Álgebra II

Segundo Cuatrimestre — 2008

Práctica 3: Grupos: acciones y teoremas de Sylow

1. Acciones

1.1. En cada uno de los siguientes casos probar que $\centerdot$ es una acción de G en X y calcular $X^G := \{x \in X \ : \ g \centerdot x \ \forall g \in G\}$ y las G-órbitas y el estabilizador E_x de cada elemento $x \in X$, para los siguiente X:

a) $G = \{f : \mathbb{R} \to \mathbb{R}, f(x) = ax + b$ con $a \in \mathbb{R}^*, b \in \mathbb{R}\}$, $X = \mathbb{R}$ y $f \centerdot x = f(x)$;

b) $G = \{f : \mathsf{End}(\mathbb{R}^2) : d(f(x), f(y)) = d(x,y) \ \forall x, y \in \mathbb{R}^2\}$, $X = \mathbb{R}^2$ y $f \centerdot x = f(x)$;

c) $G = \mathbb{R}^*$, $X = \mathbb{R}_{>0}$ y $a \centerdot x = x^a$;

d) $G = \mathsf{SL}_2(\mathbb{Z})$, $X = \mathbb{Z} \times \mathbb{Z}$ y $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \centerdot (x, y) = (ax + by, cx + dy)$.

1.2. Sea G un grupo, p primo. Probar que

a) si $|G| = p^n$, $n \in \mathbb{N}$ entonces $\mathsf{Z}(G) \neq \{1\}$. Caracterizar los grupos simples de orden p^n;

b) si $G/\mathsf{Z}(G)$ es cíclico, entonces G es abeliano;

c) si $|G| = p^2$, entonces G es abeliano;

d) si $|G| = p^3$, entonces $\mathsf{Z}(G) = [G : G]$ y caracterizar $G/\mathsf{Z}(G)$.

1.3. Si un grupo G actúa sobre un conjunto finito X, el *carácter* de X es la aplicación $\chi_X : G \to \mathbb{N}_0$ dada por

$$\chi_X(g) = |\{x \in X : gx = x\}|, \qquad \forall g \in G.$$

Si no hay ambigüedad sobre X, escribimos simplemente χ.

(a) Si G actúa transitivamente sobre X, es muestre que

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = 1.$$

Sugerencia. Considere el conjunto $S = \{(g, x) \in G \times X : gx = x\}$ y cuente sus elementos de dos formas distintas.

(b) En general, si la acción no es necesariamente transitiva, es

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = |X/G|.$$

Aquí, X/G es el conjunto de órbitas de G en X.

1.4. *Grupos lineales finitos.* Sea k un cuerpo finito de q elementos.

(a) Sea $V = k^2$ el k-espacio vectorial de vectores columna y sea X el conjunto de vectores no nulos de V. Mostrar que la acción de $\mathsf{GL}_2(k)$ sobre V por multiplicación a izquierda preserva a X y que la acción de $\mathsf{GL}_2(k)$ sobre X es transitiva.

(b) Sea $v_0 = (1, 0)^t \in X$. Determinar el estabilizador $\mathsf{GL}_2(k)_{v_0}$ de v_0 en $\mathsf{GL}_2(k)$.

(c) Mostrar que $|\mathsf{GL}_2(k)| = (q^2 - 1)(q^2 - q)$.

†*(d)* Más generalmente, mostrar que si $n \in \mathbb{N}$, es

$$|\mathsf{GL}_n(k)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

†*(e)* Sea $n \in \mathbb{N}$. Muestre que el morfismo $\mathsf{det} : \mathsf{GL}_n(k) \to k^\times$ es sobreyectivo y concluya que

$$|\mathsf{SL}_n(k)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i).$$

1.5. Sea G un grupo tal que $|G| = 2n$, G tiene n elementos de orden 2 y los restantes forman un subgrupo H. Probar que entonces n es impar y que $H \lhd G$.

1.6. Sea p primo y $|G| = n$. Probar que existe k tal que $n = p^k$ si y solo si para todo $x \in G, |x| = p^s$ para algún s, que depende de x.

1.7. Sean p, q primos, tales que $p > q$. Probar que

a) si q no divide a $p - 1$, entonces todo grupo de orden pq es cíclico,

b) si q divide a $p - 1$, entonces hay exactamente dos grupos no isomorfos de orden pq: uno cíclico y el otro no abeliano.

2. Teoremas de Sylow

2.1. Sea p un número primo. Un grupo abeliano finito de exponente p^r con $r > 0$ posee elementos de orden p.

2.2. Sea p un número primo y G un grupo de orden $p^r > 1$. Entonces $\mathsf{Z}(G)$ no es trivial.

2.3. Sea G un grupo finito de orden $|G| = p^r m$ con p primo y $(p, m) = 1$. Entonces G posee subgrupos de orden p^r.

Definición. *Sea p un número primo. Un elemento g de G es* p-primario *si su orden es una potencia de p. Un grupo G es un* p-grupo *si el orden de todo elemento de G es una potencia de p.*

2.4. Sea p un número primo.

(a) Si G es un p-grupo y H es un subgrupo de G, entonces H es un p-grupo.

(b) Si G es un p-grupo y $f : G \to H$ es un homomorfismo sobreyectivo, H es un p-grupo.

(c) Si G es un grupo, H un subgrupo normal de G y tanto H como G/H son p-grupos, entonces G es un p-grupo.

2.5. Un grupo finito G es un p-grupo sii $|G| = p^r$ para algún $r \geq 1$.

Definición. *Sea p un número primo y G un grupo. Un* p-subgrupo de Sylow *de G es un p-subgrupo maximal de G. Escribimos $\mathsf{Syl}_p(G)$ al conjunto de los p-subgrupos de Sylow de G.*

2.6. Sea G un grupo finito y p un número primo.

(a) Si $|G| = p^r m$ con $(p, m) = 1$ y $H \subset G$ es un subgrupo tal que $|H| = p^r$, entonces $H \in \mathsf{Syl}_p(G)$.

(b) Si $p \mid |G|$, entonces $\mathsf{Syl}_p(G) \neq \varnothing$.

2.7. Si G es un grupo y $H \in \mathsf{Syl}_p(G)$ y $x \in G \setminus H$ tiene orden $|x| = p^n$, entonces $x \notin \mathsf{N}(H)$.

Sugerencia. Suponga lo contrario y considere el orden del elemento xH en $\langle H \cup \{x\}\rangle / H$.

2.8. Sea G un grupo finito y $K \in \mathsf{Syl}_p(G)$. Sea $\mathcal{C}$ el conjunto de subgrupos de G conjugados de K.

(a) Sea $H \in \mathsf{Syl}_p(G)$ y sea $\sim$ la relación en $\mathcal{C}$ tal que

$$L \sim L' \text{ sii existe } h \in H \text{ tal que } hLh^{-1} = L.$$

Muestre que se trata de una relación de equivalencia.

(b) Sea $L \in \mathcal{C}$ y notemos $[L]$ a la clase de equivalencia de L. Entonces $|[L]| = [H : H \cap \mathsf{N}(L)]$. Además, si $L \neq H$ es $|[L]| > 1$ y es divisible por p. Si, por el contrario, $L = H$, entonces $|[H]| = 1$.

(c) Muestre que

$$|\mathcal{C}| \equiv \begin{cases} 0 \pmod p, & \text{si } H \notin \mathcal{C}; \\ 1 \pmod p, & \text{si } H \in \mathcal{C}. \end{cases}$$

(d) Concluya que H es conjugado de K y que $|\mathcal{C}| \cong 1 \pmod p$.

2.9. Pruebe el siguiente teorema de Peter Ludwig Mejdell Sylow (1832–1918, Noruega) que es, probablemente, el teorema más importante de la teoría de grupos finitos.

Teorema. (M. L. Sylow, Théorèmes sur les groupes de substitutions, Math. Ann. **5** (1872), no. 4, 584–594.) *Sea p un número primo. Sea G un grupo finito de orden $p^r m$ con $(p, m) = 1$. Entonces*

(a) *Un subgrupo H de G es un p-subgrupo de Sylow sii $|H| = p^r$.*
(b) *Todos los p-subgrupos de Sylow de G son conjugados.*
(c) *Sea n_p el número de p-subgrupos de Sylow de G. Entonces $n_p \equiv 1 \pmod p$.*
(d) $n_p \mid m$.

2.10. Muestre que no hay grupos simples de orden 28 ó 312.

2.11. Muestre que un grupo de orden 12 ó 56 no es simple.

2.12. Probar que

a) todo grupo de orden $17^2.19^2$ es abeliano;
b) todo grupo de orden 255 es cíclico;
c) todo grupo de orden 5.7.17 es cíclico.

2.13. Si p y q son primos distintos, un grupo de orden pq no es simple.

2.14. Sea G un grupo de orden $p^r m$ con p primo, $r \geq 1$ y $p > m$. Entonces G no es simple.

2.15. Sea G un grupo de orden $p^2 q$ con p y q primos distintos. Entonces G no es simple.

2.16. Muestre que un grupo de orden menor que 60 no es simple.

2.17. Mostrar que si G es un grupo y P es un subgrupo de Sylow de G, entonces P es un subgrupo característico de $\mathsf{N}(P)$.

2.18. Si todos los subgrupos de Sylow de un grupo finito G son normales, entonces $G \cong \prod_{p \text{ primo}} P_p$. En particular, un grupo abeliano finito es producto de sus subgrupos de Sylow.