SOLUCIONES DEL PRIMER PARCIAL
ÁLGEBRA II – SEGUNDO CUATRIMESTRE 2023

Ejercicio 1. Sea A un anillo conmutativo y $\mathfrak{m}$ un ideal maximal de A tal que para todo x en $\mathfrak{m}$ el elemento $1+x$ es una unidad de A. Probar que A es un anillo local, es decir, que tiene un único ideal maximal.

Solución 1. Sea $\mathfrak{n}$ un ideal maximal. Para ver que $\mathfrak{n} = \mathfrak{m}$ basta probar que $\mathfrak{n} \subset \mathfrak{m}$. Supongamos que esto no sucede, es decir, que existe $x \in \mathfrak{n} \setminus \mathfrak{m}$, y veamos que tal suposición nos lleva a una contradicción.

Como x no pertenece a $\mathfrak{m}$, el ideal $\langle x \rangle + \mathfrak{m}$ lo contiene propiamente. Se sigue entonces que $\langle x \rangle + \mathfrak{m} = A$; en particular, existen $c \in A$ e $y \in \mathfrak{m}$ tales que

$$1 = cx + y.$$

Aplicando la hipótesis y el hecho de que $\mathfrak{n}$ es un ideal, se sigue que $cx = 1 + (-y)$ es tanto una unidad como un elemento del ideal propio $\mathfrak{n}$. Esto es absurdo, concluyendo la prueba. □

Solución 2. Sea $\mathfrak{n}$ un ideal maximal. Consideremos $I := \mathfrak{n} + \mathfrak{m} \supset \mathfrak{m}, \mathfrak{n}$. Observemos primero que $I \neq A$, ya que si existiesen $x \in \mathfrak{n}$, $y \in \mathfrak{m}$ tales que $1 = x + y$, entonces $y = 1 + (-x)$ no podría ser una unidad. Habiendo visto que I es propio, la maximalidad de $\mathfrak{m}$ nos dice que $I = \mathfrak{m}$ y por el mismo argumento debe ser también $I = \mathfrak{n}$. Hemos visto entonces que $\mathfrak{n} = \mathfrak{m}$. □

Ejercicio 2. Sea G un grupo finito y $N \trianglelefteq G$ un subgrupo normal tal que $|N|$ y $[G : N]$ son coprimos. Probar que N es característico, es decir, que para todo $\varphi \in \mathrm{Aut}(G)$ se tiene que $\varphi(N) = N$.

Solución 1. Sea $x \in N$ y tomemos $s, t \in \mathbb{Z}$ tales que $s|N| + t[G : N] = 1$. Luego

$$x = (x^{|N|})^s (x^t)^{[G:N]}.$$

Como $\mathrm{ord}(x) \mid |N|$, es entonces $x = (x^t)^{[G:N]}$. Aplicando $\varphi \in \mathrm{Aut}(G)$, es $\varphi(x) = \varphi(x^t)^{[G:N]}$. Como G/N es un grupo, ya que N es normal, proyectando al cociente se tiene que

$$[\varphi(x)] = [\varphi(x^t)^{[G:N]}] = [\varphi(x^t)]^{[G:N]} = [1]$$

y entonces $\varphi(x) \in N$. Vemos así que $\varphi(N) \subset N$; la contención opuesta se obtiene aplicando el anterior argumento a φ^{-1}. □

Solución 2. Sea $\varphi \in \mathrm{Aut}(G)$. Consideremos la composición

$$\alpha := N \hookrightarrow G \xrightarrow{\varphi} G \twoheadrightarrow G/N.$$

Probar que $\varphi(N) \subset N$ equivale a que $\alpha(x) = [1]$ para cada $x \in N$; veremos entonces que $I := \mathrm{im}\alpha = \{[1]\}$.

Como I es subgrupo de G/N, su orden divide al $[G : N]$. Por otra parte, el primer teorema de isomorfismo nos dice que $I \cong N/\ker(\alpha)$ así que $|I|$ divide a $|N|$. Dado que $|N|$ y $[G : N]$ son por hipótesis coprimos, necesariamente $|I| = 1$ y en consecuencia α es la función constante $[1]$. □

Ejercicio 3. Clasifique los grupos de orden $182 = 2 \cdot 7 \cdot 13$ a menos de isomorfismo.
Sugerencia: *para distinguir dos tales grupos, puede considerar la cantidad de elementos de un orden dado.*

Demostración. Notemos en primer lugar que todos los subgrupos de Sylow de G son cíclicos pues tienen orden primo.

Los teoremas de Sylow nos dicen que la cantidad n_7 de 7-subgrupos de Sylow divide a $2 \cdot 13$ y cumple con $n_7 \equiv 1 \pmod 7$; el cálculo de congruencias módulo 7 de $1, 2, 13$ y $2 \cdot 13$ muestra que necesariamente $n_7 = 1$. En consecuencia, el único 7-subgrupo de Sylow P_7 de G es normal.

Sean ahora P_{13} un 13-subgrupo de Sylow y P_2 un 2-subgrupo de Sylow. Como P_7 es normal, tenemos que $P_{13}P_7$ es un subgrupo de G. Más aún $|P_{13}P_7| = |P_{13}| \cdot |P_7| = 7 \cdot 13$ ya que $P_{13} \cap P_7$ es trivial, al ser intersección de grupos de orden coprimo. Más aún, como $7 \not| 12$, por lo visto en clase[1] sobre la clasificación de grupos de orden pq con p y q primos necesariamente $P_{13} \cdot P_7 \cong \mathbb{Z}_7 \times \mathbb{Z}_{13}$.

Como $P_{13}P_7$ tiene cardinal $13 \cdot 7$, tiene índice 2 y resulta normal. En particular $(P_{13}P_7)P_2$ es un subgrupo de G, el argumento dado anteriormente muestra que $P_{13}P_7$ interseca trivialmente a P_2, y vemos así que $(P_{13}P_7)P_2 = G$ como consecuencia de la igualdad de sus cardinales.

Hasta aquí hemos visto que G es el producto de $P_{13} \cdot P_7$ y P_2, que estos subgrupos tienen intersección trivial, que $P_{13} \cdot P_7$ es un subgrupo normal de G y que $P_{13} \cdot P_7 \cong \mathbb{Z}_7 \times \mathbb{Z}_{13}$. Este conjunto de hechos implican que

$$G \cong P_{13} \cdot P_7 \rtimes_\omega P_2 \cong (\mathbb{Z}_{13} \times \mathbb{Z}_7) \rtimes_\theta \mathbb{Z}_2$$

para algún morfismo $\theta\colon \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{13} \times \mathbb{Z}_7)$.

Observemos que como los factores de este producto son abelianos, el producto semidirecto resultante será abeliano si y sólo si $\theta \equiv \mathrm{id}$. En el resto de los casos, el automorfismo θ corresponderá a la elección de un elemento de orden 2 en $\mathrm{Aut}(\mathbb{Z}_{13} \times \mathbb{Z}_7)$. Por lo visto en clase, tenemos isomorfismos

$$(*) \qquad \mathrm{Aut}(\mathbb{Z}_{13} \times \mathbb{Z}_7) \cong \mathrm{Aut}(\mathbb{Z}_{13}) \times \mathrm{Aut}(\mathbb{Z}_7) \cong \mathcal{U}_{13} \times \mathcal{U}_7 \cong \mathbb{Z}_{12} \times \mathbb{Z}_6.$$

Un cálculo muestra que los elementos de orden dos del lado derecho de esta cadena son exactamente $([6], [3])$, $([6], [0])$ y $([0], [3])$. Hasta aquí, esto ya muestra que hay a lo sumo cuatro grupos de orden 182 salvo isomorfismo. Tenemos ahora dos (o más) posibles formas de terminar de clasificarlos.

Opción 1: siguiendo la clasificación de grupos de orden 30 vista en clase, podemos exhibir cuatro grupos de orden 182 y probar que no son isomorfos entre sí. Como para los grupos de orden 30, podemos considerar el producto de grupos cíclicos con grupos diedrales:

$$\mathbb{Z}_{182}, \qquad \mathbb{Z}_7 \times \mathbb{D}_{13}, \qquad \mathbb{Z}_{13} \times \mathbb{D}_7, \qquad \mathbb{D}_{91}.$$

Para distinguirlos podemos probar que tienen distinta cantidad de elementos de orden 2, ya sea haciendo un cálculo explícito o usando la cantidad de elementos de orden dos de los grupos $\mathbb{D}_n$ vista en clase.

Opción 2: otra idea es exhibir los cuatro automorfismos explícitamente. Para esto debemos recordar cómo definimos los isomorfismos de $(*)$. El isomorfismo $\mathrm{Aut}(\mathbb{Z}_{13} \times \mathbb{Z}_7) \cong \mathrm{Aut}(\mathbb{Z}_{13}) \times \mathrm{Aut}(\mathbb{Z}_7)$ visto en clase muestra que todo automorfismo de $\mathbb{Z}_{13} \times \mathbb{Z}_7$ es de la forma $\varphi \times \psi$ con $\varphi \in \mathrm{Aut}(\mathbb{Z}_{13})$, $\psi \in \mathrm{Aut}(\mathbb{Z}_7)$. El isomorfismo $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathcal{U}_n$ está dado por asignarle a cada $[k]$, con k coprimo con n, el automorfismo $[i] \mapsto [ki]$.

Lo visto dice hay un único elemento de orden 2 en cada factor, y que los elementos de orden 1 o 2 en el producto están dados por la identidad o un automorfismo de orden 2 en cada factor. Los elementos de orden dos en $\mathcal{U}_p$, con $p \in \{7, 13\}$, corresponden a soluciones distintas de 1 a la ecuación $x^2 \equiv 1 \pmod p$, cuya única solución es $[-1]$.

Juntando todas estas observaciones, conseguimos definir los (únicos) tres automorfismos de orden dos en $\mathbb{Z}_{13} \times \mathbb{Z}_7$, en concreto:

$$\alpha_1([x], [y]) := ([-x], [-y]); \qquad \alpha_2([x], [y]) := ([-x], [y]); \qquad \alpha_3([x], [y]) := ([x], [-y]).$$

---

[1] Esta afirmación también puede probarse usando que P_{13} es normal en P_7P_{13} pues su índice es el menor primo que divide a $7 \cdot 13$.

Tenemos entonces tres posibles productos semidirectos dados por automorfismo θ_i tales que $\theta_i([1]) = \alpha_i$.

Ahora, para cada $i \in \{1, 2, 3\}$, podemos calcular explícitamente la cantidad de elementos de orden dos de cada producto semidirecto para ver que no son isomorfos entre sí. Por brevedad lo hacemos para $i = 1$; los otros casos son similares.

Sea $a = (([x], [y]), [z]) \in (\mathbb{Z}_{13} \times \mathbb{Z}_7) \rtimes_{\theta_1} \mathbb{Z}_2$. Si $[z] = [0]$, entonces a corresponde al subgrupo de $(\mathbb{Z}_{13} \times \mathbb{Z}_7) \rtimes_{\theta_1} \mathbb{Z}_2$ isomorfo a $\mathbb{Z}_{13} \times \mathbb{Z}_7$ y no puede tener orden 2. Luego necesariamente $[z] = [1]$. Ahora, explícitamente,

$$\begin{aligned} a^2 &= (([x], [y]), [1]) \cdot_{\theta_1} (([x], [y]), [1]) = (([x], [y]) + \theta_1([1])(([x], [y])), [1] + [1]) \\ &= (([x], [y]) + \alpha_1(([x], [y])), [0]) = (([x], [y]) + ([-x], [-y]), [0]) = (([0], [0]), [0]). \end{aligned}$$

Por lo tanto todo elemento de la forma $(([x], [y]), [0])$ tiene orden 2, y no hay otros, se tienen así 91 elementos de orden 2 en este caso. Similarmente se obtienen 13 elementos de orden 2 si $i = 2$ y 7 si $i = 3$. Esto muestra que estos tres productos semidirectos junto con el producto directo $\mathbb{Z}_{13} \times \mathbb{Z}_7 \times \mathbb{Z}_2$ son una lista de representantes de los grupos de orden 182 a menos de isomorfismo. □

Ejercicio 4. Sea A un dominio íntegro.

a) Sea $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$. Probar que si existe un primo $\mathfrak{p} \in \mathrm{Spec}(A)$ tal que $a_i \in \mathfrak{p}$ para todo $i \in \{0, \ldots, n-1\}$ y $a_0 \notin \mathfrak{p}^2$, entonces f es irreducible.
b) Pruebe que $X^3 + X + Y^7 \in \mathbb{R}[X, Y]$ es irreducible.

Solución 1 para el ítem a). Supongamos que f se factoriza como un producto de factores $g = b_sX^s + b_{s-1}X^{s-1} + \cdots + b_1X + b_0$, $h = c_tX^t + c_{t-1}X^{t-1} + \cdots + c_1X + c_0$ con $b_s, c_t \neq 0$. Notemos que

$$b_0 \cdot c_0 = a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2,$$

así que exactamente uno de los factores del lado izquierdo pertenece a $\mathfrak{p}$. Supongamos sin pérdida de generalidad (intercambiando los roles de g y h de ser necesario) que $b_0 \in \mathfrak{p}$ y $c_0 \notin \mathfrak{p}$. Probaremos[2] ahora que $b_k \in \mathfrak{p}$ para todo $k \in \{0, \ldots, n-1\}$, definiendo para esto $b_k := 0$ si $k > s$. El caso base fue observado previamente. Ahora, si $b_0, \ldots, b_k \in \mathfrak{p}$ para cierto $k \in \{0, \ldots, n-2\}$, entonces a_{k+1} pertenece a $\mathfrak{p}$ y luego

$$b_{k+1}c_0 = a_{k+1} - \sum_{i=0}^{k+1} b_i d_{k+1-i} \in \mathfrak{p}.$$

Por primalidad, y dado que $c_0 \notin \mathfrak{p}$, se sigue que $b_{k+1} \in \mathfrak{p}$. Esto concluye la prueba de la afirmación sobre los coeficientes de g.

Finalmente, como 1 es el n-ésimo coeficiente de f, es $1 = b_sc_t$ y entonces b_s no puede pertenecer a $\mathfrak{p}$ ya que este es un ideal propio y b_s una unidad. Lo demostrado anteriormente nos dice luego que $s \geqslant k$. Por otro lado, como A es un dominio y $g \mid f$, debe ser $s \leqslant k$. En consecuencia $\deg(g) = s = k$ y luego $t = 0$, es decir $h = c_0 = c_t \in A^\times = (A[X])^\times$. Esto concluye la demostración. □

Solución 2 para el ítem a). Supongamos que f se factoriza como un producto de factores $g = b_sX^s + b_{s-1}X^{s-1} + \cdots + b_1X + b_0$, $h = c_tX^t + c_{t-1}X^{t-1} + \cdots + c_1X + c_0$ con $b_s, c_t \neq 0$. Como en la solución previa, suponemos $b_0 \in \mathfrak{p}$ y $c_0 \notin \mathfrak{p}$.

[2]Una forma de llegar a este enunciado es primero calcular a_1 y a_2 en términos de los coeficientes de g y h; lo cual omitimos en pos de la brevedad de la resolución.

Sea $B = A/\mathfrak{p}$; observemos que es un dominio ya que $\mathfrak{p}$ es primo. Notamos $\pi\colon A \to B$ a la proyección al cociente y también al morfismo $A[X] \to B[X]$ inducido por π. Proyectando,

$$X^n = \pi(f) = \pi(gh) = \pi(g)\pi(h).$$

Como los coeficientes principales de g y h son unidades, el grado es preservado al proyectar. De igual manera a la solución previa, será suficiente probar que $s = n$.

Consideremos $i \in \{0, \dots, s\}$ el menor índice tal que $[b_i]$ es no nulo. Por definición,

$$[a_i] = \sum_{e+f=i+j} [b_e][c_f] = [b_i][c_0] \neq 0,$$

pues B es un dominio. Como $\pi(f)$ tiene un único coeficiente no nulo, se sigue que entonces $n = i$. En particular $n \leqslant i \leqslant s \leqslant n$, así que obtenemos $s = n$ como buscábamos. □

Solución al ítem b). Aplicamos el ítem previo al polinomio $Y^7 + (X^3 + X) \in (\mathbb{R}[X])[Y] \cong \mathbb{R}[X, Y]$, tomando $\mathfrak{p} = (X)$. Para concluir verificamos las hipótesis de a):

- $\mathfrak{p}$ es primo: en efecto, el morfismo sobreyectivo de evaluación $\mathrm{ev}_0\colon \mathbb{R}[X] \to \mathbb{R}$ nos da un isomorfismo $\mathbb{R}[X]/(X) \cong \mathbb{R}$. Como $\mathbb{R}$ es cuerpo, esto dice que el ideal $\mathfrak{p}$ es primo –y más aún, maximal.
- $X^3 + X \in \mathfrak{p}$**:** esto es porque $X^3 + X = X(X^2 + 1)$ es múltiplo de X.
- $X^3 + X \notin \mathfrak{p}^2$**:** para verlo, observamos primero que $\mathfrak{p}^2 = (X^2)$. Por un lado $X^2 \in \mathfrak{p}$ así que $(X^2) \subset \mathfrak{p}$. Por otro lado, si tenemos $f, g \in (X)$ entonces $f = Xh_1$, $g = Xh_2$ y $fg \in X^2h_1h_2$. Es decir, los productos de elementos de (X) pertenecen a (X^2) y luego el ideal generado por ellos también. Finalmente $X^3 + X \notin (X^2)$ pues $X^3 \in (X^2)$ pero $X \notin (X^2)$ por consideraciones de grado.

□