ALGEBRA PER INFORMATICA
Esame scritto - 11 dicembre 2006

Esercizio 1

Quali di questi insiemi sono un gruppo con l'operazione data?

- $(\{x \in \mathbb{R} \mid x \geq 0\}, \perp)$ dove $x \perp y = max\{x, y\}$;
- $(\{x \in \mathbb{C} \mid x$ è una radice ottava primitiva dell'unità$\}, \cdot)$ dove $x \cdot y$ è l'usuale prodotto in $\mathbb{C}$;
- $(\{0\} \cup \{f \in \mathbb{Q}[x] \mid \deg(f) \leq 2\}, +)$ dove $f + g$ è l'usuale somma in $\mathbb{Q}[x]$.

Soluzione

- NON è un gruppo in quanto mancano gli inversi;
- NON è un gruppo in quanto manca l'elemento neutro (1 non è una primitiva come radice ottava dell'unità) e l'insieme non è chiuso rispetto l'operazione (prodotto di radici primitive non è necessariamente primitiva);
- Questo è un sottogruppo di $\mathbb{Q}[x]$ in quanto lo zero vi appartiene, somma di polinomi nulli o di grado minore o uguale a due è un polinomio nullo o di grado minore o uguale a due e infine l'opposto di un polinomio di grado d ha anch'esso grado d.

Esercizio 2

Dato il gruppo $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, ac \neq 0 \right\}$ con l'usuale prodotto tra matrici, dimostrare che il sottoinsieme $X = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$ è un sottogruppo normale di G.

Dimostrare che il quoziente G/X è abeliano.

Soluzione

Notiamo intanto che il prodotto tra due elementi $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ di X è

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$$

e pertanto il sottoinsieme è chiuso per la somma. Inoltre la precedente osservazione ci assicura che la matrice inversa di $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ è $\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}$ e pertanto appartiene a X. Per vedere che X è un sottogruppo, basta infine notare che l'elemento neutro di G è $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ che sta sicuramente in X.

Per verificare che il sottogruppo è normale basta vedere che $ghg^{-1} \in X$ per ogni $h \in X, g \in G$. Ma questo è presto verificato facendo il prodotto

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix} = \begin{pmatrix} 1 & axc^{-1} \\ 0 & 1 \end{pmatrix} \in X$$

Verifichiamo infine che il quoziente è abeliano. Si ha infatti che, dati due elementi del quoziente $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ e $\begin{bmatrix} d & e \\ 0 & f \end{bmatrix}$, i due prodotti valgono

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} = \begin{bmatrix} ad & ae+bf \\ 0 & cf \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} ad & db+ec \\ 0 & bf \end{bmatrix}$$

che sono uguali in quanto

$$\begin{pmatrix} ad & db+ec \\ 0 & bf \end{pmatrix} \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix}^{-1} = \begin{pmatrix} ad & db+ec \\ 0 & bf \end{pmatrix} \begin{pmatrix} a^{-1}d^{-1} & -\frac{ae+bf}{acdf} \\ 0 & c^{-1}f^{-1} \end{pmatrix}^{-1} =$$

$$= \begin{pmatrix} 1 & -\frac{ae+bf}{cf} + \frac{db+ec}{ad} \\ 0 & 1 \end{pmatrix} \in X$$

Esercizio 3

Dimostrare che l'insieme $R = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, a, b \text{ coprimi}, 2 \nmid b \right\}$ con la somma e il prodotto soliti tra frazioni è un anello.

Soluzione

Bisogna dimostrare che R è un sottoanello di $\mathbb{Q}$ e che pertanto è chiuso per la somma, per il prodotto, che contiene 0 e 1 e che è chiuso per gli opposti.

Gli elementi $\frac{0}{1}$ e $\frac{1}{1}$ appartengono sicuramente a R, e d'altro canto se $\frac{a}{b} \in R$ si ha che $(a, b) = 1$ e che $2 \nmid b$. Pertanto $(-a, b) = 1$ e $2 \nmid b$, da cui $-\frac{a}{b} \in R$.

La parte più laboriosa è la dimostrazione che R è chiuso per la somma e il prodotto. Ma anche questo non è difficile in quanto basta osservare che

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{\frac{ad+cb}{(ad+cb,bd)}}{\frac{bd}{(ad+cb,bd)}}$$

e che, essendo b e d dispari, anche bd e $\frac{bd}{(ad+cb,bd)}$ lo sono. Pertanto $\frac{a}{b} + \frac{c}{d} \in R$.

Allo stesso modo

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = \frac{\frac{ac}{(ac,bd)}}{\frac{bd}{(ac,bd)}}$$

e, essendo b e d dispari, anche bd e $\frac{bd}{(ac,bd)}$ lo sono. Pertanto $\frac{a}{b}\frac{c}{d} \in R$.

Esercizio 4

Siano R, S due anelli, sia $f\colon R \to S$ un omomorfismo di anelli e sia I un ideale di S. Dimostrare che $f^{-1}(I)$ è un ideale di R.

Soluzione

Vediamo che $0 \in f^{-1}(I)$, che $f^{-1}(I)$ è chiuso per la somma, per gli inversi additivi e per il prodotto per un qualsiasi elemento di R.

Siccome $f(0) = 0 \in I$ si ha che $0 \in f^{-1}(I)$. Sia $a \in f^{-1}(I)$ un elemento del nostro sottoinsieme e sia $-a$ il suo inverso additivo. Siccome f è un omomorfismo di gruppi si ha che $f(-a) = -f(a) \in I$ in quanto I è un sottogruppo additivo. Pertanto $-a \in f^{-1}(I)$. Allo stesso modo se a, b sono due elementi di $f^{-1}(I)$, si ha che $f(a), f(b) \in I$ e $f(a + b) = f(a) + f(b)$ in quanto f è omomorfismo di gruppi. Ora essendo I un sottogruppo di S si ha che $f(a) + f(b) \in I$, cioè $a + b \in f^{-1}(I)$.

Pertanto $f^{-1}(I)$ è un sottogruppo di R.

Per vedere che si tratta di un ideale dobbiamo mostrare che dato un elemento $a \in f^{-1}(I)$ e un elemento $r \in R$, si ha che $ra \in f^{-1}(I)$. Ma $a \in f^{-1}(I)$ vuol dire che $f(a) \in I$ e pertanto $f(ra) = f(r)f(a) \in I$ perchè I è un ideale. Dunque $ra \in f^{-1}(I)$.

Esercizio 5

Scrivere le radici none dell'unità complesse (tutte le radici complesse del polinomio $x^9 - 1$), dire quali di esse sono primitive e scrivere il polinomio ciclotomico $\Phi_9(x)$ come polinomio di $\mathbb{Z}[x]$. Scomporlo quindi come prodotto di fattori irriducibili (di primo grado) in $\mathbb{C}[x]$.

Soluzione

Le radici none dell'unità sono $\{e^{-2\pi ik/9} \mid k = 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Le radici primitive sono gli elementi del precedente insieme con $(k, 9) = 1$ e cioè $\{e^{-2\pi ik/9} \mid k = 1, 2, 4, 5, 7, 8\}$.

Il nono polinomio ciclotomico risulta quindi $\Phi_9 = \Pi_{k=1,2,4,5,7,8}(x - e^{-2\pi ik/9})$ che si può agevolmente calcolare grazie alla formula $x^9 - 1 = \Phi_9\Phi_3\Phi_1$ da cui si ricava

$$\Phi_9 = \frac{x^9 - 1}{(x - 1)(x^2 + x + 1)} = x^6 + x^3 + 1$$

Esercizio 6

Dimostrare che $x^4 + x + 1$ è irriducibile in $\mathbb{Z}/2\mathbb{Z}[x]$.

Soluzione

Si vede agevolmente che in $\mathbb{Z}/2\mathbb{Z}[x]$ il polinomio $x^4 + x + 1$ non ha radici. Pertanto se fosse scomponibile, lo sarebbe in due fattori irriducibili di grado due. Ma l'unico polinomio irriducibile di grado due in $\mathbb{Z}/2\mathbb{Z}[x]$ è $x^2 + x + 1$ e pertanto l'unico polinomio prodotto di due polinomi irriducibili di secondo grado è $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1$.

Esercizio 7

Scrivere un campo con 16 elementi.

Soluzione

L'anello $(\mathbb{Z}/2\mathbb{Z}[x])/(x^4 + x + 1)$ è un anello con sedici elementi (in quanto le classi di equivalenza hanno come insieme di rappresentanti i polinomi di grado minore o uguale a tre in $\mathbb{Z}/2\mathbb{Z}[x]$ e questi sono sedici) ed è un campo (in quanto il polinomio è irriducibile e un elemento irriducibile in un P.I.D. genera un ideale massimale, modulo il quale l'anello risulta un campo).

Esercizio 8

Dimostrare che la funzione

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{\quad\phi\quad} & \mathbb{Z}/m\mathbb{Z}[x] \\ a_0 + a_1x + \ldots a_nx^n & \longmapsto & [a_0] + [a_1]x + \ldots [a_n]x^n \end{array}$$

è un omomorfismo di anelli.

Dedurre che un polinomio $a_0 + a_1x + \ldots + x^n$ è irriducibile in $\mathbb{Z}[x]$ se la sua riduzione modulo m $[a_0] + [a_1]x + \ldots + x^n$ è irriducibile in $\mathbb{Z}/m\mathbb{Z}[x]$.

Dedurne che $x^4 + 8x^2 + 3x + 1$ è irriducibile in $\mathbb{Z}[x]$.

Soluzione

Il fatto che ϕ sia un omomorfismo di anelli si dimostra molto facilmente a partire dall'omomorfismo di anelli

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/m\mathbb{Z} \ . \\ a & \longmapsto & [a] \end{array}$$

Questo vuol dire che se un polinomio $f = a_0 + a_1x + \ldots + x^n$ è riducibile in $\mathbb{Z}[x]$, si scriverà come $f = gh$ dove g e h hanno enrambi grado maggiore o uguale a 1 e i coefficienti dei termini di grado massimo di g e h possono essere considerati, senza perdita di generalità, 1.

Pertanto $\phi(f) = \phi(gh) = \phi(g)\phi(h)$ dove $\phi(g)$ ha lo stesso grado di g (perchè il suo termine di grado massimo ha coefficiente $[1] \neq [0]$) e, analogamente, $\phi(h)$ ha lo stesso grado di h.

Quindi questa è una effettiva scomposizione di $\phi(f)$ che risulta quindi riducibile.

Notiamo infine che la riduzione modulo 2 di $x^4 + 8x^2 + 3x + 1$ è $x^4 + x + 1$ che abbiamo dimostrato essere irriducibile in $\mathbb{Z}/2\mathbb{Z}[x]$ (esercizio 6). Pertanto x^4+8x^2+3x+1 è irriducibile in $\mathbb{Z}[x]$ per quanto appena detto.

Esercizio 9

Dati i polinomi

$$f(x) = 18x^4 + 27x^3 - 23x^2 - 33x - 5 \qquad \text{e} \qquad g(x) = 6x^3 + 7x^2 - 11x - 10$$

appartenenti a $\mathbb{Q}[x]$ trovarne un massimo comune divisore $M(x)$ e trovare due polinomi $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ tali che $\lambda(x)f(x) + \mu(x)g(x) = M(x)$.

Soluzione

Applichiamo l'algoritmo esteso di Euclide.

$$\begin{array}{rcrcrcrcr|l}
18x^4 & + & 27x^3 & - & 23x^2 & - & 33x & - & 5 & 6x^3 + 7x^2 - 11x - 10 \\
\cline{10-10}
18x^4 & + & 21x^3 & - & 33x^2 & - & 30x & & & 3x + 1 \\
\cline{1-9}
 & & 6x^3 & + & 10x^2 & - & 3x & - & 5 & \\
 & & 6x^3 & + & 7x^2 & - & 11x & - & 10 & \\
\cline{2-9}
 & & & & 3x^2 & + & 8x & + & 5 &
\end{array}$$

$$
\begin{array}{rcrcrcr|l}
6x^3 & + & 7x^2 & - & 11x & - & 10 & 3x^2 + 8x + 5 \\
6x^3 & + & 16x^2 & + & 10x & & & \hline 2x - 3 \\
\hline
 & - & 9x^2 & - & 21x & - & 10 & \\
 & - & 9x^2 & - & 24x & - & 15 & \\
\hline
 & & & & 3x & + & 5 &
\end{array}
$$

$$
\begin{array}{rcrcr|l}
3x^2 & + & 8x & + & 5 & 3x + 5 \\
3x^2 & + & 5x & & & \hline x + 1 \\
\hline
 & & 3x & + & 5 & \\
 & & 3x & + & 5 & \\
\hline
 & & & & 0 &
\end{array}
$$

Pertanto il massimo comune divisore è $3x + 5$ e

$$3x + 5 = 6x^3 + 7x^2 - 11x - 10 - (3x^2 + 8x + 5)(2x - 3) =$$

$$= 6x^3+7x^2-11x-10-(2x-3)(18x^4+27x^3-23x^2-33x-5-(6x^3+7x^2-11x-10)(3x+1)) =$$

$$= f(3 - 2x) + g(6x^2 - 7x - 2).$$