Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois
Curso 2021

Examen = Prueba 3. 10/08/2021.

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

1. Hallar $[K : \mathbb{Q}]$.
2. Probar $K = \mathbb{Q}(u)$, siendo $u = \sqrt{2} + \sqrt[3]{5}$.
3. Hallar los polinomios irreducibles de u sobre $\mathbb{Q}$ y sobre $\mathbb{Q}\left(\sqrt{2}\right)$.
4. Sea $F = K(w)$, siendo $w \in \mathbb{C}$ tal que $w^3 = 1$ y $w \neq 1$. Hallar $[F : \mathbb{Q}]$.
5. Determinar si $K/\mathbb{Q}$ y $F/\mathbb{Q}$ son extensiones de Galois.
6. 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 $\mathbb{Q}\left(\sqrt[3]{5}, \sqrt{2}\right)$.
7. Probar que existen $\alpha, \beta \in \mathrm{Gal}(F/\mathbb{Q})$ tales que
$$\alpha\left(\sqrt[3]{5}\right) = w\sqrt[3]{5}, \quad \alpha\left(\sqrt{2}\right) = -\sqrt{2}, \quad \alpha(w) = w;$$
$$\beta\left(\sqrt[3]{5}\right) = w\sqrt[3]{5}, \quad \beta\left(\sqrt{2}\right) = -\sqrt{2}, \quad \beta(w) = w^2.$$
8. Probar $\mathrm{Gal}(F/\mathbb{Q}) = \langle \alpha, \beta \rangle = \langle \alpha \rangle \langle \beta \rangle$.

La prueba vale 40 puntos, cada una de las partes anteriores vale 5 puntos.

Solución.

1. 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 $[K:\mathbb{Q}]=6$.

2. 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.

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

4. 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 $[F:\mathbb{Q}]=12$.

5. $K=\mathbb{Q}\left(\sqrt{2},\sqrt[3]{5}\right)$ 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 $\left(X^2-2\right)\left(X^3-5\right)$.

6. $$\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right)=X^3-5,\quad \operatorname{Irr}_{\mathbb{Q}\left(\sqrt[3]{5}\right)}\left(\sqrt{2}\right)=X^2-2,\quad \operatorname{Irr}_{\mathbb{Q}\left(\sqrt[3]{5},\sqrt{2}\right)}(w)=X^2+X+1.$$
Para probar lo anterior hay que argumentar con los grados de las extensiones.

7. Usando $\operatorname{Irr}_{\mathbb{Q}}\left(\sqrt[3]{5}\right)=X^3-5$ 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 $\operatorname{Irr}_{\mathbb{Q}\left(\sqrt[3]{5}\right)}\left(\sqrt{2}\right)=X^2-2$, 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 $\operatorname{Irr}_{\mathbb{Q}\left(\sqrt[3]{5},\sqrt{2}\right)}(w)=X^2+X+1$ que tiene raíces w y w^2, extendemos δ a dos morfismos $\alpha,\beta:F\to F$ tales que $\alpha(w)=w$ y $\beta(w)=w^2$.

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