ALGEBRA 1 PB-Z
VII. 4 V 2012

Esercizio 1. Si determini, usando l'algoritmo euclideo delle divisioni successive, il massimo comun divisore in $\mathbb{Q}[X]$ dei seguenti polinomi a coefficienti razionali

$$\begin{aligned} S(X) &= 9X^6 - 3X^5 - 18X^4 + 14X^2 + 12X + 4 \\ O(X) &= 3X^4 - X^3 - 6X^2 - 4X - 2 \end{aligned}$$

e il massimo comun divisore in $\mathbb{Z}_5[X]$ dei seguenti polinomi a coefficienti in $\mathbb{Z}_5$

$$\begin{aligned} L(X) &= X^5 + \bar{1} \\ E(X) &= \bar{3}X^3 + \bar{2} \end{aligned}$$

Soluzione.

$S(X)$ e $O(X)$.

L'algoritmo euclideo delle divisioni successive è questo

$$\begin{aligned} S(X) &= Q_1(X) \cdot O(X) + R_1(X), && Q_1(X) = 3X^2 \text{ e } R_1(X) = 4(3X^3 + 5X^2 + 3X + 1) \\ O(X) &= Q_2(X) \cdot R_1(X) + R_2(X), && Q_2(X) = \tfrac{1}{4}(X - 2) \text{ e } R_2(X) = X(X + 1) \\ R_1(X) &= Q_3(X) \cdot R_2(X) + R_3(X), && Q_3(X) = 4(3X + 2) \text{ e } R_3(X) = 4(X + 1) \\ R_2(X) &= Q_4(X) \cdot R_3(X) + 0, && Q_4(X) = \tfrac{1}{4}X \end{aligned}$$

Quindi l'unico massimo comun divisore monico di $S(X)$ e $O(X)$ è il polinomio $M(X) = \frac{1}{4}R_3(X) = (X + 1)$.

Un'identità di Bezout per $M(X)$ è, ad esempio, la seguente

$$\begin{aligned} M(X) &= \tfrac{1}{4}(1 + Q_2(X)Q_3(X)) \cdot S(X) + \tfrac{1}{4}(-Q_1(X) - Q_3(X) - Q_1(X)Q_2(X)Q_3(X)) \cdot O(X) \\ &= \tfrac{1}{4}(3X^2 - 4X - 3) \cdot S(X) + \tfrac{1}{4}(-9X^4 + 12X^3 + 9X^2 - 12X - 8) \cdot O(X), \end{aligned}$$

ottenuta percorrendo "a ritroso" l'algoritmo euclideo delle divisioni successive.

$L(X)$ e $E(X)$.

L'algoritmo euclideo delle divisioni successive è questo

$$\begin{aligned} L(X) &= Q_1(X) \cdot E(X) + R_1(X), && Q_1(X) = \bar{2}X^2 \text{ e } R_1(X) = X^2 + \bar{1} \\ E(X) &= Q_2(X) \cdot R_1(X) + R_2(X), && Q_2(X) = \bar{3}X \text{ e } R_2(X) = \bar{2}(X + \bar{1}) \\ R_1(X) &= Q_3(X) \cdot R_2(X) + R_3(X), && Q_3(X) = \bar{3}X + \bar{2} \text{ e } R_3(X) = \bar{2} \end{aligned}$$

Quindi, essendo $\bar{2}$ invertibile in $\mathbb{Z}_5[X]$, l'unico massimo comun divisore monico di $L(X)$ e $E(X)$ è il polinomio costante $N(X) = \bar{1}$.

Un'identità di Bezout per $N(X)$ è, ad esempio, la seguente

$$\begin{aligned} N(X) &= \bar{3}(1 + Q_2(X)Q_3(X)) \cdot L(X) + \bar{3}(-Q_1(X) - Q_3(X) - Q_1(X)Q_2(X)Q_3(X)) \cdot E(X) \\ &= (\bar{2}X^2 + \bar{3}X + \bar{3}) \cdot L(X) + (X^4 + \bar{4}X^3 + \bar{4}X^2 + X + \bar{4}) \cdot E(X) \end{aligned}$$

ottenuta percorrendo "a ritroso" l'algoritmo euclideo delle divisioni successive.

Esercizio 2. Siano κ un campo e $\kappa[\mathrm{X}]$ l'anello dei polinomi a coefficienti in κ.

I. Si mostri che è possibile definire su $\kappa[\mathrm{X}]$ una struttura di κ-spazio vettoriale ([1]).

II. Per ogni $n \in \mathbb{N}$ sia $\kappa[\mathrm{X}]_n = \{p(\mathrm{X}) \in \kappa[\mathrm{X}] \mid \deg(p(\mathrm{X})) \leq n\}$ l'insieme dei polinomi di grado minore o uguale a n. Mostrare che
1. per ogni $n \in \mathbb{N}$ l'insieme $\kappa[\mathrm{X}]_n$ è un sottospazio vettoriale di $\kappa[\mathrm{X}]$;
2. per ogni $n \in \mathbb{N}$ l'insieme $\kappa[\mathrm{X}]_n$ non è un sottoanello di $\kappa[\mathrm{X}]$.

Soluzione.

I. L'insieme $\kappa[\mathrm{X}]$ dotato dell'usuale operazione di somma tra polinomi è un gruppo commutativo. Definiamo l'operazione di "prodotto per uno scalare" come segue

$$\kappa \times \kappa[\mathrm{X}] \ni (a, p(\mathrm{X})) \mapsto [ap](\mathrm{X}) \in \kappa[\mathrm{X}],$$

essendo $[ap](\mathrm{X})$ il polinomio definito come polinomio prodotto del polinomio costante $cost_a(\mathrm{X}) = k$ e del polinomio $p(\mathrm{X})$; ossia, $[ap](\mathrm{X}) = [a \cdot p](\mathrm{X})$.

Essendo $\kappa[\mathrm{X}]$ un anello unitario, tutti gli assiomi presenti nella definizione di spazio vettoriale risultano essere automaticamente soddisfatti.

II.1. Iniziamo con l'osservare che il sottoinsieme $\kappa[\mathrm{X}]_n \subseteq \kappa[\mathrm{X}]$ è definito a partire da una certa condizione sul grado dei suoi ipotetici elementi. Ora, dal fatto che il grado del prodotto $[ap](\mathrm{X})$ di uno scalare $a \in \kappa$ per un qualsivoglia polinomio $p(\mathrm{X})$ è sempre uguale al grado di $p(\mathrm{X})$, segue che l'insieme $\kappa[\mathrm{X}]_n$ è chiuso per l'operazione di "prodotto per uno scalare". Infatti, per ogni $a \in \kappa$ e per ogni $p(\mathrm{X}) \in \kappa[\mathrm{X}]_n$, risulta $\deg([ap](\mathrm{X})) = \deg(p(\mathrm{X})) \leq n$ e, quindi, $[ap](\mathrm{X}) \in \kappa[\mathrm{X}]_n$. Resta dunque da mostrare che $\kappa[\mathrm{X}]_n$ è chiuso per la somma. Questo è presto fatto; infatti, dati comunque $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]_n$, con $p_1(\mathrm{X}) = a_n\mathrm{X}^n + ... + a_0$ e $p_2(\mathrm{X}) = b_n\mathrm{X}^n + ... + b_0$, risulta

$$[p_1 + p_2](\mathrm{X}) = p_1(\mathrm{X}) + p_2(\mathrm{X}) = (a_n + b_n)\mathrm{X}^n + ... + a_0 + b_0$$

che, evidentemente, è un elemento di $\kappa[\mathrm{X}]_n$ ([2]).

Gli assiomi di spazio vettoriale o sono facilmente verificabili o sono automaticamente soddisfatti.

II.2. È sufficiente esibire un esempio: siano i polinomi $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]$ entrambi uguali al polinomio $potenza_n(\mathrm{X}) = \mathrm{X}^n$. Allora, benché entrambi $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$ siano elementi di $\kappa[\mathrm{X}]_n$, risulta $[p_1 \cdot p_2](\mathrm{X}) \notin \kappa[\mathrm{X}]_n$. Infatti,

$$[p_1 \cdot p_2](\mathrm{X}) = p_1(\mathrm{X}) \cdot p_2(\mathrm{X}) = potenza_n(\mathrm{X}) \cdot potenza_n(\mathrm{X}) = \mathrm{X}^n \cdot \mathrm{X}^n = \mathrm{X}^{2n}$$

che, evidentemente, non appartiene a $\kappa[\mathrm{X}]_n$, essendo $\deg([p_1 \cdot p_2](\mathrm{X})) = 2n \gneq n$.

---

[1] *Sugg.:* ...trovare le operazioni di "somma" e "prodotto per uno scalare", poi verificare il soddisfacimento degli assiomi...

[2] Poiché " $\lneq \Rightarrow \leq$ ", il caso $a_n + b_n = 0$ è ammesso dalla definizione di $\kappa[\mathrm{X}]_n$. Infatti, se $a_n + b_n = 0$, allora $\deg([p_1 + p_2](\mathrm{X})) \lneq n$ e, quindi, $\deg([p_1 + p_2](\mathrm{X})) \leq n$.

Esercizio 3. Siano A e I insiemi. Si assuma che A sia non vuoto e che, per ogni $i \in I$, sia definita su A un'operazione n_i-aria $\omega_i : A^{n_i} \to A$.

Sia, ora, X un qualsivoglia insieme. Si mostri che, per ogni $i \in I$, l'operazione ω_i induce sull'insieme A^X un'operazione n_i-aria $\tilde{\omega}_i : (A^X)^{n_i} \to A^X$.

Soluzione. Per ogni $i \in I$, sia $\tilde{\omega}_i : (A^X)^{n_i} \to A^X$ l'operazione n_i-aria su A^X definita da

$$(A^X)^{n_i} \quad \ni \quad (\alpha_1, ..., \alpha_{n_i}) \quad \mapsto \quad \tilde{\omega}_i(\alpha_1, ..., \alpha_{n_i}) \quad \in \quad A^X,$$

essendo $\tilde{\omega}_i(\alpha_1, ..., \alpha_{n_i}) \in A^X$ la funzione definita da

$$X \quad \ni \quad x \quad \mapsto \quad [\tilde{\omega}_i(\alpha_1, ..., \alpha_{n_i})](x) = \omega_i(\alpha_1(x), ..., \alpha_{n_i}(x)) \quad \in \quad A.$$

Esercizio 4. Dire se i seguenti polinomi a coefficienti interi ammettono radici razionali

$$\begin{aligned} \mathrm{L(X)} &= \mathrm{X}^{57} - 2\mathrm{X}^{32} - 17 \\ \mathrm{E(X)} &= 3\mathrm{X}^8 + 55\mathrm{X}^6 + 2 \\ \mathrm{O(X)} &= \mathrm{X}^5 + 1 \end{aligned}$$

Soluzione. Utilizzeremo la seguente affermazione.

Affermazione. Sia $p(\mathrm{X}) \in \mathbb{Z}[\mathrm{X}]$, $p(\mathrm{X}) = a_n\mathrm{X}^n + ... + a_0$, un polinomio a coefficienti interi. Se $z \in \mathbb{Q}$ è una radice razionale di $p(\mathrm{X})$, allora, scrivendo $z = \frac{u}{v}$ con $\mathrm{MCD}(u, v) = 1$, si ha $u|a_0$ e $v|a_n$.

L(X)

Al fine di selezionare dei numeri razionali candidati ad essere radici di L(X), studiamo i divisori del termine noto e del coefficiente direttore L(X).

I divisori del termine noto (che è -17) sono 1, -1, 17 e -17; i divisori del coefficiente direttore (che è 1) sono 1 e -1. Quindi i razionali candidati ad essere radici di L(X) sono 1, -1, 17 e -17.

Un semplice verifica (fatta valutando L(X) in ± 1 e ± 17) mostra che nessuno di questi numeri è una radice di L(X).

E(X)

Al fine di selezionare dei numeri razionali candidati ad essere radici di E(X), studiamo i divisori del termine noto e del coefficiente direttore E(X).

I divisori del termine noto (che è 2) sono 1, -1, 2 e -2; i divisori del coefficiente direttore (che è 3) sono 1, -1, 3 e -3. Quindi i razionali candidati ad essere radici di E(X) sono 1, -1, 2, -2, $\frac{1}{3}$, $-\frac{1}{3}$, $\frac{2}{3}$ e $-\frac{2}{3}$.

Un semplice verifica (fatta valutando E(X) in ± 1, ± 2, $\pm\frac{1}{3}$ e $\pm\frac{2}{3}$) mostra che nessuno di questi numeri è una radice di E(X).

O(X)

Al fine di selezionare dei numeri razionali candidati ad essere radici di O(X), studiamo i divisori del termine noto e del coefficiente direttore O(X).

I divisori del termine noto (che è 1) sono 1 e -1; i divisori del coefficiente direttore (che è 1) sono 1 e -1. Quindi i razionali candidati ad essere radici di E(X) sono 1 e -1.

Un semplice verifica (fatta valutando O(X) in ± 1) mostra che 1 non è una radice di O(X) e -1 è una radice di O(X).

Esercizio 5. Siano κ un campo, $\kappa[\mathrm{X}]$ l'anello dei polinomi a coefficienti in κ e $\kappa[\mathrm{X}]_{\mathrm{mon}} \subseteq \kappa[\mathrm{X}]$ l'insieme i cui elementi sono tutti e soli i polinomi monici di $\kappa[\mathrm{X}]$.

I. Si mostri che $\kappa[\mathrm{X}]_{\mathrm{mon}}$ non è chiuso per l'operazione di somma

II. Si mostri che $(\kappa[\mathrm{X}]_{\mathrm{mon}},\ \cdot\ )$ è un monoide commutativo.

III. Si mostri che $(\kappa[\mathrm{X}]_{\mathrm{mon}},\ |\ )$ è un insieme parzialmente ordinato e tale che: per ogni $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]_{\mathrm{mon}}$ esistono unici un minimo $|$-maggiorante comune e un massimo $|$-minorante comune di $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$.

Soluzione. Iniziamo con l'osservare che il polinomio costante $u(\mathrm{X}) = 1_\kappa$ è monico; ossia, $u(\mathrm{X}) \in \kappa[\mathrm{X}]_{\mathrm{mon}}$. Inoltre, $u(\mathrm{X})$ è l'unico polinomio ad essere contemporaneamente costante e monico.

I. È sufficiente esibire un esempio: siano i polinomi $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]$ entrambi uguali al polinomio costante $u(\mathrm{X}) = 1_\kappa$. Allora, benché entrambi $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$ siano monici, risulta $[p_1 + p_2](\mathrm{X}) \notin \kappa[\mathrm{X}]_{\mathrm{mon}}$. Infatti,

$$[p_1 + p_2](\mathrm{X}) \quad = \quad p_1(\mathrm{X}) + p_2(\mathrm{X}) \quad = \quad u(\mathrm{X}) + u(\mathrm{X}) \quad = \quad 1_\kappa + 1_\kappa$$

che è (costante e) non monico, essendo sempre vero che $1_\kappa + 1_\kappa \neq 1_\kappa$.

II. L'associatività e la commutatività della moltiplicazione in $\kappa[\mathrm{X}]_{\mathrm{mon}} \subseteq \kappa[\mathrm{X}]$ seguono da quelle in $\kappa[\mathrm{X}]$. Ora, poiché abbiamo già osservato che il polinomio costante $u(\mathrm{X}) = 1_\kappa$ è un elemento di $\kappa[\mathrm{X}]_{\mathrm{mon}}$, resta da verificare solamente che $\kappa[\mathrm{X}]_{\mathrm{mon}}$ è chiuso per l'operazione di prodotto. Questo è presto fatto; infatti, dati comunque $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]_{\mathrm{mon}}$, con $p_1(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + ... + a_0$ e $p_2(\mathrm{X}) = \mathrm{X}^m + b_{m-1}\mathrm{X}^{m-1} + ... + b_0$, risulta

$$[p_1 \cdot p_2](\mathrm{X}) \quad = \quad p_1(\mathrm{X}) \cdot p_2(\mathrm{X}) \quad = \quad \mathrm{X}^{n+m} + (a_{n-1} + b_{m-1})\mathrm{X}^{n+m-1} + ... + a_0 b_0$$

che, evidentemente, è monico.

III. Bisogna mostrare che $|$ è una relazione riflessiva, antisimmetrica e transitiva. Essendo la riflessività e la transitività di $|$ vere in $\kappa[\mathrm{X}]$, esse sono vere anche in $\kappa[\mathrm{X}]_{\mathrm{mon}} \subseteq \kappa[\mathrm{X}]$. Resta dunque da dimostrare che $|$ è antisimmetrica; ossia, che per ogni $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]_{\mathrm{mon}}$ per cui $p_1(\mathrm{X}) \mid p_2(\mathrm{X})$ e $p_2(\mathrm{X}) \mid p_1(\mathrm{X})$ risulta $p_1(\mathrm{X}) = p_2(\mathrm{X})$. Questo è presto fatto; infatti, secondo la teoria generale,

$$p_1(\mathrm{X}) \mid p_2(\mathrm{X}) \text{ e } p_1(\mathrm{X}) \mid p_2(\mathrm{X}) \quad \Leftrightarrow \quad \text{esiste un unico elemento } a \in \kappa^* \text{ tale che } p_1(\mathrm{X}) = a p_2(\mathrm{X}).$$

Ora, essendo entrambi $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$ monici, necessariamente risulta $a = 1_\kappa$. Quindi, $p_1(\mathrm{X}) = a p_2(\mathrm{X}) = 1_\kappa p_2(\mathrm{X}) = p_2(\mathrm{X})$; ossia, $p_1(\mathrm{X}) = p_2(\mathrm{X})$.

Infine, dati comunque $p_1(\mathrm{X}),\ p_2(\mathrm{X}) \in \kappa[\mathrm{X}]_{\mathrm{mon}}$, un minimo $|$-maggiorante comune e un massimo $|$-minorante comune di $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$ sempre esistono, essi altro non essendo che un minimo comune multiplo $\mathrm{mcm}(p_1(\mathrm{X}), p_2(\mathrm{X}))(\mathrm{X})$ e, rispettivamente, un massimo comun divisore $\mathrm{MCD}(p_1(\mathrm{X}), p_2(\mathrm{X}))(\mathrm{X})$ di $p_1(\mathrm{X})$ e $p_2(\mathrm{X})$. L'unicità di tali elementi è garantita dalla condizione di monicità.