Raíces de la unidad y resolventes de Lagrange

Facultad de Ciencias UNAM

Introducción

En esta sección presentaremos dos resultados que serán cruciales para la demostración del teorema de Galois. Para esto, recordemos que en la sección 2.9 vimos que dada una m-raíz de un numero complejo, obtenemos el resto de sus m-raíces a través de multiplicar la raíz dada y las m-raíces de la unidad. Como las extensiones radicales involucran tomar raíces m-esimas, tiene sentido que las raíces de la unidad jueguen un rol importante en las extensiones radicales. Por eso, en esta sección estudiaremos a las raíces de la unidad para un campo arbitrario. Sin embargo, por todos los detalles y sutilezas que nacen cuando trabajamos en característica p, por el resto de esta sección (y de hecho, por el resto del curso) hacemos la siguiente convención:

Todos los campos tienen característica 0.

Recordatorios de raíces de la unidad

Antes de empezar, recordamos mas propiedades de las raíces de la unidad: Supongamos que $n \in \mathbb{Z}_{\geq 1}$ y que L es un campo con característica 0. En la sección 2.13 vimos que

- $x^n - 1$ es separable[1].
- El conjunto de las raíces de $x^n - 1$ forma un subgrupo multiplicativo de L. Mas aun, como este subgrupo es un subgrupo multiplicativo finito de un campo, entonces es cíclico[2]. Finalmente, decimos que un generador de este subgrupo es una **n-esima raíz primitiva de la unidad en L**.

Ahora bien, si ζ es una n-esima raíz primitiva de la unidad en L, entonces

- Las n distintas raíces de $x^n - 1$ son $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$.
- El campo de descomposición de $x^n - 1$ es $L(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}) = L(\zeta)$.

[1] Se demostró que $x^n - 1 \in F[x]$ y su derivada no comparten ninguna raíz si $\mathrm{ch}(F) \nmid n$ (recordemos que por el la proposición 2.13.3, esto es equivalente a que $x^n - 1$ sea separable). Por eso, si $\mathrm{ch}(F) = 0$, entonces $x^n - 1$ es separable para toda $n \in \mathbb{Z}_{\geq 1}$.

[2] c.f. Dummit, Abstract Algebra, Proposition 9.5.18.

$L(\zeta)/L$ es Galois y $\mathrm{Gal}(L(\zeta)/L)$ es abeliano

Proposición 1

Supongamos que $n \in \mathbb{Z}_{\geq 1}$ y que L es un campo con característica 0. Si ζ es una n-esima raíz primitiva de la unidad en L, entonces $L(\zeta)/L$ es Galois y $\mathrm{Gal}(L(\zeta)/L)$ es abeliano.

Demostración. Como $L(\zeta)$ es el campo de descomposición de $x^n - 1$, entonces $L(\zeta)/L$ es de Galois. Resta probar que $\mathrm{Gal}(L(\zeta)/L)$ es abeliano. Antes que nada, recordemos que como $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ es una L-base de $L(\zeta)$, entonces todo elemento de $\mathrm{Gal}(L(\zeta)/L)$ queda completamente determinado por su valor en ζ.

Ahora si, veamos que $\mathrm{Gal}(L(\zeta)/L)$ es abeliano. Supongamos que $\sigma, \tau \in \mathrm{Gal}(L(\zeta)/L)$. Por la proposición 2.18.4, $\sigma(\zeta)$ y $\tau(\zeta)$ son raíces del polinomio mínimo de ζ. En particular, también son raíces de $x^n - 1$. Pero como las raíces de $x^n - 1$ son $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, entonces

$$\sigma(\zeta) = \zeta^i \quad \text{y} \quad \tau(\zeta) = \zeta^j$$

para algunos $i, j \in \{0, 1, \ldots, n-1\}$.

En particular,

$$\sigma\tau(\zeta) = \sigma(\zeta^j) = \big(\sigma(\zeta)\big)^j = \left(\zeta^i\right)^j = \zeta^{ij}.$$

Análogamente, $\tau\sigma(\zeta) = \zeta^{ji}$ y como todo elemento de $\mathrm{Gal}(L(\zeta)/L)$ queda completamente determinados por su valor en ζ, lo anterior implica que $\sigma\tau = \tau\sigma$, es decir, $\mathrm{Gal}(L(\zeta)/L)$ es abeliano. $\square$

Una caracterización de la resolubilidad del grupo de Galois de una extensión de Galois

Proposición 2

Supongamos que L/F es una extensión de Galois. Si ζ es una m-esima raíz primitiva de la unidad, entonces las extensiones $L(\zeta)/F$ y $L(\zeta)/F(\zeta)$ son Galois y

$$\begin{aligned} \text{Gal}(L/F) \text{ es resoluble} &\iff \text{Gal}(L(\zeta)/F) \text{ es resoluble} \\ &\iff \text{Gal}(L(\zeta)/F(\zeta)) \text{ es resoluble} \end{aligned}$$

Demostración. Primero, veamos que $L(\zeta)/L$ es de Galois.

Como L/F es de Galois, entonces L es el campo de descomposición sobre F de algún polinomio $f(x) \in F[x]$. Veamos que $L(\zeta)$ es el campo de descomposición del polinomio $f(x)(x^m - 1)$ sobre F.

Para esto, recordemos que el campo de descomposición de un producto es el producto de los campos de descomposición (c.f. lema 2.10.3). Como L es el campo de descomposición de $f(x)$ sobre F y $F(\zeta)$ es el campo de descomposición de $x^m - 1$ sobre F, entonces $L \cdot F(\zeta)$ es el campo de descomposición de $f(x)(x^m - 1)$ sobre F. Para concluir, el lector podrá fácilmente verificar que $L \cdot F(\zeta) = L(\zeta)$.

Por lo tanto, $L(\zeta)$ es un campo de descomposición sobre F y en particular, $L(\zeta)/F$ es de Galois.

Usando (i) esto, (ii) las inclusiones $F \subset F(\zeta) \subset L(\zeta)$, y (ii) el corolario 2.21.10 también tenemos que $L(\zeta)/F(\zeta)$ es de Galois.

Para demostrar las equivalencias, recordemos que en el teorema 2.26.8 vimos que si G es un grupo, entonces

$$G \text{ es resoluble } \iff \exists H \lhd G \ (H \text{ y } G/H \text{ son resolubles}).$$

Ahora si, veamos que

$$\mathrm{Gal}(L/F) \text{ es resoluble } \iff \mathrm{Gal}(L(\zeta)/F) \text{ es resoluble.}$$

Considera las inclusiones $F \subset L \subset L(\zeta)$. Como $L(\zeta)/F$ y L/F son de Galois, entonces el teorema 2.23.6 implica que $\mathrm{Gal}(L(\zeta)/L)$ es un subgrupo normal de $\mathrm{Gal}(L(\zeta)/F)$ tal que

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(L(\zeta)/F)/\mathrm{Gal}(L(\zeta)/L). \tag{1}$$

Por otro lado, como $\mathrm{Gal}(L(\zeta)/L)$ es abeliano[3] y finito, entonces $\mathrm{Gal}(L(\zeta)/L)$ es resoluble (c.f. teorema 2.26.9). Juntando esto con el teorema 2.26.8 obtenemos que

$$\mathrm{Gal}(L(\zeta)/F) \text{ es resoluble } \iff \mathrm{Gal}(L(\zeta)/F)/\mathrm{Gal}(L(\zeta)/L) \text{ es resoluble.} \tag{2}$$

Finalmente, juntando (1) y (2) obtenemos lo deseado.

[3] Por la proposición 1.

Ahora, veamos que

$$\text{Gal}(L(\zeta)/F) \text{ es resoluble} \iff \text{Gal}(L(\zeta)/F(\zeta)) \text{ es resoluble}$$

Considera las inclusiones $F \subset F(\zeta) \subset L(\zeta)$. Como $L(\zeta)/F$ y $F(\zeta)/F$ son de Galois, entonces $\text{Gal}(L(\zeta)/F(\zeta)$ es un subgrupo normal de $\text{Gal}(L(\zeta)/F)$ tal que

$$\text{Gal}(F(\zeta)/F) \cong \text{Gal}(L(\zeta)/F)/\,\text{Gal}(L(\zeta)/F(\zeta))$$

Además, como $\text{Gal}(F(\zeta)/F)$ es abeliano y finito, entonces $\text{Gal}(F(\zeta)/F)$ es resoluble (c.f. teorema 2.26.9). Por otro lado, por el teorema 2.26.8 tenemos que

$$\begin{aligned} &\text{Gal}(L(\zeta)/F) \text{ es resoluble} \iff \\ &\text{Gal}(L(\zeta)/F(\zeta)) \text{ y } \text{Gal}(L(\zeta)/F)/\,\text{Gal}(L(\zeta)/F(\zeta)) \text{ son resolubles.} \end{aligned} \tag{3}$$

Pero como $\text{Gal}(F(\zeta)/F) \cong \text{Gal}(L(\zeta)/F)/\,\text{Gal}(L(\zeta)/F(\zeta))$ es abeliano[4] y finito, entonces $\text{Gal}(F(\zeta)/F) \cong \text{Gal}(L(\zeta)/F)/\,\text{Gal}(L(\zeta)/F(\zeta))$ es resoluble (c.f. teorema 2.26.9). Por lo tanto, (3) se convierte en

$$\text{Gal}(L(\zeta)/F) \text{ es resoluble} \iff \text{Gal}(L(\zeta)/F(\zeta)) \text{ es resoluble.}$$

□

[4] También por la proposición 1

Los resolventes de Lagrange

Lema 3

Supongamos que M/K es una extensión de Galois con $\mathrm{Gal}(M/K) \cong \mathbb{Z}_p$ para algún $p \in \mathbb{Z}_{\geq 1}$ primo. Si K contiene una p-esima raíz primitiva de la unidad, digamos ζ, entonces existe $\alpha \in M$ tal que $M = K(\alpha)$ y $\alpha^p \in K$.

Demostración. Por hipotesis, $\mathrm{Gal}(M/K)$ es ciclico de orden p. Sea $\sigma \in \mathrm{Gal}(M/K)$ un generador, y supongamos que $\beta \in M/K$ es arbitrario y fijo. Para cada $i = 0, 1, \ldots, p-1$ definimos el *resolvente de Lagrange* por

$$\alpha_i = \beta + \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta).$$

Aplicando σ a ambos lados de la ecuación y multiplicando por σ^{-i} obtenemos

$$\zeta^{-i}\sigma(\alpha_i) = \zeta^{-i}\sigma(\beta) + \zeta^{-2i}\sigma^2(\beta) + \cdots + \zeta^{-i(p-1)}\sigma^{p-1}(\beta) + \zeta^{-ip}\sigma^p(\beta).$$

Como $\zeta^p = 1$ y $\sigma^p = \mathrm{id}$, el ultimo sumando del lado derecho de la ecuación anterior se simplifica a β y por lo tanto, la ecuación anterior se convierte en $\zeta^{-i}\sigma(\alpha_i) = \alpha_i$ o equivalentemente,

$$\sigma(\alpha_i) = \zeta^i \alpha_i.$$

Mas aun, como $\zeta \in K$ y $\zeta^p = 1$, la ecuación $\sigma(\alpha_i) = \zeta^i \alpha_i$ implica que

$$\sigma(\alpha_i^p) = \alpha_i^p.$$

Es decir, σ fija a α_i^p. Pero σ es generador de $\mathrm{Gal}(M/K)$ y por lo tanto, $\mathrm{Gal}(M/K)$ fija a α_i^p. En particular, α_i^p pertenece al campo fijo de $\mathrm{Gal}(M/K)$, pero como M/K es de Galois, este campo fijo es precisamente K. En resumen,

$$\alpha_i^p \in K \text{ para toda } i \in \{0, 1, \ldots, p-1\}.$$

Por otro lado, notemos que si ponemos $i = 0$ en la ecuación $\sigma(\alpha_i) = \zeta^i \alpha_i$, obtenemos $\sigma(\alpha_0) = \alpha_0$. Esto implica (a través de un argumento análogo al de "$\alpha_i^p \in K$") que

$$\alpha_0 \in K.$$

En lo que sigue, demostraremos que existe una $i \in \{1, \ldots, p-1\}$ tal que $\alpha_i \neq 0$. Esto sera útil porque veremos que $\alpha = \alpha_i$ cumplirá lo deseado. Sin embargo, para demostrar esto, necesitamos antes una igualdad.

Afirmación. $1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-i(p-1)} = 0$ para toda $i \in \{1, \ldots, p-1\}$.

Supongamos lo contrario y notemos que para toda $i \in \{1, \ldots, p-1\}$ tenemos

$$\begin{aligned}
\zeta^{-i}(1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-i(p-1)}) &= \\
\zeta^{-i} + \zeta^{-i-i} + \zeta^{-2i-i} + \cdots + \zeta^{-i(p-2)-i} + \zeta^{-i(p-1)-i} &= \\
\zeta^{-i} + \zeta^{-2i} + \zeta^{-3i} + \cdots + \zeta^{-ip+2i-i} + \zeta^{-ip+i-i} &= \\
\zeta^{-i} + \zeta^{-2i} + \zeta^{-3i} + \cdots + \zeta^{-ip+i} + \zeta^{-ip} &= \\
1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-i(p-1)} &
\end{aligned}$$

Ahora bien, como $1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-i(p-1)} \neq 0$, podemos dividir en la igualdad anterior para obtener que $\zeta^{-i} = 1$. Lo cual contradice el hecho de que ζ es una raiz *primitiva* de la unidad.

Fin de afirmación.

Ahora si, estamos listos para demostrar que existe una $i \in \{1, \ldots, p-1\}$ tal que $\alpha_i \neq 0$.

Afirmación. Existe una $i \in \{1, \ldots, p-1\}$ tal que $\alpha_i \neq 0$.

De lo contrario, tendríamos la primera de las siguientes igualdades

$$\begin{aligned}
\alpha_0 &= \alpha_0 + \alpha_1 + \cdots + \alpha_{p-1} \\
&= \left(\beta + \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{p-1}(\beta)\right) + \\
&\quad \left(\beta + \zeta^{-1}\sigma(\beta) + \zeta^{-2}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)}\sigma^{p-1}(\beta)\right) + \\
&\quad \left(\beta + \zeta^{-2}\sigma(\beta) + \zeta^{-4}\sigma^2(\beta) + \cdots + \zeta^{-2(p-1)}\sigma^{p-1}(\beta)\right) + \cdots + \\
&\quad \left(\beta + \zeta^{-(p-1)}\sigma(\beta) + \zeta^{-2(p-1)}\sigma^2(\beta) + \cdots + \zeta^{-(p-1)(p-1)}\sigma^{p-1}(\beta)\right) \\
&= p\beta + \left(1 + \zeta^{-1} + \zeta^{-2} + \cdots + \zeta^{-(p-1)}\right)\sigma(\beta) + \\
&\quad \left(1 + \zeta^{-2} + \zeta^{-4} + \cdots + \zeta^{-2(p-1)}\right)\sigma^2(\beta) + \cdots + \\
&\quad \left(1 + \zeta^{-(p-1)} + \zeta^{-2(p-1)} + \cdots + \zeta^{-(p-1)(p-1)}\right)\sigma^{(p-1)}(\beta)
\end{aligned}$$

Pero como $1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-i(p-1)} = 0$ para toda $i \in \{1, \ldots, p-1\}$, entonces la ecuación anterior se convierte en $\alpha_0 = p\beta$. Sin embargo, esto contradice $\alpha_0 \in K$ y $\beta \notin K$.

Fin de afirmación.

Por lo anterior, existe una $i \in \{1, \ldots, p-1\}$ tal que $\alpha_i \neq 0$. En particular, como i esta entre 1 y $p-1$, entonces $\zeta^i \neq 1$ y por lo tanto,

$$\sigma(\alpha_i) = \zeta^i \alpha_i \neq \alpha_i.$$

Donde la primera igualdad la vimos al inicio de la demostración. En particular, α_i no esta en el campo fijo de $\mathrm{Gal}(M/K)$ y como M/K es de Galois, esto es lo mismo a decir que $\alpha_i \notin K$. Ahora bien, considera las igualdades

$$[M : K(\alpha_i)][K(\alpha_i) : K] = [M : K] = |\operatorname{Gal}(M/K)| = |\mathbb{Z}_p| = p.$$

Como $\alpha_i \notin K$, entonces $[K(\alpha_i) : K] \neq 1$ y por lo tanto, la ecuación anterior implica[5] que $[M : K(\alpha_i)] = 1$ o equivalentemente, $M = K(\alpha_i)$.

Finalmente, recordemos que ya también habíamos visto que $\alpha_i^p \in K$ y por lo tanto, $\alpha = \alpha_i$ cumple lo deseado. □

[5] Recuerda que p es primo.