Algebra III

Algunas ideas sobre como calcular el grupo de Galois

Resolvente de Galois

Sea K un cuerpo cualquiera y sea $f \in K[X]$ separable (es decir, con todas sus raices distintas) de grado $d \geqslant 1$.

$$f = \sum_{i=0}^{d} a_i X^i = a_d \prod_{i=1}^{d} (X - \alpha_i) \quad \text{con } a_d \neq 0 \text{ y los } \alpha_i \in \overline{K} \text{ distintos}$$

Sea $E = K[\alpha_1, \ldots, \alpha_d]$ el cuerpo de descomposición de f sobre K. Sea $G = \mathrm{Gal}(E/K) \subseteq \mathbb{S}_d$, donde la inclusión es la que satisace $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ para todos $\sigma \in G$ y $1 \leqslant i \leqslant d$. Construimos los siguientes dos polinomios (mónicos en X):

$$F = \prod_{\sigma \in \mathbb{S}_d} \left[X - (u_1 \alpha_{\sigma(1)} + \cdots + u_d \alpha_{\sigma(d)})\right] \in E[u_1, \ldots, u_d][X]$$

$$P = \prod_{\sigma \in G} \left[X - (u_1 \alpha_{\sigma(1)} + \cdots + u_d \alpha_{\sigma(d)})\right] \in E[u_1, \ldots, u_d][X]$$

donde $u_1, \ldots, u_d, X$ son variables.

(1) $F \in K[u_1, \ldots, u_d][X]$ y sus coeficientes son polinomios simétricos (con coeficientes enteros) en $\alpha_1, \ldots, \alpha_d$. Esto implica que los coeficientes de F son polinomios (con coeficientes enteros) en $a_0/a_d, \ldots, a_{d-1}/a_d$ y por lo tanto F puede calcularse directamente a partir de f.

(2) $P \in K[u_1, \ldots, u_d][X]$ y es irreducible.
Dem: Basta observar que $P = \mathrm{irr}(u_1\alpha_1 + \cdots + u_d\alpha_d, K(u_1, \ldots, u_d))$. □

(3) Sean $G\tau_1, \ldots, G\tau_r$ las clases a derecha de $\mathbb{S}_d/G$.

$$F = \prod_{i=1}^{r} P(u_{\tau_i^{-1}(1)}, \ldots, u_{\tau_i^{-1}(d)}, X)$$

Dem:

$$F = \prod_{i=1}^{r} \prod_{\sigma \in G} \left[X - (u_1 \alpha_{\sigma\tau_i(1)} + \cdots + u_d \alpha_{\sigma\tau_i(d)})\right] =$$

$$= \prod_{i=1}^{r} \prod_{\sigma \in G} \left[X - (u_{\tau_i^{-1}(1)} \alpha_{\sigma(1)} + \cdots + u_{\tau_i^{-1}(d)} \alpha_{\sigma(d)})\right] =$$

$$= \prod_{i=1}^{r} P(u_{\tau_i^{-1}(1)}, \ldots, u_{\tau_i^{-1}(d)}, X).$$

□

A partir de acá, llamaremos $P_i = P(u_{\tau_i^{-1}(1)}, \ldots, u_{\tau_i^{-1}(d)}, X)$ para $1 \leqslant i \leqslant d$. Notar que estos polinomios están en $K[u_1, \ldots, u_d][X]$ y son mónicos (en X) e irreducibles.

$$|G| = \deg_X(P_i) \; \forall\, i \quad \text{y} \quad r = [\mathbb{S}_d : G] = \frac{d!}{|G|}$$

Un corolario inmediato de (1), (2) y (3) es el siguiente algoritmo para calcular $|G|$.

Entrada $f \in K[X]$ separable de grado $d \geqslant 1$.

Salida $|\mathrm{Gal}(f/K)|$.

1. Calcular $F \in K[u_1, \ldots, u_d][X]$ a partir de los coeficientes de f.

2. Factorizar $F = P_1 \cdots P_r$ en $K[u_1, \ldots, u_d][X]$ utilizando un algoritmo de factorización de polinomios multivariados.

3. Devolver $|\mathrm{Gal}(f/K)| = \frac{d!}{r} = \deg_X(P_i)\ \forall\, i$.

(4) Sean $G_i = \left\{\lambda \in \mathbb{S}_d \,/\, P_i(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) \equiv P_i\right\} = \mathrm{Fix}(P_i)$ los subgrupos de $\mathbb{S}_d$ de las permutaciones que dejan fijo a P_i. Entonces $G = \tau_i G_i \tau_i^{-1}\ \forall\, 1 \leqslant i \leqslant d$.

Dem: Sea $\lambda \in \mathbb{S}_d$. Entonces

$$P_i(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) = \prod_{\sigma \in G\tau_i} \left[X - (u_{\lambda(1)}\alpha_{\sigma(1)} + \cdots + u_{\lambda(d)}\alpha_{\sigma(d)})\right] =$$

$$= \prod_{\sigma \in G\tau_i} \left[X - (u_1\alpha_{\sigma\lambda^{-1}(1)} + \cdots + u_d\alpha_{\sigma\lambda^{-1}(d)})\right] = \prod_{\sigma \in G\tau_i\lambda^{-1}} \left[X - (u_1\alpha_{\sigma(1)} + \cdots + u_d\alpha_{\sigma(d)})\right].$$

Por lo tanto $P_i(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) \equiv P_i \;\Leftrightarrow\; G\tau_i = G\tau_i\lambda^{-1} \;\Leftrightarrow\; \lambda \in \tau_i^{-1}G\tau_i$. Entonces $G_i = \tau_i^{-1}G\tau_i$ y $G = \tau_i G_i \tau_i^{-1}$. □

Esto último nos da una forma de obtener algoritmicamente G (salvo conjugación).

Entrada $f \in K[X]$ separable de grado $d \geqslant 1$.

Salida $\mathrm{Gal}(f/K) \subseteq \mathbb{S}_d$ salvo conjugación.

1. Calcular $F \in K[u_1, \ldots, u_d][X]$ a partir de los coeficientes de f.

2. Factorizar $F = P_1 \cdots P_r$ en $K[u_1, \ldots, u_d][X]$ utilizando un algoritmo de factorización de polinomios multivariados.

3. Devolver algún $G_i = \left\{\lambda \in \mathbb{S}_d \,/\, P_i(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) \equiv P_i\right\}$ para $1 \leqslant i \leqslant d$.

Grupo de Galois "módulo p"

Sea $f \in \mathbb{Z}[X]$ mónico, de grado d y separable (es decir, $\Delta(f) = \mathrm{Res}_X(f, f') \neq 0$). Sea $p \in \mathbb{N}$ un primo y supongamos que $\overline{f} \in \mathbb{F}_p$ también es separable (lo que es equivalente a $p \nmid \Delta(f)$).

$$f = (X - \alpha_1) \cdots (X - \alpha_d) \quad \text{con los } \alpha_i \in \overline{\mathbb{Q}} \text{ distintos}$$
$$\overline{f} = (X - \beta_1) \cdots (X - \beta_d) \quad \text{con los } \beta_i \in \overline{\mathbb{F}_p} \text{ distintos}$$

Sean F_f y $F_{\overline{f}}$ los polinomios del primer paso del algoritmo anterior aplicados a f y $\overline{f}$ respectivamente.

(5) $F_f \in \mathbb{Z}[u_1, \ldots, u_d][X]$
(6) $F_{\overline{f}} = \overline{F_f} \in \mathbb{F}_p[u_1, \ldots, u_d][X]$

Dem: (5) Se deduce inmediatamente de (1).
(6) Los coeficientes de F_f y $F_{\overline{f}}$ se obtienen evaluando (un mismo polinomio con coeficientes enteros) en los coeficientes de f y $\overline{f}$ respectivamente. □

Sea $P \in \mathbb{Z}[u_1, \ldots, u_d][X]$ un factor irreducible mónico (en X) de F_f (en realidad, deberiamos tomar un factor irreducible con coeficientes racionales, pero el lema de Gauss garantiza que ese factor tiene coeficientes enteros). Sea $Q \in \mathbb{F}_p[u_1, \ldots, u_d][X]$ un factor irreducible mónico (en X) de $\overline{P}$. Sean $G = \mathrm{Gal}(f/K) \subseteq \mathbb{S}_d$ y $\widehat{G} = \mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subseteq \mathbb{S}_d$.

(7) $P = \prod_{\sigma \in G\tau} \left[X - (u_1\alpha_{\sigma(1)} + \cdots + u_d\alpha_{\sigma(d)})\right]$ para algún $\tau \in \mathbb{S}_d$. Mas aún, $G = \tau \mathrm{Fix}(P)\tau^{-1}$.
(8) $Q = \prod_{\sigma \in \widehat{G}\eta} \left[X - (u_1\alpha_{\sigma(1)} + \cdots + u_d\alpha_{\sigma(d)})\right]$ para algún $\eta \in \mathbb{S}_d$. Mas aún, $\widehat{G} = \eta \mathrm{Fix}(P)\eta^{-1}$.
(9) $\mathrm{Fix}(P) = \mathrm{Fix}(\overline{P})$
Dem: (7) y (8) son consecuencia de (3) y (4).
(9) La inclusión $\mathrm{Fix}(P) \subseteq \mathrm{Fix}(\overline{P})$ es obvia. Ahora veremos que ambos conjuntos tienen el mismo cardinal. Sea $\lambda \in \mathbb{S}_d$. Supongamos que $\overline{P} = \prod_{\sigma \in A} \left[X - (u_1\beta_{\sigma(1)} + \cdots + u_d\beta_{\sigma(d)})\right]$ con $A \subseteq \mathbb{S}_d$.

$$\overline{P}(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) = \prod_{\sigma \in A} \left[X - (u_{\lambda(1)}\beta_{\sigma(1)} + \cdots + u_{\lambda(d)}\beta_{\sigma(d)})\right] =$$

$$= \prod_{\sigma \in A} \left[X - (u_1\beta_{\sigma\lambda^{-1}(1)} + \cdots + u_d\beta_{\sigma\lambda^{-1}(d)})\right] = \prod_{\sigma \in A\lambda^{-1}} \left[X - (u_1\beta_{\sigma(1)} + \cdots + u_d\beta_{\sigma(d)})\right]$$

Por lo tanto $\lambda \in \mathrm{Fix}(\overline{P}) \Leftrightarrow \overline{P}(u_{\lambda(1)}, \ldots, u_{\lambda(d)}, X) \equiv \overline{P} \Leftrightarrow A\lambda^{-1} = A$. Esto implica que $|\mathrm{Fix}(\overline{P})| \leqslant |A| = \deg_X(\overline{P}) = \deg_X(P) = |G| = |\mathrm{Fix}(P)|$. □

(10) $A = \gamma \mathrm{Fix}(\overline{P})$ para algún $\gamma \in \mathbb{S}_d$.
Dem: $\lambda \in \mathrm{Fix}(\overline{P}) \Leftrightarrow A\lambda = A$. Sea $\gamma \in A$ cualquiera. Entonces $\gamma\lambda \in A$ para todo $\lambda \in \mathrm{Fix}(\overline{P})$. Por lo tanto $\gamma\mathrm{Fix}(\overline{P}) \subseteq A$. Pero también tenemos que $|A| = |\mathrm{Fix}(\overline{P})|$. □

Ahora estamos en condiciones de anunciar y demostrar el resultado central de esta sección.

Teorema 1: Sea $f \in \mathbb{Z}[X]$ mónico separable y sea $p \in \mathbb{N}$ un primo tal que $p \nmid \Delta(f)$. Entonces $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ es isomorfo a un subgrupo de $\mathrm{Gal}(f/\mathbb{Q})$.

Dem: Como $Q|\overline{P}$, entonces $\widehat{G}\eta \subseteq A = \gamma\mathrm{Fix}(\overline{P}) = \gamma\mathrm{Fix}(P) = \gamma\tau^{-1}G\tau$. Tomando inversos, también tenemos que $\eta^{-1}\widehat{G} \subseteq \tau^{-1}G\tau\gamma^{-1}$. Multiplicando estas dos inclusiones obtenemos que $\eta^{-1}\widehat{G}\eta \subseteq \tau^{-1}G\tau$, o directamente $(\eta\tau^{-1})^{-1}\widehat{G}(\eta\tau^{-1}) \subseteq G$. □

Corolario 2: Sea $f \in \mathbb{Z}[X]$ mónico separable y sea $p \in \mathbb{N}$ un primo tal que $p \nmid \Delta(f)$. Supongamos que $\overline{f} = g_1 \cdots g_t$ con los $g_i \in \mathbb{F}_p[X]$ irreducibles de grado $n_i = \deg(g_i) \geqslant 1$. Entonces en $\mathrm{Gal}(f/\mathbb{Q}) \subseteq \mathbb{S}_d$ hay una permutación que es producto de ciclos disjuntos de longitudes $n_1, n_2, \ldots, n_t$.

Dem: El grupo $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ es generado por el morfismo de Frobenius que, visto en $\mathbb{S}_d$, es un producto de ciclos disjuntos de longitudes $n_i = \deg(g_i)$. □

Problema: ¿Qué pasa si $p \,|\, \Delta(f)$? Probar que en este caso, $\mathrm{Gal}(\overline{f}/\mathbb{F}_p)$ es isomorfo al grupo cociente entre un subgrupo $H \subseteq \mathrm{Gal}(f/\mathbb{Q})$ por un subgrupo normal $N \lhd H$.

El corolario 2, tiene una "recíproca" llamada Teorema de Chebotarev.

Teor (Chebotarev): Sea $f \in \mathbb{Z}[X]$ mónico separable de grado $d = \deg(f)$ y sea $G = \mathrm{Gal}(f/\mathbb{Q}) \subseteq \mathbb{S}_d$. Supongamos que en G hay una permutación que se escribe como producto de ciclos disjuntos

de longitudes $n_1, n_2, \ldots, n_t$ con $\sum_{i=1}^{t} n_i = d$. Entonces existen infinitos primos $p \nmid \Delta(f)$ tales que $\overline{f}$ se factoriza en $\mathbb{F}_p[X]$ como producto de polinomios de grados n_i.

Las demostraciones conocidas de este teorema son muy complicadas y ninguna es totalmente algebraica (siempre usan cosas de análisis complejo, L-series, etc.). Sin embargo yo creo tener una demostración "elemental" del siguiente caso particular.

Teorema: Sea $f = X^n - a \in \mathbb{Z}[X]$ irreducible. Entonces existen infinitos primos $p \in \mathbb{N}$ tales que $\overline{f} \in \mathbb{F}_p[X]$ es irreducible.

Dejo como problema tratar de probar el teorema anterior y de entender por que es un caso particular del teorema de Chebotarev. Por último, para terminar con esta sección les dejo el problema que motivó estas notas:

Problema (IMO 2003 - Japón): Sea $q \in \mathbb{N}$ primo. Probar que existe un primo $p \in \mathbb{N}$ tal que $p \nmid n^q - q$ para todo $n \in \mathbb{Z}$.