Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer semestre de 2021

Práctico 4

1. Sea $H = \{\sigma \in \mathcal{S}_4 : \ \sigma(4) = 4\}$. Probar que H es un subgrupo de $\mathcal{S}_4$ que no es normal.

2. Probar que si H es un subgrupo de índice 2 de G, entonces H es normal en G.

3. Para este ejercicio conviene recordar el ejercicio 14 del Práctico 2.

   a) Determinar todos los subgrupos normales de D_4. Identificar $Z(D_4)$. *Sug.:* Recordar el Pr. 1.

   b) Encontrar dos subgrupos $H \subset K \subset D_4$ tales que $H \lhd K$ y $K \lhd D_4$, pero H no es normal en D_4.

   c) Probar que todos los subgrupos de Q son normales. (Notar que Q no es abeliano.)

4. Si G es un grupo y $g \in G$, definimos $\mathrm{Int}_g : G \to G$ mediante $\mathrm{Int}_g(x) = gxg^{-1}$, para todo $x \in G$. Sea $\mathrm{Int}(G) = \{\mathrm{Int}_g : \ g \in G\}$. Probar que $\mathrm{Int}(G)$ es un subgupo normal de $\mathrm{Aut}(G)$ isomorfo a $G/Z(G)$.

5. Un subgrupo H de un grupo G se dice que es *característico* si $\varphi(H) = H$, para todo $\varphi \in \mathrm{Aut}(G)$.

   a) Probar que todo subgrupo característico es normal.

   b) Dar un ejemplo de un grupo con un subgrupo normal que no es característico.

   c) Probar que si H es el único subgrupo de G que tiene cierto orden $n < \infty$, entonces H es característico.

   d) Probar que si G es cíclico (finito o infinito), entonces todos sus subgrupos son característicos.

   e) Probar que si G es un grupo y $K \subset H \subset G$ son subgrupos tales que K es característico en H y H es normal en G, entonces K es normal en G. Comparar con el ejercicio 3*b*.

6. Sea G un grupo tal que $|G| = pn$, con p primo y $p > n$. Probar que G tiene un único subgrupo H de orden p. Deducir que H es normal.

7. Probar que si H es un subgrupo cíclico y normal de G, entonces todo subgrupo de H es normal en G.

8. Probar que si G es un grupo tal que $G/Z(G)$ es cíclico, entonces G es abeliano.

9. *a*) Probar que si un grupo G está generado por un conjunto S entonces $g \in Z(G)$ (el centro de G) si y solo si $gs = sg$, para todo $s \in S$.

   b) Determinar el centro del grupo diedral D_n. *Pista*: depende de la paridad de n.

10. Sea G un grupo que contiene un subgrupo H tal que $H \neq G$ y $[G : H] < \infty$. Probar que G contiene un subgrupo normal N tal que $N \neq G$ y $[G : N] < \infty$.

11. Sea G un grupo que contiene subgrupos normales finitos $K_1, \dots, K_r$ que tienen órdenes primos dos a dos. Probar que $K_1 \cdots K_r = \{k_1 \cdots k_r : \ k_i \in K_i, \ \forall i = 1, \dots, r\}$ es un subgrupo normal de G y que $K_1 \cdots K_r \simeq K_1 \times \cdots \times K_r$ como grupos. *Sugerencia:* probarlo primero para $r = 2$ y luego usar inducción; recordar el ejercicio 5b) del Práctico 2.

12. Sean $m_1, \ldots, m_n$ enteros positivos tales que $\operatorname{mcd}(m_i, m_j) = 1$ si $i \neq j$ y sea $m = m_1 \cdots m_n$.

a) Probar que tiene sentido definir $\alpha : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ por $\alpha(\overline{x}) = (\overline{x}, \ldots, \overline{x})$, $\forall x \in \mathbb{Z}$.

b) Probar que α es inyectiva. Concluir que α es un isomorfismo de grupos aditivos.

c) Probar

$$\mathbb{Z}_m^\times \simeq (\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r})^\times \simeq \mathbb{Z}_{m_1}^\times \cdots \times \mathbb{Z}_{m_1}^\times$$

como grupos multiplicativos.

Sugerencia. El producto cartesiano de monoides es un monoide, operando coordenada a coordenada. Luego $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ es un monoide, considerando $\mathbb{Z}_{m_1}, \ldots, \mathbb{Z}_{m_r}$ como monoides con la multiplicación. Notar que α verifica $\alpha\left(\overline{1}\right) = \left(\overline{1}, \ldots, \overline{1}\right)$; $\alpha\left(\overline{x} \cdot \overline{y}\right) = \alpha\left(\overline{x}\right) \cdot \alpha\left(\overline{y}\right)$, $\forall \overline{x}, \overline{y} \in \mathbb{Z}_m$.

13. Se define la *función de Euler* $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ mediante

$$\varphi(n) = |\{a : \ 1 \leq a \leq n \text{ y } \operatorname{mcd}(a, n) = 1\}|, \quad \forall n \in \mathbb{Z}^+.$$

a) Probar que $\varphi(n) = |\mathbb{Z}_n^\times| = |\operatorname{Aut}(\mathbb{Z}_n)|$, para todo $n \in \mathbb{Z}^+$.

b) Sean $m_1, \ldots, m_n$ enteros positivos tales que $\operatorname{mcd}(m_i, m_j) = 1$ si $i \neq j$ y sea $m = m_1 \cdots m_n$. Probar $\varphi(m) = \varphi(m_1) \cdots \varphi(m_r)$. *Sugerencia:* recordar el ejercicio 12.

c) Sea p un número primo y $n \in \mathbb{Z}^+$.

1) Probar que el mapa identidad de $\mathbb{Z}$ induce un epimorfismo de grupos aditivos $\psi : \mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$.
2) Probar que ψ induce un morfismo de grupos multiplicativos $\varphi : \mathbb{Z}_{p^{n+1}}^\times \to \mathbb{Z}_{p^n}^\times$.
3) Probar que φ es sobreyectivo y $\operatorname{Ker} \varphi = \{\overline{x_0}, \ldots, \overline{x_{p-1}}\}$ siendo $x_i = 1 + i\, p^n$, $i = 0, \ldots, p-1$. Deducir $\varphi\left(p^n\right) = (p-1)p^{n-1}$.

d) Deducir el cálculo de $\varphi(n)$ para n arbitrario.

14. *a*) Sean $a \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$. Probar que si $\operatorname{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\operatorname{mod}\ n)$.

b) (Euler-Fermat.) Sea p un número primo y a un número entero tal que $p \nmid a$.
Probar que $a^{p-1} \equiv 1 (\operatorname{mod}\ p)$. Deducir que $a^p \equiv a (\operatorname{mod}\ p)$ para *todo* entero a.