Fonaments d'Àlgebra

Llista 7 de Problemes

Anell de Polinomis, Màxim Comú Divisor, $\mathbb{Z}[i]$.

Curs 2001/02, 1er semestre

1. Sigui R un anell i I un ideal bilàter de R. Enuncieu i desmostreu la propietat universal de R/I (o més precisament de $\pi : R \to R/I$).

2. Siguin R un anell, S un anell, $\varphi : R \to S$ un morfime, i $s \in S$ tal que s commuta amb tot element de $\varphi(R)$, és a dir $s\varphi(r) = \varphi(r)s \ \forall r \in R$. Demostreu que existeix un únic morfisme d'anells $\psi : R[x] \to S$ fent commutatiu el diagrama

$$\begin{array}{ccc} R & \to & R[x] \\ \varphi \downarrow & \swarrow \psi & \\ S & & \end{array}$$

   tal que $\psi(x) = s$.(Aquesta és la propietat universal de $R[x]$).

3. Sigui K un cos, V un K-espai vectorial, $End_K(V)$ l'anell d'endomorfismes K-lineals de V, i $f \in End_K(V)$.

   (a) Demostreu que existeix un morfisme d'anells $\varphi : K \to End_K(V)$ i que $\varphi(K)$ commuta amb f.

   (b) Considereu
   $$\psi : K[X] \to K[f]$$
   donat per
   $$p(x) = \sum_i a_i x^i \mapsto p(f) = \sum_i \varphi(a_i) f^i,$$
   amb $a_i \in K$. Proveu que està ben definida, és un morfisme d'anells exhaustiva i ψ és K-lineal.

   (c) Proveu que $ker(\psi)$ és un ideal principal. (Si $ker(\psi)$ no és zero, està generat pel polinomi que s'anomena el *polinomi mínim* de l'endomorfisme f).

   (d) * Si $dim_K V < \infty$ demostreu $dim_K End_K(V) < \infty$ i $ker(\psi) \neq 0$.

4. Considerem el subanell de $\mathbb{Q}[x, y]$ següent: $D = \mathbb{Z} + x\mathbb{Q}[x, y] + y\mathbb{Q}[x, y]$. Proveu que x^2, xy no tenen màxim comú divisor en D.

5. Utilitzant l'algorisme d'Euclides amb matrius donat a classe de teoria calculeu el $mcd(x^{27}-1, x^{15}-1)$. Trobeu a més dos polinomis $f, g \in \mathbb{Q}[x]$ que satisfacin la igualtat

$$(x^{27}-1)f(x) + (x^{15}-1)g(x) = mcd(x^{27}-1, x^{15}-1).$$

Són únics aquests $f(x)$ i $g(x)$?

6. Sigui p un primer de $\mathbb{Z}$. En aquest exercici volem decidir quan l'equació

$$x^2 + y^2 = p$$

amb $x, y \in \mathbb{Z}$ té solució. Per exemple $2 = 1^2 + 1^2$, on l'anterior equació té solució si $p = 2$. Tenim que $\mathbb{Z}[i]$ és un DE amb $d(x+iy) = x^2 + y^2$. Resoldre l'equació és equivalent a trobar $w \in \mathbb{Z}[i]$ amb $d(w) = p$. Proveu,

   (a) si $p = rs$ amb $r, s \in \mathbb{Z}[i]$, llavors $p^2 = d(r)d(s)$;

   (b) $\forall r \in \mathbb{Z}[i]$, tenim $d(r) = 1 \Leftrightarrow r$ és una unitat de $\mathbb{Z}[i] \Leftrightarrow r \in \{\pm 1, \pm i\}$.

   (c) si (p) és un ideal primer de $\mathbb{Z}[i]$ llavors $\nexists x, y \in \mathbb{Z}$ satisfent $x^2 + y^2 = p$.

   (d) si (p) no és un ideal primer llavors $\exists x, y \in \mathbb{Z}$ amb $x^2 + y^2 = p$.

   (e) (p) és ideal primer de $\mathbb{Z}[i] \Leftrightarrow x^2 + 1$ és irreductible a $\mathbb{F}_p[x] \Leftrightarrow -1$ és un quadrat a $\mathbb{F}_p^* \Leftrightarrow x^2 \equiv -1 (mod\ p)$ té solució.

   (f) si p és primer senar, $x^2 \equiv -1 (mod\ p)$ té solució $\Leftrightarrow$ hi ha un element d'ordre 4 en el grup $\mathbb{F}_p^*$.

   (g) $\mathbb{F}_p^*$ és cíclic. Llavors $\mathbb{F}_p^*$ té un subgrup d'ordre $4 \Leftrightarrow 4 | p-1 \Leftrightarrow p - 1 \equiv 0 (mod\ 4)$.

   Per tant el problema té solució per $p = 2$ i per tot primer senar complint $p \equiv 1 (mod\ 4)$.

7. **Exercici suplementari** Sigui $f \in End_K(V)$ una aplicació K-lineal, on K denota un cos i V un K-espai vectorial de dimensió finita. Sigui L un cos que contingui K, $K \subseteq L$ de tal manera que V sigui també un L-espai vectorial. Definim el següents elements,

$$\sum_{i \in \mathbb{N}} l_i f^i \in End_K(V), \ amb \ l_i \in L \ l_i = 0 \overset{\circ}{\forall} i \in \mathbb{N},$$

on f^0 és la identitat. Hi podem definir una suma via $\sum_{i\in\mathbb{N}} l_i f^i + \sum_{j\in\mathbb{N}}^{m} l'_j f^j := \sum_{k\in\mathbb{N}}(l_k + l'_k) f^k$.

Definim un producte, via la composició a $End_K(V)$. Això dóna una estructura d'anell. Denotem aquest anell $L\{f\}$. (En l'exercici tres $L = K$ i denotavem aquest anell per $K[f]$).

Seguint la notació introduida, considerem $K = \mathbb{F}_3$ i $V = L = \mathbb{F}_3[X]/(X^2+1)$.

(a) Proveu que l'ideal generat per X^2+1 a $\mathbb{F}_3[X]$ és un ideal maximal.

(b) Donat el cos L considerem el morfime

$$f : V \to V, \ x \mapsto x^3.$$

Proveu que és $\mathbb{F}_3$-lineal, és a dir pertany a $End_{\mathbb{F}_3}(V)$ i que no és el morfisme identitat.

(c) Proveu $fl = l^3 f$ amb $l \in L$. Per tant és un anell commutatiu tot i que L sigui un anell commutatiu.

(d) Podeu definir un morfisme d'anells L-lineal

$$\psi : L[X] \to L\{f\}$$

on f pertenyi a la imatge?