Extensiones radicales y resolubles

Facultad de Ciencias UNAM

Introducción

Antes de empezar, recordemos que en la proposición 2.6.7 vimos el siguiente resultado: Supongamos que F es un campo con $\mathrm{ch}(F) \neq 2$ y sea

$$p(x) = x^2 + bx + c \in F[x].$$

Entonces las raíces de $p(x)$ son

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

donde $\sqrt{b^2 - 4c} \in K$ es una raíz del polinomio $x^2 - (b^2 - 4c)$.

En otras palabras, lo anterior nos dice que dado un polinomio de grado 2 con coeficientes en un campo F con característica $\neq 2$ podemos dar una expresión algebraica en F de sus raíces. Cuando decimos expresión algebraica en F, nos referimos a un elemento que es formado a traves de elementos de F usando suma, resta, multiplicación, división, y raíces n-esimas. Por ejemplo, algunos expresiones algebraicas en $\mathbb{Q}$ son

$$\sqrt{2} + \sqrt{3}, \quad \sqrt{2 + \sqrt[3]{2}}, \quad \text{y} \quad \sqrt[7]{12 + 7i} = \sqrt[7]{12 + 7\sqrt{-1}}.$$

En esta sección definiremos y estudiaremos a un tipo de extensión cuyos elementos son precisamente aquellos que pueden ser escritos como expresiones algebraicas en el campo chico de la extensión.

La razón por la que nos interesa hacer esto es la siguiente: el objetivo del resto del curso es demostrar que no existe un análogo de la proposición 2.6.7 para polinomios de grado ≥ 5. En otras palabras, que no existe un análogo de la formula chicharronera para ecuaciones de grado ≥ 5. Este resultado se conoce como el *teorema de Abel-Ruffini*.

Cabe recalcar que también demostraremos que si existen análogos de la formula chicharronera para ecuaciones de grado 3 y 4, pero no las presentaremos explícitamente. Al lector interesado lo invitamos a googlear "formulas de Cardano" y "formulas de Ferrari".

Con esto en mente, procedemos a dar la definición mencionada anteriormente.

Extensiones radicales

Definición

Supongamos que F/L es una extensión de campos. Decimos que L/F es **radical** si existen $F_0, F_1, \ldots, F_n$ subcampos de L tales que

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L \quad \text{y}$$
$$\forall i \in \{1, \ldots, n\}\ \exists \gamma_i \in F_i \left(F_i = F_{i-1}(\gamma_i) \text{ y } \gamma_i^{m_i} \in F_{i-1} \text{ para alguna } m_i \in \mathbb{Z}_{\geq 0}\right).$$

Notemos que de esta manera (y con esta notación),

$$L = F_{n-1}(\gamma_n) = \left(F_{n-2}(\gamma_{n-1})\right)(\gamma_n) = F_{n-2}(\gamma_{n-1}, \gamma_n) = \cdots = F(\gamma_1, \ldots, \gamma_n).$$

Por otro lado, también notemos que si denotamos $b_i := \gamma_i^{m_i} \in F_{i-1}$, entonces podemos escribir $\gamma_i = \sqrt[m_i]{\gamma_i}$, de manera que

$$F_i = F_{i-1}(\sqrt[m_i]{\gamma_i}), \quad b_i \in F_{i-1}.$$

Finalmente, el lector podrá fácilmente verificar que si usamos la notación de la introducción, entonces las raíces de $x^2 + bx + c$ pertenecen a una extensión radical: $F(\sqrt{b^2 - 4c})/F$.

Comentario

Supongamos que F es un campo. Es muy importante que el lector se *convenza* de que los elementos de una extensión radical de F son expresiones algebraicas en F (en el sentido mencionado en la introducción). Para esto, es útil observar

a. que la definición nos permite tomar raíces n-esimas de elementos formados con raíces m-esimas y

b. que (usando la notación de la definición) existen $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0}$ t.q.

$$\left\{ \gamma_1^{k_1} \cdots \gamma_n^{k_n} \mid k_i \in \{0, \ldots, n_i - 1\} \right\}$$

es una F-base de $L = F(\gamma_1, \ldots, \gamma_n)$.

Una consecuencia inmediata de esto es que las raíces de un polinomio con coeficientes en F pertenecen a una extensión radical de F si y solo si podemos dar una expresión algebraica de las raíces del polinomio. Con esto en mente, introducimos otra definición esencial.

Extensiones resolubles

Definición

Supongamos que L/F es una extensión de campos. Decimos que L/F es **resoluble por radicales** (o simplemente **resoluble**) si existe una extensión M/L tal que M/F es radical.

En la diapositiva anterior mencionamos que las raíces de un polinomio $f(x) \in F[x]$ pertenecen a una extensión radical de F si y solo si podemos dar una expresión algebraica de las raíces de $f(x)$.

Ahora bien, supongamos que K es un campo de descomposición de $f(x) \in F[x]$. Si K/F es resoluble, lo anterior implica que todas las raíces de $f(x)$ son expresiones algebraicas de F. *Esto* es la razón por la que nos interesan las extensiones radicales y las extensiones resolubles (recuerda que el objetivo del resto del curso es demostrar el teorema de Abel-Ruffini).

$\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es una extensión radical

En lo que sigue, veremos que $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es una extensión radical. Usando la notación de la definición de extensión radical, definimos

$$\gamma_1 = \sqrt{2}, \;\; m_1 = 2; \;\; \gamma_2 = \sqrt{2+\sqrt{2}}, \;\; m_2 = 2$$

Entonces

$$\mathbb{Q} \subset \mathbb{Q}(\gamma_1) = \underbrace{\mathbb{Q}(\sqrt{2})}_{F_1} \subset \mathbb{Q}(\sqrt{2})(\gamma_2) = \underbrace{\mathbb{Q}(\sqrt{2})\left(\sqrt{2+\sqrt{2}}\right)}_{F_2},$$

$$\gamma_1^2 = (\sqrt{2})^2 = 2 \in \mathbb{Q}, \quad \text{y} \quad \gamma_2^2 = \left(\sqrt{2+\sqrt{2}}\right)^2 = 2+\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\gamma_1).$$

Finalmente, como

$$\mathbb{Q}(\sqrt{2})\left(\sqrt{2+\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right),$$

entonces lo anterior demuestra que $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ es una extensión radical.

Propiedades básicas de extensiones radicales

Lema 1

1. Si L/F y M/L son radicales, entonces M/F es radical.
2. Si K_1 y K_2 son campos intermedios de L/F y K_1/F es radical, entonces K_1K_2/K_2 es radical.
3. Si K_1 y K_2 son campos intermedios de L/F tales que K_1/F y K_2/F son radicales, entonces K_1K_2/F es radical.

Demostración.

1. Supongamos que L/F y M/L son radicales. Si "pegamos" la sucesión de L/F con la sucesión de M/L, obtendremos una sucesión que demuestre que M/F es radical. Dejamos los detalles al lector.
2. Supongamos que K_1 y K_2 son campos intermedios de L/F y que K_1/F es radical. Entonces existen $F_0, F_1, \ldots, F_n$ subcampos de K_1 tales que

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = K_1 \quad \text{y}$$
$$\forall i \in \{1, \ldots, n\}\ \exists \gamma_i \in F_i \left(F_i = F_{i-1}(\gamma_i) \text{ y } \gamma_i^{m_i} \in F_{i-1} \text{ p.a. } m_i \in \mathbb{Z}_{\geq 0}\right).$$

Para ver que K_1K_2/K_2 es radical, considera

$$F'_0 \coloneqq K_2, \quad F'_1 \coloneqq F'_0(\gamma_1), \quad \ldots, \quad F'_n \coloneqq F'_{n-1}(\gamma_n).$$

El lector podrá fácilmente verificar que si demostramos (i) que $F'_n = K_1K_2$ y (ii) que para toda $i \in \{1, \ldots, n\}$ existe $M_i \in \mathbb{Z}_{\geq 0}$ tal que $\gamma_i^{M_i} \in F'_{i-1}$, entonces obtendremos lo deseado.

Empecemos por ver que $F'_n = K_1K_2$. Antes que nada, recordemos que por la observacion después de la definición de extensión radical, tenemos que

$$K_1 = F(\gamma_1, \ldots, \gamma_n)$$

y (por las mismas razones) también tenemos que

$$F'_n = F'_{n-1}(\gamma_n) = \left(F'_{n-2}(\gamma_{n-1})\right)(\gamma_n) = F'_{n-2}(\gamma_{n-1}, \gamma_n) = \cdots = F'_0(\gamma_1, \ldots, \gamma_n) = K_2(\gamma_1, \ldots, \gamma_n)$$

Por lo tanto, para ver que $F'_n = K_1K_2$, basta demostrar que

$$K_2(\gamma_1, \ldots, \gamma_n) = F(\gamma_1, \ldots, \gamma_n)K_2.$$

Sin embargo, esto es muy sencillo y se lo dejamos al lector.

Finalmente, veamos que $\gamma_i^{m_i} \in F'_{i-1}$ para toda $i \in \{1, \ldots, n\}$.

Para esto, demostraremos por inducción que $F_i \subset F'_i$ para toda $i \in \{0, 1, \ldots, n\}$. El paso base $i = 0$ es trivial porque $F_0 = F \subset K_2 = F'_0$. Por eso, supongamos que $i > 0$ y supongamos que $F_{i-1} \subset F'_{i-1}$. El lector podrá fácilmente verificar que esto implica que $F_{i-1}(\gamma_i) \subset F'_{i-1}(\gamma_i)$. Pero (por definición) podemos reescribir la inclusión anterior como $F_i \subset F'_i$. Como $\gamma_i^{m_i} \in F_i$, lo anterior implica lo deseado.

Esto concluye la demostración de (2).

3. Supongamos que K_1 y K_2 son campos intermedios de L/F tales que K_1/F y K_2/F son radicales. Queremos ver que K_1K_2/F es radical. Por el inciso anterior las hipótesis implican que, K_1K_2/K_2 es radical. Juntando esto con el hecho de que K_2/F es radical y el primer inciso, obtenemos que K_1K_2/F también es radical.

□

$\sigma(F(\gamma)) = (\sigma F)(\sigma\gamma)$

Lema 2

Supongamos que F, L, M son campos tales que $F \subset L \subset M$. Si $\sigma \in \mathrm{Gal}(M/F)$ y $\gamma \in M$, entonces $\sigma(F(\gamma)) = (\sigma F)(\sigma\gamma)$.

En palabras, la imagen directa bajo σ de $F(\gamma)$ es el subcampo mas chico de M que contiene a σF y a $\sigma\gamma$.

Demostración.

$\supset$) Como $\sigma(F(\gamma)) = \{\sigma(x) \mid x \in F(\gamma)\}$, entonces $\sigma(F(\gamma))$ es un subcampo que contiene a σF y a $\sigma\gamma$. Usando esto y la definición de $(\sigma F)(\sigma\gamma)$ obtenemos lo deseado.

$\subset$) Supongamos que S es un subcampo de M que contiene a σF y a $\sigma\gamma$. Queremos ver que $\sigma(F(\gamma)) \subset S$. Para esto, recordemos que si $n = \deg_F \gamma$, entonces $\{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ es una F-base de $F(\gamma)$. Usando (i) esto, (ii) la definición de $\sigma(F(\gamma))$, y (iii) la hipótesis de que S contiene a σF y a $\sigma\gamma$, obtenemos lo deseado.

$\square$

L/F radical $\Longrightarrow$ $\sigma L/F$ radical

Lema 3

Supongamos que F, L, M son campos tales que $F \subset L \subset M$ y M/F es una extensión finita. Si $\sigma \in \mathrm{Gal}(M/F)$ y L/F es radical, entonces $\sigma L/F$ también es radical.

Demostración. Como L/F es radical, entonces existen $F_0, F_1, \ldots, F_n$ subcampos de L tales que

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L \quad \text{y}$$
$$\forall i \in \{1, \ldots, n\}\ \exists \gamma_i \in F_i \left(F_i = F_{i-1}(\gamma_i) \text{ y } \gamma_i^{m_i} \in F_{i-1} \text{ para alguna } m_i \in \mathbb{Z}_{\geq 0}\right).$$

Para ver que $\sigma L/F$ es radical, considera

$$F = F_0 \subset \sigma F_1 \subset \cdots \subset \sigma F_{n-1} \subset \sigma F_n = \sigma L.$$

Queremos ver que para toda $i \in \{1, \ldots, n\}$, existe $\delta_i \in \sigma F_i$ tal que $\sigma F_i = (\sigma F_{i-1})(\delta_i)$ y $\delta_i^{M_i} \in \sigma F_{i-1}$ para alguna $M_i \in \mathbb{Z}_{\geq 0}$.

Veamos que $\delta_i := \sigma\gamma_i$ y $M_i = m_i$ cumplen lo deseado.

Primero veamos que si $\delta_i := \sigma\gamma_i$, entonces $\sigma F_i = (\sigma F_{i-1})(\delta_i)$. Desarrollando directamente, obtenemos

$$\sigma F_i = \sigma\left(F_{i-1}(\gamma_i)\right) = (\sigma F_{i-1})(\sigma\gamma_i) = (\sigma F_{i-1})(\delta_i)$$

donde la segunda igualdad se cumple por el lema anterior.

Finalmente, veamos que si $M_i := m_i$, entonces $\delta_i^{M_i} \in F_{i-1}$. De nuevo desarrollando directamente, obtenemos

$$\delta_i^{M_i} = (\sigma\gamma_i)^{m_i} = \sigma(\gamma_i^{m_i}) \in \sigma F_{i-1}$$

donde la pertenencia se cumple porque (por hipótesis) $\gamma_i^{m_i} \in F_{i-1}$.

Esto concluye la demostración de que $\sigma L/F$ es radical. $\square$

La cerradura de Galois de una extensión separable y radical es radical

Proposición 4

Si una extensión L/F es separable y radical, entonces su cerradura de Galois también es radical.

Demostración. Antes que nada, notemos que como L/F es radical, en particular es finita y por lo tanto, L/F es finita separable. Esto nos permite garantizar la existencia de una cerradura de Galois de L/F, digamos M (c.f. corolario 2.22.2).

Para ver que M/F es radical, recuerda que

- L/F radical $\implies$ $\sigma L/F$ radical p.t. $\sigma \in \mathrm{Gal}(M/F)$ (c.f. lema 3),
- si K_1 y K_2 son campos intermedios de L/F tales que K_1/F y K_2/F son radicales, entonces K_1K_2/F es radical (c.f. lema 1),
- si $\mathrm{Gal}(M/F) = \{\sigma_1, \ldots, \sigma_n\}$, entonces $(\sigma_1 L)(\sigma_2 L)\cdots(\sigma_n L)$ es la cerradura de Galois de L/F (c.f. proposición 2.23.8).

Usando esto, el lector podrá fácilmente verificar que tenemos lo deseado. $\square$

Si K/F es radical, $\phi(K)/\phi(L)$ también

El siguiente resultado sera ocupado para poder entender porque el enunciado formal de Abel-Ruffini coincide con nuestra intuición.

Lema 5

Supongamos que F, K, L, M son campos, que $F \subset K \subset L$, y que $\phi : L \to M$ es un homomorfismo de campos. Si K/F es radical, entonces $\phi(K)/\phi(F)$ también es radical.

Demostración. Como K/F es radical, existen $F_0, F_1, \ldots, F_n$ subcampos de K tales que

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = K \quad \text{y}$$
$$\forall i \in \{1, \ldots, n\}\ \exists \gamma_i \in F_i \left(F_i = F_{i-1}(\gamma_i) \text{ y } \gamma_i^{m_i} \in F_{i-1} \text{ para alguna } m_i \in \mathbb{Z}_{\geq 0}\right).$$

Usando esto, el lector podrá fácilmente verificar que

$$\phi(F) = \phi(F_0) \subset \phi(F_1) \subset \cdots \subset \phi(F_{n-1}) \subset \phi(F_n) = \phi(K) \quad \text{y}$$
$$\forall i \in \{1, \ldots, n\} \left(\phi(F_i) = \phi(F_{i-1}) \left((\phi(\gamma_i)\right) \text{ y } \left(\phi(\gamma_i)\right)^{m_i} \in \phi(F_{i-1})\right).$$

Esto demuestra que $\phi(K)/\phi(F)$ es radical, como deseábamos. $\square$

La cerradura de Galois de una extensión finita resoluble de característica 0 es resoluble

Corolario 6

Supongamos que L/F es una extensión finita de característica 0. Si L/F es resoluble, entonces su cerradura de Galois también es resoluble.

Demostración. Como L/F es resoluble, entonces existe una extensión L'/L tal que L'/F es radical. Mas aun, como L'/F es finita[1] separable[2], entonces existe la cerradura de Galois de L'/F, digamos M. Como L'/F es radical, la proposición 4 implica que M/F es también es radical.

Por otro lado, considera las inclusiones $F \subset L \subset M$. Como M/F es de Galois, entonces M contiene a la cerradura de Galois de L/F (por definición de cerradura de Galois). Juntando esto con el hecho de que M/F es radical, obtenemos lo deseado. □

[1] Por hipótesis.

[2] Recuerda (i) que en esta sección todos los campos tienen característica 0 y (ii) que en campos con característica 0 tenemos que "polinomio irreducible $\Longrightarrow$ polinomio separable".