Teoría Algebraica de Números

Índice general

Capítulo 1

Enteros Algebraicos

1. Los Enteros Gaussianos

En el siglo XVII, Pierre de Fermat estudió diversos temas de Teoría de Números. Entre ellos, uno de sus temas favoritos fue el de representabilidad de números primos por distintas formas cuadráticas. Por ejemplo, Fermat estudió cuáles primos p se pueden representar como una suma de dos cuadrados. Es decir, la solubilidad de la ecuación diofántica

$$p = x^2 + y^2$$

con $p \in \mathbb{Z}_{\geq 1}$ un primo y $x, y \in \mathbb{Z}$. Algunos ejemplos son:

$$\begin{array}{lll} 2 = 1^2 + 1^2 & 13 = 2^2 + 3^2 & 29 = 2^2 + 5^2 \\ 5 = 1^2 + 2^2 & 17 = 1^2 + 4^2 & 37 = 1^2 + 6^2 \end{array}$$

Si se observan estos ejemplos con cuidado, se nota que salvo el 2, los únicos primos que aparecen en esta lista cumplen que

$$p \equiv 1 (\text{mód} 4).$$

Esto es pues módulo 4, los cuadrados de un entero sólo pueden ser

$$\begin{aligned} n \equiv 0 (\text{mód} 4) &\Rightarrow n^2 \equiv 0 (\text{mód} 4) \\ n \equiv 1 (\text{mód} 4) &\Rightarrow n^2 \equiv 1 (\text{mód} 4) \\ n \equiv 2 (\text{mód} 4) &\Rightarrow n^2 \equiv 4 \equiv 0 (\text{mód} 4) \\ n \equiv 3 (\text{mód} 4) &\Rightarrow n^2 \equiv 9 \equiv 1 (\text{mód} 4), \end{aligned}$$

es decir, los cuadrados (mód4) son 0 y 1. Es por esto que sólo se pueden tener las posibilidades

$$\begin{aligned} x^2 + y^2 &\equiv 0 + 0 \equiv 0 (\text{mód} 4) \\ x^2 + y^2 &\equiv 1 + 0 \equiv 1 (\text{mód} 4) \\ x^2 + y^2 &\equiv 0 + 1 \equiv 1 (\text{mód} 4) \\ x^2 + y^2 &\equiv 1 + 1 \equiv 2 (\text{mód} 4). \end{aligned}$$

Esto muestra que ningún entero $\equiv 3 (\text{ mód } 4)$ puede ser una suma de dos cuadrados. Lo que es más sorprendente es que si p es un primo $\equiv 1 (\text{ mód } 4)$, p siempre se puede expresar como suma de dos cuadrados.

Teorema 1.1 (Fermat). *Para todos los números primos $p \neq 2$, se tiene que*

$$p = a^2 + b^2, \ a, b \in \mathbb{Z} \iff p \equiv 1 (\text{mód} 4).$$

Este teorema cuenta con muchas demostraciones hoy en día. Sin embargo, una bastante importante y que es considerada "natural", pasa por estudiar el dominio de los enteros Gaussianos

$$\mathbb{Z}[i] = \{\, a + bi \mid a, b \in \mathbb{Z} \,\}, \quad i = \sqrt{-1}.$$

En $\mathbb{Z}[i]$ la representación

$$p = x^2 + y^2$$

se puede escribir como $p = (x + iy)(x - iy)$, por lo que la pregunta se transforma en ¿cuándo y cómo se factoriza un primo $p \in \mathbb{Z}$ en $\mathbb{Z}[i]$?

Para esto, primero probamos lo siguiente.

PROPOSICIÓN 1.2. *El anillo $\mathbb{Z}[i]$ es Euclideano, y por lo tanto factorial (es decir, es un dominio de factorización única DFU).*

DEMOSTRACIÓN. Recordemos que un dominio entero R es Euclideano si existe una función $\varphi\colon R \setminus \{\, 0_R \,\} \to \mathbb{Z}_{\geq 0}$ tal que

(I) Si $a, b \in R \setminus \{\, 0_R \,\}$, entonces $\varphi(a) \leq \varphi(ab)$;
(II) Si $a, b \in R$ y $b \neq 0_R$, entonces existen $q, r \in R$ (no necesariamente únicos) tales que $a = qb + r$ con $r = 0_R$ ó $r \neq 0_R$ y $\varphi(r) < \varphi(b)$.

Es bien sabido que todo dominio entero Euclideano es un dominio de factorización única.

Definimos entonces la función

$$\begin{aligned} \varphi\colon \mathbb{Z}[i] \setminus \{\, 0 \,\} &\to \mathbb{Z}_{\geq 0} \\ \alpha &\mapsto |\alpha|^2, \end{aligned}$$

donde $|\alpha|$ es el módulo complejo, es deicr, si $\alpha = a + bi$, con $a, b \in \mathbb{Z}$, $|\alpha|^2 = (\sqrt{a^2 + b^2})^2 = a^2 + b^2$.

Es claro que si $\alpha, \beta \in \mathbb{Z}[i] \setminus \{\, 0 \,\}$ entonces

$$\varphi(\alpha) \leq \varphi(\alpha\beta)$$

pues $\varphi(\alpha) = |\alpha|^2$ y $\varphi(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2$ y $|\beta| \geq 1$. Entonces φ satisface la propiedad (I).

Para ver que φ satisface la propiedad (II), sean $\alpha, \beta \in \mathbb{Z}[i] \setminus \{\, 0 \,\}$ con $\beta \neq 0$. Debemos mostrar que existen enteros Gaussianos $\gamma, \rho \in \mathbb{Z}[i]$ tales que

$$\alpha = \gamma\beta + \rho \quad \text{con} \quad |\rho|^2 < |\beta|^2.$$

Ahora, note que en $\mathbb{C}$ se tiene que

$$\frac{\alpha}{\beta} = x + iy \quad \text{para algunos} \quad x, y \in \mathbb{R}.$$

De hecho, como $\alpha, \beta \in \mathbb{Z}[i]$, se tiene que $x, y \in \mathbb{Q}$. En $\mathbb{C}$, los enteros Gaussianos forman el retículo de puntos con coordenadas enteras, como se ve en la siguiente figura: Es claro entonces que el número complejo $\frac{\alpha}{\beta} = x + iy$ estará ubicado en alguno de los cuadrados determinados por este retículo: De la geometría de esta figura que la distancia de $\frac{\alpha}{\beta} = x + iy$ al punto más cercano en el retículo $\mathbb{Z}[i]$ es menor o igual que la mitad de la diagonal del cuadrado, es decir, que existe al menos un $\gamma \in \mathbb{Z}[i]$ tal que

$$\left| \frac{\alpha}{\beta} - \gamma \right| \leq \frac{\sqrt{2}}{2} < 1.$$

Definimos entonces $\rho = \alpha - \gamma\beta$. Luego, $\rho \in \mathbb{Z}[i]$ y

$$\begin{aligned} |\rho|^2 < |\beta|^2 &\iff |\rho| < |\beta| \\ &\iff |\alpha - \gamma\beta| < |\beta| \\ &\iff \left|\frac{\alpha}{\beta} - \gamma\right| < 1 \quad \text{(dividiendo por } |\beta| \text{ a ambos lados)}, \end{aligned}$$

pero esta última desigualdad ya fue establecida. Esto termina la demostración. □

Con este resultado, podemos demostrar el teorema de Fermat como sigue.

Demostración del teorema 1.1 de Fermat. ($\Rightarrow$) Esta dirección ya la discutimos.

($\Leftarrow$) Sea $p \equiv 1(\text{mód}4)$ un primo en $\mathbb{Z}_{\geq 1}$. Vamos a mostrar que p no es irreducible en $\mathbb{Z}[i]$, es decir, que exiten $\alpha, \beta \in \mathbb{Z}[i]$ ninguno de los cuales es una unidad en $\mathbb{Z}[i]$, tales que

$$p = \alpha \cdot \beta.$$

Definimos la norma

$$\begin{aligned} N\colon \mathbb{Z}[i] &\to \mathbb{Z}_{\geq 0} \\ \alpha = a + bi &\mapsto N(\alpha) \colon = |\alpha|^2 = a^2 + b^2. \end{aligned}$$

Es un ejercicio ver que la norma satisface:

(I) $N(\alpha) = 0 \iff \alpha = 0$

(II) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$

(III) $N(\alpha) = 1 \iff \alpha$ es una unidad en $\mathbb{Z}[i]$.

Con esto, si p se descompone como

$$p = \alpha\beta$$

conα, β no unidades en $\mathbb{Z}[i]$, tomando normas tendríamos que

$$\begin{aligned} N(p) &= N(\alpha) \cdot N(\beta) \\ \Rightarrow p^2 &= N(\alpha) \cdot N(\beta). \end{aligned}$$

Como ninguno de α o β es una unidad y las unidades satisfacen $N(\alpha) = 1$, se debe tener que $N(\alpha) = N(\beta) = p$, es decir, si $\alpha = a + bi$,

$$p = N(\alpha) = a^2 + b^2,$$

lo que probaría el teorema.

Resta por ver entonces, que p no es irreducible en $\mathbb{Z}[i]$. Para esto, como $p \equiv 1(\text{mód}4)$, existe $n \in \mathbb{Z}$ tal que

$$p = 1 + 4n.$$

Luego, la congruencia

$$x^2 \equiv -1(\text{mód}p)$$

tiene la solución $x = (2n)! = \left(\frac{p-1}{2}\right)!$, pues por el teorema de Wilson

$$-1 \equiv (p-1)!(\text{mód}p)$$

y

$$\begin{aligned}(p-1)! = (4n)! &= (1\cdot 2\cdot \ldots \cdot 2n)\cdot(4n\cdot(4n-1)\cdot\ldots\cdot(2n+1)) \\ &= (1\cdot 2\cdot \ldots \cdot 2n)\cdot((p-1)\cdot(p-2)\cdot\ldots\cdot(p-2n)) \\ &\equiv (1\cdot 2\cdot \ldots \cdot 2n)\cdot((-1)\cdot(-2)\cdot\ldots\cdot(-2n))(\text{mód}p) \\ &\equiv (2n)!\cdot(-1)^{2n}\cdot(2n)!(\text{mód}p) \\ &\equiv [(2n)!]^2(\text{mód}p),\end{aligned}$$

por lo que

$$[(2n)!]^2 \equiv -1(\text{mód}p),$$

o sea que la congruencia

$$x^2 \equiv -1(\text{mód}p)$$

tiene solución. Como tal, $p \mid x^2+1$, es decir,

$$p \mid (x+i)(x-i) \quad \text{en} \quad \mathbb{Z}[i].$$

Luego, p no puede ser un elemento primo en $\mathbb{Z}[i]$ pues entonces se tendría que $p|x+i$ ó $p \mid x-i$ y esto implicaría que

$$\frac{x}{p} \pm \frac{i}{p} \in \mathbb{Z}[i],$$

lo cual es falso. Entonces, como $\mathbb{Z}[i]$ es un dominio Euclideano, al no ser pirmo p en $\mathbb{Z}[i]$, tampoco es irreducible, y esto completa la demostración del teorema de Fermat.

□

Recuerde realizar el ejercicio de probar las propiedades de la norma. Con esto facilmente se corrobora la siguiente proposición.

PROPOSICIÓN 1.3. *El grupo de unidades del anillo $\mathbb{Z}[i]$ es el grupo de las raíces cuartas de la unidad, es decir*

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}.$$

Caracterizamos ahora los elementos irreducibles de $\mathbb{Z}[i]$, recuerde que dos elementos α, β de un anillo R son asociados si existe una unidad $u \in R$ tal que $\alpha = u\beta$. A su vez, el producto de un irreducible π con una unidad u es irreducible. Es decir, $u\pi$ es un elemento irreducible. Con esto tenemos el siguiente resultado.

TEOREMA 1.4. *Los elementos π en $\mathbb{Z}[i]$, hasta asociados, son los siguientes:*

1. $\pi = 1+i$,
2. $\pi = a+bi$, *con* $a^2+b^2 = p$ *y* $p \in \mathbb{Z}$ *tal que* $p \equiv 1(\text{mód}4)$ *y* $a > |b| > 0$.
3. $\pi = p$, *con* $p \equiv 3(\text{mód}4)$ *un primo en* $\mathbb{Z}$.

DEMOSTRACIÓN. Una dirección es fácil. Ahora, sea $\pi \in \mathbb{Z}[i]$ un irreducible. Hay que mostrar que π es uno de los números de la lista. Se tiene que

$$N(\pi) = \pi\cdot\overline{\pi} = p_1\cdot\ldots\cdot p_r, \quad \text{con} \quad p_i \in \mathbb{Z}_{\geq 1}, \quad \text{primos}.$$

Como π es irreducible (y por lo tanto primo pues $\mathbb{Z}[i]$ es un DFU), $\pi \mid p = p_i$ para algún p_i, por lo que $N(\pi) \mid N(p) = p^2$.

- $N(\pi) = p \Rightarrow p = \pi\overline{\pi} = (a+bi)(a-bi) \Rightarrow \pi = a+bi$ con $a^2+b^2 = p$.

- $N(\pi) = p^2 \Rightarrow \pi \sim p$ pues como $N(\pi) = p^2$ entonces $\pi\overline{\pi} = p^2 \Rightarrow \pi \mid p$ y así $\frac{p}{\pi} \in \mathbb{Z}[i]$ y $N\left(\frac{p}{\pi}\right) = 1$ por lo que $\frac{p}{\pi} \in \mathbb{Z}[i]^\times$. Es decir, $\pi \sim p$.

  Entonces, se debe tener $p \equiv 3(\text{mód}4)$ pues si no se tendría $p \equiv 1(\text{mód}\ 4)$ ó $p = 2$ y entonces como consecuencia del teorema 1.1 de Fermat de dos cuadrados, se tendría que

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

  y por ende p no sería irreducible.

□

De aquí nos preguntamos entonces:

¿Cómo se factorizan los primos $p \in \mathbb{Z}$ en los enteros Gaussianos?

- El número 2 se puede factorizar como

$$2 = 1^2 + 1^2 = (1 + i)(1 - i) = -i(1 + i)^2 \Rightarrow 2 \sim (1 + i)^2$$

  y entonces 2 es el cuadrado de un irreducible. En este caso diremos que 2 se ramifica (del inglés *ramifies*).
- $p \equiv 1(\text{mód}4)$ escinde como producto de dos irreducibles conjugados: $p = (a + bi)(a - bi)$ con $a + bi$ irreducible.
- Si $p \equiv 3(\text{mód}4)$ entonces p permanece primo y le llamamos inerte.

PROPOSICIÓN 1.5. *$\mathbb{Z}[i]$ consiste precisamente de los elementos de la extensión $\mathbb{Q}(i)|\mathbb{Q} = \{\, a + bi \mid a, b \in \mathbb{Q} \,\}$ que satisfacen la ecuación polinomial mónica*

$$x^2 + ax + b = 0$$

con coeficientees $a, b \in \mathbb{Z}$.

DEMOSTRACIÓN. Hay que mostrar que

$$\mathbb{Z}[i] = \left\{\, \alpha \in \mathbb{Q}(i) \mid \alpha \quad \text{es raíz de un polinomio} \quad x^2 + ax + b,\ a, b \in \mathbb{Z} \,\right\}.$$

Sea $\alpha = c + di \in \mathbb{Q}(i)$ entonces α es raíz del polinomio

$$\begin{aligned} f_\alpha(x) = (x - \alpha)(x - \overline{\alpha}) &= x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} \\ &= x^2 - 2cx + c^2 + d^2 \\ &= x^2 + ax + b,\ a = -2c,\ b = c^2 + d^2. \end{aligned}$$

Claramente si $c, d \in \mathbb{Z}$, entonces $a, b \in \mathbb{Z}$. Inversamente, si a y b son enteros, entonces $2c, 2d \in \mathbb{Z}$ y por tanto $c, d \in \frac{1}{2}\mathbb{Z}$. Ahora $4b = (2c)^2 + (2d)^2 \equiv 0(\text{mód}4)$ y así tanto $(2c)^2$ como $(2d)^2$ son congruentes a $0(\text{mód}4)$. Por lo tanto $c, d \in \mathbb{Z}$. □

2. Nociones básicas de Teoría de Cuerpos

En general si K, L son cuerpos y $\varphi\colon K \to L$ es un monomorfismo, decimos que L es una extensión de K. Denotamos por $L|K$ a la extensión. Como podemos identificar K con $\varphi(K)$, en general al hablar de extensiones simplemente asumiremos que es una inclusión $K \subset L$ de cuerpos. Le llamamos a K el cuerpo base.

Podemos ver a L como un K-espacio vectorial. Si se define la multiplicación escalar

$$\circ\colon K \times L \to L,\ (\alpha, \beta) \mapsto \alpha\beta$$

donde $\alpha\beta$ es simplemente la multiplicación en L.

DEFINICIÓN 2.1. El grado de extensión de la extensión $L|K$ es $\dim_K(L)$ y lo denotamos $[L:K]$. En el caso que $[L:K] < \infty$, diremos que $L|K$ es una extensión finita. Caso contrario se le llamará una extensión infinita.

EJEMPLO 2.2. Sea $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} | a, b \in \mathbb{Q} \right\}$. La extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ claramente es una extensión de $\mathbb{Q}$ de grado 2, es decir $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

EJEMPLO 2.3. $\mathbb{C}|\mathbb{R}$ es una extensión de grado $[\mathbb{C} : \mathbb{R}] = 2$ pues $\mathbb{C} = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i$ como un $\mathbb{R}$-espacio vectorial.

EJEMPLO 2.4. Sea $K = \mathbb{Q}(\sqrt[3]{2})$, veremos que $K|\mathbb{Q}$ es una extensión de grado $[K : \mathbb{Q}] = 3$ y que $\left\{ 1, \sqrt[3]{2}, \sqrt[3]{4} \right\}$ es una $\mathbb{Q}$-base para K, es decir, que

$$K = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q} \right\}.$$

2.1. Generadores de cuerpos.

DEFINICIÓN 2.5. Sea K una extensión de F. Si $X \subseteq K$ es un subconjunto, entonces el anillo $F[X]$ generado por F y X es la intersección de todos los subanillos de K que contienen a F y X. El cuerpo $F(X)$ generado por F y X es la intersección de todos los subcuerpos de K que contienen a F y X. Si $X = \{ a_1, \ldots, a_n \}$ es finito, escribimos $F[X] = F[[a_1, \ldots, a_n]$ y $F(X) = F(a_1, \ldots, a_n)$. Si X es finito, diremos que $F(X)$ es una extensión finitamente generada.

Podemos describir estos conjuntos de manera más explicita.

PROPOSICIÓN 2.6. *Sea $K|F$ una extensión y $a \in K$. Entonces*

$$F[a] = \{ f(a) | f \in F[x] \}$$
$$F(a) = \left\{ \frac{f(a)}{g(a)} \;\middle|\; f, g \in F[x],\ g(a) \neq 0 \right\}.$$

Más aún, $F(a)$ es el cuerpo de cocientes de $F[a]$.

Podemos generalizar a lo siguiente.

PROPOSICIÓN 2.7. *Sea $K|F$ una extensión y $a_1, \ldots, a_n \in K$. Entonces*

$$F[[a_1, \ldots, a_n] = \{ f(a_1, \ldots, a_n) | f \in F[x_1, \ldots, x_n] \}$$
$$F(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \;\middle|\; f, g \in F[x_1, \ldots, x_n],\ g(a_1, \ldots, a_n) \neq 0 \right\}.$$

Más aún, $F(a_1, \ldots, a_n)$ es el cuerpo de cocientes de $F[[a_1, \ldots, a_n]$.

En este curso, nuestro interés está en estudiar conjuntos de números algebraicos que definimos a continuación.

DEFINICIÓN 2.8.
- Si $K|F$ es una extensión de cuerpos, entonces diremos que un elemento α de K es algebraico sobre F si existe un polinomio no nulo $f \in F[x]$ con $f(\alpha) = 0$.
- Si α no es algebraico sobre F, decimos que α es trascendental sobre F.
- Si todo elementos de K es algebraico sobre F, decimos que K es algebraico sobre F, y que $K|F$ es una extensión algebraica.

EJEMPLO 2.9. La extensión $\mathbb{C}|\mathbb{R}$ es algebraica pues si $\alpha \in \mathbb{C}$ entonces α es la raíz del polinomio

$$p_\alpha(x) \colon = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2\Re(\alpha)x + |\alpha|^2$$

y claramente $p_\alpha \in \mathbb{R}[x]$.

EJEMPLO 2.10. Por el contrario, la extensión $\mathbb{R}|\mathbb{Q}$ no es algebraica. Por ejemplo es bien conocido que $\pi \approx 3{,}1415\ldots$ no satisface ninguna ecuación polinomial con coeficientes racionales. Este es un resultado de Lindemann de 1882.

DEFINICIÓN 2.11. Si α es algebraico sobre un cuerpo F, el polinomio minimal de α, es polinomio mónico irreducible p de menor grado en $F[x]$ para el cual $p(\alpha) = 0$. Denotamos $\text{mín}(F, \alpha)$.

EJEMPLO 2.12. Es importante recalcar que el polinomio minimal depende del cuerpo base.

- $\text{mín}(i, \mathbb{Q}) = x^2 + 1$,
- $\text{mín}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$,
- $\text{mín}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$,
- $\text{mín}(i, \mathbb{C}) = x - i$,

Las propiedades de los polinomios minimales se resumen en la siguiente proposición.

PROPOSICIÓN 2.13. *Sea $K|F$ una extensión y $\alpha \in K$ algebraico sobre F. Entonces se tiene lo siguiente:*

(I) El polinomio minimal $\text{mín}(F, \alpha)$ *es irreducible sobre F.*
(II) Si $g \in F[x]$, entonces $g(\alpha) = 0$ si y sólo si $\text{mín}(F, \alpha) \mid g$.
(III) Si $\deg(\text{mín}(F, \alpha))$*, entonces los elementos $1, \alpha, \ldots, \alpha^{n-1}$ forman una base para $F(\alpha)$ sobre F, y por lo tanto $[F(\alpha) : F]$ coincide con el grado del polinomio minimal. Más aún, en este caso vale $F[\alpha] = F(\alpha)$.*

EJEMPLO 2.14. Considere la extensión $\mathbb{Q}(\sqrt[5]{3})|\mathbb{Q}$. Note que $\sqrt[5]{3}$ es raíz del polinomio $p(x) = x^5 - 3$ y este polinomio es irreducible sobre $\mathbb{Q}$, basta aplicar el criterio de Eisenstein. Por lo tanto $x^5 - 3$ es el polinomio minimal de $\sqrt[5]{3}$ sobre $\mathbb{Q}$.

Por la proposición concluimos que $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$ y que los elementos $1, \sqrt[5]{3}, 3^{\frac{2}{5}}, 3^{\frac{3}{5}}, 3^{\frac{4}{5}}$ forman una $\mathbb{Q}$-base para $\mathbb{Q}(\sqrt[5]{3})$.

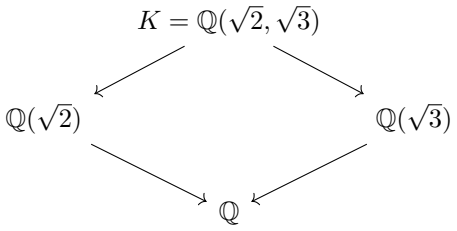
Un teorema básico en la teoría es el siguiente, que nos da la propiedad de multiplicatividad de grados en una cadena de extensiones.

TEOREMA 2.15 (Teorema de la torre). *Sean $F \subseteq L \subseteq K$ cuerpos. Entonces vale*

$$[K : F] = [K : L][L : F].$$

La idea de la demostración básicamente es que si $\{ a_i \}$ es una base para $L|F$ y $\{ b_j \}$ es una base para $K|L$, entonces el conjunto de productos $\{ a_i b_j \}$ es una base para $K|F$.

EJEMPLO 2.16. Considere $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note que se tiene las inclusiones $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq K$ y $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq K$. Gráficamente podemos verlo como el siguiente retículo:



Una base para $K|\mathbb{Q}(\sqrt{2})$ es $\{ 1, \sqrt{3} \}$ y una base para $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ es $\{ 1, \sqrt{2} \}$. Por lo tanto una base para $K|\mathbb{Q}$ es el conjunto de productos $\{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \}$. Además, $[K : \mathbb{Q}] = 4$.

El nombre del teorema anterior se debe a que a una cadena de extensiones de cuerpos

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n$$

se le suele conocer como una torre de cuerpo. Usando el teorema de la torre podemos demostrar lo siguiente.

TEOREMA 2.17. *Si $K|F$ es una extensión de cuerpos finita, entonces K es algebraico y finitamente generado sobre F.*

TEOREMA 2.18. *Si $K|F$ es una extensión, cada $\alpha_i \in K$ es algebraico sobre F para $i = 1, \ldots, n$, entonces $F[\alpha_1, \ldots, \alpha_n]$ es una extensión de cuerpos finita de F con*

$$[F[\alpha_1, \ldots, \alpha_n] : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

COROLARIO 2.19. *Si $K|F$ es una extensión, entonces un elemento $\alpha \in K$ es algebraico sobre F si y sólo si $[F(\alpha) : F] < \infty$. Además, si $[K : F] < \infty$ entonces $K|F$ es una extensión algebraica.*

También la propiedad de ser algebraica es transitiva sobre cadenas de extensiones.

TEOREMA 2.20. *Sea $F \subseteq L \subseteq K$ una torre de cuerpos. Si $L|F$ y $K|L$ son algebraicas, entonces $K|F$ es algebraica.*

DEFINICIÓN 2.21. Sea $K|F$ una extensión. El conjunto

$$\{ \alpha \in K \mid \alpha \quad \text{es algebraico sobre} \quad F \}$$

se llama la clausura algebraica de F en K.

TEOREMA 2.22. *Sea $K|F$ una extensión y L, la clausura algebraica de F en K. Entonces L es un cuerpo y por tanto es la extensión algebraica de F más grande que está contenida en K.*

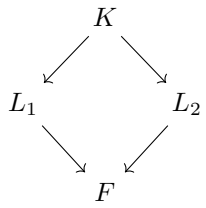
DEMOSTRACIÓN. Sean $\alpha, \beta \in L$. Como α, β son algebraicos sobre F, el cuerpo $F(\alpha, \beta)$ es de dimensión finita sobre F y por lo tanto $F(\alpha, \beta)|F$ es algebraica. Esto implica que $F(\alpha, \beta) \subseteq L$ y como $\alpha \pm \beta, \alpha\beta$ y $\frac{\alpha}{\beta}$ (para $\beta \neq 0$) están en $F(\alpha, \beta)$, estos también están en L. Esto prueba que L es un cuerpo. □

EJEMPLO 2.23. Considere la extensión $\mathbb{C}|bQ$. La clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$ se denota por

$$\overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \mid \alpha \quad \text{es algebraico sobre} \quad \mathbb{Q} \}.$$

Por el teorema anterior, $\overline{\mathbb{Q}}$ es un subcuerpo de $\mathbb{C}$. Es un ejercicio ver que $\overline{\mathbb{Q}}|\mathbb{Q}$ es una extensión infinita. En buena medida, el estudio que haremos en el curso se concentra en los subcuerpos de $\overline{\mathbb{Q}}|\mathbb{Q}$.

2.2. El compuesto de extensiones de cuerpos. Sea F un cuerpo y sean $L_1|F, L_2|F$ extensiones contenidas en un cuerpo común K, como en la figura siguiente.



Entonces, el compuesto L_1L_2 de L_1 y L_2 es el subcuerpo de K generado por L_1 y L_2. Es decir, $\overline{L_1L_2 = L_1}(L_2) = L_2(L_1)$.

Ejemplo 2.24. El compuesto de $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{3})$ es $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Un concepto sumamente importante para nosotros es el de automorfismos y homomorfismos de cuerpos. Sean $K|F$ y $L|F$ extensiones. Un F-homomorfismo $\sigma\colon K \hookrightarrow L$ es un homomorfismo de anillos tal que $\sigma(\alpha) = \alpha$ para $\alpha \in F$. Es decir, $\sigma\,|_F = \mathrm{id}_F$. Si σ es biyectivo, decimos que σ es un F-isomorfismo. Además un F-isomorfismo $\sigma : K \to K$ se llamará un F-automorfismo.

Algunas propiedades básicas son las siguientes:

1. Un F-homomorfismo $\sigma\colon K \to L$ es una transformación lineal de F-espacios vectoriales. Esto pues si $a \in F$ y $\alpha \in K$, entonces $\sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\sigma(\alpha)$.
2. τ es inyectivo.
3. Si $[K : F] = [L : F] < \infty$, entonces τ también es sobreyectivo, por el teorema de rango y nulidad por ejemplo. Por ende todo F-homomorfismo entre extensiones finitas de la misma dimensión es un F-isomorfismo.
4. Si $K|F$ es una extensión finita, entonces todo F-isomorfismo $\sigma\colon K \to K$ es un F-automorfismo.

El siguiente es uno de los objetos más importantes de la Teoría de Galois.

Definición 2.25 (Grupo de Galois). Sea $K|F$ una extensión de cuerpos. El grupo de Galois de $K|F$ es el conjunto

$$\mathrm{Gal}(K|F)\colon = \{\, \tau\colon K \to K \mid \tau \quad \text{es un} \quad F\text{-automorfismo} \,\}.$$

El siguiente resultado nos dice que si $K = F(X)$ es el cuerpo generado por un conjunto X sobre F, entonces los F-automorfismos de K se pueden determinar respecto a su acción sobre los elementos de X.

Proposición 2.26. *Sea $K = F(X)$ una extensión de cuerpos de F generada sobre F por un subconjunto X de un cuerpo K. Si $\sigma, \tau \in \mathrm{Gal}(K|F)$ y $\sigma|_X = \tau|_X$, entonces $\sigma = \tau$. Por lo tanto, los F-automorfismos de K están determinados por su acción sobre un conjunto generador.*

Proposición 2.27. *Sea $\sigma\colon K \to L$ un F-homomorfismo y sea $\alpha \in K$ algebraico sobre F. Si $f \in F[x]$ y $f(\alpha) = 0$, entonces $f(\sigma(\alpha)) = 0$. Por lo tanto, σ permuta las raíces de* $\mathrm{mín}(F, \alpha)$. *Además,* $\mathrm{mín}(F, \alpha) = \mathrm{mín}(F, \sigma(\alpha))$.

Un corolario de esto es lo siguiente.

COROLARIO 2.28. *Si* $[K : F] < \infty$, *entonces* $|\operatorname{Gal}(K|F)| < \infty$.

EJEMPLO 2.29. Considere la extensión $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. Sea σ un $\mathbb{Q}$-automorfismo. Entonces σ está completamente determinado por su acción sobre $\sqrt{2}$. Como el polinomio minimal de $\sqrt{2}$ sobre $\mathbb{Q}$ es $p(x) = x^2 - 2$ y sus raíces son $\pm\sqrt{2}$, debe tenerse $\sigma(\sqrt{2}) = \pm\sqrt{2}$.