Solución Taller 2

16 de abril de 2020

Ejercicio 1

Sean $f(x) = x^3 - x + 1$ y $g(x) = x^3 - x - 1$ dos polinomios irreducibles en $\mathbb{F}_3[x]$. Muestre que $\mathbb{F}_3[x]/(f(x)) \cong \mathbb{F}_3[x]/(g(x))$.
[*Sugerencia: muestre primero que existe un* $\alpha \in \mathbb{F}_3[x]/(g(x))$ *tal que* $f(\alpha) = 0$ *en ese campo. Utilice el primer teorema de isomofismos de anillos.*]

Solución. Mostramos que existe una raíz de $f(x)$ en $K = \mathbb{F}_3[x]/(g(x))$. De hecho $f(2x) = (2x)^3 - 2x + 1 = 2x^3 - 2x - 1$. Ahora, en K tenemos $x^3 - x - 1 = 0$ entonces $x^3 = x + 1$. Por eso $f(2x) = 2(x + 1) - 2x - 1 = 3 = 0$.
Consideramos el homomorfísmo $\varphi\colon \mathbb{F}_3[x] \to K$ que envía un polinomio $p(x)$ en $p(2x)$. Este homomorfísmo es claramente sobre, siendo $2x = -x$ en $\mathbb{F}_3[x]$. Además, sabemos que $(f(x)) \subseteq \ker\varphi$. Vamos a mostrar la otra inclusión. Sea $p(x) \in \ker\varphi$. Por división entre polinomios, podemos escribir

$$p(x) = q(x)f(x) + r(x),$$

donde $r(x) = 0$ o $\deg r(x) < \deg f(x) = 3$. Ahora, siendo $p(x)$ y $f(x) \in \ker\varphi$ se tiene $0 = p(2x) = q(2x)f(2x)+r(2x) = r(2x)$. Es decir $r(2x) \in (g(x))$. Siendo $\deg g(x) = 3$, si $r(2x)$ no es el polinomio cero, necesariamente $\deg r(2x) = \deg r(x) \geq \deg g(x) = \deg f(x) = 3$. Esto implica que $r(2x)$ es el polinomio cero y, por la tanto $r(x)$ también es el polinomio cero. Finalmente, esto demuestra que $f(x) \mid p(x)$ y entonces $\ker\varphi \subseteq (f(x))$.
Hemos mostrado que $\ker\varphi = (f(x))$. Por el primer teorema de isomorfísmo

$$\mathbb{F}_3[x]/(f(x)) = \mathbb{F}_3[x]/\ker\varphi \cong \operatorname{Im}\varphi = \mathbb{F}_3[x]/(g(x)).$$

Nota: En realidad, había una manera más sencilla de solucionar el ejercicio, como alguien me dijo: simplemente se podía considerar el homomorfísmo $\varphi\colon \mathbb{F}_3[x]/(f(x)) \to \mathbb{F}_3[x]/(g(x))$ *que envía un polinomio* $p(x)$ *en* $p(2x) = p(-x)$ *y mostrar que eso es un isomorfísmo.* □

Ejercicio 2

Sean G y G' dos grupos. Demuestre que $G \times G' = \{(g, g'), g \in G \text{ y } g' \in G'\}$ es un grupo con las operación definida por

$$(g, g')(h, h') = (gh, g'h'),$$

donde gh es el producto de g con h en G, y de manera similar para $g'h' \in G'$. El grupo $G \times G'$ con esta operación se llama *grupo producto.*

Solución. Vamos a verificar los axiomas de grupo.

- Cierre: sean g, $h \in G$ y g', $h' \in G'$. Se tiene $(g, g')(h, h') = (gh, g'h')$. Siendo G y G' grupos, $gh \in G$ y $g'h' \in G'$. Luego $(gh, g'h') \in G \times G'$ como queríamos.
- Asociatividad: sean g, h, $j \in G$ y g', h', $j' \in G'$. Se tiene

$$\begin{aligned}((g, g')(h, h'))(j, j') = (gh, g'h')(j, j') &= ((gh)j, (g'h')j') \\ &= (g(hj), g'(h'j')) = (g, g')(hj, h'j') = (g, g')((h, h'), j, j')\end{aligned}$$

  done hemos utilizado que, siendo G y G' grupos, sus operaciones son asociativas.

- Identidad: sean $e \in G$ y $e' \in G'$ las identidades en los respectivos grupos. Si $g \in G$ y $g' \in G'$ tenemos $(g, g')(e, e') = (ge, g'e') = (g, g')$ y, de manera similar, $(e, e')(g, g') = (eg, e'g') = (g, g')$.
- Inverso: sean $g \in G$ y $g' \in G'$. Siendo ellos grupos, existen los inversos $g^{-1} \in G$ y $(g')^{-1} \in G'$. Tenemos: $(g, g')(g^{-1}, (g')^{-1}) = (g(g^{-1}, g'(g')^{-1})) = (e, e')$. De manera similar $(g^{-1}, (g')^{-1})(g, g') = (g^{-1}g, (g')^{-1}g') = (e, e')$.

Entonces $G \times G'$ es un grupo. □

Ejercicio 3

Sean H y K dos subgrupos de un grupo G.

1. Si $H \cap K = \{e\}$, la aplicación producto $p\colon H \times K \to G$, definida por $p(h, k) = hk$ es inyectiva. La imagen de p es el conjunto $HK = \{g \in G, g = hk, \text{ con } h \in H \text{ y } k \in K\}$.
2. Si H o K son subgrupos normales de G, entonces $HK = KH$ y HK es un subgrupo de G.
3. Si H y K son normales y $H \cap K = \{e\}$ y $HK = G$, entonces G es isomorfo al grupo producto $H \times K$.

Solución. 1. Sean (h_1, k_1) y (h_2, k_2) elementos de $H \times K$ tales que $h_1k_1 = h_2k_2$. Multiplicando ambos lados por h_1^{-1} a la izquierda y k_2^{-1} a la derecha, obtenemos $k_1k_2^{-1} = h_1^{-1}h_2$. El lado izquierdo pertenece a K y el derecho a H. Siendo $H \cap K = \{e\}$, necesariamente $k_1k_2^{-1} = e = h_1^{-1}h_2$. Entonces $h_1 = h_2$ y $k_1 = k_2$. Por eso p es inyectiva.

2. Asumamos que H sea normal; el caso en que K sea normal es similar. Mostramos que $KH \subseteq HK$. Sean $h \in H$ y $k \in K$. Hay $kh = (khk^{-1})k$. Siendo H normal, $khk^{-1} \in H$, entonces $kh \in HK$ y $KH \subseteq HK$. La otra inclusión es parecida.

   Para mostrar que $HK \leq G$ utilizamos segundo test de subgrupo. Sean h_1, $h_2 \in H$, k_1, $k_2 \in K$. Tenemos

   $$h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1(k_1k_2^{-1})h_2{-}1 = h_1k_3h_2^{-1} = h_1(k_3h_2^{-1}) = h_1(h_3k_4) = h_1h_3k_4$$

   que pertenece a HK. Arriba hemos utilizado que, siendo $HK = KH$, dado $hk \in HK$ existe $k'h' \in KH$ tal que $hk = k'h'$.

3. Asumamos ahora que ambos H y K sean normales en G y que $H \cap K = \{e\}$. Para el primer punto, la aplicación p es inyectiva y, por hipótesis, es sobre. Entonces, para mostrar que $G \cong H \times K$ solamente hay que mostrar que p sea un homomorfísmo de grupos.

   Vamos a mostrar primero que los elementos de H y de K conmutan. Es decir, si $h \in H$ y $k \in K$ tenemos $hk = kh$. Consideramos $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Siendo K normal, el lado izquierdo pertenece a K. De manera similar, siendo H normal, el lado derecho pertenece a H. Siendo $H \cap K = \{e\}$, necesariamente hay $hkk^{-1}h^{-1} = e$, o, equivalentemente, $hk = kh$. Ahora va a ser fácil mostrar que p sea un homomorfísmo de grupos, sean h_1, $h_2 \in H$ y k_1, $k_2 \in K$, se tiene

   $$p((h_1, k_1)(h_2, k_2)) = p(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = p(h_1, k_1)p(h_2, k_2).$$

   Entonces p es un homomorfísmo de grupos entre $H \times K$ y G. Por lo que hemos dicho al comienzo de este punto, p es invertible y entonces es un isomorfísmo entre $H \times K$ y G.

□

Ejercicio 4

Sean H y K subgrupos de un grupo *finito* G tales que $K \leq H \leq G$. Demuestre la fórmula

$$|G : K| = |G : H||H : K|.$$

Solución. Para el teorema de Lagrange, se tiene

$$|G| = |H||G : H|.$$

Siendo H un subgrupo, podemos considerarlo como un grupo, olvidándonos que esté adentro de G. Aplicando el teorema de Lagrange a $K \leq H$ se tiene

$$|H| = |K||H : K|.$$

Substituyendo $|H|$ en la ecuación de arriba obtenemos

$$|G| = |K||G : H||H : K|.$$

Siendo $K \leq H \leq G$, en particular $K \leq G$. Utilizando una vez más el teorema de Lagrange, esta vez para K y G, obtenemos

$$|G| = |K||G : K|.$$

Esta fórmula y la de antes nos dicen que $|G : K| = |G : H||H : K|$. □