Reducción módulo p y teorema de Dedekind

Matías Saucedo

En este artículo vamos a ver otra herramienta que nos ayudará a calcular grupos de Galois de polinomios sin necesidad de conocer explícitamente sus raíces.
Sea $f \in \mathbb{Z}[X]$ un polinomio mónico de grado n, y sea G_f el grupo de Galois de f sobre $\mathbb{Q}$ (es decir, el grupo de Galois de la extensión $E/\mathbb{Q}$ donde E es un cuerpo de descomposición de f). Recordemos que si f es separable entonces podemos pensar a G como un subgrupo de S_n.
Para cada primo p, tenemos un morfismo canónico $\mathbb{Z}[X] \to \mathbb{F}_p[X]$; sea f_p la imagen de f por este morfismo. Notar que, como f era mónico, f_p tiene el mismo grado n. Si resulta que f_p también es separable, entonces el grupo de Galois de f_p sobre $\mathbb{F}_p$, al que llamaremos G_{f_p}, también se puede pensar como un subgrupo de S_n.

Idea.
Obtener información sobre G_f a partir de G_{f_p}.

A este segundo grupo lo entendemos muy bien: ¡es cíclico! Y está generado por (la permutación correspondiente a) el morfismo de Frobenius $x \mapsto x^p$. Llamemos β a esta permutación. ¿Cómo es β? ¿Qué estructura cíclica tiene?
Supongamos que $f_p = h_1 \cdot \ldots \cdot h_r$ con los $h_i \in \mathbb{F}_p[X]$ irreducibles. Entonces β permuta cíclicamente las raíces de cada factor. Si $d_i = \deg(h_i)$, resulta que β tiene estructura cíclica de tipo $(d_1, \ldots, d_r)$ (es decir, es producto de ciclos disjuntos de longitudes $d_1, \ldots, d_r$).
El teorema de Dedekind que probaremos en breve afirma que G_f también contiene un elemento con esa misma estructura cíclica.

Teorema 1 (Dedekind)**.**
Sea $f \in \mathbb{Z}[X]$ un polinomio mónico y separable de grado n, y sea p un número primo. Supongamos que f_p se factoriza en $\mathbb{F}_p[X]$ como $f_p = h_1 \cdot \ldots \cdot h_r$, con los h_i irreducibles y *distintos dos a dos*. Sea d_i el grado de cada polinomio h_i. Entonces G_f (pensado como subgrupo de S_n) contiene un elemento σ cuya estructura cíclica es de tipo $(d_1, \ldots, d_r)$.

Observación. Este teorema **no** pide que f sea irreducible.

Antes de meternos de lleno a la demostración del teorema, veamos un ejemplo de cómo se usa.

Ejemplo 2.
Sea $f = X^5 - 3X + 3$. Probar que $G_f = S_5$.

Solución. Como f es irreducible (Eisenstein, $p = 3$) y 5 es primo, ya sabemos que G_f contiene un 5-ciclo. Así que nos bastará probar que G_f también contiene una trasposición.
Ahora bien, $f_2 = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$, y estos factores son irreducibles sobre $\mathbb{F}_2$ pues tienen grado menor o igual que 3 y ni 0 ni 1 son raíces. Por el teorema de Dedekind, existe $\sigma = (ij)(klm) \in G_f$. Pero entonces también $\sigma^3 = (ij)$ está en G_f. Así que G_f contiene una trasposición y un 5-ciclo, lo cual implica $G_f = S_5$, como queríamos. □

Observación. Con los métodos vistos anteriormente en la materia no habríamos podido resolver este problema, ya que f tiene 4 raíces no reales en vez de 2.

Ahora sí, vamos a por la demostración del teorema. La parte más complicada es probar el siguiente lema, a partir del cual podremos deducir más o menos rápido el teorema de Dedekind:

Lema 3.

Sean f y p como en el enunciado del teorema de Dedekind. Sean $r_1, \dots, r_n$ las raíces de f, sea E un cuerpo de descomposición de f sobre $\mathbb{Q}$ y sea E_p un cuerpo de descomposición de f_p sobre $\mathbb{F}_p$. Entonces:

(i) Existe un morfismo de anillos $\psi : \mathbb{Z}[r_1, \dots, r_n] \to E_p$.

(ii) Si $\psi, \psi' : \mathbb{Z}[r_1, \dots, r_n] \to E_p$ son morfismos de anillos, entonces existe $\sigma \in Gal(E/\mathbb{Q})$ tal que $\psi' = \psi\sigma|_{\mathbb{Z}[r_1,\dots,r_n]}$.

Demostración. (i) Llamamos $D = \mathbb{Z}[r_1, \dots, r_n]$. D está generado como $\mathbb{Z}$-módulo por los monomios $r_1^{e_1} \dots r_n^{e_n}$ con $e_i \in \mathbb{N}_0$. Como cada r_i es raíz de f, r_i^k se puede escribir como combinación lineal con coeficientes en $\mathbb{Z}$ de $1, r_i, \dots, r_i^{n-1}$ para todo $k \geq n$. Entonces $\{r_1^{e_1} \dots r_n^{e_n} : 0 \leq e_i < n\}$ generan D como $\mathbb{Z}$-módulo. Por otra parte, como $D \subseteq E$, y $\text{char}(E) = 0$, D no tiene elementos de torsión.
Es decir que D es un $\mathbb{Z}$-módulo finitamente generado sin torsión. Por el teorema de estructura, D es *libre*, es decir, existe una $\mathbb{Z}$-base $\{u_1, \dots, u_m\}$ para D.
Afirmamos que $\{u_1, \dots, u_m\}$ también es una base de E como $\mathbb{Q}$-espacio vectorial. Que son linealmente independientes es fácil de ver (si hubiera una combinación lineal no trivial que da 0, multiplicando por alguna constante obtendríamos una combinación lineal no trivial con coeficientes en $\mathbb{Z}$ que da 0, absurdo). Veamos que generan.
Sea $S = \langle u_1, \dots, u_m \rangle_{\mathbb{Q}} = \mathbb{Q} \cdot u_1 \oplus \dots \oplus \mathbb{Q} \cdot u_m$. Entonces S es un subanillo de E que contiene a $\mathbb{Q}$ (verificar). Como la extensión $E/\mathbb{Q}$ es algebraica, resulta que S es un cuerpo (ver ejercicio 6, práctica 2)[1]. Y como S contiene a D, contiene a todos los r_i. Sigue que $S = E$, como queríamos.
Ahora, sea $I = pD$ (es decir, el ideal generado por p en D), y sea $\mathcal{M}$ un ideal maximal de D que contiene a I. Entonces $D/\mathcal{M}$ es un cuerpo de característica p. Más aún, si $\pi : D \to D/\mathcal{M}$ es la proyección al cociente, entonces $D/\mathcal{M} = \mathbb{F}_p[\pi(r_1), \dots, \pi(r_n)]$. Pero $\pi(r_1), \dots, \pi(r_n)$ son las raíces de $\pi(f)$, que es f_p. Sigue que $D/\mathcal{M}$ es un cuerpo de descomposición de f_p sobre $\mathbb{F}_p$, y por lo tanto existe un isomorfismo $\alpha : D/\mathcal{M} \to E_p$.
Tomando $\psi = \alpha\pi$ conseguimos lo que queríamos.
(ii) Fijamos un morfismo de anillos $\psi : D \to E_p$. Es claro que ψ manda biyectivamente las raíces de f en las raíces de f_p. Dado $\sigma \in Gal(E/\mathbb{Q})$, como σ permuta los r_i, es $\sigma(D) \subseteq D$, y entonces tiene sentido hacer la composición $\psi\sigma|_D$, que nos da un morfismo de anillos de D en E_p. Más aún, si $\sigma' \neq \sigma$ entonces $\psi\sigma'|_D \neq \psi\sigma|_D$. Luego $|Hom(D, E_p)| \geq |Gal(E/\mathbb{Q})| = [E : \mathbb{Q}] = m$.
Vamos a probar que también vale el $\leq$, de donde se deduce que los morfismos de la forma $\psi\sigma|_D$ con $\sigma \in Gal(E/\mathbb{Q})$ son **todos** los elementos de $Hom(D, E_p)$.

[1] Al menos esta es la numeración en 2017.

Supongamos que $\psi_1, \ldots, \psi_{m+1}$ son morfismos distintos en $Hom(D, E_p)$. Consideramos el sistema de ecuaciones

$$\begin{pmatrix} \psi_1(u_1) & \psi_2(u_1) & \cdots & \psi_{m+1}(u_1) \\ \psi_1(u_2) & \psi_2(u_2) & \cdots & \psi_{m+1}(u_2) \\ \vdots & \vdots & \ddots & \vdots \\ \psi_1(u_m) & \psi_2(u_m) & \cdots & \psi_{m+1}(u_m) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ x_{m+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Como hay más incógnitas que ecuaciones, el sistema tiene una solución no trivial en $(E_p)^{m+1}$, digamos que es el vector $(a_1, a_2, \ldots, a_{m+1})$. Esto significa que $a_1\psi_1 + a_2\psi_2 + \ldots + a_{m+1}\psi_{m+1}$, que es un morfismo para la estructura aditiva de D, se anula sobre todos los u_i. Como los u_i generaban D como $\mathbb{Z}$-módulo, debe ser la función idénticamente nula. Pero esto no puede ser, por el teorema de independencia lineal de caracteres. (Pensar en los ψ_i restringidos al grupo de unidades de D y cayendo en $E_p^\times$.) □

Veamos ahora cómo probar el teorema de Dedekind a partir de este lema.

Demostración. Como E_p es un cuerpo finito, la función $\beta(x) = x^p$ es un automorfismo de E_p. Luego, si $\psi \in Hom(D, E_p)$, también $\beta\psi \in Hom(D, E_p)$. Por el Lema 3, existe $\sigma \in Gal(E/\mathbb{Q})$ tal que $\beta\psi = \psi\sigma|_D$. Restringiéndonos al conjunto de raíces de f y usando que ψ es una biyección entre las raíces de f y las raíces de f_p, obtenemos la igualdad $\sigma = \psi^{-1}\beta\psi$. Esto implica que σ y β, pensados como elementos de S_n, tienen la misma estructura cíclica. ¡Listo! □

Cerraremos el artículo probando, como aplicación de este teorema, que existen polinomios en $\mathbb{Z}[X]$ con grupo de Galois S_n para cualquier n. Necesitaremos el siguiente lema.

Lema 4.
Sea G un subgrupo *transitivo* de S_n que contiene una trasposición y un $(n-1)$-ciclo. Entonces $G = S_n$.

Demostración. Sin pérdida de generalidad podemos suponer que $\sigma = (1\,2\,3\ldots n-1) \in G$, y sea $(a\,b)$ una trasposición en G. Como G es transitivo, existe $\tau \in G$ tal que $\tau(b) = n$. Entonces $\tau(a\,b)\tau^{-1} = (\tau(a)\,\tau(b)) = (\tau(a)\,n) \in G$.
Ahora, como $\tau(a) \neq n$, para todo $i = 1, 2, \ldots, n-1$ existe j tal que $\sigma^j(\tau(a)) = i$. Luego $\sigma^j(\tau(a)\,n)\sigma^{-j} = (i\,n) \in G$.
Finalmente, si $j \neq i$ entonces $(j\,n)(i\,n)(j\,n) = (i\,j) \in G$. Así que G contiene todas las trasposiciones, y por lo tanto es $G = S_n$. □

Ahora sí, el resultado prometido.

Ejemplo 5.
Probar que para todo $n \in \mathbb{N}$, existe $f \in \mathbb{Z}[X]$ irreducible de grado n tal que $G_f = S_n$.

Demostración. Suponemos $n > 2$, ya que los otros casos no son interesantes.
Sean $g \in \mathbb{F}_2[X]$ irreducible de grado n, $h \in \mathbb{F}_3[X]$ irreducible de grado $n-1$ (ambos mónicos) y sea $p > n$ un primo de la forma $4k + 3$.

Por el teorema chino del resto, podemos obtener $f \in \mathbb{Z}[X]$ tal que:

$$\begin{cases} f_2 = g \\ f_3 = X \cdot h \\ f_p = (X^2+1)(X-1)(X-2)\cdots(X-(n-2)) \end{cases}$$

Entonces:

- f es irreducible pues f_2 lo es, luego G es transitivo.
- Por Dedekind con el primo 3, G contiene un $(n-1)$-ciclo.
- X^2+1 es irreducible en $\mathbb{F}_p[X]$ pues no tiene raíces en $\mathbb{F}_p$ (-1 es un residuo cuadrático módulo p sii $p \equiv 1 \pmod 4$). Por Dedekind con el primo p, G_f contiene una trasposición.

Finalmente, por el Lema 4, $G_f = S_n$. □

Referencias

[1] Jacobson, Nathan, *Basic Algebra I*, W. H. Freeman and Company, 1985.