ALGEBRA 1
Seconda prova di accertamento - 6 dicembre 2006

Tema A

Esercizio 1

In quale degli anelli $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}/5\mathbb{Z}[x]$ è irriducibile il polinomio $f = x^4 + 4x^2 - 6$?

Soluzione

Il polinomio f ha grado 4 e pertanto è sicuramente riducibile in $\mathbb{R}[x]$ (dove tutti i polinomi irriducibili hanno grado minore o uguale a 2) e in $\mathbb{C}[x]$ (dove tutti i polinomi irriducibili hanno grado 1).

Il polinomio è inoltre riducibile su $\mathbb{Z}/5\mathbb{Z}[x]$ in quanto in questo anello vale $f = x^4 + 4x^2 - 6 = x^4 + 4x^2 + 4 = (x^2 + 2)^2$.

In $\mathbb{Q}[x]$, invece, f è irriducibile per il criterio di Eisenstein applicato usando il numero primo 2.

Esercizio 2

a) Si completi la definizione: "Il polinomio $f \in \mathbb{Z}[x]$ si dice primitivo se ..."
b) Si dimostri che il prodotto di due polinomi primitivi è primitivo (*Lemma di Gauss.*)

Soluzione

Il polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ si dice primitivo se il massimo comune divisore $MCD(a_0, a_1, \ldots, a_n)$ dei suoi coefficienti è 1.

Siano $f = a_0 + a_1x + \ldots + a_nx^n$ e $g = b_0 + b_1x + \ldots + b_mx^m$ due polinomi primitivi. Supponiamo per assurdo che fg non sia primitivo. Allora esiste un primo p che divide tutti i coefficienti di fg. Essendo f e g primitivi, p non potrà dividere tutti i coefficienti dell'uno né tutti i coefficienti dell'altro.

Siano a_h, b_k i coefficienti di grado minimo che non sono divisi da p. Scriviamo il coefficiente c_{h+k} di grado $h+k$ di fg. Si ha $c_{h+k} = (a_0b_{h+k} + \ldots + a_{h-1}b_{k+1}) + a_hb_k + (a_{h+1}b_{k-1} + \ldots + a_{h+k}b_0)$. I due termini tra parentesi sono divisibili per p per la minimalità di k, h rispettivamente. Anche c_{h+k} è divisibile per p per ipotesi.

Pertanto p divide a_hb_k e quindi divide uno dei due fattori, contraddizione.

Esercizio 3

Sia $g = x^3 - 2 \in \mathbb{R}[x]$. Definiamo la relazione $\equiv$ in $\mathbb{R}[x]$ ponendo $f_1 \equiv f_2$ se e solo se $g \mid f_2 - f_1$ in $\mathbb{R}[x]$.
a) Si verifichi che $\equiv$ è un'equivalenza.
b) Si dimostri che in ogni classe di equivalenza modulo $\equiv$ c'è uno e un solo polinomio della forma $a_0 + a_1x + a_2x^2$.

Soluzione

Per dimostrare che $\equiv$ è un'equivalenza dobbiamo vedere che è una relazione riflessiva, simmetrica e transitiva.

- Riflessiva: dato un polinomio f di $\mathbb{R}[x]$ si ha che $g \mid 0$, cioè che $g \mid (f - f)$ e pertanto che $f \equiv f$.
- Simmetrica: dati due polinomi $f_1, f_2 \in \mathbb{R}[x]$ tali che $f_1 \equiv f_2$, si ha che $g \mid (f_2 - f_1)$, pertanto che $g \mid (f_1 - f_2)$ e quindi che $f_2 \equiv f_1$.
- Transitiva: dati tre polinomi $f_1, f_2, f_3 \in \mathbb{R}[x]$ tali che $f_1 \equiv f_2$ e che $f_2 \equiv f_3$, si ha che g divide $f_2 - f_1$ e $f_3 - f_2$ e dunque divide la loro somma $f_3 - f_2 + f_2 - f_1 = f_3 - f_1$. Quindi $f_1 \equiv f_3$.

Sia f un polinomio in $\mathbb{R}[x]$. Dobbiamo dimostrare che esiste un polinomio $r \in \mathbb{R}[x]$ della forma $a_0 + a_1x + a_2x^2$ tale che $r \in [f]_\equiv$ e che se r' è un polinomio della forma $a_0 + a_1x + a_2x^2$ e $r' \in [f]_\equiv$, allora $r' = r$.

Per cominciare notiamo che, eseguendo la divisione con resto di f con g si ha che $f = gq + r$ per qualche $q, r \in \mathbb{R}[x]$ con $r = 0$ o $\deg(r) < \deg(g) = 3$. Pertanto r è della forma $a_0 + a_1x + a_2x^2$. Inoltre $f - r = gq$ e pertanto $g \mid (f - r)$, cioè $r \in [f]_\equiv$ e siamo sicuri che esista almeno un polinomio della forma voluta nella classe di f.

Vediamo che è unico. Se r' è un polinomio della forma $a_0 + a_1x + a_2x^2$ e $r' \in [f]_\equiv$, allora $r \equiv r'$ e dunque $g \mid (r' - r)$. Scriviamo $r' - r = gh$. Se $h \neq 0$ si ha che $2 \geq \deg(r' - r) = \deg(gh) = \deg(g) + \deg(h) \geq 3$, assurdo. Pertanto $h = 0$, da cui $r' - r = gh = 0$ e pertanto $r' = r$ come desiderato.

Esercizio 4

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 $\mathbb{Q}[x]$ trovare il loro 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.

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

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

$$\begin{array}{rcrcr|rcr}
3x^2 & + & 8x & + & 5 & 3x & + & 5 \\
3x^2 & + & 5x & & & x & + & 1 \\
\cline{1-5}
 & & 3x & + & 5 & & & \\
 & & 3x & + & 5 & & & \\
\cline{3-5}
 & & & & 0 & & &
\end{array}$$

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

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

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

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

Esercizio 5

Si consideri la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 5 & 2 & 6 & 9 & 8 & 1 \end{pmatrix}.$$

La si scriva come prodotto di cicli disgiunti, se ne calcoli l'ordine, la classe e la permutazione inversa.

Soluzione

La permutazione scritta in cicli disgiunti è $(1379)(245)(6)(8) = (1379)(245)$. Pertanto la sua inversa è $(9731)(542)$ e il suo ordine è il minimo comune multiplo tra gli ordini di (1379) (che ha ordine 4) e di (245) (che ha ordine 3) e quindi è 12.

Inoltre è prodotto di una permutazione dispari ((1379) che può essere scritta come prodotto di 3 trasposizioni) e di una permutazione pari ((245) che può essere scritta come prodotto di 2 trasposizioni) ed è quindi dispari.

ALGEBRA 1
Seconda prova di accertamento - 6 dicembre 2006

Tema B

Esercizio 1

In quale degli anelli $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}/5\mathbb{Z}[x]$ è irriducibile il polinomio $f = x^4 - 4x^2 - 6$?

Soluzione

Il polinomio f ha grado 4 e pertanto è sicuramente riducibile in $\mathbb{R}[x]$ (dove tutti i polinomi irriducibili hanno grado minore o uguale a 2) e in $\mathbb{C}[x]$ (dove tutti i polinomi irriducibili hanno grado 1).

Il polinomio è inoltre riducibile su $\mathbb{Z}/5\mathbb{Z}[x]$ in quanto in questo anello vale $f = x^4 - 4x^2 - 6 = x^4 - 4x^2 + 4 = (x^2 - 2)^2$.

In $\mathbb{Q}[x]$, invece, f è irriducibile per il criterio di Eisenstein applicato usando il numero primo 2.

Esercizio 2

a) Si completi la definizione: "Il polinomio $f \in \mathbb{Z}[x]$ si dice primitivo se ..."
b) Si dimostri che il prodotto di due polinomi primitivi è primitivo (*Lemma di Gauss.*)

Soluzione

Il polinomio $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ si dice primitivo se il massimo comune divisore $MCD(a_0, a_1, \ldots, a_n)$ dei suoi coefficienti è 1.

Siano $f = a_0 + a_1x + \ldots + a_nx^n$ e $g = b_0 + b_1x + \ldots + b_mx^m$ due polinomi primitivi. Supponiamo per assurdo che fg non sia primitivo. Allora esiste un primo p che divide tutti i coefficienti di fg. Essendo f e g primitivi, p non potrà dividere tutti i coefficienti dell'uno né tutti i coefficienti dell'altro.

Siano a_h, b_k i coefficienti di grado minimo che non sono divisi da p. Scriviamo il coefficiente c_{h+k} di grado $h+k$ di fg. Si ha $c_{h+k} = (a_0b_{h+k} + \ldots + a_{h-1}b_{k+1}) + a_hb_k + (a_{h+1}b_{k-1} + \ldots + a_{h+k}b_0)$. I due termini tra parentesi sono divisibili per p per la minimalità di k, h rispettivamente. Anche c_{h+k} è divisibile per p per ipotesi.

Pertanto p divide a_hb_k e quindi divide uno dei due fattori, contraddizione.

Esercizio 3

Sia $g = x^3 + 5 \in \mathbb{R}[x]$. Definiamo la relazione $\equiv$ in $\mathbb{R}[x]$ ponendo $f_1 \equiv f_2$ se e solo se $g \mid f_2 - f_1$ in $\mathbb{R}[x]$.
a) Si verifichi che $\equiv$ è un'equivalenza.
b) Si dimostri che in ogni classe di equivalenza modulo $\equiv$ c'è uno e un solo polinomio della forma $a_0 + a_1x + a_2x^2$.

Soluzione

Per dimostrare che $\equiv$ è un'equivalenza dobbiamo vedere che è una relazione riflessiva, simmetrica e transitiva.

- Riflessiva: dato un polinomio f di $\mathbb{R}[x]$ si ha che $g \mid 0$, cioè che $g \mid (f - f)$ e pertanto che $f \equiv f$.
- Simmetrica: dati due polinomi $f_1, f_2 \in \mathbb{R}[x]$ tali che $f_1 \equiv f_2$, si ha che $g \mid (f_2 - f_1)$, pertanto che $g \mid (f_1 - f_2)$ e quindi che $f_2 \equiv f_1$.
- Transitiva: dati tre polinomi $f_1, f_2, f_3 \in \mathbb{R}[x]$ tali che $f_1 \equiv f_2$ e che $f_2 \equiv f_3$, si ha che g divide $f_2 - f_1$ e $f_3 - f_2$ e dunque divide la loro somma $f_3 - f_2 + f_2 - f_1 = f_3 - f_1$. Quindi $f_1 \equiv f_3$.

Sia f un polinomio in $\mathbb{R}[x]$. Dobbiamo dimostrare che esiste un polinomio $r \in \mathbb{R}[x]$ della forma $a_0 + a_1x + a_2x^2$ tale che $r \in [f]_\equiv$ e che se r' è un polinomio della forma $a_0 + a_1x + a_2x^2$ e $r' \in [f]_\equiv$, allora $r' = r$.

Per cominciare notiamo che, eseguendo la divisione con resto di f con g si ha che $f = gq + r$ per qualche $q, r \in \mathbb{R}[x]$ con $r = 0$ o $\deg(r) < \deg(g) = 3$. Pertanto r è della forma $a_0 + a_1x + a_2x^2$. Inoltre $f - r = gq$ e pertanto $g \mid (f - r)$, cioè $r \in [f]_\equiv$ e siamo sicuri che esista almeno un polinomio della forma voluta nella classe di f.

Vediamo che è unico. Se r' è un polinomio della forma $a_0 + a_1x + a_2x^2$ e $r' \in [f]_\equiv$, allora $r \equiv r'$ e dunque $g \mid (r' - r)$. Scriviamo $r' - r = gh$. Se $h \neq 0$ si ha che $2 \geq \deg(r' - r) = \deg(gh) = \deg(g) + \deg(h) \geq 3$, assurdo. Pertanto $h = 0$, da cui $r' - r = gh = 0$ e pertanto $r' = r$ come desiderato.

Esercizio 4

Dati i polinomi

$$f(x) = 18x^4 - 9x^3 - 41x^2 + 49x + 15 \qquad \text{e} \qquad g(x) = 6x^3 - 5x^2 - 13x + 20$$

appartenenti a $\mathbb{Q}[x]$ trovare il loro 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.

$$\begin{array}{rcrcrcrcr|l}
18x^4 & - & 9x^3 & - & 41x^2 & + & 49x & + & 15 & 6x^3 - 5x^2 - 13x + 20 \\
18x^4 & - & 15x^3 & - & 39x^2 & + & 60x & & & \hline 3x + 1 \\
\hline
 & & 6x^3 & - & 2x^2 & - & 11x & + & 15 & \\
 & & 6x^3 & - & 5x^2 & - & 13x & + & 20 & \\
\hline
 & & & & 3x^2 & + & 2x & - & 5 &
\end{array}$$

$$\begin{array}{rcrcrcrcr|l}
6x^3 & - & 5x^2 & - & 13x & + & 20 & 3x^2 + 2x - 5 \\
6x^3 & + & 4x^2 & - & 10x & & & \hline 2x - 3 \\
\hline
 & - & 9x^2 & - & 3x & + & 20 & \\
 & - & 9x^2 & - & 6x & + & 15 & \\
\hline
 & & & & 3x & + & 5 &
\end{array}$$

$$\begin{array}{rcrcr|rcr}
3x^2 & + & 2x & - & 5 & 3x & + & 5 \\
3x^2 & + & 5x & & & x & - & 1 \\
\cline{1-5}
 & - & 3x & - & 5 & & & \\
 & - & 3x & - & 5 & & & \\
\cline{3-5}
 & & & & 0 & & &
\end{array}$$

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

$$3x + 5 = 6x^3 - 5x^2 - 13x + 20 - (3x^2 + 2x - 5)(2x - 3) =$$

$$= 6x^3 - 5x^2 - 13x + 20 - (2x - 3)(18x^4 - 9x^3 - 41x^2 + 49x + 15 - (6x^3 - 5x^2 - 13x + 20)(3x + 1)) =$$

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

Esercizio 5

Si consideri la permutazione

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 7 & 4 & 3 & 1 & 5 & 6 & 9 \end{pmatrix}.$$

La si scriva come prodotto di cicli disgiunti, se ne calcoli l'ordine, la classe e la permutazione inversa.

Soluzione

La permutazione scritta in cicli disgiunti è $(1286)(375)(4)(9) = (1286)(375)$. Pertanto la sua inversa è $(6821)(573)$ e il suo ordine è il minimo comune multiplo tra gli ordini di (6821) (che ha ordine 4) e di (375) (che ha ordine 3) e quindi è 12.

Inoltre è prodotto di una permutazione dispari ((6821) che può essere scritta come prodotto di 3 trasposizioni) e di una permutazione pari ((375) che può essere scritta come prodotto di 2 trasposizioni) ed è quindi dispari.