Ejercicios de Álgebra

semana 2

POR MILLER SILVA

1. Supongamos que existe $H \leqslant G$ talque $|H| = n-1$. Como $|G| = n$ entonces existe un único $x \in G \setminus H$. Sea $y \in H$ tal que $y \neq e$ entonces $xy \in G \setminus H$, ya que si $xy \in H \Rightarrow x \in H$. Así $xy = x$, luego $y = e$, contradicción.

   Consideremos el grupo $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ y el subgrupo $H = \{\bar{0}\}$, luego $|\mathbb{Z}_3| = 3$ y $|H| = 3-2$.

2.

   a) Supongamos que $(a,n) \in \{2, \ldots, n\}$ entonces $\sigma_a(r^{n/(a,n)}) = r^{\frac{n}{(a,n)}a} = r^{n \times \frac{a}{(a,n)}} = 1 \Rightarrow r^{n/(a,n)} \in \operatorname{Ker}(\sigma_a) = \{1\} \Rightarrow n \Big| \frac{n}{(a,n)}$, pero $\frac{n}{(a,n)} < n$, contradicción. Por lo tanto $(a, n) = 1$.

   Sean $r^{k_1}, r^{k_2} \in Z_n$, donde $k_i \in \{0, \ldots, n-1\}$. Luego

   $$\sigma_a(r^{k_1} r^{k_2}) = (r^{k_1} r^{k_2})^a = r^{(k_1+k_2)a} = r^{k_1 a} r^{k_2 a} = \sigma_a(r^{k_1})\sigma(r^{k_2}).$$

   σ_a es un homomorfismo. Además $\sigma_a(r^k) = 1 \Rightarrow r^{ka} = 1 \Rightarrow n | ka$ y como $(n, a) = 1 \Rightarrow n | k \Rightarrow r^k = 1$. Luego $\operatorname{Ker} \sigma_a = \{1\}$, así σ_a es inyectiva. También el dominio y el conjunto de llegada tienen el mismo orden, por tanto σ_a es sobreyectiva y por ende isomorfismo.

   b) $\sigma_a = \sigma_b \Leftrightarrow r^a = r^b \Leftrightarrow r^{a-b} = 1 \Leftrightarrow n | a-b \Leftrightarrow a - b = 0 \bmod n \Leftrightarrow a = b \bmod n$.

   c) Sean $f, g \in \operatorname{Aut}(G)$, luego $f \circ g : G \to G$ es biyectiva y

   $$f \circ g(xy) = f(g(x)g(y)) = f \circ g(x) f \circ g(y)$$

   por lo tanto $f \circ g$ es automorfismo, así $\operatorname{Aut}(G)$ es cerrada bajo la composición.

   - $f, g, h \in G \Rightarrow f \circ (g \circ h) = (f \circ g) \circ h$
   - $\exists I : G \to G \in \operatorname{Aut}(G)$ con $I(g) = g$, tal que $f \circ I = I \circ f = f$ para todo $f \in \operatorname{Aut}(G)$
   - Para $f \in \operatorname{Aut}(G)$ existe $f^{-1} : G \to G$ tal que $f \circ f^{-1} = f^{-1} \circ f = I$. Y

     $$f(f^{-1}(x) f^{-1}(y)) = xy = f(f^{-1}(xy)) \Rightarrow f^{-1}(x) f^{-1}(y) = f^{-1}(xy),$$

     así $f^{-1} \in \operatorname{Aut}(G)$.

   Por lo tanto $(\operatorname{Aut}(G), \circ)$ es un grupo.

   d)

   $$\begin{aligned} F: \ (\mathbb{Z}_n)^\times &\to \operatorname{Aut}(Z_n) \\ \bar{a} &\mapsto \sigma_a \end{aligned}$$

Veamos si está bien definida. Sea $\bar{a} \in \mathbb{Z}_n^\times$, entonces existe $\bar{b} \in \mathbb{Z}_n^\times$ tal que $\bar{a}\bar{b} = \overline{ab} = \bar{1}$, $ab = 1 \bmod n = nk + 1$, remplazamos usando $a = (n,a)\frac{a}{(n,a)}, n = (n,a)\frac{n}{(n,a)}$

$$(n,a)\frac{a}{(n,a)}b = (n,a)\frac{n}{(n,a)}k + 1 \Rightarrow (n,a)\left(\frac{a}{(n,a)}b - \frac{n}{(n,a)}k\right) = 1 \Rightarrow (n,a) = 1,$$

luego por el item (a), $\sigma_a \in \mathrm{Aut}(Z_n)$.

Sean $a, b \in \mathbb{Z}$ tal que $\bar{a} = \bar{b}$ entonces $a = b \bmod n$, luego por el item (b), $F(\bar{a}) = \sigma_a = \sigma_b = F(\bar{b})$.

F es un homomorfismo:

$$F(\bar{a}\bar{b}) = F(\overline{ab}) = \sigma_{ab} = \sigma_a\sigma_b = F(\bar{a})F(\bar{b}).$$

F es inyectiva:

$$F(\bar{a}) = \sigma_1 \Rightarrow \sigma_a = \sigma_1 \Rightarrow a = 1 \bmod n \Rightarrow \bar{a} = \bar{1} \Rightarrow \mathrm{Ker}\, F = \{\bar{1}\}.$$

F es sobreyectiva:

Sea $f: Z_n \to Z_n$ un isomorfismo, luego existe $k \in \{0, \ldots, n-1\}$ tal que $f(r) = r^k$. Así tomando cualquier elemento $r^{k_1} \in Z_n$ tenemos

$$f(r^{k_1}) = f(r)^{k_1} = r^{kk_1} = (r^{k_1})^k \Rightarrow f = \sigma_k \Rightarrow (k,n) = 1 \Rightarrow \exists z_1, z_2 \in \mathbb{Z} \,\mathrm{tq}\, z_1k + z_2n = 1$$

$$z_1k = -z_2n + 1 \Rightarrow \bar{z_1}\bar{k} = \bar{1} \Rightarrow \bar{k} \in \mathbb{Z}_n^\times \Rightarrow F(\bar{k}) = \sigma_k = f$$

Por lo tanto F es un isomorfismo.

Sean $x, y \in \mathrm{Aut}(Z_n)$, entonces existen $i, j \in \mathbb{Z}$ tal que $x = F(\bar{i})$ e $y = F(\bar{j})$, luego

$$xy = F(\bar{i})F(\bar{j}) = F(\bar{i}\bar{j}) = F(\bar{j}\ \bar{i}) = F(\bar{j})F(\bar{i}) = yx,$$

Por lo tanto $\mathrm{Aut}(Z_n)$ es abeliano.

3. Los elementos de G tienen orden finito, ya que si existiera $x \in G$ tal que $|x| = \infty$, podríamos crear los siguientes subgrupos

$$\langle x \rangle, \langle x^2 \rangle, \ldots, \langle x^n \rangle, \ldots$$

todos distintos, y así G tendría infinitos subgrupos. Ahora sea $x_1 \in G$, luego $\langle x_1 \rangle \leqslant G$, si $\langle x_1 \rangle \neq G$, tomamos $x_2 \in G \setminus \langle x_1 \rangle$ y tendríamos $\langle x_2 \rangle \leqslant G$, si $\langle x_1 \rangle \cup \langle x_2 \rangle \neq G$, tomamos $x_3 \in G \setminus \langle x_1 \rangle \cup \langle x_2 \rangle$, luego $\langle x_3 \rangle \leqslant G$, si $\langle x_1 \rangle \cup \langle x_2 \rangle \cup \langle x_3 \rangle \neq G$ continuamos con el procedimiento. Esta construcción tiene que parar en algún momento ya que si no tendríamos infinitos subgrupos (todos diferentes)

$$\langle x_1 \rangle, \langle x_2 \rangle, \ldots, \langle x_k \rangle, \ldots$$

Por lo tanto $\langle x_1 \rangle \cup \cdots \cup \langle x_n \rangle = G$ (para algún $n \in \mathbb{N}$), donde cada subgrupo cíclico es finito, entonces G es finito.