Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y teoría de Galois
Curso 2021

Examen = Prueba 3. 23/07/2021.

Sean $f = X^4 - 4X^3 + 6X^2 - 4X - 2 \in \mathbb{Q}[X]$ y $F = \mathbb{Q}(u, i)$, siendo $u = \sqrt[4]{3}$.

1. Probar que f es irreducible en $\mathbb{Q}[X]$.
2. Probar que F es el cuerpo de descomposición de f.
   Sugerencia: el polinomio $X^2 - 2X + 1 + \sqrt{3}$ divide a f.
3. Hallar $[F : \mathbb{Q}]$ y $[F : [\mathbb{Q}(\sqrt{3})]$ (notar $\sqrt{3} \in \mathbb{Q}(u) \subset F$).
4. Hallar una base de F como $\mathbb{Q}(\sqrt{3})$-espacio vectorial.
5. Hallar todos los morfismos σ tal que

$$\begin{tikzcd} \mathbb{Q}(u) \arrow[rr, "\sigma"] & & F \\ & \mathbb{Q}(\sqrt{3}) \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

   Sugerencia: notar que $\mathbb{Q}(u)/\mathbb{Q}(\sqrt{3})$ es una extensión simple.

6. Probar que $F/\mathbb{Q}(\sqrt{3})$ es una extensión de Galois y hallar todos los elementos de $G = \mathrm{Gal}\left(F/\mathbb{Q}(\sqrt{3})\right)$.
7. Determinar el grupo G.
8. Hallar todos los cuerpos intermedios entre F y $\mathbb{Q}(\sqrt{3})$.

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

Solución.

1. Se aplica el criterio de Eisenstein con $p = 2$.

2. Las raíces de f son $1 \pm u$ y $1 \pm ui$ y por lo tanto su cuerpo de descomposición es $\mathbb{Q}(1 \pm u, 1 \pm ui) = \mathbb{Q}(u, i)$.

3. Considerando $\mathbb{Q} \subset \mathbb{Q}(u) \subset F$, es $[F : \mathbb{Q}(u)] = 2$ y $[\mathbb{Q}(u) : \mathbb{Q}] = 4$. Luego $[F : \mathbb{Q}] = 8$.
   Como es $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, deducimos $\left[F : [\mathbb{Q}\left(\sqrt{3}\right)\right] = 4$.

4. Considerando $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(u) \subset F$, deducimos que $\mathcal{B} = \{1,\, u,\, i,\, ui\}$ es una base de F como $\mathbb{Q}(\sqrt{3})$-espacio vectorial.

5. La extensión $\mathbb{Q}(u)/\mathbb{Q}(\sqrt{3})$ es simple: $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{3}, u) = \mathbb{Q}(\sqrt{3})(u)$. Es $\operatorname{Irr}_{\mathbb{Q}(\sqrt{3})}(u) = X^2 - \sqrt{3}$. Las raíces de $\operatorname{Irr}_{\mathbb{Q}(\sqrt{3})}(u) = X^2 - \sqrt{3}$ en $\mathbb{Q}(\sqrt{3})$ son $\pm u \in F$. Luego hay solo dos morfismos: uno es la inclusión $\mathbb{Q}(u) \hookrightarrow F$ y el otro es $\sigma : \mathbb{Q}(u) \to F$ tal que $\sigma(u) = -u$ (esto implica $\sigma\left(\sqrt{3}\right) = \sqrt{3}$).

6. La primera parte implica que F/Q es normal, luego $F/\mathbb{Q}(\sqrt{3})$ también es normal y por lo tanto es de Galois. Esto implica $\left|\operatorname{Gal}\left(F/\mathbb{Q}(\sqrt{3})\right)\right| = \left[F : \mathbb{Q}(\sqrt{3})\right] = 4$.

   Como es $F = \mathbb{Q}(u, i) = \mathbb{Q}(u)(i)$ e $\operatorname{Irr}_{\mathbb{Q}(u)}(i) = X^2 + 1$ tiene raíces $\pm i$, entonces cada uno de los morfismos de la parte anterior tiene dos extensiones, lo cual da lugar a los cuatro morfismos de G. Luego $G = \{\mathrm{id},\, \alpha,\, \beta,\, \gamma\}$, quedando estos determinados por

   $$\alpha(u) = u,\ \alpha(i) = -i; \quad \beta(u) = -u,\ \beta(i) = i; \quad \gamma(u) = -u,\ \gamma(i) = -i.$$

7. Sabemos $|G| = 4$, luego $G = C_4$ o $G \simeq C_2 \times C_2$. De la tabla anterior se deduce $\alpha^2 = \beta^2 = \mathrm{id}$, luego $G \simeq C_2 \times C_2$ (en C_4 hay solo un elemento de orden 2).

8. Los subgrupos propios de G son $\langle\alpha\rangle$, $\langle\beta\rangle$ y $\langle\gamma\rangle$. Luego los cuerpos intermedios son $F^{\langle\alpha\rangle}$, $F^{\langle\beta\rangle}$ y $F^{\langle\gamma\rangle}$. Ya vimos que $\mathbb{Q}(u)$ es un cuerpo intermedio y como es $\alpha(u) = u$, deducimos $F^{\langle\alpha\rangle} = \mathbb{Q}(u)$. También $\mathbb{Q}(ui)$ es un cuerpo intermedio e inspeccionando la tabla obtenemos $F^{\langle\gamma\rangle} = \mathbb{Q}(ui)$. Para determinar $F^{\langle\beta\rangle}$, sea $w = x + yu + zi + tui \in F$, con $x, y, z, t \in \mathbb{Q}(\sqrt{3})$. Entonces

   $$\beta(w) = w \quad \Leftrightarrow \quad x - yu + zi - tui = x + yu + zi + tui \quad \Leftrightarrow \quad y = t = 0.$$

   Luego $F^{\langle\beta\rangle} = \mathbb{Q}(\sqrt{3})(i) = \mathbb{Q}(\sqrt{3},\, i)$. En resumen, los cuerpos intermedios entre F y $\mathbb{Q}(\sqrt{3})$ son

   $$F^{\langle\alpha\rangle} = \mathbb{Q}(u), \quad F^{\langle\gamma\rangle} = \mathbb{Q}(ui), \quad F^{\langle\beta\rangle} = \mathbb{Q}(\sqrt{3},\, i).$$

   Nota: operando se obtiene $\mathbb{Q}(\sqrt{3},\, i) = \mathbb{Q}(\sqrt{3} + i)$.