Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois
Primer semestre 2020

Examen. 13/08/2020.

1. (**30 puntos**) Sea $\mathcal{M}$ el grupo de movimientos del espacio y $\mathcal{M}_+$ el subgrupo de los movimientos directos. Consideremos el cubo $\mathcal{C}$. Sean $G = \{\varphi \in \mathcal{M} : \ \varphi(\mathcal{C}) = \mathcal{C}\}$ y $G_+ = G \cap \mathcal{M}_+$. Notar que G actúa naturalmente en los vértices y caras de $\mathcal{C}$, y que todo $\varphi \in G$ queda determinado por sus valores en las caras o en los vértices de $\mathcal{C}$. Se sabe que G_+ es finito y que sus elementos son rotaciones cuyos ejes pasan por el centro de $\mathcal{C}$.

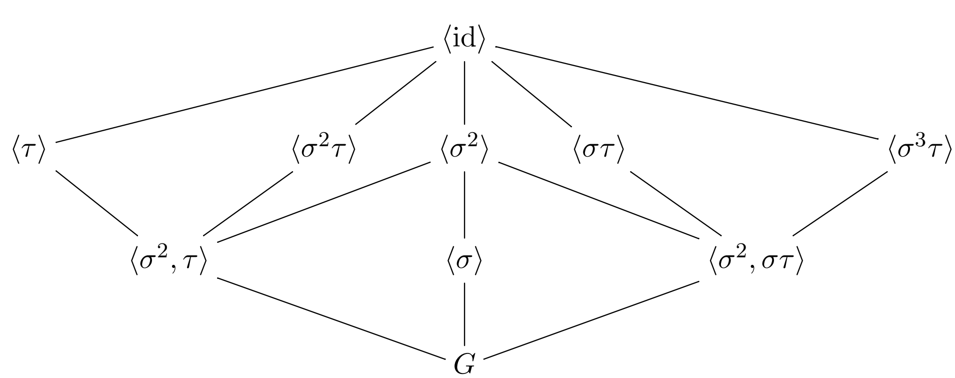
    a) Probar que la acción de G_+ en el conjunto de las caras de $\mathcal{C}$ es transitiva y determinar el estabilizador de una cara. Usar esto para deducir el orden de G_+.
    b) Notando que G_+ actúa en el conjunto de vértices opuestos de $\mathcal{C}$, deducir $G_+ \simeq \mathcal{S}_4$.
    c) Hallar el orden de G. *Sugerencia:* notar $\gamma_c \in G$, siendo γ_c la simetría central respecto a c (que es un movimiento indirecto). Recordar que siempre vale $G = G_+$ o $[G : G_+] = 2$.
    d) Sea $H = \langle \gamma_c \rangle$. Notar que γ_c conmuta con toda rotación cuyo eje contenga al centro de $\mathcal{C}$.
        1) Probar $H \lhd G$, $G_+ \lhd G$ y $G = G_+H$.
        2) Probar $G \simeq \mathcal{S}_4 \times C_2$, siendo C_2 el grupo cíclico de 2 elementos.

2. (**20 puntos**) Probar que si G es un grupo de orden 48 o 56, entonces G no es un grupo simple.

3. (**50 puntos**) Sea $f = X^4 + X^2 - 1 \in \mathbb{Q}[X]$.

    a) Estudiar la irreducibilidad de f en $\mathbb{Q}[X]$.
    b) Probar que el cuerpo de descomposición de f es $K = \mathbb{Q}(u, i)$, siendo $u = \sqrt{\frac{\sqrt{5}-1}{2}}$.
    Hallar una base de $K/\mathbb{Q}$ y escribir u^{-1} y u^{-2} en función de esa base.
    c) Determinar[1] $H = \mathrm{Gal}\big(K/\mathbb{Q}(u)\big)$ y $J = \mathrm{Gal}\big(K/\mathbb{Q}(i)\big)$. Hallar[2] todos sus elementos.
    d) Sea $G = \mathrm{Gal}(K/\mathbb{Q})$. Probar $G \simeq D_4$ (grupo diedral) y hallar todos sus elementos.
    e) Encontrar $\sigma \in G$ tal que $|\sigma| = 4$. Identificar $K^{\langle \sigma^2 \rangle}$.
    f) Hallar todas las extensiones de grado 2 de $\mathbb{Q}$ contenidas en K.

Dato: el retículo de subgrupos de $D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = \mathrm{id},\ \tau\sigma\tau = \sigma^3 \rangle$ es



[1] Por "determinar" nos referimos a identificar el grupo en la lista de los grupos de orden menor que 16.
[2] Por "hallar los elementos" nos referimos a describir sus valores en u e i.

Solución.

1. *a*) Si ρ es la rotación de ángulo $\pi/2$ cuyo eje pasa por el centro de una cara F y el centro del cubo, entonces esa rotación permuta las cuatro caras adyacentes. Haciendo lo mismo con las otras caras deducimos que la acción de G_+ en las caras es transitiva.

   Si fijamos una cara F del cubo, las rotaciones que están en G_+ y dejan invariante a F forman el grupo cíclico $\langle\rho\rangle$, siendo ρ como antes. Luego el estabilizador es $(G_+)_F = \langle\rho\rangle = C_4$.

   Como la acción de G_+ en el conjunto de las caras es transitiva y el cubo tiene 6 caras, obtenemos

$$\#\{\text{caras del cubo}\} = [G_+ : (G_+)_F] \quad \Rightarrow \quad 6 = \frac{|G_+|}{4} \quad \Rightarrow \quad |G_+| = 24.$$

   b) Sea $\mathcal{O}$ el conjunto de los pares de vértices opuestos del cubo. Como el cubo tiene 8 vértices entonces $|\mathcal{O}| = 4$. Como todo $\varphi \in G_+$ queda determinado por lo que vale en los vértices del cubo, deducimos que la acción de G_+ en $\mathcal{O}$ es fiel, luego el morfismo asociado $\Phi : G_+ \to \mathrm{Biy}(\mathcal{O})$ es inyectivo, y como ambos grupos tienen igual orden, deducimos $G_+ \simeq \mathrm{Biy}(\mathcal{O}) \simeq \mathcal{S}_4$.

   c) Por la sugerencia es $G \neq G_+$, luego $[G : G_+] = 2$. Como $|G_+| = 24$ entonces $|G| = 48$.

   d) Sea $H = \langle\gamma_c\rangle$. Notar que γ_c conmuta con toda rotación cuyo eje contenga a c.

      1) Como $[G : G_+] = 2$, entonces $G_+ \lhd G$. Es $|G_+| = 24$, $|H| = 2$ y $G_+ \cap H = \{\mathrm{id}\}$, luego tomando órdenes deducimos $G = G_+H$. Como γ_c conmuta con los elementos de G_+, entonces γ_c conmuta con todos los de G. Luego $H \subset Z(G)$ y por lo tanto $H \lhd G$.

      2) Por la parte anterior es $G = G_+H$, $G_+ \cap H = \{\mathrm{id}\}$ con $G_+ \lhd G$ y $H \lhd G$, luego $G \simeq G_+ \times H$. La última afirmación se deduce de $G_+ \simeq \mathcal{S}_4$ y $H \simeq C_2$.

2. Sea $|G| = 48 = 2^4 \times 3$. Es $n_2 = 1$ o 3. Si $n_2 = 1$ entonces $S_2 \lhd G$. Si $n_2 = 3$, entonces

$$[G : N_G(S_2)] = 3 \quad \Rightarrow \quad |G| \nmid [G : N_G(S_2)]!$$

   luego existe $\{1\} \neq K \lhd G$ tal que $K \subset N_G(S_2) \subsetneq G$.

   Sea $|G| = 56 = 2^3 \times 7$. Es $n_7 = 1$ o 8. Si $n_7 = 1$ entonces $S_7 \lhd G$. Si $n_7 = 8$, entonces en G hay $8 \times 6 = 48$ elementos de orden 7 y restan solo 8 elementos en G. Como $|S_2| = 8$, entonces necesariamente es $n_2 = 1$ y por lo tanto $S_2 \lhd G$.

3. Sea $f = X^4 + X^2 - 1 \in \mathbb{Q}[X]$.

   a) El polinomio f no tiene raíces racionales y tampoco se factoriza en producto de polinomios de grado 2 (usar el Lema de Gauss). Luego f es irreducible en $\mathbb{Q}[X]$.

   b) Las raíces de $X^2 + X - 1$ son $\frac{-1\pm\sqrt{5}}{2}$. Luego las raíces de f son $\pm u$ y $\pm iv$, siendo $u = \sqrt{\frac{\sqrt{5}-1}{2}}$ y $v = \sqrt{\frac{\sqrt{5}+1}{2}}$. Notar $uv = 1$, luego $K = \mathbb{Q}(\pm u, \pm iv) = \mathbb{Q}(u, i)$.

   Por la primer parte es $\mathrm{Irr}_{\mathbb{Q}}(u) = f$; luego $[\mathbb{Q}(u) : \mathbb{Q}] = 4$. Como $i \notin \mathbb{Q}(u) \subset \mathbb{R}$, se deduce $\mathrm{Irr}_{\mathbb{Q}(u)}(i) = X^2 + 1$, luego $[K : \mathbb{Q}(u)] = 2$ y por lo tanto $[K : \mathbb{Q}] = 8$.

   Usando lo anterior se prueba que $\{1, u, u^2, u^3\}$ es una base de $\mathbb{Q}(u)/\mathbb{Q}$ y $\{1, i\}$ es una base de $K/\mathbb{Q}(u)$. Luego $\{1, u, u^2, u^3, i, ui, u^2i, u^3i\}$ es una base de $K/\mathbb{Q}$. De $u^4 + u^2 - 1 = 0$ deducimos $u^{-1} = u^3 + u$ y $u^{-2} = u^2 + 1$.

c) Consideremos $H = \operatorname{Gal}\big(K/\mathbb{Q}(u)\big)$. Es $\operatorname{Irr}_{\mathbb{Q}(u)}(i) = X^2+1$ que tiene raíces $\pm i \in K$. Luego $H = \{\mathrm{id}, \tau\} \simeq \mathbb{Z}_2$ en que $\tau \in G$ queda determinado por $\tau(i) = -i$ y $\tau(u) = u$.

Consideremos $J = \operatorname{Gal}\big(K/\mathbb{Q}(i)\big)$. Es $[K : \mathbb{Q}(i)] = 4$, luego $\operatorname{Irr}_{\mathbb{Q}(i)}(u) = f$ que tiene raíces $\pm u, \pm iu^{-1} \in K$. Luego $J = \{\mathrm{id}, \eta_1, \eta_2, \eta_3\}$ en que $\eta_l(i) = i$, para todo l y $\eta_1(u) = -u$, $\eta_2(u) = iu^{-1}$ y $\eta_3(u) = -iu^{-1}$. En este caso es $\eta_l^2 = \mathrm{id}$, para todo l, luego $J \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

d) Sea $G = \operatorname{Gal}(K/\mathbb{Q})$. Como $K/\mathbb{Q}$ es normal, entonces es de Galois y por lo tanto $|G| = [K : \mathbb{Q}] = 8$. Las raíces de $\operatorname{Irr}_{\mathbb{Q}}(u) = f$ son $\pm u$ y $\pm iv$. Como $\pm iv \notin \mathbb{Q}(u)$ deducimos que $\mathbb{Q}(u)/\mathbb{Q}$ no es de Galois y por lo tanto $H = \operatorname{Gal}\big(K/\mathbb{Q}(u)\big)$ no es normal en G. Usando la clasificación de los grupos de orden 8, sabemos que G tiene que ser isomorfo a Q, D_4 o es abeliano. Como en los casos Q o abeliano todos los subgrupos son normales, concluimos $G \simeq D_4$.

Es fácil de probar que vale $\mathbb{Q}(u) \cap \mathbb{Q}(i) = \mathbb{Q}$, luego

$$G = HJ = \{\mathrm{id}, \eta_1, \eta_2, \eta_3, \tau, \tau\eta_1, \tau\eta_2, \tau\eta_3\}$$

Los valores en u e i son

	η_1	η_2	η_3	τ	$\tau\eta_1$	$\tau\eta_2$	$\tau\eta_3$
u	$-u$	iu^{-1}	$-iu^{-1}$	u	$-u$	$-iu^{-1}$	iu^{-1}
i	i	i	i	$-i$	$-i$	$-i$	$-i$

e) Sabemos $|\tau| = |\eta_l| = 2$, $\forall l$. En los otros vale $|\tau\eta_1| = |\tau\eta_2| = 2$ y $|\tau\eta_3| = 4$. Luego $\sigma = \tau\eta_3$.

Sabemos $u^{-1} = u^3 + u$ y $u^{-2} = u^2 + 1$. Esto implica $\sigma(u) = ui + u^3 i$, $\sigma(u^2) = ui + u^3 i$ El conjunto $\{1, u, u^2, u^3, i, ui, u^2 i, u^3 i\}$ es una base de $K/\mathbb{Q}$. Operando en esa base deducimos $K^{\langle\sigma^2\rangle} = \mathbb{Q}(u^2, i)$.

f) Observar que $\sigma \in G$ y $\tau \in H$ verifican $|\sigma| = 4$, $|\tau| = 2$ y $\tau\sigma\tau = \sigma^3$. Por la correspondencia de Galois los cuerpos E tales que $\mathbb{Q} \subset E \subset K$ y $[E : \mathbb{Q}] = 2$ se corresponden con los subgrupos de índice 2 de G, que son $\langle\sigma^2, \tau\rangle$, $\langle\sigma^2, \sigma\tau\rangle$ y $\langle\sigma\rangle$. Luego tenemos que hallar $K^{\langle\sigma^2,\tau\rangle}$, $K^{\langle\sigma^2,\sigma\tau\rangle}$ y $K^{\langle\sigma\rangle}$. Usando la tabla anterior obtenemos

	τ	σ	σ^2	$\sigma\tau$
u	u	iu^{-1}	$-u$	$-iu^{-1}$
i	$-i$	$-i$	i	i

Luego $\sigma^2 = \eta_1$ y $\sigma\tau = \eta_3$.

Es $\langle\sigma^2, \sigma\tau\rangle = \langle\eta_1, \eta_3\rangle = J = \operatorname{Gal}\big(K/\mathbb{Q}(i)\big)$. Luego $K^{\langle\sigma^2,\sigma\tau\rangle} = \mathbb{Q}(i)$.

Es $\langle\tau\rangle = H = \operatorname{Gal}\big(K/\mathbb{Q}(u)\big)$, luego $K^{\langle\tau\rangle} = \mathbb{Q}(u)$. El conjunto $\{1, u, u^2, u^3\}$ es una base de $\mathbb{Q}(u)/\mathbb{Q}$. Operando en esa base deducimos $K^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}(u^2) = \mathbb{Q}\left(\sqrt{5}\right)$.

El conjunto $\{1, u^2, i, u^2 i\}$ es una base de $K^{\langle\sigma^2\rangle}/\mathbb{Q}$. Operando en esa base deducimos $K^{\langle\sigma\rangle} = \mathbb{Q}\big((2u^2+1)i\big) = \mathbb{Q}\left(i\sqrt{5}\right)$. En conclusión obtuvimos

$$K^{\langle\sigma^2,\sigma\tau\rangle} = \mathbb{Q}(i), \quad K^{\langle\sigma^2,\tau\rangle} = \mathbb{Q}\left(\sqrt{5}\right), \quad K^{\langle\sigma\rangle} = \mathbb{Q}\left(i\sqrt{5}\right).$$