Universidad Nacional Autónoma de México

Facultad de Ciencias

MATEMÁTICAS

Algebra Moderna II

Examen 2

Por: Lorenzo Antonio Alvarado Cabrera

Problema 1. –

(6 puntos) Sea R un dominio entero.

a) Si $r \in R[x]$ es unidad (invertible), entonces $r \in R \setminus \{0\}$.
Sugerencia: considera $\mathrm{grad}(r)$.

b) Considera $r = 2x+1 \in \mathbb{Z}_4[x]$, demuestra que $r^2 = 1$ (en $\mathbb{Z}_4[x]$). Concluye que en el inciso anterior la hipótesis de que R es dominio entero es necesaria.

c) Demuestra que $R[x]$ nunca es un campo.

d) Supongamos ahora que R es campo, demuestra que $r \in R[x]$ es unidad (invertible) si, y sólo, si $r \in R \setminus \{0\}$.

Demostración:

(*a*) Sea $r \in R[x]$ unidad (no es cero, pues 0 no es unidad), entonces existe $t \in R[x]$ distinto de cero tal que $r \cdot t = 1$, y entonces $grad(r \cdot t) = grad(1) = 0$, por lo que[Ω] $grad(r) + grad(t) = 0$ $\underset{grad \geq 0}{\Rightarrow}$ $grad(r) = grad(t) = 0$ por lo que $r, t \in R \backslash \{0\}$.

(*b*) Tenemos que $r^2 = (2x+1)(2x+1) = (2 \cdot 2)x^2 + (2+2)x + 1 = 4x^2 + 4x + 1 = 0x^2 + 0x + 1 = 1$. Con lo que r es unidad en $R[x]$ pero $r \notin R$, esto es pues al no ser dominio entero no podemos asegurar que para cualesquiera dos polinomios distintos de cero se tenga que $grad(p \cdot q) = grad(p) + grad(q)$ y en efecto, $0 = grad(r \cdot r) < 1 + 1 = grad(r) + grad(r)$.

(*c*) En efecto, pues por el inciso *a*) tenemos que $U(R[x]) \subseteq R \subset R[x]$ $\therefore$ $U(R[x]) \neq R[x]$, por lo que no puede ser campo ya que hay elementos invertibles que no están en $R[x]$.

(*d*) Por lo visto en clase sabemos que al ser R un campo tendremos que $R[x]$ es un dominio euclidiano, con valuación el grado de los polinomios, de esta manera por el problema 16 de la

---

[Ω] Esto pues R es dominio entero si y solo si $R[x]$ es dominio entero, y en tal caso $grad(p \cdot q) = grad(p) + grad(q)$

segunda lista de problemas tenemos que $r \in R[x]$ es unidad si y solo si $grad(r) = grad(1) = 0$ es decir si y solo si $r \in R \backslash \{0\}$.

■

Problema 2. –

(2 puntos) Considera la siguiente prueba de que $x + 1 \in R[x]$ no es irreducible.

Sea $q(x), r(x) \in R[x]$ con $q(x) = \sqrt{x} + 1$ y $r(x) = \sqrt{x} - 1$, entonces $q(x)r(x) = x + 1$.

¿Es su prueba correcta? Si lo es justifica cuidadosamente que $q(x), r(x) \in R[x]$, si no lo es explica el error.

Demostración: Falso.

Primeramente, para que todo funcione bien se debe de tener que R sea dominio entero, así $R[x]$ lo será y podemos hablar de irreducibles. Ahora, si nosotros queremos probar que $x+1 \in R[x]$ no es irreducible, por definición debemos de dar $r, q \in R[x]$ no unidades tales que $x + 1 = rq$. Pero en este caso $q, r \notin R[x]$, pues no existe $t(x) \in R[x]$ tal que $t(x)t(x) = x$ ya que de ser así $grad(t \cdot t) = grad(x) = 1 \Rightarrow 2grad(t) = 1$ (nuevamente pues $R[x]$ es dominio entero) pero esto es imposible pues $grad(t) \in \mathbb{Z}_{\geq 0}$, por lo que $\sqrt{x} \notin R[x]$.

■

Problema 3. –

(2 puntos) Sea K un campo considera

$$R = \{p(x) \in K[x] : (p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0) \to a_1 = 0\}$$

Es decir, el conjunto de todos los polinomios sobre K que no tienen término lineal.

a) Demuestra que R es un subanillo de $K[x]$, y que $x^5, x^6 \in R$ no tienen máximo común divisor **en** R.

Sugerencia: Supón que sí tienen mcd y estudia el grado del polinomio que es mcd.

b) Argumenta que R no es dominio de máximo común divisor (MCD), ni dominio de factorización única (DFU), ni dominio de ideales principales (DIP), ni dominio euclideano.

Demostración: Como K es campo entonces $K[x]$ es dominio entero. Además, es claro que $R \subseteq K[x]$.

(a)

⊙ R es no vacío, pues $1 \in R$ ya que no tiene termino lineal. Ahora sean $p(x), q(x) \in R$ con

$$p(x) = a_0 + 0x + a_2 x^2 + \cdots + a_n x^n \quad \text{y} \quad q(x) = b_0 + 0x + b_2 x^2 + \cdots + b_n x^n$$

entonces, ya que $K[x]$ es dominio entero, tenemos que

$$p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k \text{ con } c_k = \sum_{i=0}^{k} a_k b_{k-i}$$

pero notemos que $c_1 = a_0 b_1 + a_1 b_0 = a_0 0 + 0 b_1 = 0$, por lo que $p(x)q(x)$ no tiene termino lineal, es decir, $p(x)q(x) \in R$. E igualmente suponiendo sin pérdida de generalidad que $n \geq m$ tendremos que

$$p(x) - q(x) = (a_0 - b_0) + (0-0)x + (a_2 - b_2)x^2 + \cdots + (a_m - b_m)x^m + \cdots + a_n x^n$$
$$p(x) - q(x) = c_0 + 0x + c_2 x^2 + \cdots + c_m x^m + \cdots + c_n x^n$$

por lo que no tiene termino lineal, es decir, $p(x) - q(x) \in R$.
Por lo ultimo tenemos que $R \subset K[x]$ y las operaciones son cerradas, por lo que R es subanillo. Mas aun, como $K[x]$ es dominio entero y R es subanillo, entonces R es dominio entero también (visto en clase). Eso lo usaremos en todo lo siguiente para asegurar que se cumplen las sumas de los grados de un producto.

$\odot$ Ahora veamos que x^5, x^6 no tienen máximo común divisor.
Supongamos que sí, y sea $d = mcd(x^5, x^6)$, entonces como x^5 es común divisor de ambos (ya que $x^5 = 1x^5$ y $x^6 = xx^5$) entonces $x^5 \mid d$ por lo que $d = x^5 \cdot t(x)$ para algún $t(x) \in R$, pero esto me diría que $grad(d) = 5 + grad(t(x)) \geq 5$ y pero por otro lado tenemos que $d \mid x^6$ por lo que $grad(d) \leq 6$, entonces $6 \geq grad(d) \geq 5$. Si $grad(d) = 6$ entonces tendríamos que $6 = 5 + grad(t(x)) \Rightarrow grad(t(x)) = 1$!!!, pero esto contradice que $t(x) \in R$, por lo que $grad(d) = 5$, en este caso tendríamos entonces que $grad(t(x)) = 0$ por lo que $t \in K$ y $d = tx^5$, pero como $d \mid x^6$ entonces tendríamos que $x^6 = d \cdot r(x)$ para algún $r(x) \in R \Rightarrow x^6 = tx^5 \cdot r(x)$ y entones $grad(r(x)) = 1$!!! lo cual contradice que $r(x) \in R$. Por lo que no puede pasar que $x^5 \mid d$!!! Pero esto contradice que d sea máximo común divisor. Por lo tanto, no puede haber un máximo común divisor en R

■

(b) Por el inciso anterior tendemos que R no es un dominio MCD, pues existen dos elementos sin máximo común divisor, y por lo visto en clase sabemos que

$$\text{Dominio } MCD \supseteq DFU \supseteq DIP \supseteq \text{Dominio Euclidiano}$$

por lo que al no ser un dominio MCD no puede ser DFU, DIP ni dominio Euclidiano.

■