Extensiones ciclotómicas y teoría de Kummer

Mariano Suárez-Alvarez

27 de agosto, 2011

§1. El cuerpo $\mathbb{Q}(\omega)$ con ω una raíz de la unidad

Sea $\omega \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad y sea $\mu_n = \{\omega^i : 0 \leq i < n\}$.

Proposición 1.1. *La extensión $\mathbb{Q}(\omega)/\mathbb{Q}$ es normal.*

Demostración. El conjunto μ_n tiene exactamente n elementos. Es inmediato que todos ellos son raíces n-ésimas de la unidad, así que el polinomio $f = X^n - 1$ se descompone en $\mathbb{Q}(\omega)$. Como $\mathbb{Q}(\omega)$ está evidentemente generado por las raíces de f, se trata de un cuerpo de descomposición de f. Esto implica [5, Theorem V.3.3] que es una extensión normal de $\mathbb{Q}$. □

Sea $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ el grupo de Galois de la extensión. Si $\sigma \in G$, entonces $\sigma(\omega)$ está en μ_n, así que existe un $i \in \mathbb{Z}_n$, bien determinado, tal que $\sigma(\omega) = \omega^i$. Más aún, el elemento i es *inversible* en $\mathbb{Z}_n$: si no fuese ese el caso existiría $j \in \mathbb{Z}_n$ tal que $ij \equiv 0 \bmod n$ y, en consecuencia, $\sigma(\omega^j) = \omega^{ij} = 1$: esto es imposible ya que $\omega^j \neq 1$. De esta forma vemos que hay una función $\iota : G \to \mathbb{Z}_n^\times$ determinada por la condición de que

$$\sigma(\omega) = \omega^{\iota(\sigma)} \text{ para todo } \sigma \in G.$$

Si σ, $\tau \in G$, entonces $(\sigma\tau)(\omega) = \sigma(\tau(\omega)) = \sigma(\omega^{\iota(\tau)}) = \omega^{\iota(\sigma)\iota(\tau)}$; esto nos dice que ι es un morfismo de grupos. Además, como ω genera la extensión $\mathbb{Q}(\omega)/\mathbb{Q}$, un elemento de G queda determinado por su acción sobre ω y entonces la función ι es inyectiva. En particular, $|G| \leq |\mathbb{Z}_n^\times| = \phi(n)$.

Proposición 1.2. *El polinomio minimal de ω sobre $\mathbb{Q}$ tiene coeficientes enteros y grado $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$. El morfismo $\iota : G \to \mathbb{Z}_n^\times$ es un isomorfismo de grupos.*

Compilado: 14 de mayo de 2015

Demostración. Sea $f(X) \in \mathbb{Q}[X]$ el polinomio minimal de ω sobre $\mathbb{Q}$, que es irreducible. Como ω es una raíz n-ésima de la unidad, es raíz de $X^n - 1$ y entonces existe $g \in \mathbb{Q}[X]$ tal que $X^n - 1 = f(X)g(X)$; es claro que $g(X)$ es mónico. El lema de Gauss[1] implica que $f(X)$, $g(X) \in \mathbb{Z}[X]$.

Mostremos que

> *si p es un numero primo tal que $p \nmid n$ y λ es una raíz de $f(X)$, entonces también $f(\lambda^p) = 0$.* (1)

Supongamos que no es ese el caso, de manera que $f(\lambda^p) \neq 0$. Debe ser $g(\lambda^p) = 0$ y, en consecuencia, λ es raíz de $g(X^p)$: la elección de $f(X)$ implica entonces que existe $h(X) \in \mathbb{Z}[X]$ tal que $g(X^p) = f(X)h(X)$. Si denotamos $\bar{u}(X)$ a la imagen de un polinomio $u(X) \in \mathbb{Z}[X]$ por el morfismo evidente $\mathbb{Z}[X] \to \mathbb{Z}_p[X]$, esta igualdad implica que $\bar{g}(X)^p = \bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$ en $\mathbb{Z}_p[X]$. Se sigue de esto que $\bar{f}(X)$ y $\bar{g}(X)$ no son coprimos en $\mathbb{Z}_p[X]$ y $X^n - \bar{1} = \bar{f}(X)\bar{g}(X)$ tiene factores irreducibles repetidos: esto es absurdo, porque $X^n - \bar{1}$ y su derivada son elementos coprimos en $\mathbb{Z}_p[X]$.

Sea ahora $i \in \mathbb{Z}_n^\times$. Existen números primos $p_1, \ldots, p_k$, todos coprimos con n pero no necesariamente distintos, tales que $i = p_1 \cdots p_k$. Usando (1), vemos inductivamente que para cada $s \in \{1, \ldots, k\}$ es $f(\omega^{p_1 \cdots p_s}) = 0$ así que, en particular, $f(\omega^i) = 0$.

Como ω es una raíz n-ésima primitiva, esto nos dice que f tiene al menos $\phi(n)$ raíces distintas y, entonces, que

$$\phi(n) \leq \deg f = [\mathbb{Q}(\omega) : \mathbb{Q}] = |G| \leq |\mathbb{Z}_n^\times| = \phi(n).$$

Esto prueba el que f y la extensión $\mathbb{Q}(\omega)/\mathbb{Q}$ tienen grado $\phi(n)$ y, a su vez, esto implica que el morfismo $\iota : G \to \mathbb{Z}_n^\times$, que sabemos que es inyectivo, debe ser sobreyectivo. □

Usando esta proposición, podemos hacer explícito el polinomio minimal de ω:

Corolario 1.3. *Sea $\mu_n^\times \subseteq \mu_n$ el conjunto de las raíces n-ésimas primitivas de la unidad. El polinomio minimal de ω sobre $\mathbb{Q}$ es*

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^\times} (X - \zeta).$$

Si notamos $\mu : \mathbb{Z} \to \mathbb{Z}$ a la función clásica de Möbius, entonces

$$\Phi_n(X) = \prod_{m|n} (X^m - 1)^{\mu(m)}, \tag{2}$$

Llamamos a $\Phi_n(X)$ el *n-ésimo polinómio ciclotómico*. La expresión (2) para $\Phi_n(X)$ permite calcular fácilmente sus valores; en la tabla 1 en la página siguiente damos los primeros.

Demostración. Sea f el polinomio minimal de ω sobre $\mathbb{Q}$. En la prueba de la proposición vimos que f tiene a los elementos de $\mu_n^\times$ como raices simples. Como el polinomio del enunciado del corolario tiene el mismo grado, las mismas raíces y el mismo coeficiente principal que f, debe coincidir con f.

[1] Ver [5, Corollary IV.2.3]

n	$\Phi_n(X)$
1	$X-1$
2	$X+1$
3	X^2+X+1
4	X^2+1
5	$X^4+X^3+X^2+X+1$
6	X^2-X+1
7	$X^6+X^5+X^4+X^3+X^2+X+1$
8	X^4+1
9	X^6+X^3+1
10	$X^4-X^3+X^2-X+1$
11	$X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1$
12	X^4-X^2+1
13	$X^{12}+X^{11}+X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1$
14	$X^6-X^5+X^4-X^3+X^2-X+1$
15	$X^8-X^7+X^5-X^4+X^3-X+1$

Tabla 1. Los primeros polinómios ciclotómicos.

El polinomio X^n-1 tiene todas sus raíces simples y cada una de ellas pertenece exactamente a un conjunto $\mu_m^\times$ con $m \mid n$. Esto implica inmediatamente que

$$X^n-1 = \prod_{m|n} \Phi_n(X),$$

y entonces, como esto vale cualquiera sea $n \in \mathbb{N}$, la fórmula de inversión de Möbius[2] nos da la expresión (2) del enunciado. □

§2. Una aplicación aritmética

El objetivo de esta sección es mostrar que para cada $d \in \mathbb{N}$ hay infinitos primos en el conjunto $\{1+nd : n \in \mathbb{N}\}$. El caso particular en que $d=1$ dice precisamente que hay infinitos números primos y, de hecho, la prueba que damos es una generalización de la prueba clásica de Euclides para ese caso.

Lema 2.1. *Sean $n, d \in \mathbb{N}$. Si p es un primo tal que $p \mid \Phi_d(n)$, entonces $p \equiv 1 \mod d$.*

Demostración. Si $p \mid \Phi_d(n)$, entonces $p \mid \prod_{r|d} \Phi_r(n) = n^d - 1$ y, en particular, es $p \nmid n$ así que la clase de n en $\mathbb{Z}_p$ es un elemento del grupo multiplicativo $\mathbb{Z}_p^\times$. Como $n^d \equiv 1 \mod p$, el orden s de n en $\mathbb{Z}_p^\times$ divide a d.

[2] Ver, por ejemplo, http://en.wikipedia.org/wiki/Moebius_inversion_formula.

Supongamos que $s \neq d$. Entonces $p \mid n^s - 1 = \prod_{e|s} \Phi_e(n)$, así que existe $e \in \mathbb{N}$ tal que $e \mid s$ y $p \mid \Phi_e(n)$. Como $e \neq d$, vemos que

$$p^2 \mid \Phi_d(n)\Phi_e(n) \mid \prod_{f|d} \Phi_f(n) = n^d - 1. \tag{3}$$

Por otro lado, como $n + p \equiv n \mod p$, se tiene que $\Phi_d(n+p) \equiv \Phi_d(n) \equiv 0 \mod p$ y $\Phi_e(n+p) \equiv \Phi_e(n) \equiv 0 \mod p$, y entonces también

$$p^2 \mid \Phi_d(n+p)\Phi_e(n+p) \mid \prod_{f|d} \Phi_f(n+p) = (n+p)^d - 1. \tag{4}$$

Como $(n+p)^d - 1 \equiv n^d + dn^{d-1}p - 1 \mod p^2$, de (3) y (4) deducimos que $p^2 \mid dn^{p-1}p$. Esto es imposible porque $p \nmid n$ y $p \nmid d$.

Concluimos de esta forma que d es el orden de n en $\mathbb{Z}_p^\times$. El teorema de Lagrange, entonces, nos dice que $d \mid |\mathbb{Z}_p^\times| = p - 1$, así que $p \equiv 1 \mod d$. □

Proposición 2.2. *Sea $d \in \mathbb{N}$. Hay infinitos primos p tales que $p \equiv 1 \mod d$.*

Demostración. Supongamos que $p_1, \ldots, p_k$ son primos congruentes con 1 módulo d y mostremos que existe un primo distinto de éstos que satisface la misma condición.

Sea $N = dp_1 \cdots p_k$. Para cada $n \in \mathbb{Z}$ es $nN \equiv 0 \mod N$, así que $\Phi_d(nN) \equiv \Phi_d(0) \mod N$. Como el entero $\varepsilon = \Phi_d(0)$ es, a menos de un signo, el producto de las raíces d-ésimas primitivas de la unidad, es él mismo una raíz de la unidad: debe ser entonces $\varepsilon \in \{\pm 1\}$. Por otro lado, $\Phi_d(nN) \to \infty$ si $n \to \infty$, porque $\Phi_d(X)$ es un polinomio mónico de grado positivo, así que existen $n \in \mathbb{N}$ y un primo p tales que $p \mid \Phi_d(nN)$. En vista del lema anterior, entonces, podemos concluir que $p \equiv 1 \mod d$. De existir $i \in \{1, \ldots, k\}$ tal que $p = p_i$, tendríamos que $p \mid N \mid \Phi_d(nN) - \varepsilon$, de manera que $p \mid \varepsilon$, lo que es absurdo: esto implica que p es distinto de $p_1, \ldots, p_k$. □

Corolario 2.3. *Todo grupo abeliano finito es isomorfo a un cociente de un grupo de la forma $\mathbb{Z}_n^\times$.*

Demostración. Sea G un grupo abeliano finito. De acuerdo al teorema de estructura de grupos abelianos finitamente generados existen $n_1, \ldots, n_k \in \mathbb{N}$ tales que $G \cong \prod_{i=1}^n \mathbb{Z}_{n_i}$.

La Proposición 2.2 implica que existen primos *distintos* $p_1, \ldots, p_k$ tales que $p_i \equiv 1 \mod n_i$ para cada $i \in \{1, \ldots, k\}$. Más aún, si $i \in \{1, \ldots, n\}$, el número n_i divide a $p_i - 1$, el orden del grupo cíclico $\mathbb{Z}_{p_1}^\times$, así que existe un subgrupo $H_i \subseteq \mathbb{Z}_{p_1}^\times$ tal que $\mathbb{Z}_{p_1}^\times / H_i \cong \mathbb{Z}_{n_i}$.

Si $N = p_1 \cdots p_k$, entonces el teorema chino del resto nos dice que hay un isomorfismo $\phi : \prod_{i=1}^k \mathbb{Z}_{p_i}^\times \to \mathbb{Z}_N^\times$. Si ponemos $H = \prod_{i=1}^k H_i$, es claro que $\mathbb{Z}_N^\times / \phi(H) \cong G$, y esto prueba el corolario. □

§3. Extensiones ciclotómicas

Si K es un cuerpo de números, una *extensión ciclotómica de K* es una extensión de K contenida en un cuerpo de la forma $K(\omega)$ con ω una raíz de la unidad. Un *cuerpo ciclotómico* es una extensión ciclotómica de $\mathbb{Q}$.

Proposición 3.1. *Si K es un cuerpo de números y $\omega \in \mu_n^\times$, entonces la extensión $K(\omega)/K$ es galoisiana, para cada $\sigma \in \mathrm{Gal}(K(\omega)/K)$ la restricción $\sigma|_{\mathbb{Q}(\omega)}$ es un elemento de $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, y la aplicación*

$$\sigma \in \mathrm{Gal}(K(\omega)/K) \longmapsto \sigma|_{\mathbb{Q}(\omega)} \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \tag{5}$$

es un monomorfismo de grupos. En particular, $\mathrm{Gal}(K(\omega)/K)$ es un grupo abeliano.

Demostración. El cuerpo $K(\omega)$ es un cuerpo de descomposición de $X^n - 1$ sobre K, así que la extensión $K(\omega)/K$ es normal. Un elemento $\sigma \in \mathrm{Gal}(K(\omega)/K)$ deja fijo a $\mathbb{Q} \subseteq K$ y envía ω sobre alguna raíz n-esima de la unidad: esto implica inmediatamente que σ se restringe a un automorfismo $\sigma|_{\mathbb{Q}(\omega)} : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ que está en $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. Como σ queda determinado por $\sigma(\omega)$, la función (5) es inyectiva. Finalmente, que es un homomorfismo de grupos es claro. □

Corolario 3.2. *Sea K es un cuerpo de números y sea L/K es una extensión ciclotómica de K. Entonces la extensión L/K es galoisiana y su grupo de Galois $\mathrm{Gal}(L/K)$ es abeliano.*

Demostración. Supongamos que $L \subseteq K(\omega)$ para algún $\omega \in \mu_n^\times$. Del teorema fundamental de la teoría de Galois, sabemos que existe un subgrupo $H \subseteq \mathrm{Gal}(K(\omega)/K)$ tal que $L = K(\omega)^H$. Como $\mathrm{Gal}(K(\omega)/K)$ es abeliano H es un subgrupo normal de $\mathrm{Gal}(K(\omega)$ y, en consecuencia[3], L/K es una extensión galoisiana cuyo grupo de Galois es imagen homomórfica de $\mathrm{Gal}(K(\omega)/K)$. □

Proposición 3.3. *Si G es un grupo abeliano finito, entonces existe un extensión ciclotómica K de $\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.*

Demostración. De acuerdo al Corolario 2.3, existe $n \in \mathbb{N}$ y un subgrupo $H \subseteq \mathbb{Z}_n^\times$ tal que $\mathbb{Z}_n^\times/N \cong G$. Sea $\omega \in \mu_n^\times$, sea $\iota : \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \to \mathbb{Z}_n^\times$ el isomorfismo de la Proposición 1.2 y sea $K = \mathbb{Q}(\omega)^{\iota^{-1}(H)}$ el cuerpo fijo de $\iota^{-1}(H)$ en $\mathbb{Q}(\omega)$. El teorema fundamental de la teoría de Galois nos dice que la extensión ciclotómica $K/\mathbb{Q}$ tiene grupo de Galois $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})/N \cong G$. □

Teorema 3.4. (Kronecker-Weber) *Una extensión galoisiana finita de $\mathbb{Q}$ de grupo de Galois abeliano es una extensión ciclotómica de $\mathbb{Q}$.*

Este teorema implica, en particular, que un número algebraico ξ puede escribirse como una suma finita de la forma

$$\xi = \sum_j a_j e^{2\pi i k_i/\nu_i} \tag{6}$$

con $a_j \in \mathbb{Q}$, $\nu_i \in \mathbb{N}$ y $0 \leq k_i < \nu_i$ si y solamente si el grupo de Galois del cuerpo de descomposición de su polinomio minimal es abeliano. Por ejemplo, podemos escribir

$$\sqrt{5} = e^{2\pi i/5} - e^{4\pi i/5} - e^{6\pi i/5} + e^{8\pi i/5}$$

[3] Ver [5, Teorema VI.1.10]

porque $\sqrt{5}$ tiene polinomio minimal $X^2 - 5$ y grupo de Galois evidentemente abeliano. Por el contrario,

$$\sqrt[3]{\frac{\sqrt{5}-1}{2}} - \sqrt[3]{\frac{\sqrt{5}+1}{2}}$$

no puede escribirse como en (6) porque su polinomio minimal es $t^3 + 3t + 1$, que tiene grupo de Galois S_3. En efecto, es discriminante de este polinomio es -135, que no es un cuadrado en $\mathbb{Q}$, así que su grupo de Galois no está contenido en el grupo alternante $A_3 \subset S_3$ y entonces necesariamente debe ser S_3.

No podemos dar una prueba del teorema de Kronecker-Weber. Fue probado originalmente por Leopold Kronecker [4], con correcciones de Heinrich Martin Weber [6] y más tarde de Hilbert [3]; en [1] y [2] se da un aprueba 'elemental'. Consideremos, sin embargo, el siguiente caso particular:

Proposición 3.5. *Una extensión cuadrática de $\mathbb{Q}$ es una extensión ciclotómica de $\mathbb{Q}$.*

Demostración. Sea p un número primo impar. El cuerpo $\mathbb{Z}_p^\times$ tiene $p-1$ elementos y es cíclico, así que $[\mathbb{Z}_p^\times : (\mathbb{Z}_p^\times)^2] = 2$ y existe entonces exactamente un homomorfismo de grupos $\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p^\times \to \{\pm 1\}$ cuyo núcleo es $(\mathbb{Z}_p^\times)^2$. Explícitamente, si $x \in \mathbb{Z}_p^\times$ es

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{si } x \in (\mathbb{Z}_p^\times)^2; \\ -1, & \text{si ese no es el caso.} \end{cases}$$

Por otro lado, si fijamos una raíz primitiva $\omega_p \in \mu_p^\times$, hay un isomorfismo de grupos $\chi : x \in \mathbb{Z}_p \mapsto \omega_p^i \in \mu_p$.

Consideremos el número $\gamma = \sum_{x \in \mathbb{Z}_p^\times} \left(\frac{x}{p}\right)\chi(x) \in \mathbb{Q}(\omega_p)$. Es

$$\gamma^2 = \sum_{x,y \in \mathbb{Z}_p^\times} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\chi(x)\chi(y) = \sum_{x,y \in \mathbb{Z}_p^\times} \left(\frac{xy}{p}\right)\chi(x+y).$$

Fijado $y \in \mathbb{Z}_p^\times$, es claro que x y xy recorren simultáneamente $\mathbb{Z}_p^\times$, así que

$$\begin{aligned} \gamma^2 &= \sum_{x,y \in \mathbb{Z}_p^\times} \left(\frac{xy^2}{p}\right)\chi((x+1)y) = \sum_{x,y \in \mathbb{Z}_p^\times} \left(\frac{x}{p}\right)\chi((x+1)y) \\ &= \sum_{y \in \mathbb{Z}_p^\times} \left(\frac{-1}{p}\right) + \sum_{\substack{x \in \mathbb{Z}_p^\times \\ x \neq -1}} \left(\frac{x}{p}\right) \sum_{y \in \mathbb{Z}_p^\times} \chi((x+1)y) \end{aligned}$$

Como $\sum_{\zeta \in \mu_n^\times} \zeta = -1$ y que $y \in \mathbb{Z}_p^\times \mapsto (x+1)y \in \mathbb{Z}_p^\times$ es una biyección cuando $x \neq -1$, sabemos que $\sum_{y \in \mathbb{Z}_p^\times} \chi((x+1)y) = -1$. Luego

$$\gamma^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{\substack{x \in \mathbb{Z}_p^\times \\ x \neq -1}} \left(\frac{x}{p}\right) = p\left(\frac{-1}{p}\right) - \sum_{x \in \mathbb{Z}_p^\times} \left(\frac{x}{p}\right) = p\left(\frac{-1}{p}\right).$$

Esto nos dice que

- si $\left(\frac{-1}{p}\right) = 1$, γ es una raíz cuadrada de p, así que $\sqrt{p} \in \mathbb{Q}(\omega_p)$, mientras que
- si $\left(\frac{-1}{p}\right) = -1$, γ es una raíz cuadrada de $-p$, de manera que es $\sqrt{p} \in \mathbb{Q}(\omega_p, i)$.

Si $p = 2$ es el primo par, es inmediato que $\sqrt{2} = -i(1+i)^2 \in \mathbb{Q}(i)$ y, pr supuesto, también $\sqrt{-2}$ß$\mathbb{Q}(i)$.

Ahora bien, una extensión cuadrática de $\mathbb{Q}$ es de la forma $\mathbb{Q}(\sqrt{n})$ con $n = \varepsilon 2^a p_1 \cdots p_k$ con $\varepsilon \in \{\pm 1\}$, $a \in \{0, 1\}$ y $p_1, \ldots, p_k$ primos impares distintos, así que

$$\sqrt{n} = \sqrt{\varepsilon 2^a}\sqrt{p_1} \cdots \sqrt{p_k} \in \mathbb{Q}(i, \omega_{p_1}, \ldots, \omega_{p_k}).$$

De acuerdo a siguiente lema, esté último cuerpo coincide con $\mathbb{Q}(\omega)$ con $\omega \in \mu^\times_{4p_1\cdots p_k}$, así que $\mathbb{Q}(\sqrt{n})$ es una extensión ciclotómica de $\mathbb{Q}$. □

La suma que define al escalar γ que aparece en esta prueba se llama una *suma gaussiana*, y fue famosamente considerada por Carl Friedrich Gauss en sus *Disquisitiones Arithmeticæ*. Gauss determinó exactamente cuál de las dos raíces cuadradas de $p\left(\frac{-1}{p}\right)$ es γ.

Lema 3.6. *Sean $n_1, \ldots, n_k \in \mathbb{N}$ números naturales coprimos dos a dos y, para cada $i \in \{1, \ldots, k\}$ sea $\omega_i \in \mu^\times_{n_i}$. Si $n = n_1 \cdots n_k$ y $\omega \in \mu^\times_n$, entonces $\mathbb{Q}(\omega_1, \ldots, \omega_k) = \mathbb{Q}(\omega_n)$.*

Demostración. Una inducción evidente prueba que basta considerar el caso en que $k = 2$. Como $\omega^m \in \mu^\times_n$ y $\omega^n \in \mu^\times_m$, $\mathbb{Q}(\omega_1, \omega_2) \subseteq \mathbb{Q}(\omega)$. Por otro lado, $\omega_1\omega_2 \in \mu^\times_n$, así que de hecho esta inclusión es una igualdad. □

§4. Extensiones cíclicas

Teorema 4.1. *Sea K un cuerpo y sea $n \in \mathbb{N}$ coprimo con la característica de K. Supongamos que K contiene una raíz n-ésima primitiva de la unidad. Si $a \in K$ y b es una raíz de $X^n - a$ en alguna clausura algebraica de K, entonces la extensión $K(b)/K$ es cíclica. Si d es su grado, entonces $d \mid n$ y $b^d \in K$.*

Demostración. Sea $\mu_n \subseteq K^\times$ el grupo multiplicativo de las raíces n-ésimas de la unidad de K, que por hipótesis es cíclico de orden n.

El cuerpo $k(b)$ contiene los elementos ζb con $\zeta \in \mu_n$, que son n, distintos dos a dos, y todos raíces de $X^n - a$. Esto nos dice que $K(b)$, que está generado por ellos, es un cuerpo de descomposición de $X^n - a$ sobre K, así que es normal. Como las raíces de ese polinomio son visiblemente simples, la extensión $K(b)/K$ es también separable, así que es galoisiana. Sea $G = \mathrm{Gal}(K(b)/K)$ su grupo de Galois.

Es claro que si $\sigma \in G$ el cociente $\sigma(b)/b$ es un elemento de μ_n, así que tenemos una función $\rho : \sigma \in G \mapsto \sigma(b)/b \in \mu_n$. Como b genera a $K(b)$ sobre K, un elemento de G queda determinado por su acción sobre b y, en consecuencia, la función ρ es inyectiva. Un cálculo inmediato muestra que es además un morfismo de grupos, así que determina un isomorfismo de G con un subgrupo de μ_n. Se sigue de esto que G es cíclico de un orden d que divide a n. Más aún, si $\sigma \in G$ es un generador, $\omega = \rho(\sigma)$ es un elemento de μ_n de orden d y $\sigma(b) = \omega b$, de manera que $\sigma(b^d) = \omega^d b^b = b^d$: como σ genera a G, esto implica que $b^d \in K(b)^G = K$. □

Lema 4.2. (Hilbert) *Sea L/K una extensión cíclica de grado n y grupo de Galois $G = \mathrm{Gal}(L/K)$ generado por σ, y sea $x \in K$. Entonces $N_{L/K}(x) = 1$ sii existe $y \in L^\times$ tal que $x = y/\sigma(y)$.*

Demostración. La necesidad de la condición sigue inmediatamente de un cálculo directo de la norma $N_{L/K}(x)$ cuando $x = y/\sigma(y)$ para algún $y \in K^\times$.

Supongamos entonces que $x \in K$ es un elemento de norma $N_{L/K}(x) = 1$. Del teorema de Artin sabemos que los elementos de G, vistos como funciones $L^\times \to L^\times$, son linealmente independientes sobre L. En particular, la función

$$f : z \in L^\times \mapsto z + x\sigma(z) + x\sigma(x)\sigma^2(z) + \cdots + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^n(z) \in L^\times$$

no es identicamente nula. Sea $z \in L^\times$ tal que $y = f(z) \neq 0$. Calculando y usando el hecho de que $N_{L/K}(x) = 1$, vemos fácilmente que $x\sigma(y) = y$ así que $x = y/\sigma(y)$. □

Teorema 4.3. *Sea K un cuerpo y sea $n \in \mathbb{N}$ coprimo con la característica de K. Supongamos que K contiene una raíz n-ésima primitiva de la unidad. Si L/K es una extensión cíclica de grado n, entonces existe $b \in L$ tal que $L = K(b)$ y que es raíz de un polinomio de la forma $X^n - a$ con $a \in K$.*

Demostración. Sea ω una raíz n-ésima primitiva de la unidad de K. Sea G el grupo de Galois de L/K y sea $\sigma \in G$ un generador. Es $N_{L/K}(\omega^{-1}) = 1$, así que el lema nos dice que existe $b \in L$ tal que $b/\sigma(b) = \omega^{-1}$, de manera que $\sigma(b) = \omega b$.

Es $\sigma(b^n) = \sigma(b)^n = \omega^n b^n = b^n$, así que como σ genera a G, es $a = b^n \in K$.

Como $\omega \in K$, es $\sigma^i(b) = \omega^i b$ para cada $i \in \{0, \ldots, n-1\}$. Los escalares b, $\sigma(b)$, $\ldots$, $\sigma^{n-1}(b)$ son entonces raíces de $X^n - a$, y son distintos porque ω es una raíz primitiva. entonces $[K(b) : K] \geq n$; como $[L : K] = n$, concluimos así que $L = K(b)$. □

Ejemplo 4.4. Si L/K es una extensión cíclica de orden m pero K no posee ninguna raíz m-ésima primitiva de la unidad, entonces la extensión *no* es radical. En efecto, supongamos que existe $b \in L$ tal que $b^m \in K$ y que $L = K(b)$, y sea $G = \mathrm{Gal}(L/K)$ y $\mu_m \subseteq K^\times$ el grupo de las raíces m-ésimas de la unidad que hay en K. Si $\sigma \in G$, entonces $\sigma(b)^m = \sigma(b^m) = b^m$, así que $\sigma(b)/b \in \mu_m$. De esta manera, vemos que hay una función $\iota : \sigma \in G \mapsto \sigma(b)/b \in \mu_m$, que resulta un homomorfismo de grupos. Por hipótesis, $|\mu_m| < m = |G|$, así que ι no es inyectiva: esto implica que existe $\sigma \in G$, distinta de id_L, tal que $\sigma(b) = b$, y esto es absurdo porque b genera a L sobre K.

Construyamos un ejemplo de esta situación. Sea $\omega = e^{2\pi i/9}$, que no es real, y sea $K = \mathbb{Q}(\omega) \cap \mathbb{R}$. El grupo de Galois de $\mathbb{Q}(\omega)/\mathbb{Q}$ es isomorfo a $\mathbb{Z}_9^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ y posee entonces un único elemento ρ de orden 2, que debe ser la conjugación compleja. Se sigue de ésto que $K = \mathbb{Q}(\omega)^\rho$ es el cuerpo fijo de ρ y que la extensión $K/\mathbb{Q}$ es galoisiana de grupo de Galois $G \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})/(\rho)$ de orden 3; en particular, G es cíclico. Por supuesto, $\mathbb{Q}$ no contiene ninguna raíz cúbica primitiva de la unidad.

§5. Extensiones abelianas de exponente finito: teoría de Kummer

Fijemos un cuerpo K, sea $m \in \mathbb{N}$ y supongamos que m es coprimo con la caracterítica de K y que K contiene una raíz m-ésima primitiva de la unidad. Sea $K^\times$ el grupo multiplicativo de K y sean $K^{\times m} = \{x^m : x \in K^\times\}$ el subgrupo de las potencias m-ésimas

de $K^\times$ y $\mu_m \subseteq K^\times$ el subgrupo de las raíces m-ésimas de la unidad. Fijemos, finalmente, una clausura algebraica $\bar{K}$ de K.

Sea $b \in K$ y sea $a \in \bar{K}$ tal que $a^m = b$. El cuerpo $K(a)$ depende solamente de b y no de la elección de a: en efecto, si $a' \in \bar{K}$ es otro elemento tal que $a'^m = b$, entonces existe $\omega \in \mu_m$ tal que $a' = \omega b$ y, como $\omega \in K$, es claro que $K(a') = K(a)$. En esta situación, escribiremos $K(b^{1/m})$ en lugar de $K(a)$. Como μ_m tiene exactamente m elementos, el polinomio $X^n - b$ se descompone en $K(b^{1/m})$ y tiene allí todas sus raíces simples: esto nos dice que la extensión $K(b^{1/m})/K$ es galoisiana. Es inmediato que $K(b^{1/m}) = K$ si y solamente si $b \in K^{\times m}$.

Si $B \subseteq K^\times$ es un subgrupo tal que $B \supseteq K^{\times m}$, escribamos $K(B^{1/m})$ a la subextensión de K compuesta de todos los cuerpos de la forma $K(b^{1/m})$ con $b \in B$. Siendo compuesta de extensiones galoisianas, $K(B^{1/m})/K$ es galoisiana.

Lema 5.1. *Sea $G = \mathrm{Gal}(K(B^{1/m})/K)$. Existe un bihomomorfismo de grupos*

$$(\sigma, b) \in G \times B \longmapsto \langle \sigma, b \rangle \in \mu_m$$

unívocamente determinado por la siguiente condición:

si $\sigma \in G$ y $b \in B$, y $a \in K(B^{1/m})$ es tal que $a^m = b$, entonces $\sigma(a) = \langle \sigma, b \rangle a$.

El núcleo a izquierda de $\langle -, - \rangle$ es trivial, mientras que el núcleo a derecha contiene al subgrupo $K^{\times m}$ de B. En particular, $\langle -, - \rangle$ induce una bihomomorfismo no degenerado

$$(\sigma, b) \in G \times B/K^{\times m} \longmapsto \langle \sigma, b \rangle \in \mu_m. \tag{7}$$

Demostración. Sean $\sigma \in G$ y $b \in B$, y sea $a \in K(B^{1/m})$ tal que $a^m = b$. Entonces $\sigma(a)^m = \sigma(a^m) = \sigma(b) = b = a^m$ y, en consecuencia, $\omega_{\sigma,b} := \sigma(a)/a \in \mu_m$. El elemento $\omega_{\sigma,b}$ depende solamente de b y no de la elección de a: si $a' \in K(B^{1/m})$ es otro elemento tal que $a'^m = b$, entonces existe $\zeta \in \mu_m$ tal que $a' = \zeta a$ y $\sigma(a')/a' = \sigma(\zeta a)/(\zeta a) = \sigma(a)/a$ porque $\zeta \in K$. Esto nos dice que podemos definir una función

$$(\sigma, b) \in G \times B \longmapsto \langle \sigma, b \rangle := \omega_{\sigma,b} \in \mu_m.$$

Sean σ, $\tau \in G$ y b_1, $b_2 \in B$, y sean a_1, $a_2 \in K(B^{1/m})$ tales que $a_i^m = b_i$ para cada $i \in \{1, 2\}$. Como $(a_1 a_2)^m = b_1 b_2$, es

$$\langle \sigma, b_1 b_2 \rangle = \frac{\sigma(a_1 a_2)}{a_1 a_2} = \frac{\sigma(a_1)}{a_1} \frac{\sigma(a_2)}{a_2} = \langle \sigma, b_1 \rangle \langle \sigma, b_2 \rangle.$$

Por otro lado, tenemos que

$$\langle \sigma\tau, b_1 \rangle = \frac{(\sigma\tau)(a_1)}{a_1} = \frac{\sigma(\tau(a_1))}{a_1} = \frac{\sigma(\langle \tau, b_1 \rangle a_1)}{a_1} = \langle \sigma, b_1 \rangle \langle \tau, b_1 \rangle.$$

Estas dos igualdades nos dicen que $\langle -, - \rangle$ es un bihomomorfismo.

Si $\sigma \in G$ está en el núcleo a izquierda de $\langle -, - \rangle$, entonces para cada $a \in K(B^{1/m})$ tal que $a^m \in B$ se tiene que $\sigma(a) = a$: como $K(B^{1/m})$ está generado por estos elementos sobre K, esto implica que σ actúa trivialmente sobre $K(B^{1/m})$ y, en consecuencia,

$\sigma = \mathrm{id}_{K(B^{1/m})}$. Así, el núcleo a izquierda es trivial. Por otro lado, si $\sigma \in G$ y $b \in K^{\times m}$, es claro que $\sigma(a) = a$ para todo $a \in K(B^{1/m})$ tal que $a^m = b$, así que $\langle \sigma, b\rangle = 1$. Esto muestra que $K^{\times m}$ está contenido en el núcleo a derecha de $\langle -, -\rangle$.

Nos queda probar que el bihomomorfismo inducido (7) es no degenerado a derecha. Sea $a \in B \setminus K^{\times m}$ y pongamos $b = a^m$, de manera que $K(b^{1/m}) = K(a)$. Hay un automorfismo $\sigma_0 \in \mathrm{Gal}(K(b^{1/m})/K)$ tal que $\sigma_0(a) \neq a$, y σ_0 extiende a un automorfismo $\sigma \in G$ tal que $\sigma(a) \neq a$. Entonces $\langle \sigma, b\rangle = \sigma(a)/a \neq 1$. □

Teorema 5.2. *Sea K un cuerpo, sea $m \in \mathbb{N}$ y supongamos que m es coprimo con la característica de K y que K contiene una raíz m-ésima primitiva de la unidad. Si $B \subseteq K^\times$ es un subgrupo que contiene a $K^{\times m}$, entonces la extensión $K(B^{1/m})$ es abeliana de exponente divisor de m. Es finita sii $[B : K^{1/m}] < \infty$ y en ese caso hay un isomorfismo*

$$\mathrm{Gal}(K(B^{1/m})/K) \cong \hom(B/K^{\times m}, \mu_m)$$

y el grado de la extensión es $[K(B^{1/m}) : K] = [B : K^{1/m}]$.

Demostración. Escribamos como antes $G = \mathrm{Gal}(K(B^{1/m})/K)$. La función

$$f : \sigma \in G \mapsto \langle \sigma, -\rangle \in \hom(B/K^{\times m}, \mu_m)$$

es un homomorfismo de grupos inyectivo, así que G es abeliano y, como μ_m tiene exponente m, el exponente de G divide a m. Si $B/K^{\times m}$ es finito, G es finito y el Lema 5.3 siguiente prueba que f es, de hecho, un isomorfismo; en ese caso, como la extensión es galoisiana, es

$$[K(B^{1/m}) : K] = |G| = |\hom(B/K^{\times m}, \mu_m)| = |B/K^{\times m}| = [B : K^{\times m}].$$

Recíprocamente, si la extensión tiene grado finito, entonces G es finito y otra vez el Lema 5.3 implica que $[B : K^{\times m}] < \infty$. □

Lema 5.3. *Sea C un grupo cíclico de orden m y sea $\phi : A \times B \to C$ un bihomomorfismo no degenerado. Si B es finito, entonces $A \cong \hom(B, C)$.*

Demostración. La función $f : a \in A \mapsto \phi(a, -) \in \hom(B, C)$ es un homomorfismo de grupos que es inyectivo porque el bihomomorfismo ϕ es no degenerado. Como B es finito, esto implica que A es finito y que $|A| \leq |\hom(B, C)|$. Sabiendo ahora que A es finito, un razonamiento simétrico nos muestra que $|B| \leq |\hom(A, C)|$. Para probar el lema, bastará mostrar que f es sobreyectivo y para ello, en vista de las desigualdades obtenidas, que $\hom(A, C) \cong A$ y $\hom(B, C) \cong B$. Por supuesto, es suficiente ocuparnos del primer isomorfismo.

Sea $a \in A$. Si $ma \neq 0$, existe $b \in B$ tal que $0 \neq \phi(ma, b) = m\phi(a, b)$: esto es imposible porque C tiene orden m. Esto muestra que el exponente de A divide a m y entonces el teorema de estructura de los grupos abelianos finitos nos dice que existen subgrupos cíclicos $A_1, \ldots, A_k \subseteq A$ de ordenes que dividen a m tales que $A = \bigoplus_{i=1}^k A_i$. Como $\hom(A, C) \cong \prod_{i=1}^k \hom(A_i, C)$, vemos que podemos suponer sin pérdida de generalidad que A es cíclico. En ese caso, que $\hom(A, C) \cong A$ es inmediato. □

Proposición 5.4. *Sea K un cuerpo, sea $m \in \mathbb{N}$ y supongamos que m es coprimo con la característica de K y que K contiene una raíz m-ésima primitiva de la unidad. Sean B_1 $B_2 \subseteq K^\times$ subgrupos tales que que contienen a $K^{\times m}$. Entonces $K(B_1^{1/m}) \subseteq K(B_2^{1/m})$ si y solamente $B_1 \subseteq B_2$.*

Demostración. La suficiencia de la condición es inmediata. Veamos la necesidad.

Supongamos que $K(B_1^{1/m}) \subseteq K(B_2^{1/m})$ y sea $b \in B_1$. Como $K(b^{1/m}) \subseteq K(B_2^{1/m})$, existe un subgrupo B_2' de B_2 que tiene a $K^{\times m}$ como subgrupo de índice finito y tal que $K(b^{1/m}) \subseteq K(B_2'^{1/m})$. Sea B_3 el subgrupo generado por B_2' y b en $K^\times$. Las elecciones implican que $K(B_3^{1/m}) = K(B_2'^{1/m})$ y, dado que $K^{\times m}$ tiene índice finito tanto en $K(B_3^{1/m})$ como en $K(B_2'^{1/m})$, el teorema anterior nos dice que

$$[B_3 : K^{\times m}] = [K(B_3^{1/m} : K] = [K(B_2'^{1/m} : K] = [B_2' : K^{\times m}].$$

Ahora bien, estas igualdades y el hecho de que $K^{\times m} \subseteq B_2' \subseteq B_3$, nos permiten concluir que $B_2' = B_3$ y, en particular, que $b \in B_2' \subseteq B_2$. □

Teorema 5.5. *Sea K un cuerpo, sea $m \in \mathbb{N}$ y supongamos que m es coprimo con la característica de K y que K contiene una raíz m-ésima primitiva de la unidad. La asignación*

$$B \longmapsto K(B^{1/m})$$

establece una biyección entre el conjunto de los subgrupos de $K^\times$ que contienen a $K^{\times m}$ y las extensiones abelianas de K cuyo exponente divide a m.

Demostración. Se sigue del Teorema 5.2 y de la proposición anterior que la función descripta en el enunciado está bien definida y es inyectiva. Veamos que es sobreyectiva.

Sea L/K una extensión abeliana de exponente divisor de m. Si L'/K es una subextensión finita y $G = \mathrm{Gal}(L'/K)$ es su grupo de Galois, entonces G es abeliano de exponente divisor de m así que existen subgrupos cíclicos $G_1, \ldots, G_k \subseteq G$ de exponente divisor de m tales que $G = \prod_{i=1}^k G_i$. Para cada $i \in \{1, \ldots, k\}$ pongamos $H_i = \prod_{j \neq i} G_j$ y sea $L_i' = L'^{H_i}$. Sabemos que L' es la extensión compuesta de las L_i'/K y que existen $b_1, \ldots, b_k \in K^\times$ tales que $L_i' = K(b_i^{1/m})$ para cada $i \in \{1, \ldots, k\}$. Si B' es el subgrupo de $K^\times$ generado por $b_1, \ldots, b_k$ y $K^{\times m}$, entonces esto nos dice que $L' = K(B'^{1/m})$.

Esto implica inmediatamente que $L = K(B^{1/m})$ para algún subgrupo $B \subseteq K^\times$ que contiene a $K^{\times m}$. □

Referencias

[1] M. J. Greenberg, *An elementary proof of the Kronecker-Weber theorem*, Amer. Math. Monthly **81** (1974), 601–607. MR0340214 (49 #4970)

[2] ———, *Correction to: "An elementary proof of the Kronecker-Weber theorem" (Amer. Math. Monthly* **81** *(1974), 601–607)*, Amer. Math. Monthly **82** (1975), no. 8, 803. MR0376605 (51 #12780)

[3] D. Hilbert, *Der Theorie der algebraischer Zahlkörper*, Jahresber. der Deutsch. Math. Ver. **4** (1897), 177–546.

[4] L. Kronecker, *Uber die algebraisch auflösbaren Gleichungen I*, Sber. preuss. Akad. Wiss. (1853), 365–374.

[5] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)

[6] H. Weber, *Theorie der Abel'schen Zahlkörper I, II*, Acta Math. Stockh. **8,9** (1886, 1887).