Soluciones Parcial 2

17 de abril de 2020

Ejercicio 1 [1 punto]

Recuerde la demostración de Euclides de la existencia de infinitos primos: si $p_1, \ldots, p_k$ fueron todos los primos, habría que cualquier factor primo p de $n = p_1 \ldots p_k + 1$ sería diferente de los p_i. Adapte esa demostración para mostrar que, dado cualquier campo F, existen infinitos polinomios mónicos[1] irreducibles en $F[x]$.

Demostración. Solución Supongamos, por absurdo, que existan un número finito de polinomios mónicos irreducibles en $F[x]$. Sean $f_1(x), \ldots, f_n(x)$ todos los polinomios mónicos irreducibles.
Consideramos el polinomio $g(x) = f_1(x) \cdots f_n(x) + 1$. Siendo F un campo, $F[x]$ es un dominio euclidiano y, en particular, un dominio de integridad. Entonces, $g \neq 0$ es un polinomio mónico. Siendo $\deg g > \deg f_i$, para todos f_i, en particular $g \neq f_i$. Por hipótesis, $g(x)$ tiene que ser reducible. Siendo $g(x)$ mónico, podemos suponer que sus factores irreducibles sean mónicos. Siendo f_i los únicos polinomios mónicos irreducibles en $F[x]$, alguno de los $f_i(x)$ divide a g. Esto pero es imposible, siendo que ningún polinomio non constante puede dividir 1. Entonces g es irreducible, que es una contradicción. Entonces, hay infinitos polinomios mónicos irreducibles en $F[x]$. □

Ejercicio 2 [1 punto]

Sea p un número natural primo. Sea $f(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado n. Hemos visto que el campo $\mathbb{F}[x]/(f(x))$ tiene p^n elementos. Construya un campo con 16 elementos.
[*Cuidado: un polinomio de grado 4 puede no tener raíces y ser reducible como producto de dos polinomios de grado 2:* $x^4 + 3x^2 + 2 = (x^2 + 2)(x^2 + 1)$ *es reducible en los reales, pero no tiene ceros reales.*]

Demostración. Solución Consideramos el polinomio $f(x) = x^4 + x^3 + 1$. Siendo $f(0) = f(1) = 1$, f no tiene raíces en $\mathbb{F}_2$. Para mostrar que sea irreducible, falta mostrar que no se puede escribir como producto de dos polinomios irreducibles de grado 2. Ahora, el único polinomio irreducible de grado 2 en $\mathbb{F}_2[x]$ es el polinomio $q(x) = x^2 + x + 1$, siendo que x^2 y $x^2 + 1$ ambos tienen raíces en $\mathbb{F}_2$. Ahora $(q(x))^2 = (x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x^3 + 1 = f(x)$.
Por lo que hemos visto en clase, el ideal $(f(x))$ es un ideal maximal y entonces $\mathbb{F}_2[x]/(f(x))$ es un campo que tiene $x^4 = 16$ elementos. □

Ejercicio 3 [1 punto]

Sea $(G, \cdot)$ un grupo (en notación multiplicativa). Definimos el *grupo opuesto* G^o en la siguiente manera. Como conjuntos $G^o = G$. La operación es al revés: $a \circ b = ba$, para a y $b \in G$. Demuestre que G^o es un grupo.

Demostración. Solución Vamos a revisar que se cumplen los axiomas de grupo.

- Cierre: Sean $a, b \in G^o = G$. Tenemos $a \circ b = ba \in G$ siendo G un grupo. Por lo tanto $a \circ b \in G^o$.
- Asociatividad: Sean $a, b, c \in G^o$. Tenemos: $a \circ (b \circ c) = a \circ (cb) = cba = (ba) \circ c = (a \circ b) \circ c$, donde hemos utilizado que el producto en G es asociativo, siendo G un grupo.

[1] Un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0$ se dice *mónico* si $a_n = 1$.

- Identidad: Sea $e \in G$ la identidad por la operación de G. Para todos $g \in G^o$ tenemos: $g \circ e = eg = g$ y $e \circ g = ge = g$.
- Elemento inverso: Siendo G un grupo, para todos $g \in G$ existe un inverso g^{-1}. Ahora, tenemos $g \circ g^{-1} = g^{-1}g = e$ y $g^{-1} \circ g = gg^{-1} = e$.

Por lo tanto G^o es un grupo. □

Ejercicio 4 [1 punto]
Sea G un grupo tal que todos los elementos de G que no sean la identidad tengan orden 2. Demuestre que G es abeliano.

Demostración. Solución Sean g y $h \in G$. Por hipótesis $g^2 = e = h^2$. También tenemos: $ghgh = (gh)^2 = e$. Multiplicando ambos lado por la derecha por h y por la izquierda por g, obtenemos: $g(ghgh)h = (gg)hg(hh) = hg = gh$. Siendo g y h genéricos, G es abeliano. □

Ejercicio 5 [1 punto] Sean G y G' dos grupos, y sea $\varphi\colon G \to G'$ un homomorfísmo sobreyectivo de grupos. Demuestre que

1. Si G es abeliano, también lo es G'.
2. Si G es cíclico, también lo es G';

Demostración. Solución

1. Sean g' y $h' \in G'$. Siendo φ sobreyectivo, existen g y $h \in G$ tales que $\varphi(g) = g'$ y $\varphi(h) = h'$. Siendo φ un homomorfísmo tenemos

$$g'h' = \varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g) = h'g',$$

   donde hemos utilizado que $gh = hg$ porque G es abeliano. Siendo g' y h' genéricos, G' es abeliano.

2. Siendo G cíclico, existe un $g \in G$ tal que $\langle g \rangle = G$. Llamamos $\varphi(g) = g' \in G'$. Vamos a mostrar que $G' = \langle g' \rangle$.

   Sea $h' \in G'$. Siendo φ sobreyectivo, existe un $h \in G$ tal que $\varphi(h) = h'$. Siendo G cíclico, existe un $n \in \mathbb{Z}$ tal que $g^n = h$. Al ser φ un homomorfísmo, tenemos

$$h' = \varphi(h) = \varphi(g^n) = \varphi(g)^n = (g')^n.$$

   Siendo $h' \in G'$ genérico, G' es cíclico, generado por g'.

□