Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois
Primer semestre 2020

Examen. 12/02/2021.

1. **20 puntos.**
   a) Probar $\mathrm{Aut}(Z_n) \simeq \mathbb{Z}_n^\times$ (el grupo multiplicativo de invertibles de $\mathbb{Z}_n$), siendo $n \geq 2$.
   b) Sea G un grupo tal que $\mathrm{Aut}(G) = \{\mathrm{id}\}$. Probar que G es abeliano y que todo elemento distinto del neutro tiene orden 2.

2. **30 puntos.** Sea G un grupo de orden 231. Probar.
   a) G contiene subgrupos normales de orden 7 y 11.
   b) G contiene un subgrupo de orden 33.
   c) G contiene un subgrupo normal de orden 77.
   d) El subgrupo de orden 11 está contenido en el centro de G.

3. **50 puntos.**
   a) Probar que $X^4 + X^3 + X^2 + X + 1$ es irreducible en $\mathbb{Q}[X]$.
   Sugerencia: $p(X)$ es irreducible si y solo si $p(X+1)$ es irreducible.
   b) Sea $\mu \in \mathbb{C}$ una raíz primitiva de orden 5 de 1 y $F = \mathbb{Q}(\mu)$.
      1) Probar que $F/\mathbb{Q}$ es de Galois y determinar $\mathrm{Gal}(F/\mathbb{Q})$.
      2) Probar que $\mu^2 + \mu^3$ es raíz de $X^2 + X - 1$ y deducir que vale $\mathbb{Q}\left(\mu^2 + \mu^3\right) = \mathbb{Q}\left(\sqrt{5}\right)$.
      3) Probar que $\mathbb{Q}\left(\sqrt{5}\right)$ es el único cuerpo intermedio entre $\mathbb{Q}$ y F.
   c) Determinar el grupo de Galois de cada uno de los siguientes polinomios con coeficientes en $\mathbb{Q}$:
      1) $\left(X^5 - 1\right)\left(X^2 - 5\right)$.
      2) $\left(X^5 - 1\right)\left(X^2 - 3\right)$.

Solución.

1. *a*) Si $\overline{m} \in \mathbb{Z}_n^\times$, entonces $\lambda_{\overline{m}} \in \mathrm{Aut}(Z_n)$, definiendo $\lambda_{\overline{m}}(\overline{n}) = \overline{m} \cdot \overline{n}$, para todo $n \in \mathbb{Z}$. Es fácil de probar que la correspondencia $\overline{m} \mapsto \lambda_{\overline{m}}$ es un isomorfismo.

   b) Considerando los automorfismos internos se deduce que G es abeliano. Como G es abeliano, entonces ι definido por $\iota(g) = g^{-1}$ es un automorfismo; luego $\iota = \mathrm{id}$ lo cual equivale a que todo elemento distinto del neutro tiene orden 2.

2. $|G| = 231 = 3 \times 7 \times 11$.

   a) Aplicando los teorema de Sylow es fácil de probar que valen $n_7 = n_{11} = 1$, luego $S_7 \lhd G$ y $S_{11} \lhd G$.

   b) Sea S_3 un 3-subgrupo de Sylow. Como $S_{11} \lhd G$, entonces $S_3S_{11} < G$ y al tener órdenes primos se deduce $|S_3S_{11}| = 33$.

   c) Por el mismo argumento de antes, al ser $S_7 \lhd G$ y $S_{11} \lhd G$, deducimos $S_7S_{11} \lhd G$ y $|S_7S_{11}| = 77$.

   d) Es fácil de probar que vale $G = S_3S_7S_{11}$. Notar que estos subgrupos de Sylow tienen orden primo, luego son cíclicos. Sean $S_3 = \langle g_3 \rangle$, $S_7 = \langle g_7 \rangle$ y $S_{11} = \langle g_{11} \rangle$. Luego $G = \langle g_3, g_7, g_{11} \rangle$. Usando la clasificación de los grupos de orden pq deducimos que S_3S_{11} y S_7S_{11} son grupos abelianos, luego g_{11} conmuta con g_3 y con g_7, y al ser $G = \langle g_3, g_7, g_{11} \rangle$, concluimos $g_{11} \in Z(G)$ lo cual implica $S_{11} \subset Z(G)$.

3. *a*) Si $p(X) = X^4 + X^3 + X^2 + X + 1$, entonces $p(X+1) = X^4 + 5X^3 + 10X^2 + 5X + 5$. Este último es irreducible por el criterio de Eisenstein.

   b) Sea $\mu \in \mathbb{C}$ una raíz primitiva de orden 5 de 1 y $F = \mathbb{Q}(\mu)$.

      1) F es el cuerpo de descomposición de $X^5 - 1$; $\mathrm{Irr}_{\mathbb{Q}}(u) = X^4 + X^3 + X^2 + X + 1$, luego $[F : \mathbb{Q}] = 4$ y por lo tanto $|\mathrm{Gal}(F/\mathbb{Q})| = 4$. Como es $F = \mathbb{Q}(\mu)$, los elementos de $\mathrm{Gal}(F/\mathbb{Q})$ quedan determinados por su valor en μ, que es una de las raíces de $p(X)$ que son μ, μ^2, μ^3, μ^4. Es fácil de probar que vale $\mathrm{Gal}(F/\mathbb{Q}) = \langle \sigma \rangle$, siendo $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ determinada por $\sigma(\mu) = \mu^2$. Luego $\mathrm{Gal}(F/\mathbb{Q}) = C_4$.

      2) Es fácil (usar $\mu^5 = 1$ e $\mathrm{Irr}_{\mathbb{Q}}(u)$).

      3) El grupo cíclico C_4 tiene un único subgrupo de orden 2, luego por la correspondencia de Galois sabemos que hay un único cuerpo intermedio entre $\mathbb{Q}$ y F. Como $\mathbb{Q}\left(\mu^2 + \mu^3\right) = \mathbb{Q}\left(\sqrt{5}\right)$ es un cuerpo intermedio, entonces es el único cuerpo intermedio entre $\mathbb{Q}$ y F.

   c) 1) El cuerpo de descomposición de $\left(X^5 - 1\right)\left(X^2 - 5\right)$ es $\mathbb{Q}(\mu, \sqrt{5})$, pero $\sqrt{5} \in F$, luego el cuerpo de descomposición de $\left(X^5 - 1\right)\left(X^2 - 5\right)$ es F y el grupo de Galois es C_4.

      2) El cuerpo de descomposición de $X^5 - 1$ es $F = \mathbb{Q}(\mu)$ y el de $X^2 - 3$ es $\mathbb{Q}\left(\sqrt{3}\right)$. Luego el cuerpo de descomposición de $f = \left(X^5 - 1\right)\left(X^2 - 3\right)$ es $\mathbb{Q}\left(\mu, \sqrt{3}\right)$. Sean $G = \mathrm{Gal}\left(\mathbb{Q}\left(\mu, \sqrt{3}\right)/\mathbb{Q}\right)$, $H = \mathrm{Gal}\left(\mathbb{Q}\left(\mu, \sqrt{3}\right)/\mathbb{Q}(\mu)\right)$ y $K = \mathrm{Gal}\left(\mathbb{Q}\left(\mu, \sqrt{3}\right)/\mathbb{Q}(\sqrt{3})\right)$. Como $\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}$ y $\mathbb{Q}(\mu)/\mathbb{Q}$ son de Galois, entonces H y K son subgrupos normales de G. De $\mathbb{Q}(\mu)\mathbb{Q}\left(\sqrt{3}\right) = \mathbb{Q}\left(\mu, \sqrt{3}\right)$, deducimos $H \cap K = \{\mathrm{id}\}$. Además $\mathbb{Q}(\mu) \cap \mathbb{Q}\left(\sqrt{3}\right)$ es un subcuerpo de $\mathbb{Q}(\mu)$ y tiene grado 2 o 1 sobre $\mathbb{Q}$; pero el único cuerpo intermedio entre $\mathbb{Q}$ y F es $\mathbb{Q}\left(\sqrt{5}\right)$, y es fácil de probar que es $\mathbb{Q}\left(\sqrt{5}\right) \neq \mathbb{Q}\left(\sqrt{3}\right)$. Luego $\mathbb{Q}(\mu) \cap \mathbb{Q}\left(\sqrt{3}\right) = \mathbb{Q}$. Esto implica $HK = G$. Por lo anterior es $G \simeq H \times K = C_2 \times C_4$.