d} \in A$ (cioè A è un sottogruppo additivo di $\mathbb{Q}$
- $\frac{a}{b}\frac{c}{d} \in A$ (cioè A è chiuso rispetto alla moltiplicazione)

la verifica di queste proprietà è un facile esercizio.

(b) $\frac{a}{b} \in A$ è invertibile se e solamente se esiste $\frac{c}{d} \in A$ tale che

$$\frac{a}{b}\frac{c}{d} = 1 \Leftrightarrow ad = bc$$

Da cui $\frac{a}{b}$ è invertibile $\Leftrightarrow 5 \not| a$, e il suo inverso è $\frac{b}{a}$.

(c) Verifichiamo che ϕ è un omomorfismo

$$\begin{aligned}
\phi\left(\frac{a}{b} + \frac{c}{d}\right) &= \phi\left(\frac{ad+bc}{bd}\right) \\
&= (\overline{ad+bc})(\overline{bd}^{-1}) \\
&= \overline{a}\overline{d}(\overline{b}^{-1})(\overline{d}^{-1}) + \overline{b}\overline{c}(\overline{b}^{-1})(\overline{d}^{-1}) \\
&= \overline{a}\overline{b}^{-1} + \overline{c}\overline{d}^{-1} \\
&= \phi\left(\frac{a}{b}\right) + \phi\left(\frac{c}{d}\right)
\end{aligned}$$

$$\begin{aligned}
\phi\left(\frac{a}{b}\frac{c}{d}\right) &= \phi\left(\frac{ac}{bd}\right) \\
&= (\overline{ac})(\overline{bd}^{-1}) \\
&= \overline{ac}(\overline{b}^{-1})(\overline{d}^{-1}) \\
&= \overline{a}\overline{b}^{-1}\overline{c}\overline{d}^{-1} \\
&= \phi\left(\frac{a}{b}\right)\phi\left(\frac{c}{d}\right)
\end{aligned}$$

Quindi ϕ è un omomorfismo di anelli. Per applicare il teorema di omomorfismo dobbiamo determinare il nucleo e l'immagine di ϕ. Si ha

$$\begin{aligned} \mathtt{Im}\,\phi &= \mathbb{Z}_5 \\ \ker\phi &= 5A = \left\{\frac{a}{b} \in A : 5|a\right\} \end{aligned}$$

Dunque usando il teorema di omomorfismo si ha

$$A/5A \cong \mathbb{Z}_5$$

Poichè $\mathbb{Z}_5$ è un campo $5A$ è un ideale massimale di A

(d) Osserviamo che $5A$ è un ideale massimale e che $A = U(A) \cup 5A$ disgiunta, con $U(A)$ l'insieme degli elementi invertibili di A. Supponiamo che esista m ideale massimale di A diverso da $5A$ allora esiste $x \in m$ tale che $x \notin 5A$ quindi $x \in U(A)$ e dunque $m = A$. Quindi $5A$ è l'unico ideale massimale di A.

2. Sia $p(X) = X^2 + 3X + 1 \in \mathbb{Z}_7[X]$:

   (a) Dimostrare che $K = \mathbb{Z}_7[X] / (p(X))$ è un campo.

   (b) Descrivere esplicitamente gli elementi di K.

   (c) Determinare l'inverso di $X^3 + \overline{5}X + \overline{6} + (p(X))$ in K.

   Soluzione

   (a) K è un campo $\Leftrightarrow$ $(p(X))$ è un ideale massimale $\Leftrightarrow$ $p(X)$ è irriducibile, perché $\mathbb{Z}_7[X]$ è euclideo. Poiché $p(X)$ ha grado 2 per vedere che è irriducibile basta far vedere che non ha radici.

$$\begin{aligned} p(0) &= 1 \\ p(1) &= 5 \\ p(2) &= 4 \\ p(3) &= 5 \\ p(4) &= 1 \\ p(5) &= 6 \\ p(6) &= 4 \end{aligned}$$

   Quindi $p(X)$ è irriducibile e dunque K è un campo.

   (b) Siano f e $g \in \mathbb{Z}_7[X]$, posto $f(X) = r(X) + h(X)p(X)$ e $g(X) = R(X) + k(X)p(X)$ con $\deg r(X) \leq 1$ e $\deg R(X) \leq 1$, si ha

$$f \equiv g + (p(X)) \Leftrightarrow r(X) = R(X)$$

   Quindi

$$K = \{r(X) + (p(X)) : deg(r(X)) \leq 1\}$$

   Che possiamo scrivere anche nella forma seguente

$$K = \{a + b\overline{x} : a, b \in \mathbb{Z}_7\}$$

   dove $\overline{x} = X + (p(X))$.

   (c) Osserviamo che

$$X^3 + \overline{5}X + \overline{6} + (p(X)) = \overline{6}X + \overline{2} + (p(X))$$

   Quindi calcoliamo l'inverso di $\overline{6}X + \overline{2} + (p(X))$ usando il sistema

$$(\overline{6}X + \overline{2})(aX + b) \equiv 1 + (p(X))$$

   Otteniamo che l'inverso di $X^3 + \overline{5}X + \overline{6} + (p(X))$ è $\overline{2}X + \overline{3} + (p(X))$

3. Sia $\alpha = \sqrt{2} + i \in \mathbb{C}$.

   (a) Mostrare che α è algebrico su $\mathbb{Q}$.

   (b) Determinare il polinomio minimo di α su $\mathbb{Q}$ e $\mathbb{Q}(i)$.

   (c) Costruire il campo $K = \mathbb{Q}(\alpha)$ e determinare una sua base su $\mathbb{Q}$ come spazio vettoriale.

   Soluzione

   (a) α è algebrico su $\mathbb{Q}$ se esiste un polinomio $p(X)$, *non nullo*, a coefficienti in $\mathbb{Q}$ di cui α è radice. Osserviamo che

$$\begin{array}{rcl} \alpha & = & \sqrt{2} + i \\ (\alpha - i)^2 & = & (\sqrt{2})^2 \\ \alpha^2 - 2i\alpha - 1 & = & 2 \\ (\alpha^2 - 3)^2 & = & (2i)^2 \\ \alpha^4 - 6\alpha + 9 & = & -4 \\ \alpha^4 - 6\alpha + 13 & = & 0 \end{array}$$

   Quindi α è radice di $p(X) = X^4 - 6X + 13$.

   (b) Vediamo che $p(X)$ è il polinomio minimo di α su $\mathbb{Q}$. Poiché $p(X)$ è monico, dobbiamo verificare che $p(X)$ è irriducibile. Osserviamo che $p(X)$ non ha radici in $\mathbb{Q}$, quindi l'unica possibilità è che esistano due polinomi h e k di grado due tali che $p(X) = h(X)k(X)$. Ma si vede subito che il sistema che si ottiene è incompatibile. Quindi $p(X)$ è il polinomio minimo di α su $\mathbb{Q}$. Per trovare il polinomio minimo di α su $\mathbb{Q}[i]$ ripetiamo lo stesso ragionamento. Otteniamo che $p'(X) = X^2 - 2iX + 3$ è il polinomio minimo di α su $\mathbb{Q}[i]$

   (c)
$$K = \left\{a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in \mathbb{Q}\right\}$$

   E una base di K su $\mathbb{Q}$ è $\left\{1, \alpha, \alpha^2, \alpha^3\right\}$.

4. Dimostrare che in $\mathbb{Z}\left[\sqrt{-6}\right]$ l'elemento $\alpha = 10$ ha due fattorizzazioni distinte in elementi irriducibili non associati.

Soluzione

Ricordiamo che su $\mathbb{Z}\left[\sqrt{-6}\right]$ possiamo definire una norma tramite

$$N(a + b\sqrt{-6}) = a^2 + 6b^2$$

Osserviamo che $10 = 5 * 2$ e che 5 e 2 sono irriducibili non associati. Per esempio vediamo che 2 è irriducibile. Supponiamo che esistano $a + b\sqrt{-6}$ e $c + d\sqrt{-6} \in \mathbb{Z}\left[\sqrt{-6}\right]$ tali che

$$2 = (a + b\sqrt{-6})(c + d\sqrt{-6})$$

Ne segue che

$$4 = N(2) = N(a + b\sqrt{-6})N(c + d\sqrt{-6})$$

Quindi $N(a+b\sqrt{-6})|4$ cioè $N(a+b\sqrt{-6}) = 1, 2$ o 4. Se $N(a+b\sqrt{-6}) = 1$ allora l'unica possibilità è che $a = \pm 1$ e $b = 0$ e che $N(c+d\sqrt{-6}) = 4$ quindi $c = \pm 2$ e $d = 0$, abbiomo ottenuto la decomposizione banale. Mentre è facile vedere che non ci sono elementi tali che $N(a+b\sqrt{-6}) = 2$. Quindi 2 è irriducibile. Analogamente si ottiene che 5 è irriducibile. Ricordiamo che due elementi $a + b\sqrt{-6}$ e $(c + d\sqrt{-6}$ sono associati se esiste un'unità u tale che

$$a + b\sqrt{-6} = u(c + d\sqrt{-6})$$

le unità di $\mathbb{Z}_7[\sqrt{-6}]$ sono

$$U(\mathbb{Z}_7[\sqrt{-6}]) = \{-1, 1\}$$

Quindi 2 e 5 non sono associati. Vediamo adesso se esiste un'altra decomposizione di 10. $N(10) = 100$, i divisori di 100 sono 1, 2, 4, 5, 10, 20, 25, 50 e 100. Osserviamo che non ci sono elementi di norma 2 e 5 di conseguenza possiamo escludere gli eventuali elementi di norma 20 e 50. Norma 4 e 25 ci da la decomposizione $10 = 2 * 5$. Per cui non ci resta che il caso di norma 10. Osserviamo che esistono 4 elementi di norma 10, dati da $\pm(2+\sqrt{-6})$ e $\pm(2-\sqrt{-6})$ e $10 = (2+\sqrt{-6})(2-\sqrt{-6})$. La verifica che questi due elementi sono irriducibili è non associati è analoga al caso della decomposizione precedente. Quindi

$$10 = 5 * 2 = (2 + \sqrt{-6})(2 - \sqrt{-6})$$

sono due fattorizzazioni in irriducibili due a due non associati.