Certamen 1 – Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Sebastián Fuentes

Departamento de Matemática, Universidad Técnica Federico Santa María

Nombre y Apellido: **ROL USM:**

Problema A (80 puntos)

Sean p y q dos números primos tales que $p < q$ y $p \nmid (q-1)$. El objetivo de este problema es clasificar **todos** los grupos finitos G de orden p^2q.

1. Probar que G contiene un único p-subgrupo de Sylow, que denotaremos P. ¿Es P normal en G?
2. Probar que G contiene un único q-subgrupo de Sylow, que denotaremos Q. ¿Es Q normal en G?
3. Definamos el conjunto
$$PQ := \{xy \text{ tal que } x \in P, y \in Q\}.$$
Probar que PQ es un sub-grupo de G y que $PQ = G$.
4. Probar que $P \cap Q = \{e\}$.
5. Probar que todo elemento de P conmuta con todo elemento de Q.
Indicación: $x \in P$ e $y \in Q$ conmutan si y sólo si el **conmutador** $[x,y] := xyx^{-1}y^{-1}$ *es trivial, i.e.,* $[x,y] = e$.
6. Deducir que G es un grupo abeliano.
7. Clasificar todos los grupos de orden p^2q (salvo isomorfismo).
Indicación: Utilizar adecuadamente el Teorema de estructura de grupos abelianos finitamente generados junto con el Teorema Chino del Resto.
8. ¿Existen primos $p < q$ con $p|(q-1)$ y un grupo G de orden p^2q de tal suerte que G **no** sea abeliano?

Problema B (20 puntos)

Resuelva los siguientes ejercicios.

1. Considerar el sub-grupo de $\mathbf{Z}^2$ dado por
$$H = \{(a,b) \in \mathbf{Z}^2 \text{ tal que } a - b \text{ es divisible por } 10\}.$$
Calcular su rango, determinar una base y describir el grupo cociente $\mathbf{Z}^2/H$.
Indicación: Para describir el grupo cociente, es conveniente utilizar una base de $\mathbf{Z}^2$ *adaptada a* H.
2. Sea p un número primo impar (i.e., $p \geq 3$). Probar que existe $x \in \mathbf{F}_p$ que **no** es un cuadrado, i.e., tal que no existe $y \in \mathbf{F}_p$ de tal suerte que $x = y^2$.
Indicación: Sea $\varphi : \mathbf{F}_p^\times \to \mathbf{F}_p^\times,\ x \mapsto x^2$. *Mostrar que* φ *es un morfismo de grupos y estudiar* $\ker(\varphi)$ *e* $\mathrm{Im}(\varphi)$.

Bonus (20 puntos)

Sea p un número primo impar. El objetivo de este problema es estudiar **residuos cuadráticos** módulo p. Más precisamente, decimos que $a \in \mathbf{Z}$ con $p \nmid a$ es un residuo cuadrático de p si $a \equiv b^2 \pmod{p}$ para algún $b \in \mathbf{Z}$. Para estudiar si a es o no un residuo cuadrático, definimos el **símbolo de Legendre** de a en p como

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático de } p, \\ -1 & \text{en otro caso.} \end{cases}$$

Así, el símbolo de Legendre define una función $\left(\frac{\cdot}{p}\right) : (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$ que (por el Problema B.2) es sobreyectiva.

(B1) Pruebe el **criterio de Euler** siguiente: $x^2 \equiv a \pmod{p}$ tiene solución $x \in \mathbf{F}_p^\times$ (resp. no tiene solución) si y sólo si $a^{(p-1)/2} \equiv 1 \pmod{p}$ (resp. si $a^{(p-1)/2} \equiv -1 \pmod{p}$).

Indicación: Sea g un generador de $\mathbf{F}_p^\times$, y escriba $a = g^k$. Distinga los casos k par y k impar, y recuerde que el pequeño Teorema de Fermat asegura que $h^{p-1} \equiv 1$ (mod p) para todo $h \in \mathbf{F}_p^\times$.

Así, el resultado anterior implica que para todo $a \in \mathbf{Z}$ con $p \nmid a$ se tiene

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

(B2) Demuestre que $\left(\frac{\cdot}{p}\right) : (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}$ es un morfismo de grupos y que

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

(B3) Determinar si la ecuación cuadrática $x^2 \equiv -72 \pmod{131}$ tiene solución o no.

En lo que sigue, puede usar (sin demostración) el siguiente importante resultado de Teoría de Números:

Hecho (Ley de Reciprocidad Cuadrática, Gauss 1801): Sea p un primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Más aún, si q es otro primo impar entonces se verifica que

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2}(-1)^{(q-1)/2}.$$

(B4) Usando la Ley de Reciprocidad Cuadrática, determine si la ecuación cuadrática $x^2 \equiv 31 \pmod{103}$ tiene o no solución.

Mini-bonus (1 punto)

Sea $R = x_1x_2x_3x_4x_5x_6x_7x_8$ un número entero positivo de 8 dígitos, donde $x_i \in \{0, \ldots, 9\}$ es el i-ésimo dígito, y sea

$$V := 3x_1 + 2x_2 + 7x_3 + 6x_4 + 5x_5 + 4x_6 + 3x_7 + 2x_8 \in \mathbf{N}.$$

Consideremos el grupo finito $(\mathbf{Z}/11\mathbf{Z}, +)$, cuyos elementos denotaremos

$$0 := [0]_{11}, 1 := [1]_{11}, \ldots, 9 := [9]_{11}, \mathrm{K} := [10]_{11}.$$

Verificar que si R es el entero positivo formado por los primeros 8 dígitos de su RUT, entonces el dígito verificador (que viene luego del guión) está dado por $[-V]_{11} \in \mathbf{Z}/11\mathbf{Z}$, usando la notación anterior.

Pauta Certamen 1 – Estructuras Algebraicas

Profesor: Pedro Montero, Ayudante: Sebastián Fuentes

Departamento de Matemática, Universidad Técnica Federico Santa María

Problema A (80 puntos)

1. Como $n_p \mid q$ entonces $n_p \in \{1, q\}$. Además, $n_p \equiv 1 \pmod{p}$ y $p \nmid q-1$ (i.e., $q \not\equiv 1 \pmod{p}$) se tiene $n_p = 1$, y luego $P \trianglelefteq G$ es normal (por ser único).

2. Como $n_q \mid p^2$ entonces $n_q \in \{1, p, p^2\}$. Como $n_q \equiv 1 \pmod{q}$ y $p < q$ entonces $n_q \neq p$. Si $n_q = p^2$ entonces q divide $p^2 - 1 = (p-1)(p+1)$ y luego q divide $p+1$, de donde deducimos que $q = p+1$ (pues $p < q$). Esto último contradice $p \nmid (q-1)$ y así deducimos que $n_q = 1$, por lo que $Q \trianglelefteq G$ es normal (por ser único).

3. Sean $x, x' \in P$, $y, y' \in Q$ arbitrarios. Entonces $(xy)(x'y') = xyx'y^{-1}yy' = xx''yy' \in PQ$ para cierto $x'' = yx'y^{-1} \in P$ (por normalidad de P). Del mismo modo, $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}(xy^{-1}x^{-1}) = x^{-1}y'' \in PQ$ para cierto $y'' = xy^{-1}x^{-1} \in Q$ (por normalidad de Q). Como $e \in PQ$, tenemos así que $PQ \leq G$. Además, $P \leq PQ$ y $Q \leq PQ$ por lo que $|P| = p^2$ y $|Q| = q$ dividen $|PQ|$ (Teorema de Lagrange), i.e., $|G| = p^2q$ divide $|PQ|$ y luego $PQ = G$.

4. $|P \cap Q|$ divide $|P| = p^2$ y $|Q| = q$ (Teorema de Lagrange) y luego $|P \cap Q| = 1$, i.e., $P \cap Q = \{e\}$.

5. Si $x \in P$, $y \in Q$ entonces $xyx^{-1} \in Q$ por normalidad de Q y luego $[x, y] = xyx^{-1}y^{-1} \in Q$. Del mismo modo, $[x, y] \in P$ y luego $[x, y] \in P \cap Q = \{e\}$, i.e., $[x, y] = e$.

6. Dado que $|P| = p^2$ y $|Q| = q$ con p, q primos, tenemos que P y Q son abelianos (visto en clases). Por (3), todo $g \in G$ es de la forma $g = xy$ con $x \in P$, $y \in Q$. Así, $gg' = xyx'y' = xx'yy'$ (por 5) $= x'xy'y$ (pues P y Q abelianos) $= x'y'xy$ (por 5) $= g'g$, i.e., G es un grupo abeliano.

7. Calculando factores invariantes en el Teorema Fundamental de grupos abelianos finitamente generados, deducimos que los únicos grupos abelianos de orden p^2q son $G_1 = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/pq\mathbf{Z}$ y $G_2 = \mathbf{Z}/p^2q\mathbf{Z}$.

8. Si $p = 2$ y $q = 3$ tenemos que $|G| = 12$. Hay grupos de orden 12 no-abelianos (e.g. D_6, A_4, $\mathbf{Z}/2\mathbf{Z} \times S_3$ sirven).

Problema B (20 puntos)

1. $(a, b) \in H$ si y sólo si existe $k \in \mathbf{Z}$ tal que $b = a + 10k$, y luego $H = \{(a, a+10k), (a, k) \in \mathbf{Z}^2\} = \mathbf{Z}v_1 \times \mathbf{Z}v_2$ donde $v_1 = (1, 1)$ y $v_2 = (0, 10)$ forman una base de H. En particular, $\mathrm{rg}(H) = 2$. Además, $e_1 = (1, 1)$ y $e_2 = (0, 1)$ es una base de $\mathbf{Z}^2$ adaptada a H pues $d_1e_1 = v_1$ y $d_2e_2 = v_2$ donde $d_1 = 1$ y $d_2 = 10$. Así, $\mathbf{Z}^2/H \cong \mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z} \cong \mathbf{Z}/10\mathbf{Z}$.

2. Como $\mathbf{F}_p^\times$ es abeliano, $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$ es un morfimo de grupos. Por el Teorema del isomorfismo de Noether, $\mathrm{Im}(\varphi) \cong \mathbf{F}_p^\times / \ker(\varphi)$. Como $p \geq 3$, tenemos que $1 \neq -1$ en $\mathbf{F}_p^\times$ y luego $|\ker(\varphi)| \geq 2$[1]. Así, $|\mathrm{Im}(\varphi)| \leq |\mathbf{F}_p^\times|/2 = (p-1)/2 < p-1 = |\mathbf{F}_p^\times|$ y luego φ no es sobreyectivo.

[1] De hecho, $\ker(\varphi) = \{\pm 1\}$.