Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois
Curso 2021

Examen. 10/08/2021.

1. (**50 puntos**)

   a) Sea G un grupo, H un subgrupo y $N_G(H) = \{g \in G : gHg^{-1} = H\}$ el normalizador de H en G. Probar que si $\alpha \in \mathrm{Aut}(G)$ es tal que $\alpha(H) = H$, entonces $\alpha(N_G(H)) = N_G(H)$.

   b) Calcular los 3-subgrupos de Sylow del grupo simétrico $\mathcal{S}_4$, y sus normalizadores.

   c) Probar que si $\alpha \in \mathrm{Aut}(\mathcal{S}_4)$ es tal que $\alpha(P) = P$ para todo 3-subgrupo de Sylow de $\mathcal{S}_4$, entonces $\alpha = \mathrm{id}$. *Sugerencia:* aplicar la parte 1*a* y observar que la intersección de los normalizadores de dos 3-subgrupos de Sylow diferentes tiene orden 2.

   d) Sea X el conjunto de los 3-subgrupos de Sylow de $\mathcal{S}_4$. Probar que si $\alpha \in \mathrm{Aut}(\mathcal{S}_4)$ entonces el mapa $\hat{\alpha} : X \to X$ definido por $\hat{\alpha}(P) = \alpha(P)$ es inyectivo.
   Esto induce una función $T : \mathrm{Aut}(\mathcal{S}_4) \to \mathrm{Biy}(X)$ definida por $T(\alpha) = \hat{\alpha}$, para todo $\alpha \in \mathrm{Aut}(\mathcal{S}_4)$.

   e) Probar que $T : \mathrm{Aut}(\mathcal{S}_4) \to \mathrm{Biy}(X)$ es un morfismo inyectivo de grupos. Deducir $|\mathrm{Aut}(S_4)| \leq |\mathcal{S}_4|$.

   f) Sea $\mathrm{Int} : \mathcal{S}_4 \to \mathrm{Aut}(\mathcal{S}_4)$ definido por $\mathrm{Int}_\sigma(\tau) = \sigma\tau\sigma^{-1}$. Probar que Int es un isomorfismo.

2. (**50 puntos**) Sea $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}\right)$.

   a) Hallar $[K : \mathbb{Q}]$.

   b) Probar $K = \mathbb{Q}(u)$, siendo $u = \sqrt{2} + \sqrt[3]{5}$.

   c) Hallar los polinomios irreducibles de u sobre $\mathbb{Q}$ y sobre $\mathbb{Q}\left(\sqrt{2}\right)$.

   d) Sea $F = K(w)$, siendo $w \in \mathbb{C}$ tal que $w^3 = 1$ y $w \neq 1$. Hallar $[F : \mathbb{Q}]$.

   e) Determinar si $K/\mathbb{Q}$ y $F/\mathbb{Q}$ son extensiones de Galois.

   f) Hallar el polinomio irreducible de $\sqrt[3]{5}$ sobre $\mathbb{Q}$, el polinomio irreducible de $\sqrt{2}$ sobre $\mathbb{Q}\left(\sqrt[3]{5}\right)$ y el polinomio irreducible de w sobre $\mathbb{Q}\left(\sqrt[3]{5}, \sqrt{2}\right)$.

   g) Probar que existen $\alpha, \beta \in \mathrm{Gal}(F/\mathbb{Q})$ tales que

$$\alpha\left(\sqrt[3]{5}\right) = w\sqrt[3]{5}, \quad \alpha\left(\sqrt{2}\right) = -\sqrt{2}, \quad \alpha(w) = w;$$
$$\beta\left(\sqrt[3]{5}\right) = w\sqrt[3]{5}, \quad \beta\left(\sqrt{2}\right) = -\sqrt{2}, \quad \beta(w) = w^2.$$

   h) Probar $\mathrm{Gal}(F/\mathbb{Q}) = \langle \alpha, \beta \rangle = \langle \alpha \rangle \langle \beta \rangle$.

Solución.

1. *a*) Sea $n \in N_G(H)$. Si $h \in H$, entonces existe $k \in H$ tal que $h = \alpha(k)$. Entonces $\alpha(n)h\alpha(n)^{-1} = \alpha\left(nkn^{-1}\right) \in \alpha(H) = H$. Esto implica $\alpha\left(N_G(H)\right) \subset N_G(H)$. Razonando análogamente con α^{-1} se obtiene la otra inclusión.

   b) Es $n_3 = 4$, luego los 3-subgrupos de Sylow son los siguientes $\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$. Usando $[G : N_G(S_p)] = n_p$, deducimos $|N_G(S_3)| = 6$, luego

$$N_{\mathcal{S}_4}\big(\langle(abc)\rangle\big) = \langle(abc)\rangle \cup \{(ab),\, (ac),\, (bc)\}.$$

   c) Sea $\alpha \in \operatorname{Aut}(\mathcal{S}_4)$ tal que $\alpha(P) = P$ para todo 3-subgrupo de Sylow de $\mathcal{S}_4$. Por la sugerencia, si $N_4 = N_{\mathcal{S}_4}\big(\langle(123)\rangle\big)$ y $N_3 = N_{\mathcal{S}_4}\big(\langle(124)\rangle\big)$, entonces

$$\alpha\big((12)\big) \in \alpha\big(\langle(12)\rangle\big) = \alpha(N_3 \cap N_4) \subset \alpha(N_3) \cap \alpha(N_4) = N_3 \cap N_4 = \langle(12)\rangle \Rightarrow \alpha\big((12)\big) = (12).$$

   Luego α deja fijas a todas las trasposiciones y eso implica $\alpha = \mathrm{id}$.

   d) Sea $\alpha \in \operatorname{Aut}(\mathcal{S}_4)$. Sean $P_1 = \langle\sigma_1\rangle$ y $P_2 = \langle\sigma_2\rangle$ dos 3-subgrupos de Sylow. Si $\alpha(P_1) = \alpha(P_2)$, entonces $\alpha(\sigma_1) = \alpha\left(\sigma_2\right)^{\pm 1}$. Luego $\sigma_1 = \sigma_2^{\pm 1}$ y por lo tanto $P_1 = P_2$.

   e) Es claro que $T : \operatorname{Aut}(\mathcal{S}_4) \to \operatorname{Biy}(X)$ es un morfismo de grupos. La inyectividad se deduce la parte 1*c*. Usando $\operatorname{Biy}(X) \simeq \mathcal{S}_4$ deducimos $|\operatorname{Aut}(S_4)| \leq |\mathcal{S}_4|$.

   f) El núcleo de $\operatorname{Int} : \mathcal{S}_4 \to \operatorname{Aut}(\mathcal{S}_4)$ es el centro de $\mathcal{S}_4$. Usando la descomposición en producto de ciclos, sabemos que todo elemento $\sigma \in \mathcal{S}_4$, $\sigma \neq \mathrm{id}$ es de una de las formas siguientes

$$(ab), \quad (abc), \quad (ab)(cd).$$

   Es fácil de probar que para cualquiera de los σ anteriores existe una trasposición τ tal que $\tau\sigma\tau^{-1} \neq \sigma$. Luego $Z\left(\mathcal{S}_4\right) = \{\mathrm{id}\}$ y por lo tanto $\operatorname{Int} : \mathcal{S}_4 \to \operatorname{Aut}(\mathcal{S}_4)$ es inyectivo. Esto junto con la parte anterior implican que Int es un isomorfismo.

2. *a*) Consideremos $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}\right) \supset \mathbb{Q}\left(\sqrt{2}\right) \supset \mathbb{Q}$. Es fácil probar $[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}] = 2$ y $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right) = X^3 - 5$. Las raíces de $X^3 - 5$ son $w^l \sqrt[3]{5}$, $l = 0, 1, 2$. Para probar que $X^3 - 5$ es irreducible en $\mathbb{Q}\left(\sqrt{2}\right)[X]$ alcanza con probar $\sqrt[3]{5} \notin \mathbb{Q}\left(\sqrt{2}\right)$, lo cual no es difícil (pero hay que hacerlo). Luego $\left[K : \mathbb{Q}\left(\sqrt{2}\right)\right] = 3$ y por lo tanto $[K : \mathbb{Q}] = 6$.

   b) De $u = \sqrt{2} + \sqrt[3]{5}$ se tiene

$$u - \sqrt{2} = \sqrt[3]{5} \quad \Rightarrow \quad u^3 - 3\sqrt{2}u^2 + 6u - 2\sqrt{2} = 5 \quad \Rightarrow \quad u^3 + 6u - 5 = \sqrt{2}(3u + 2).$$

   Esto implica $\sqrt{2} \in \mathbb{Q}(u)$, y al ser $\sqrt[3]{5} = u - \sqrt{2}$, deducimos $\mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}\right) \subset \mathbb{Q}(u)$. El resto es fácil.

   c)

$$\operatorname{Irr}_{\mathbb{Q}}(u) = X^6 - 6X^4 - 10X^3 + 12X^2 - 60X + 17, \quad \operatorname{Irr}_{Q(\sqrt{2})}(u) = X^3 - 3\sqrt{2}X^2 + 6X - 2\sqrt{2} - 5.$$

   d) Es $\operatorname{Irr}_{\mathbb{Q}}(w) = X^2 + X + 1$, cuyas raíces raíces w y $w^2 = \overline{w}$ no son reales. Como es $K \subset \mathbb{R}$, concluimos que $\operatorname{Irr}_{\mathbb{Q}}(w) = X^2 + X + 1$ es irreducible en K y por lo tanto $[F : K] = 2$. Luego $[F : \mathbb{Q}] = 12$.

   e) $K = \mathbb{Q}\left(\sqrt{2}, \sqrt[3]{5}\right)$ y $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right) = X^3 - 5$ tiene raíces $w^l \sqrt[3]{5}$, $l = 0, 1, 2$. Como $w \notin K$, entonces $w\sqrt[3]{5} \notin K$ y por lo tanto $K/\mathbb{Q}$ no es de Galois. Por otro lado $F/\mathbb{Q}$ es de Galois por que F es el cuerpo de descomposición de $\left(X^2 - 2\right)\left(X^3 - 5\right)$.

f)
$$\mathrm{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right) = X^3 - 5, \quad \mathrm{Irr}_{\mathbb{Q}\left(\sqrt[3]{5}\right)}\left(\sqrt{2}\right) = X^2 - 2, \quad \mathrm{Irr}_{\mathbb{Q}\left(\sqrt[3]{5},\sqrt{2}\right)}(w) = X^2 + X + 1.$$

Para probar lo anterior hay que argumentar con los grados de las extensiones.

g) Usando $\mathrm{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right) = X^3 - 5$ encontramos un morfismo $\gamma : \mathbb{Q}\left(\sqrt[3]{5}\right) \to F$ tal que $\gamma\left(\sqrt[3]{5}\right) = w\sqrt[3]{5}$. Usando $\mathrm{Irr}_{\mathbb{Q}\left(\sqrt[3]{5}\right)}\left(\sqrt{2}\right) = X^2 - 2$, extendemos γ a un morfismo $\delta : \mathbb{Q}\left(\sqrt[3]{5}, \sqrt{2}\right) \to F$ tal que $\delta\left(\sqrt{2}\right) = -\sqrt{2}$. Usando $\mathrm{Irr}_{\mathbb{Q}\left(\sqrt[3]{5},\sqrt{2}\right)}(w) = X^2 + X + 1$ que tiene raíces w y w^2, extendemos δ a dos morfismos $\alpha, \beta : F \to F$ tales que $\alpha(w) = w$ y $\beta(w) = w^2$.

h) Es $|\alpha| = 6$ y $|\beta| = 2$. Además $\beta \notin \langle\alpha\rangle$, luego $\langle\alpha\rangle \cap \langle\beta\rangle = \{\mathrm{id}\}$. Esto implica $|\langle\alpha\rangle\langle\beta\rangle| = 12 = |\mathrm{Gal}(F/\mathbb{Q})|$. Luego $\langle\alpha\rangle\langle\beta\rangle = \mathrm{Gal}(F/\mathbb{Q})$.