Universidad de El Salvador. 25.06.2018
Álgebra I: Estructuras algebraicas y la teoría de grupos
Soluciones del examen parcial 3

Problema 1 (1 punto)**.** Enumere todos los grupos abelianos de orden 666 salvo isomorfismo.

Solución. Tenemos $666 = 2 \cdot 3^2 \cdot 37$, entonces hay dos grupos abelianos de orden 666,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z} \quad \text{y} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}.$$

■

Problema 2 (1 punto)**.** Sea G un grupo y N su subgrupo normal. Sea $K \subset G/N$ un subgrupo del grupo cociente. Demuestre que $K = H/N$ donde H es un subgrupo de G que contiene a N.
Sugerencia: considere el homomorfismo canónico $p\colon G \twoheadrightarrow G/N$ y $p^{-1}(K) \subset G$.

Solución. Sea $H := p^{-1}(K)$. Esto es un subgrupo de G. Efectivamente, $p(1_G) = 1_{G/N} \in K$, así que $1_G \in p^{-1}(K)$. Luego, si para $g_1, g_2 \in G$ se tiene $p(g_1) = x_1 \in K$ y $p(g_2) = x_2 \in K$, entonces $p(g_1 g_2) = x_1 x_2 \in K$. Esto significa que $g_1, g_2 \in p^{-1}(K)$ implica $g_1 g_2 \in p^{-1}(K)$. De la misma manera, si $p(g) = x \in K$, entonces $p(g^{-1}) = x^{-1} \in K$, lo que quiere decir que $g \in p^{-1}(K)$ implica $g^{-1} \in p^{-1}(K)$. (Hasta el momento hemos usado solo el hecho de que p sea un homomorfismo de grupos, así que demostramos un resultado general: la preimagen de un subgrupo respecto a cualquier homomorfismo es un subgrupo.)

Ahora, puesto que p es sobreyectivo, tenemos $K = p(p^{-1}(K)) = p(H) = H/N$. ■

Problema 3 (2 puntos)**.** Sea p un número primo. Supongamos que el grupo $\mathbb{Z}/p\mathbb{Z}$ actúa sobre un conjunto X.

1) Demuestre que todo elemento de X es un punto fijo o pertenece a una órbita de orden p.

2) Supongamos que X es finito y $p \mid |X|$. Demuestre que el número de puntos fijos es también divisible por p.

Solución. Recordamos que cuando un grupo G actúa sobre un conjunto X, para un punto $x \in X$ hay una biyección natural entre la órbita O_x y las clases laterales G/G_x donde G_x es el estabilizador de x. En particular, cuando G es finito, tenemos $|O_x| = |G|/|G_x|$. En este caso $G = \mathbb{Z}/p\mathbb{Z}$ es de orden primo, así que $|O_x| = p$ o 1, y en el último caso x es un punto fijo. Esto establece la parte 1).

Para la parte 2), consideremos la ecuación de clase $|X| = |X^G| + \sum_{1 \le i \le n} |G : G_{x_i}|$ donde X^G denota los puntos fijos y O_{x_i} son las órbitas que contienen más de un elemento. Acabamos de ver que $|G : G_{x_i}| = p$ cuando $G = \mathbb{Z}/p\mathbb{Z}$, y luego $|X| \equiv |X^G| \pmod{p}$. ■

Problema 4 (2 puntos)**.** Sea G un grupo finito y sea p un número primo tal que $p \mid |G|$. En este problema vamos a probar que en G hay un elemento de orden p. Para esto consideremos el conjunto

$$X := \{(g_0, g_1, \ldots, g_{p-1}) \mid g_i \in G,\ g_0 g_1 \cdots g_{p-1} = 1\}.$$

1) Demuestre que $|X| = |G|^{p-1}$.

2) Para $[n]_p \in \mathbb{Z}/p\mathbb{Z}$ sea $[n]_p \cdot (g_0, g_1, \ldots, g_{p-1}) := (g_{[0+n]}, g_{[1+n]}, \ldots, g_{[p-1+n]})$. Demuestre que esto define una acción de $\mathbb{Z}/p\mathbb{Z}$ sobre X y sus puntos fijos son $(g, g, \ldots, g)$ donde $g^p = 1$.

3) Usando el problema anterior, demuestre que el número de elementos $g \in G$ tales que $g^p = 1$ es divisible por p. Demuestre que existe $g \neq 1$ tal que $g^p = 1$.

Solución. En la parte 1) basta notar que $g_0 g_1 \cdots g_{p-1} = 1$ es equivalente a tener $g_{p-1} = (g_0 g_1 \cdots g_{p-2})^{-1}$. Entonces, los elementos $g_0, g_1, \ldots, g_{p-2}$ pueden ser escogidos de manera arbitraria, y hay $|G|^{p-1}$ posibilidades de hacerlo, y luego g_{p-1} está definido de modo único.

En la parte 2) la acción es por las permutaciones cíclicas de $(g_0, g_1, \ldots, g_{p-1}) \in G^p$, falta solo ver que esta acción se restringe correctamente al conjunto X. Sería suficiente considerar la acción de $[1]_p \in \mathbb{Z}/p\mathbb{Z}$. En efecto,

$$g_0 g_1 g_2 \cdots g_{p-1} = 1 \iff g_1 g_2 \cdots g_{p-1} = g_0^{-1} \iff g_1 g_2 \cdots g_{p-1} g_0 = 1.$$

Si $(g_0, g_1, g_2, \ldots, g_{p-1}) = (g_1, g_2, \ldots, g_{p-1}, g_0)$, entonces $g_0 = g_1 = g_2 = \cdots = g_{p-1}$, lo que demuestra que los puntos fijos de la acción corresponden a elementos $g \in G$ tales que $g^p = 1$.

En la parte 3), tenemos $p \mid |X| = |G|^{p-1}$, dado que $p \mid |G|$ por nuestra hipótesis. Entonces, el problema anterior implica que el número de elementos $g \in G$ tales que $g^p = 1$ es divisible por p. Uno de estos elementos es $g = 1$, así que hay por lo menos $p - 1$ otros elementos con esta propiedad. Son elementos de orden p. ■

Problema 5 (2 puntos)**.**

1) Consideremos el grupo alternante A_4 y sus subgrupos $V := \{\mathrm{id}, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3)\}$ y $H := \langle (1\,2\,3) \rangle$. Demuestre que A_4 es el producto semidirecto de V y H.

2) Demuestre que para $n \geq 5$ el grupo alternante A_n no puede ser isomorfo a un producto semidirecto $N \rtimes_\phi H$ donde N y H no son triviales.

Solución. En la primera parte, el subgrupo V es normal y $V \cap H = \{\mathrm{id}\}$. Además, se tiene $A_4 = NH$. En efecto,

$$H = \{\mathrm{id}, (1\,2\,3), (1\,3\,2)\},$$

y en A_4 hay otros 3-ciclos, pero estos se obtienen como productos de un elemento de N y un elemento de H:

$$\begin{aligned}
(1\,2\,4) &= (1\,4)\,(2\,3) \circ (1\,3\,2),\\
(1\,3\,4) &= (1\,4)\,(2\,3) \circ (1\,2\,3),\\
(1\,4\,2) &= (1\,3)\,(2\,4) \circ (1\,2\,3),\\
(1\,4\,3) &= (1\,2)\,(3\,4) \circ (1\,3\,2),\\
(2\,3\,4) &= (1\,2)\,(3\,4) \circ (1\,3\,2),\\
(2\,4\,3) &= (1\,2)\,(3\,4) \circ (1\,2\,3).
\end{aligned}$$

Podemos concluir que $A_4 = V \rtimes H$.

En la segunda parte, basta notar que A_n para $n \geq 5$ no tiene subgrupos normales propios, mientras que en un producto semidirecto $N \rtimes_\phi H$ el subgrupo $N \times \{1_H\}$ es normal. Entonces, $A_n \cong N \rtimes_\phi H$ implica que N o H es trivial. ■

Problema 6 (2 puntos)**.** Se dice que dos sucesiones exactas cortas (extensiones de grupos)

$$1 \to H \xrightarrow{i} G \xrightarrow{p} K \to 1 \quad \text{y} \quad 1 \to H \xrightarrow{i'} G' \xrightarrow{p'} K \to 1$$

son **equivalentes** si existe un homomorfismo $f\colon G \to G'$ tal que el diagrama

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H & \xrightarrow{\;i\;} & G & \xrightarrow{\;p\;} & K & \longrightarrow & 1\\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\
1 & \longrightarrow & H & \xrightarrow{\;i'\;} & G' & \xrightarrow{\;p'\;} & K & \longrightarrow & 1
\end{array}$$

es conmutativo (hemos probado en clase que en este caso f es un isomorfismo).

Sea p un número primo. Consideremos una sucesión de homomorfismos

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{[1]_p \mapsto [p]_{p^2}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{[1]_{p^2} \mapsto [n]_p} \mathbb{Z}/p\mathbb{Z} \to 0$$

1) Demuestre que para todo $n = 1, 2, \ldots, p-1$ es una sucesión exacta corta.

2) Demuestre que estas sucesiones no son equivalentes para diferentes $n = 1, 2, \ldots, p-1$.

Solución. El homomorfismo

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p^2\mathbb{Z}, \\ [1]_p &\mapsto [p]_{p^2}, \\ [a]_p &\mapsto [ap]_{p^2}, \end{aligned}$$

es inyectivo: $ap \equiv bp \pmod{p^2}$ implica $a \equiv b \pmod{p}$. El homomorfismo

$$\begin{aligned} \mathbb{Z}/p^2\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z}, \\ [1]_{p^2} &\mapsto [n]_p, \\ [a]_{p^2} &\mapsto [an]_p \end{aligned}$$

es sobreyectivo: si $n = 1, 2, \ldots, p-1$, entonces $[an]_p = [a]_p \cdot [n]_p$ para $a = 0, 1, 2, \ldots, p-1$ son todos los restos módulo p: se tiene $[n]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$, así que la multiplicación por $[n]_p$ es un automorfismo del grupo $\mathbb{Z}/p\mathbb{Z}$. Finalmente,

$$\begin{aligned} \ker([a]_{p^2} \mapsto [an]_p) = \{[a]_{p^2} \mid an \equiv 0 \pmod{p}\} &= \{[a]_{p^2} \mid a \equiv 0 \pmod{p}\} \\ &= \{[ap]_{p^2} \mid [a]_p \in \mathbb{Z}/p\mathbb{Z}\} = \operatorname{im}([a]_p \mapsto [ap]_{p^2}). \end{aligned}$$

Todo esto significa que se tiene una sucesión exacta corta. Ahora supongamos que hay una equivalencia de tales sucesiones exactas cortas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{[1]_p \mapsto [p]_{p^2}} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{[1]_{p^2} \mapsto [n_1]_p} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{[1]_p \mapsto [p]_{p^2}} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{[a]_{p^2} \mapsto [an_2]_p} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \end{array}$$

La conmutatividad del primer cuadrado significa que $f([p]_{p^2}) = [p]_{p^2}$, mientras que la conmutatividad del segundo cuadrado nos dice que $f([1]_{p^2}) = [a]_{p^2}$ donde $n_1 \equiv an_2 \pmod{p}$. Luego,

$$[p]_{p^2} = f([p]_{p^2}) = p \cdot f([1]_{p^2}) = p \cdot [a]_{p^2} = [ap]_{p^2}.$$

Entonces, $ap \equiv p \pmod{p^2}$, lo que implica $a \equiv 1 \pmod{p}$. Junto con la congruencia $n_1 \equiv an_2 \pmod{p}$ esto nos da $n_1 \equiv n_2 \pmod{p}$. ■