Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer semestre de 2020

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, entones 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. Sea G un grupo, el *conmutador* de $g, f \in G$ es $[g, f] = gfg^{-1}f^{-1}$, para todo $g, f \in G$ El *conmutador* de G es el subgrupo $[G, G] = \langle [g, f] : g, f \in G\rangle$. Probar.

   a) Si $\varphi : G \to F$ es un morfismo, entonces $\varphi([g, f]) = [\varphi(g), \varphi(f)]$, para todo $g, f \in G$.

   b) Valen $[g, f]^{-1} = [f, g]$ y $h[g, f]h^{-1} = \left[hgh^{-1}, hfh^{-1}\right]$, para todo $g, f, h \in G$.

   c) Vale $[G, G] \lhd G$ y $G/[G, G]$ es abeliano. El grupo $G_{ab} := G/[G, G]$ se llama el *abelianizado* de G.

   d) Si $N \lhd G$ es tal que G/N es abeliano, entonces $[G, G] \subset N$.

   e) Si H es un subgrupo de G y $[G, G] \subset H$, entonces $H \lhd G$.

   f) Si $\varphi : G \to F$ es un morfismo, siendo F un grupo abeliano, entonces existe un único morfismo $\tilde{\varphi} : G_{ab} \to F$ tal que $\tilde{\varphi}(\overline{g}) = \varphi(g)$, para todo $g \in G$.

   g) Si $G = D_n = \langle a, b : \ a^2 = b^n = 1, \ ba = ab^{n-1}\rangle$ el diedral, entonces $[G, G] = \langle b^2\rangle$.
   Probar $(D_3)_{ab} \simeq \mathbb{Z}_2$ y $(D_4)_{ab} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

10. Sean $m_1, \dots, m_n$ 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 $\alpha(\overline{x}) = (\overline{x}, \dots, \overline{x})$, $\forall x \in \mathbb{Z}$.

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

   c) Observando que α preserva el producto concluir

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

   como grupos multiplicativos.

11. 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 $m_1, \dots, m_n$ 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 10.

   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 $\operatorname{Ker} \varphi = \{\overline{x_0}, \dots, \overline{x_{p-1}}\}$ siendo $x_i = 1 + i\,p^n$, $i = 0, \dots, p-1$. Deducir $\varphi(p^n) = (p-1)p^{n-1}$.

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

12. *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.