Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois

Examen. 02/03/2022.

1. (**30 puntos.**)
   Sea G un grupo finito. Probar:
   a) Si $H < G$ es el único subgrupo de orden $|H|$, entonces H es característico[1].
   b) Si $H < G$ es un subgrupo característico, entonces $H \lhd G$.
   c) Si $N \lhd G$ y $H < N$ es un subgrupo característico de N, entonces $H \lhd G$.

2. (**30 puntos.**)
   Sea G un grupo de orden 30. Escribimos S_p a los p-subgrupos de Sylow.
   a) Probar $S_3 \lhd G$ o $S_5 \lhd G$.
   b) Probar que G contiene un subgrupo de orden 15.
   c) Probar $S_3 \lhd G$ y $S_5 \lhd G$. *Sugerencia:* recordar el ejercicio 1.

3. (**40 puntos.**)
   Sean $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ y $u = \sqrt{\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)}$.
   a) Hallar $[K : \mathbb{Q}]$ y dar una base de K como $\mathbb{Q}$-espacio.
   b) Probar que existe $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ tal que $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$, $\sigma\left(\sqrt{3}\right) = \sqrt{3}$. Deducir $\sigma^2 = \mathrm{id}$.
   c) Probar $\sigma\left(u^2\right) = \left(\left(\sqrt{2}-1\right)u\right)^2$.
   d) Probar $u \notin K$. *Sugerencia*: suponer $u \in K$ y usar la parte anterior para hallar los posibles valores de $\sigma(u)$; luego calcular $\sigma\big(\sigma(u)\big)$ y ver que se llega a una contradicción con la parte 3*b*.
   e) Sea $F = K(u)$, siendo u el de la parte anterior. Probar $[F : \mathbb{Q}] = 8$.
   f) Probar que $\sigma : K \to F$ se puede extender a dos morfismos $\sigma_\pm : F \to F$ tales que $\sigma_+(u) = \left(\sqrt{2}-1\right)u$ y $\sigma_-(u) = \left(1-\sqrt{2}\right)u$.

[1] Recordar que un subgrupo $H < G$ es *característico* si verifica $\varphi(H) = H$, para todo $\varphi \in \operatorname{Aut}(G)$.

Solución.

1. *a*) Si $\varphi \in \operatorname{Aut}(G)$, entonces $\varphi(H) < G$ y $|\varphi(H)| = |H|$; luego $\varphi(H) = H$.

   b) Es $\operatorname{int}_g(H) = H$, para todo $g \in G$; luego $H \lhd G$.

   c) Sea $g \in G$. De $N \lhd G$ deducimos $\operatorname{int}_g(N) = N$ y por lo tanto $\varphi = \operatorname{int}_g|_N \in \operatorname{Aut}(N)$. Luego vale $\operatorname{int}_g|_N(H) = H$, lo cual equivale a $\operatorname{int}_g(H) = H$. Como g es arbitrario, deducimos $H \lhd G$.

2. *a*) Si fuese $S_3 \ntriangleleft G$ y $S_5 \ntriangleleft G$, tendríamos (usando Sylow) 20 elementos de orden 3 y 24 elementos de orden 5, superando el orden de G.

   b) Si $S_3 \lhd G$ o $S_5 \lhd G$, entonces $K = S_3 S_5$ es un subgrupo; es fácil de probar $|K| = 15$.

   c) Aplicando Sylow en K es fácil probar $S_3 \lhd K$ y $S_5 \lhd K$. Luego $n_3 = n_5 = 1$ y por el ejercicio $1a$, obtenemos que S_3 y S_5 son subgrupos característicos[2] de K.

   Notar $[G : K] = 2$, luego $K \lhd G$. Como S_3 y S_5 son subgrupos característicos de H, entonces son normales en G (ejercicio 1).

3. *a*) Considerando $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset K$ se obtiene $[K : \mathbb{Q}] = 4$ y $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ es una $\mathbb{Q}$-base de K.

   b) Es $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt{2}\right) = X^2 - 2$, cuyas raices son $\pm\sqrt{2} \in K$. Luego existe $\alpha : \mathbb{Q}\left(\sqrt{2}\right) \to K$ tal que $\alpha\left(\sqrt{2}\right) = -\sqrt{2}$. El morfismo $\alpha : \mathbb{Q}\left(\sqrt{2}\right) \to K$ se extiende a $\sigma : K \to K$, usando $\operatorname{Irr}_{\mathbb{Q}(\sqrt{2})}\left(\sqrt{3}\right) = X^2 - 3$ (lo cual se obtiene probando $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$).

   c) Es

$$\sigma\left(u^2\right) = \sigma\left(\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)\right) = \left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)$$
$$\left(\left(\sqrt{2}-1\right)u\right)^2 = \left(3-2\sqrt{2}\right)\left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)$$

   Es fácil de probar que ambas expresiones coinciden.

   d) Si es $u \in K$, entonces de $\sigma\left(u^2\right) = \left(\left(\sqrt{2}-1\right)u\right)^2$, deducimos $\sigma(u) = \pm\left(\sqrt{2}-1\right)u$. Esto implica

$$\sigma(\sigma(u)) = \pm\sigma\left(\left(\sqrt{2}-1\right)u\right) = \pm\left(-\sqrt{2}-1\right)\left(\pm\left(\sqrt{2}-1\right)u\right) = -u \;\Rightarrow\; \sigma^2(u) = -u.$$

   Esto contradice $\sigma^2 = \mathrm{id}$.

   e) Como $u \notin K$, entonces $\operatorname{Irr}_K(u) = X^2 - \left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)$. Luego $[F : \mathbb{Q}] = [F : K][K : \mathbb{Q}] = 8$.

   f) Sea $f = X^2 - \left(2+\sqrt{2}\right)\left(3+\sqrt{3}\right)$, cuyas raíces son $\pm u \in F$. Es $\sigma f = X^2 - \left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)$. Notar $\left(\left(\sqrt{2}-1\right)u\right)^2 = \left(2-\sqrt{2}\right)\left(3+\sqrt{3}\right)$; luego las raíces de σf son $\pm\left(\sqrt{2}-1\right)u$. Esto implica que σ se puede extender a dos morfismos $\sigma_\pm : F \to F$ tal que $\sigma_\pm(u) = \pm\left(\sqrt{2}-1\right)u$.

[2]Otra forma es usar que $|K| = 15$ implica que H es cíclico ($5 \neq 1 \mod 3$), luego $n_3 = n_5 = 1$ y sigue como antes. Notar también que en el teórico vimos que si $n_p = 1$, entonces S_p es característico (por el ejercicio $1a$).