ESERCIZI SU ANELLI DI POLINOMI

ESERCIZIO 1

Sia $\phi : R \to S$ un omomorfismo unitario tra due anelli commutativi con identità. Dimostrare che esiste un unico omomorfismo unitario $\overline{\phi} : R[x_1, \ldots, x_n] \to S[x_1, \ldots, x_n]$ che si restringe all'omomorfismo ϕ sui polinomi costanti e che manda ogni monomio x^I in sé stesso.

ESERCIZIO 2(Proprietà universale dell'anello di polinomi)

Dimostrare che l'anello di polinomi $R[x_1, \ldots, x_n]$ in n variabili a coefficienti su anello R commutativo con identità soddisfa la seguente proprietà universale: dato un anello commutativo con unità S, un omomorfismo unitario $\phi : R \to S$ e n elementi $u_1, \ldots, u_n$ di S, esiste ed è unico un omomorfismo unitario $\Phi : R[x_1, \ldots, x_n] \to S$ tale che $\Phi_{|R} = \phi$ e $\Phi(x_i) = u_i$ per ogni $1 \leq i \leq n$.

ESERCIZIO 3(Anelli monoidali)

Sia R un anello commutativo con unità e sia $M = (M, ., 0)$ un monoide. Si definisca l'*anello monoidale* $R[M]$ come l'insieme delle funzioni $f : M \to R$ tali che $f(u) \neq 0$ solo per un numero finito di elementi di M e si definiscano

$$\begin{aligned}(f+g)(m) &= f(m) + g(m),\\ (f \cdot g)(m) &= \sum_{p.q=m} f(p)g(q),\\ 0(m) &= 0,\\ 1(m) &= 1.\end{aligned}$$

(i) Mostrare che $R[M] = (R[M], +, 0, \cdot, 1)$ è un anello con identità, che è commutativo se e solo se il monoide M è commutativo.

(ii) Mostrare che $R[\mathbb{N}^n] \cong R[x_1, \ldots, x_n]$.

ESERCIZIO 4

Si consideri l'anello di polinomi $R[x_1, \ldots, x_n]$ (con R anello commutativo con identità).

(i) Per ogni $\sigma \in S_n$, dimostrare che esiste un'unico automorfismo $\zeta(\sigma)$ di $R[x_1, \ldots, x_n]$ che è l'identità su R e manda x_i in $x_{\sigma(i)}$ per ogni $1 \leq i \leq n$.
[Suggerimento: usare la proprietà universale di $R[x_1, \ldots, x_n]$, vedi Esercizio 2.]

(ii) Dimostrare che $\zeta(\sigma\tau) = \zeta(\sigma) \circ \zeta(\tau)$ per ogni $\sigma, \tau \in S_n$ (cioè che ζ definisce un'azione di S_n su $R[x_1, \ldots, x_n]$).

(iii) Si consideri il polinomio $\Delta = \prod_{1 \leq i < j \leq n}(x_i - x_j) \in R[x_1, \ldots, x_n]$. Dimostrare che

$$\zeta(\sigma)(\Delta) = (-1)^{|\mathrm{inv}(\sigma)|}\Delta.$$

(iv) Mettendo insieme (ii) e (iii), si deduca che

$$\begin{aligned}\widetilde{\mathrm{sgn}} : S_n &\longrightarrow \{\pm 1\},\\ \sigma &\mapsto (-1)^{|\mathrm{inv}(\sigma)|},\end{aligned}$$

è un omomorfismo di gruppi.

(v) Per ogni $1 \leq k \leq n$, si considerino i seguenti polinomi (chiamati *polinomi simmetrici elementari*)

$$e_k = e_k(x_1, \ldots, x_n) := \prod_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} \ldots x_{i_k}.$$

Dimostrare che i polinomi e_k sono invarianti per S_n, cioè $\zeta(\sigma)(e_k) = e_k$ per ogni $\sigma \in S_n$.

ESERCIZIO 5 (Anello delle serie formali) [NUOVA VERSIONE]

Sia R un anello commutativo con identità e si consideri l'insieme delle *serie formali* a coefficienti in R

$$R[|x|] := \{f(x) = \sum_{n\geq 0} a_n x^n \ : a_n \in R\},$$

munito delle seguenti operazioni

$$\begin{cases} \sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} (a_n + b_n) x^n, \\ \sum_{n\geq 0} a_n x^n \cdot \sum_{m\geq 0} b_m x^m = \sum_{k\geq 0} \left(\sum_{n+m=k} a_n b_m \right) x^k. \end{cases}$$

(i) Si dimostri che $R[|x|]$ è un anello commutativo con identità rispetto alle operazioni sopra definite con 0 dato dalla serie nulla e $1 = 1 \cdot x^0$.

(ii) Dimostrare che $R[x]$ è un sottoanello unitario di $R[|x|]$.

(iii) Si definisca la funzione (chiamata valutazione)

$$\begin{aligned} \text{val} : R[|x|] &\longrightarrow \mathbb{N} \cup \{+\infty\}, \\ 0 &\mapsto +\infty, \\ 0 \neq f(x) = \sum_{n\geq 0} a_n x^n &\mapsto \min\{n \in \mathbb{N} \ : a_n \neq 0\}. \end{aligned}$$

Mostrare che

$$\begin{cases} \text{val}(f+g) \geq \min\{\text{val}(f), \text{val}(g)\} & \text{con uguaglianza se } \text{val}(f) \neq \text{val}(g), \\ \text{val}(fg) \geq \text{val}(f) + \text{val}(g) & \text{con uguaglianza se } D \text{ è un dominio.} \end{cases}$$

(iv) Dimostrare che se R è un dominio allora $R[|x|]$ è un dominio.
[Suggerimento: si usi la valutazione del punto precedente.]

(v) Dimostrare che $f(x) = \sum_{n\geq 0} a_n x^n$ è un'unità di $R[|x|]$ se e solo se a_0 è un'unità di R. In particolare, se R è un campo, allora $f(x) \in R[|x|]$ è invertibile se e solo se $\text{val}(f) = 0$.

(vi) Dimostrare che se K è un campo, allora $K[|x|]$ è un PID in cui tutti gli ideali non nulli sono della forma (x^n) al variare di $n \geq 0$. In particolare, $K[|x|]$ ha unico ideale primo (equivalentemente massimale), e cioè (x).

ESERCIZIO 6

Sia D un dominio. Dimostrare che il campo dei quozienti di $D[x]$ è isomorfo al campo dei quozienti di $Q(D)[x]$.

ESERCIZIO 7(Interpolazione polinomiale)

Sia K un campo. Siano $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ elementi di K tali che $x_i \neq x_j$ per ogni $i \neq j$. Dimostrare che esiste ed è unico un polinomio $p(x) \in K[x]$ di grado minore di n tale che $p(x_i) = y_i$ per ogni $1 \leq i \leq n$.

[Suggerimento: per l'unicità, usare che un polinomio non-nullo $p(x)$ di grado m può avere al più m radici in K. Per l'esistenza si consideri

$$p(x) = \sum_{i=1}^{n} y_i \prod_{j\neq i} \frac{x - x_j}{x_i - x_j}.]$$

ESERCIZIO 8

Mostrare che:

(i) Se K è un campo algebricamente chiuso (esempio: $K = \mathbb{C}$) allora gli elementi irriducibili di $K[x]$ sono associati a $x - a$, con $a \in K$.
[Suggerimento: si usi che dato $f(x) \in K[x]$ e $a \in K$, vale che $f(a) = 0$ se e solo se $(x - a)|f(x)$.]

(ii) Gli elementi irriducibili di $\mathbb{R}[x]$ sono associati a $x-a$ con $a \in \mathbb{R}$ oppure a $x^2+\alpha x+\beta$ con $\alpha, \beta \in \mathbb{R}$ tali che $\alpha^2 - 4\beta^2 < 0$.
[Suggerimento: dato $f(x) \in \mathbb{R}[x]$ si consideri la sua fattorizzazione in irriducibili in $\mathbb{C}[x]$...]

(iii) Dimostrare che per ogni $\alpha, \beta \in \mathbb{R}$ tali che $\alpha^2 - 4\beta^2 < 0$ si ha che

$$\mathbb{R}[x]/(x^2 + \alpha x + \beta) \cong \mathbb{C}.$$

ESERCIZIO 9

Sia p un primo.

(i) Se $f(x) \in \mathbb{Z}_p[x]$ è irriducibile di grado $n \geq 1$ allora $\mathbb{Z}_p[x]/(f(x))$ è un campo con p^n elementi.

Sia ora F un campo finito.

(ii) Dimostrare che la cardinalità di F è p^n per qualche primo p e $n \geq 1$.
[Suggerimento: mostrare che $\mathrm{car}(F) = p$ con p primo e che F è uno spazio vettoriale di dimensione finita su $\mathbb{Z}_p$.]

(iii) Dimostrare che F^* è un gruppo ciclico (di cardinalità uguale a $p^n - 1$).
[Suggerimento: mostrare che per ogni primo q e per ogni $m \geq 1$, F^* ha al più q^m elementi di ordine che divide q^m. Usare la struttura dei gruppi abeliani finiti.]

(iv) Fissato un generatore g di F^*, si mostri che l'omomorfismo unitario di anelli

$$\Psi : \mathbb{Z}_p[x] \longrightarrow F$$

che estende l'inclusione $\mathbb{Z}_p \subseteq F$ e che manda x in g è suriettivo. Dedurre che $F \cong \mathbb{Z}_p[x]/(f(x))$ per un certo polinomio $f(x) \in \mathbb{Z}_p[x]$ è irriducibile di grado n.

ESERCIZIO 10

Mostrare che dato un elemento p non nullo e non invertibile in un dominio integrale D, l'ideale (p, x) in $D[x]$ non è principale.

Dedurre che se D è un dominio integrale che non è un campo, allora $D[x]$ non è un PID.

[Suggerimento: se (p, x) fosse principale uguale a $(m(x))$ con $m(x) \in D[x]$, allora $m(x)$ sarebbe il massimo comun divisore di p e x....]

ESERCIZIO 11

Dato un anello commutativo R con identità, si consideri l'anello di polinomi in infinite variabili

$$R[x_1, x_2, \ldots] := \bigcup_{n \geq 0} R[x_1, \ldots, x_n],$$

dove l'unione è fatta rispetto alle inclusioni canoniche

$$R \subset R[x_1] \subset R[x_1, x_2] \subset \ldots ...$$

(i) Dimostrare che $R[x_1, x_2, \ldots]$ non è Noetheriano, cioé non soddisfa la condizione sulle catene ascendenti di ideali.

(ii) Dimostrare che se R è un UFD, allora $R[x_1, x_2, \ldots]$ è un UFD.

ESERCIZIO 12

Sia K un campo e si consideri il campo $K(x) := Q(K[x])$ (chiamato campo delle *funzioni razionali* in una variabile a coefficienti in K).

Sia $f(x) \in K[x]$ di grado positivo e si consideri la sua fattorizzazione in irriducibili $f(x) = p_1(x)^{e_1} \dots p_r(x)^{e_r}$.

(i) Dimostrare che per ogni polinomio $g(x) \in K[x]$, possiamo scrivere l'elemento $g/f \in K(x)$ nella seguente forma (chiamata *decomposizione in frazioni parziali*)

$$\frac{g(x)}{f(x)} = q(x) + \sum_{i=1}^{r} \frac{g_i(x)}{p_i(x)^{e_i}} = \sum_{i=1}^{r} \left[\sum_{k=1}^{e_i} \frac{a_{i,k}(x)}{p_i(x)^k} \right], \tag{0.1}$$

per certi polinomi $q(x), g_i(x), a_i^k(x) \in K[x]$ tali che $\deg g_i(x) < e_i \deg p_i(x)$ e $\deg a_{i,k}(x) < \deg p_i(x)$.

[Suggerimento: per la prima uguaglianza si scriva prima $g(x) = q(x)f(x) + r(x)$ con $\deg r(x) < \deg f(x)$. Si mostri poi che se $f(x) = f_1(x)f_2(x)$ con polinomi $f_1(x), f_2(x)$ relativamente primi, allora possiamo scrivere $r(x) = u_1(x)f_1(x) + u_2(x)f_2(x)$ con $\deg u_i(x) < \deg f_i(x)$. Per la seconda uguaglianza, si mostri che possiamo scrivere $g_i(x) = a_{i,e_i}(x) + a_{i,e_i-1}(x)p_i(x) + \ldots + a_{i,1}p_i(x)^{e_i-1}$.]

(ii) Si discuta l'unicità della decomposizione (0.1).

ESERCIZIO 13 (Criterio di irriducibilità di Eisenstein)

Si consideri un polinomio $f(x) = a_0 + a_1x + \ldots a_nx^n \in \mathbb{Z}[x]$ di grado $n \geq 2$. Se esiste un numero primo p tale che:

- $p|a_i$ per ogni $0 \leq i \leq n-1$,
- $p \not| a_n$,
- $p^2 \not| a_0$,

allora $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

[Suggerimento: per assurdo, se $f(x)$ si fattorizzasse in $\mathbb{Q}[x]$, allora per quanto visto a lezione esisterebbe una fattorizzazione $f(x) = g(x)h(x)$ con $g(x), h(x) \in \mathbb{Z}[x]$ di grado positivo. Riducendo modulo p, otterremmo che $0 \neq \overline{a}_n x^n = \overline{f(x)} = \overline{g(x)h(x)}$ in $\mathbb{Z}_p[x]$ (perché?) il che implica che i termini noti di $f(x)$ e $g(x)$ sono divisibilie per p (perché?). Dunque otterremmo che il termine noto di $f(x)$ sarebbe divisibile per p^2 (perché?), assurdo.]

ESERCIZIO 14 (Polinomio ciclotomico p-esimo)

Per ogni primo p, si consideri il polinomio $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$ (chiamato *polinomio ciclotomico p-esimo*).

(i) Dimostrare che le radici di $\Phi_p(x)$ in $\mathbb{C}$ sono tutte e sole le radici p-esime non triviali dell'unità.

(ii) Dimostrare che $\Phi_p(x+1)$ verifica le ipotesi del criterio di Eisenstein rispetto al primo p. Concludere che $\Phi_p(x)$ è irriducibile in $\mathbb{Q}[x]$ e anche in $\mathbb{Z}[x]$.

[Suggerimento: usare la formula $\Phi_p(x) \cdot (x-1) = x^p - 1$ in $\mathbb{Z}[x]$.]

ESERCIZIO 15

Sia D un UFD e sia $f(x) \in D[x]$ un polinomio non constante monico (cioè con coefficiente direttore uguale a 1).

(i) Dimostrare che ogni fattore irriducibile monico di $f(x)$ in $Q(D)[x]$ è contenuto in $D[x]$.

(ii) Dimostrare che ogni radice di $f(x)$ in $Q(D)$ è contenuta in D.

ESERCIZIO 16

Sia D un UFD. Dimostrare che gli elementi irriducibili (o equivalentemente primi) di $D[x]$ sono gli elementi irriducibili di D (visti come polinomi costanti) e i polinomi non costanti $f(x) \in D[x]$ tali che $C(f) \sim 1$ e $f(x)$ è irriducibile in $Q(D)[x]$.

ESERCIZIO 17

Sia D un dominio integrale con campo dei quozienti $F = Q(D)$.

(i) Dimostrare che ogni automorfismo $\phi : D[x] \xrightarrow{\cong} D[x]$ (come anello) che induce l'identità su D è univocamente determinato dalla formula

$$\phi(x) = ax + b,$$

per certi elementi (unici) $a \in U(D)$ e $b \in D$.

(ii) Dimostrare che ogni automorfismo $\phi : F(x) := Q(F[x]) \xrightarrow{\cong} F(x)$ (come anello) che induce l'identità su F è univocamente determinato dalla formula

$$\phi(x) = \frac{ax + b}{cx + d},$$

per certi elementi (unici a meno di moltiplicazione per un comune elemento non nullo di F) $a, b, c, d \in F$ tali che $ad - bc \neq 0$.