Las leyes de reciprocidad de Gauss a Artin

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. Julio de 2018

Resumen

En este minicurso hablaré de las leyes de reciprocidad en la teoría de números. El primer resultado de este tipo fue la ley de reciprocidad cuadrática descubierta por Gauss y publicada en su tratado "Disquisitiones Arithmeticae" en 1801. Luego hubo varias generalizaciones que culminaron en la ley de reciprocidad establecida por Emil Artin en 1930. Aquí trataré de explicar los enunciados y la relación entre estos teoremas.

Para preparar estas charlas he usado entre otras cosas mis apuntes de un curso impartido por Keith Conrad en Yaroslavl, Rusia, en 2011.

1 El símbolo de Legendre y la ley de reciprocidad cuadrática

lunes, 9 de julio

La primera lección será elemental: voy a asumir solamente que el lector conozca qué es un número primo y una congruencia módulo n.

Para un número fijo $n = 2, 3, 4, 5, \ldots$ se dice que un entero $a \in \mathbb{Z}$ es un **cuadrado** módulo n si $a \equiv x^2 \pmod{n}$ para algún $x \in \mathbb{Z}$. Empecemos por la definición del **símbolo de Legendre**.

1.1. Definición. Para un número primo impar[*] p y un número entero a tal que $p \nmid a$, pongamos

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } a \text{ es un cuadrado módulo } p, \\ -1, & \text{si } a \text{ no es un cuadrado módulo } p, \end{cases}$$

y si $p \mid a$, definamos

$$\left(\frac{a}{p}\right) := 0.$$

1.2. Ejemplo. Los cuadrados módulo 7 son $0, 1, 2, 4$, así que $\left(\frac{3}{7}\right) = -1$. ▲

He aquí algunas propiedades del símbolo de Legendre.

1.3. Proposición.

1) *Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

2) *Se cumple la* ***congruencia de Euler:***

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

3) *El símbolo de Legendre es multiplicativo: para cualesquiera $a, b \in \mathbb{Z}$ se tiene*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

[*] El número 2 es un primo muy especial en varios aspectos y por el momento lo vamos a descartar. Como dice una broma intraducible, *all primes are odd and 2 is the oddest*.

Se sigue que para calcular un símbolo de Legendre es suficiente saber los valores de $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ y $\left(\frac{q}{p}\right)$ para q primo impar. Por ejemplo,

$$\left(\frac{-30}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{5}{p}\right).$$

La propiedad 1) es evidente: la definición del símbolo de Legendre depende solamente del resto de a módulo p. Las propiedades 2) y 3) ya no son tan inmediatas: por ejemplo, 3) quiere decir que el producto de dos cuadrados es un cuadrado (esto es obvio) y el producto de dos no-cuadrados es un cuadrado (ya no es tan obvio). Para deducir 2) y 3), se puede usar el hecho de que los restos módulo p invertibles (en este caso no nulos) respecto a la multiplicación formen un grupo *cíclico* $(\mathbb{Z}/p\mathbb{Z})^\times$. En otras palabras, existe un resto $[x]_p$ tal que sus potencias nos dan todos los restos no nulos. Luego, las potencias pares de $[x]_p$ son cuadrados y las potencias impares no son cuadrados.

El símbolo de Legendre puede ser calculado mediante el siguiente famoso resultado que será el punto de partida para nuestro minicurso.

1.4. Teorema (La ley de reciprocidad cuadrática).

1) Para diferentes primos impares p y q se tiene

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{si } p \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right) & \text{si } p \text{ y } q \equiv 3 \pmod 4. \end{cases}$$

2)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

3)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1,7 \pmod 8, \\ -1, & p \equiv 3,5 \pmod 8. \end{cases}$$

La primera parte es la **ley de reciprocidad principal**, mientras que las partes 2) y 3) se conocen como las **leyes de reciprocidad suplementarias**.

Evidentemente, el símbolo $\left(\frac{a}{p}\right)$ es una función periódica en a, de periodo p. Resulta que es también periódica en p en el siguiente sentido.

1.5. Proposición. *Sean p y q dos primos impares.*

- *Si $p \equiv q \pmod{4a}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*
- *Si $p \equiv -q \pmod{4a}$, entonces $\left(\frac{a}{p}\right) = \operatorname{sgn} a \cdot \left(\frac{a}{q}\right)$, donde $\operatorname{sgn} a = \pm 1$ es el signo de a.*

La propiedad de arriba es *equivalente* a la ley de reciprocidad cuadrática y de hecho fue descubierta por Euler en 1744, pero sin prueba. El problema fue resuelto por Gauss: en su tratado "Disquisitiones Arithmeticae" ("Investigaciones aritméticas") aparecen ocho pruebas diferentes, y hoy en día se conocen alrededor de 250[*]. Creo que esto es un buen motivo para no dar *ninguna* prueba de la reciprocidad cuadrática aquí: el lector encontrará alguna en cualquier curso o libro de texto de la teoría de números elemental. Nuestro objetivo no es *probar* el teorema, sino *entenderlo*.

[*] Véase http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

1.6. Ejemplo. Tenemos

$$\left(\frac{14}{57}\right) = \left(\frac{2}{57}\right)\left(\frac{7}{57}\right) = (+1)\cdot\left(\frac{1}{7}\right) = +1.$$

Aquí hemos usado que $57 \equiv 1 \pmod 8$ y $57 \equiv 1 \pmod 7$...

Hay solo un pequeño problema: $57 = 3\cdot 19$ es un número compuesto, así que el símbolo de Legendre $\left(\frac{14}{57}\right)$ no está definido. En realidad, si 14 fuera un cuadrado módulo 57, esta también sería un cuadrado módulo 3, pero $14 \equiv 2 \pmod 3$ no lo es. ▲

Esto significa que las propiedades del símbolo de Legendre no se pueden aplicar de modo puramente formal cuando el mismo símbolo no tiene sentido. Sin embargo, el error tonto que acabamos de cometer nos llevará a algunos resultados importantes en la siguiente sección.

1.7. Ejemplo. El número 2017 sí que es primo. Usando las congruencias

$$2017 \equiv 1 \pmod 4, \quad 2017 \equiv 1 \pmod 3, \quad 2017 \equiv 2 \pmod 5,$$

calculamos a partir de la ley de reciprocidad que

$$\left(\frac{15}{2017}\right) = \left(\frac{3}{2017}\right)\left(\frac{5}{2017}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = (+1)(-1) = -1.$$

Entonces, 15 no es un cuadrado módulo 2017. De la misma manera, podemos calcular

$$\left(\frac{21}{2017}\right) = \left(\frac{3}{2017}\right)\left(\frac{7}{2017}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{7}\right) = +1,$$

y por lo tanto 21 es un cuadrado módulo 2017. ▲

Note que aunque el último cálculo nos dice que la congruencia $x^2 \equiv 21 \pmod{2017}$ tiene una solución, el símbolo de Legendre no ayuda a encontrarla. El **algoritmo de Cipolla**[*] es un método eficaz *probabilístico*[**] de encontrar a este x. El lector puede buscar más información en internet.

En nuestro caso, podemos ver con ayuda de computadora que

$$1843^2 \equiv 21 \pmod{2017}.$$

El número 2017 es el último año primo, mientras que 1843 es el año cuando Hamilton descubrió los cuaterniones.

2 El símbolo de Jacobi

El símbolo de Legendre $\left(\frac{a}{p}\right)$ está definido solamente para p primo impar. Si en lugar de p tenemos un número compuesto, podemos tratar de aplicar las mismas reglas, pero como vimos en 1.6, esto nos puede llevar a conclusiones equivocadas. Para entender qué está pasando, se introduce la siguiente generalización.

2.1. Definición. Sea n un entero positivo impar y a cualquier entero. Sea $n = p_1 p_2 \cdots p_k$ la factorización de n en números primos. Entonces, el **símbolo de Jacobi** $\left(\frac{a}{n}\right)$ está definido como el siguiente producto de los símbolos de Legendre:

$$\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

[*] Véase http://people.math.gatech.edu/~mbaker/pdf/cipolla2011.pdf

[**] Para un ejemplo de algoritmos probabilísticos, véase la siguiente sección.

Notamos que cuando $\mathrm{mcd}(a,n)=1$, tenemos $\left(\frac{a}{p_i}\right)=\pm 1$ para todo i, así que $\left(\frac{a}{n}\right)=\pm 1$. En el caso contrario, si $\mathrm{mcd}(a,n)\neq 1$, algún primo p_i divide a a, y luego $\left(\frac{a}{p_i}\right)=0$ y $\left(\frac{a}{n}\right)=0$.

Cuando $\left(\frac{a}{n}\right)=-1$, entre los símbolos de Legendre $\left(\frac{a}{p_i}\right)$ hay por lo menos uno que es igual a -1, así que a no es un cuadrado módulo n. Sin embargo, cuando $\left(\frac{a}{n}\right)=+1$, esto *no significa* que a sea un cuadrado módulo n: podemos tener $\left(\frac{a}{p_i}\right)=-1$ para algunos i, solo sabemos que esto ocurre para un número par de los p_i.

2.2. Ejemplo. Tenemos

$$\left(\frac{14}{57}\right):=\left(\frac{14}{3}\right)\left(\frac{14}{19}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{19}\right)\left(\frac{7}{19}\right)=-\left(\frac{19}{7}\right)=-\left(\frac{5}{7}\right)=+1.$$

Aquí hemos usado que $\left(\frac{2}{3}\right)=-1$ (obvio), $\left(\frac{2}{19}\right)=-1$ (por la ley de reciprocidad suplementaria correspondiente) y $\left(\frac{7}{19}\right)=-\left(\frac{19}{7}\right)$ (por la ley de reciprocidad principal, dado que $7\equiv 19\equiv 3 \pmod 4$). Sin embargo, ya notamos que 14 no es un cuadrado módulo 57. ▲

El símbolo de Jacobi tiene las siguientes propiedades.

2.3. Proposición.

1) Si $a\equiv b \pmod n$, entonces $\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)$.

2) Se cumple $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

3) También $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

4) Si m y n son diferentes enteros positivos impares, entonces

$$\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

5)

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}.$$

6)

$$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}.$$

Las partes 1)–3) se deducen de la definición del símbolo de Jacobi y las propiedades similares para el símbolo de Legendre (use la inducción sobre el número de los factores primos en n). Las partes 4)–6) son análogas a la ley de reciprocidad.

2.4. Ejemplo. Ya que $21\equiv 1 \pmod 4$, tenemos $\left(\frac{21}{2017}\right)=\left(\frac{2017}{21}\right)$. Luego, $2017\equiv 1 \pmod{21}$, y por lo tanto $\left(\frac{2017}{21}\right)=\left(\frac{1}{21}\right)=+1$. Aunque hemos usado las propiedades del símbolo de Jacobi, $\left(\frac{21}{2017}\right)$ es un símbolo de Legendre legítimo, y el resultado de este calculo nos permite concluir que 21 es un cuadrado módulo 2017. ▲

2.5. Ejemplo. Calculemos $\left(\frac{30}{127}\right)$. No podemos relacionar este símbolo con $\left(\frac{127}{30}\right)$ porque 30 es par. Sin embargo, podemos escribir

$$\left(\frac{30}{127}\right)=\left(\frac{2}{127}\right)\left(\frac{15}{127}\right).$$

Luego, $127\equiv 7 \pmod 8$, así que $\left(\frac{2}{127}\right)=+1$. También $127\equiv 3 \pmod 4$ y $15\equiv 3 \pmod 4$, y la ley de reciprocidad para el símbolo de Jacobi nos dice que

$$\left(\frac{15}{127}\right)=-\left(\frac{127}{15}\right)=-\left(\frac{7}{15}\right)=+\left(\frac{15}{7}\right)=\left(\frac{1}{7}\right)=+1.$$

Entonces, $\left(\frac{30}{127}\right)=+1$. ▲

El último ejemplo explica la utilidad del símbolo de Jacobi: para calcular $\left(\frac{a}{n}\right)$ (y en particular $\left(\frac{a}{p}\right)$ donde p es un primo impar) mediante la ley de reciprocidad, no hace falta factorizar a en números primos como lo haríamos en el caso del símbolo de Legendre. La única parte problemática es que tenemos que sacar un posible factor 2^k cuando a es par. Y de hecho, *se supone* que no existe ningún algoritmo eficaz (polinomial) de factorización de un número en primos (en esta conjetura se basa una gran parte de la criptografía), pero el factor 2^k se encuentra fácilmente. Módulo este pequeño detalle, el cálculo del símbolo de Jacobi consiste en reducciones consecutivas de un número módulo otro. Esto es algo similar al algoritmo de Euclides.

Sería interesante interpretar de alguna manera el símbolo $\left(\frac{a}{n}\right)$ para n compuesto. Este no necesariamente detecta si a es un cuadrado módulo n, pero refleja lo siguiente. Cuando $\operatorname{mcd}(a,n)=1$, tenemos $\left(\frac{a}{n}\right)=\pm 1$. En este caso a es un número invertible módulo n y la aplicación

$$\begin{aligned} m_a\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z},\\ [x]_n &\mapsto [ax]_n \end{aligned}$$

es biyectiva; es decir, una permutación del conjunto $\{[0]_n,[1]_n,\dots,[n-1]_n\}$. Notamos que al multiplicar un elemento invertible por a se obtiene también un elemento invertible, así que m_a se restringe a una biyección

$$\begin{aligned} m_a\colon (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times,\\ [x]_n &\mapsto [ax]_n \end{aligned}$$

(permutación de $(\mathbb{Z}/n\mathbb{Z})^\times = \{[x]_n \mid \operatorname{mcd}(x,n)=1\}$). Zolotariov* descubrió que el símbolo de Jacobi es precisamente el signo de esta permutación:

$$\left(\frac{a}{n}\right) = \operatorname{sgn} m_a.$$

2.6. Ejemplo. Tenemos $\left(\frac{5}{21}\right)=\left(\frac{21}{5}\right)=\left(\frac{1}{5}\right)=1$. Los restos módulo 21 invertibles son

$$1,2,4,5,8,10,11,13,16,17,19,20.$$

Se puede calcular que la multiplicación de estos números por 5 nos da la permutación

$$m_5 = (1\ 5\ 4\ 20\ 16\ 17)\,(2\ 10\ 8\ 19\ 11\ 13);$$

es decir, la composición de dos permutaciones cíclicas disjuntas

$$1\mapsto 5\mapsto 4\mapsto 20\mapsto 16\mapsto 17\mapsto 1 \quad \text{y} \quad 2\mapsto 10\mapsto 8\mapsto 19\mapsto 11\mapsto 13\mapsto 2.$$

Cada uno de estos ciclos tiene orden 6, y entonces el signo negativo. Luego,

$$\operatorname{sgn} m_5 = (-1)\cdot(-1) = +1 = \left(\frac{5}{21}\right).$$

▲

Al comparar nuestras listas de propiedades del símbolo de Jacobi y el símbolo de Legendre, se nota que el último cumple una propiedad especial: la congruencia de Euler. Tenemos

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod n,$$

si n es un primo impar. Si n no es primo, para esta congruencia hay contraejemplos, y de hecho muchos:

$$\{[a]_n \mid a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \mod n\} \geq n/2.$$

*Yegor Ivánovich Zolotariov (1847–1878), matemático ruso, de San Petersburgo. Obtuvo varios resultados importantes, pero murió joven atropellado por un tren.

2.7. Ejemplo. Tenemos $\left(\frac{5}{21}\right) = 1$, mientras que

$$5^{10} = 25^5 \equiv 4^5 \equiv 1024 \equiv 16 \pmod{21}.$$

▲

Esta falla de la congruencia de Euler para n compuesto se usa en el **test de primalidad de Solovey–Strassen**. Es un algoritmo *probabilístico* que comprueba si n es un número primo. Se escoge un número a de manera aleatoria y se calculan por separado $a^{\frac{n-1}{2}}$ y $\left(\frac{a}{n}\right)$. Si la congruencia de Euler no se cumple, entonces n no es primo. Si la congruencia se cumple, el proceso se repite *hasta que estemos convencidos* de que n sea primo con una probabilidad suficientemente alta. Esto es posible, puesto que para n compuesto hay muchos a que dan un contraejemplo. En realidad, bajo la **hipótesis de Riemann generalizada** (!) hay un contraejemplo bastante pequeño

$$a \leq 2\,(\log n)^2.$$

El test de Solovay–Strassen es uno de los primeros algoritmos probabilísticos[*] y fue descubierto en los años 70 del siglo pasado. Sin embargo, en la misma época apareció el **test de Rabin–Miller** que es más rápido, y por esto el test de Solovay–Strassen tiene más interés histórico.

También hay que mencionar que en 2002 Agrawal, Kayal y Saxena encontraron un algoritmo determinista (no probabilístico), eficaz (polinomial) e independiente de cualquier hipótesis (a diferencia de los algoritmos de Solovay, Strassen, Rabin y Miller) que verifica la primalidad. Esto es uno de los resultados más importantes en la teoría de computación: ya que *conjeturalmente* no existen algoritmos eficaces de factorización, fue bastante sorprendente por fin encontrar un test de primalidad eficaz. A pesar de esto, el resultado de Agrawal, Kayal y Saxena tiene más importancia teórica: en práctica (por ejemplo, en las aplicaciones criptográficas), es suficiente tener números que son primos con una probabilidad muy alta y bajo la hipótesis de Riemann (que por supuesto es cierta, solo que no ha sido demostrada :-)

3 Los números p-ádicos

martes, 10 de julio

Para ver otra faceta de la ley de reciprocidad, necesitaremos los números p-ádicos. Esta sección contiene un resumen muy breve y pragmático; para más detalles, el lector puede consultar, por ejemplo, mis apuntes

cadadr.org/san-salvador/2018-04-numeros-p-adicos/numeros-p-adicos.pdf

3.1. Definición. Sea n un número entero no nulo. Para todo primo p el número $v_p(n)$ se define como la potencia de p que aparece en la factorización de n:

$$n = \pm \prod_{p \text{ primo}} p^{v_p(n)}.$$

Además, si $n = 0$, pongamos

$$v_p(0) := \infty.$$

El número $v_p(n)$ se llama la **valuación p-ádica** de n. La **ńorma p-ádica** se define mediante la fórmula

$$|n|_p := p^{-v_p(n)}.$$

Notamos que $|m - n|_p \leq p^{-k}$ significa que $m \equiv n \pmod{p^k}$.

3.2. Proposición. *La norma p-ádica se extiende a los números racionales mediante la fórmula*

$$\left|\frac{m}{n}\right|_p := \frac{|m|_p}{|n|_p}.$$

Se cumplen las siguientes propiedades.

[*] Otro test de primalidad probabilístico, menos eficaz, es el **test de Fermat** que busca contraejemplos para el pequeño teorema de Fermat $a^{n-1} \equiv 1 \pmod{n}$. La última congruencia funciona solo para n primo.

1) $|x|_p = 0$ *si y solo si* $x = 0$.

2) $|xy|_p = |x|_p \cdot |y|_p$.

3) $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ *y además, cuando* $|x|_p \neq |y|_p$*, se cumple la igualdad* $|x+y|_p = \max\{|x|_p, |y|_p\}$.

Esto podría ser un buen ejercicio para el lector. La propiedad 3) es más fuerte que la desigualdad triangular

$$|x+y| \leq |x| + |y|.$$

Por esto se dice que el valor absoluto habitual $|\cdot|$ es una **norma arquimediana**, mientras que las normas p-ádicas son **no arquimedianas**.

Recordemos del curso de análisis que los números reales surgen de la siguiente manera. No toda sucesión de Cauchy de números racionales converge a un número racional. Entonces, se puede considerar de manera formal el conjunto de todas las sucesiones de Cauchy en $\mathbb{Q}$ respecto a las operaciones

$$(x_n)_n \pm (y_n)_n := (x_n \pm y_n)_n, \quad (x_n)_n \cdot (y_n)_n := (x_n \cdot y_n)_n.$$

Se obtiene un anillo (muy grande). Las sucesiones que convergen a 0 forman un ideal maximal, y el cociente por este ideal es el cuerpo $\mathbb{R}$. Este proceso se llama la **completación**.

El mismo proceso de completación puede ser aplicado a las normas p-ádicas, solo que las sucesiones de Cauchy y los límites se toman respecto a $|\cdot|_p$.

3.3. Definición. El **cuerpo de los números p-ádicos** $\mathbb{Q}_p$ es la completación de $\mathbb{Q}$ respecto a la norma p-ádica.

Entonces, $\mathbb{Q}_p$ es una extensión del cuerpo $\mathbb{Q}$ (de hecho, no numerable). La norma $|\cdot|_p$ se extiende a $\mathbb{Q}_p$ mediante la fórmula

$$|(x_n)_n|_p := \lim_{n\to\infty} |x_n|_p,$$

y toda sucesión de Cauchy en $\mathbb{Q}_p$ converge respecto a este valor absoluto. La extensión de la norma satisface las mismas propiedades de 3.2. Para tratar de la misma manera a $\mathbb{R}$ y a los cuerpos p-ádicos $\mathbb{Q}_p$, vamos a denotar $\mathbb{R}$ por $\mathbb{Q}_\infty$: se puede imaginar que el valor absoluto habitual surge de cierto "primo infinito ∞".

3.4. Definición. El **anillo de los enteros p-ádicos** viene dado por

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

(Es fácil comprobar que esto es un anillo: hay que ocupar las propiedades de la norma p-ádica.)

Notamos que

$$\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} := \left\{ \frac{m}{n} \;\middle|\; p \nmid n \right\}.$$

3.5. Proposición. *El anillo de los enteros p-ádicos tiene las siguientes propiedades.*

1) Los elementos invertibles vienen dados por $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$.

2) Todo elemento de $\mathbb{Q}_p^\times$ *puede ser escrito de modo único como* $p^n u$ *donde* $n \in \mathbb{Z}$ *y* $u \in \mathbb{Z}_p^\times$*. Esto nos da un producto directo de grupos multiplicativos*

$$\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

3) El único ideal maximal de $\mathbb{Z}_p$ *es* $p\mathbb{Z}_p$.

4) Tenemos $\mathbb{Z}_p / p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$ *para todo* $n \geq 1$*, y en particular* $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{F}_p$.

Las propiedades 1)–3) son fáciles: de nuevo, se trata de las propiedades de las normas p-ádicas y un poco del álgebra conmutativa elemental. La propiedad 4) es mucho más profunda y usa el hecho de que $\mathbb{Q}_p$ sea la completación de $\mathbb{Q}$ respecto a $|\cdot|_p$.

Terminemos nuestro repaso de los números p-ádicos por el siguiente resultado importante.

3.6. Teorema (Lema de Hensel). *Sea $f(X) \in \mathbb{Z}_p[X]$ un polinomio con coeficientes en $\mathbb{Z}_p$. Supongamos que existe $x_0 \in \mathbb{Z}_p$ tal que*

$$|f(x_0)|_p < |f'(x_0)|_p^2.$$

Luego, existe un único $x \in \mathbb{Z}_p$ tal que $f(X) = 0$ y $|x - x_0|_p < |f'(x_0)|_p$.

Intuitivamente, x_0 es una aproximación inicial a una raíz de f, y el número x es una raíz de f que está en un entorno de x_0. La prueba es constructiva y se basa en el **método de Newton**: a partir de x_0 se considera la sucesión

$$x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)}$$

y se toma su límite p-ádico

$$x := \lim_{n\to\infty} x_n.$$

El método de Newton no necesariamente converge cuando las aproximaciones se consideran respecto al valor absoluto habitual, pero nunca falla en el mundo p-ádico. Para entender cómo funciona el lema de Hensel, consideremos su aplicación típica.

3.7. Proposición.

1) *Si p es un primo impar, entonces un número $u \in \mathbb{Z}_p^\times$ es un cuadrado en $\mathbb{Q}_p$ (es decir, existe $x \in \mathbb{Q}_p$ tal que $u = x^2$) si y solamente si u es un cuadrado en $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.*

2) *$u \in \mathbb{Z}_2^\times$ es un cuadrado en $\mathbb{Q}_2$ si y solamente si $u \equiv 1 \pmod 8$.*

Demostración. Veamos la parte 1). En una dirección, si tenemos $u = x^2$ en $\mathbb{Q}_p$, entonces $|x|_p^2 = |x^2|_p = |u|_p = 1$, lo que significa que también $x \in \mathbb{Z}_p^\times$. Reduciendo la identidad $u = x^2$ módulo p, se obtiene una identidad $\overline{u} = \overline{x}^2$ en $\mathbb{F}_p$.

En la otra dirección, supongamos que u es un cuadrado módulo p. Esto significa que el polinomio $f(X) := X^2 - u \in \mathbb{Z}_p[X]$ tiene una raíz módulo p: existe $x_0 \in \mathbb{Z}_p$ tal que

$$|f(x_0)|_p = |x_0^2 - u|_p \le 1/p.$$

Notamos que

$$|x_0|_p^2 = |x_0^2|_p = |x_0^2 - u + u|_p = \max\{\underbrace{|x_0^2 - u|_p}_{<1}, \underbrace{|u|_p}_{=1}\} = 1,$$

así que $|x_0|_p = 1$, y luego

$$|f'(x_0)|_p = |2x_0|_p = |2|_p \cdot |x_0|_p = 1.$$

Se cumple la desigualdad

$$|f(x_0)|_p < |f'(x_0)|_p^2 = 1,$$

y podemos aplicar el lema de Hensel para encontrar una raíz de $f(X)$ en $\mathbb{Z}_p$. Note que hemos usado que $|2|_p = 1$. Para $p = 2$ este argumento falla, y de hecho el criterio para los cuadrados en $\mathbb{Z}_2^\times$ es diferente.

En la parte 2), primero notamos que si $u = x^2$ para $u \in \mathbb{Z}_2^\times$, entonces la reducción módulo $8 = 2^3$ nos da $\overline{u} = \overline{x}^2$ para algunos $\overline{u}, \overline{x} \in (\mathbb{Z}/8\mathbb{Z})^\times$. Los residuos módulo 8 invertibles son $1, 3, 5, 7$. Luego,

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8.$$

Podemos concluir que todos los cuadrados en $\mathbb{Z}_2^\times$ se reducen a 1 módulo 8. Para ver que esto es una condición suficiente, notamos que si $u \equiv 1 \pmod 8$, entonces para el polinomio $f(X) = X^2 - u \in \mathbb{Z}_2[X]$ y $x_0 = 1$ se tiene

$$|f(x_0)|_2 = |1-u|_2 \le 1/8, \quad |f'(x_0)|_2 = |2|_2 = 1/2, \quad |f(x_0)|_2 > |f'(x_0)|_2^2,$$

y de nuevo se puede aplicar el lema de Hensel. ■

Hemos caracterizado los cuadrados en $\mathbb{Z}_p^\times$. Para describir los cuadrados en $\mathbb{Q}_p^\times$, se puede usar la descomposición $\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$. Dejo los detalles al lector.

4 El símbolo de Hilbert

4.1. Definición. Sea v un primo, posiblemente infinito. Para $a, b \in \mathbb{Q}_v^\times$ el **símbolo de Hilbert** está definido por

$$(a,b)_v := \begin{cases} +1, & \text{si } ax^2 + by^2 = 1 \text{ tiene una solución en } \mathbb{Q}_v, \\ -1, & \text{en el caso contrario.} \end{cases}$$

El caso de $v = \infty$ es fácil: ya sabemos resolver las ecuaciones reales $ax^2 + by^2 = 1$.

4.2. Ejemplo. Tenemos

$$(a,b)_\infty = \begin{cases} +1, & \text{si } a > 0 \text{ o } b > 0, \\ -1, & \text{en el caso contrario.} \end{cases}.$$

▲

Lo que no está claro es cómo calcular $(a,b)_p$ cuando $p < \infty$.

4.3. Ejemplo. Probemos que $(2,5)_3 = 1$. Tenemos que encontrar una solución de $2x^2 + 5y^2 = 1$ en $\mathbb{Q}_3$. Sea $x = 1$. Entonces, la ecuación nos dice que $y^2 = -\frac{1}{5} \in \mathbb{Z}_3^\times$. Notamos que $-\frac{1}{5} \equiv 1 \pmod 3$, puesto que

$$\left|1 - \left(-\frac{1}{5}\right)\right|_3 = \left|\frac{6}{5}\right|_3 = \frac{1}{3}.$$

Pero 1 es un cuadrado en $\mathbb{F}_3$, así que $y^2 = -1/5$ tiene una solución en $\mathbb{Q}_3$ según 3.7. ▲

Las siguientes propiedades siguen de la definición del símbolo de Hilbert.

4.4. Proposición.

1) $(a,b)_v = (b,a)_v$ *para cualesquiera* $a, b \in \mathbb{Q}_v^\times$.

2) $(a,1)_v = 1$ *para todo* $a \in \mathbb{Q}_v^\times$.

3) $(a, c^2 b)_v = (a,b)_v$ *para cualesquiera* $a, b, c \in \mathbb{Q}_v^\times$.

4) $(a, b^2)_v = 1$ *para cualesquiera* $a, b \in \mathbb{Q}_v^\times$.

Demostración. 1) es evidente. En 2), la ecuación es $ax^2 + y^2 = 1$, y podemos tomar $x = 0$, $y = 1$. En 3), basta hacer un cambio de variables $y' := cy$, y luego

$$a x^2 + c^2 b y^2 = 1 \iff a x^2 + b y'^2 = 1.$$

La propiedad 4) sigue de 2) y 3). ■

Para probar la propiedad más importante del símbolo de Hilbert, necesitamos otra caracterización.

4.5. Lema. *Supongamos que b no es un cuadrado en $\mathbb{Q}_v$. Consideremos la extensión cuadrática de cuerpos $\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v$. Su **norma** viene dada por*

$$N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}(x + y\sqrt{b}) = x^2 - b\,y^2.$$

Se tiene $(a,b)_v = 1$ si y solamente si a es la norma de algún $x + y\sqrt{b} \in \mathbb{Q}_v(\sqrt{b})$.

(Omití la prueba por falta de tiempo.)

4.6. Proposición. *El símbolo de Hilbert es multiplicativo: se tiene*

$$(aa', b)_v = (a,b)_v \cdot (a',b)_v$$

(y lo mismo para el segundo argumento, puesto que el símbolo es simétrico).

Bosquejo de la demostración. Si b es un cuadrado, entonces la propiedad se cumple, dado que $(a,b)_v = 1$ para cualesquiera x según la propiedad 4) de 4.4. Podemos entonces asumir que b no es un cuadrado. En este caso $(a,b)_v = 1$ si y solamente si a pertenece a la imagen del homomorfismo

$$N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v} \colon \mathbb{Q}_v(\sqrt{b})^\times \to \mathbb{Q}_v^\times$$

(la norma es siempre multiplicativa). Esto demuestra la identidad en los casos cuando $(a,b)_v = (a',b)_v = 1$ y cuando $(a,b)_v = \pm 1$, $(a',b)_v = \mp 1$. Efectivamente, si $a, a' \in \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$, entonces $aa' \in \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$. Si $a \in \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$, $a' \notin N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$, entonces $aa' \notin \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$.

El caso más interesante es cuando $(a,b)_v = (a',b)_v = -1$. Si $a \notin \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$ y $a' \notin \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$, se puede deducir que $aa' \in \operatorname{im} N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$ gracias al hecho de que la imagen de $N_{\mathbb{Q}_v(\sqrt{b})/\mathbb{Q}_v}$ tenga índice 2 en $\mathbb{Q}_v^\times$[*]. ■

4.7. Corolario. *Se tiene $(a^{-1}, b)_v = (a,b)_v$.*

Demostración. Tenemos

$$(a^{-1},b)_v\,(a,b)_v = (a^{-1}a, b)_v = (1,b)_v = 1.$$

Entonces, $(a^{-1},b)_v = (a,b)_v^{-1}$, pero el último símbolo es igual a ± 1 y por ende coincide con $(a,b)_v$. ■

Nuestro objetivo es probar e interpretar el siguiente resultado curioso.

4.8. Teorema (La ley de reciprocidad de Hilbert). *Para dos números racionales no nulos fijos $a, b \in \mathbb{Q}^\times$*

1) *$(a,b)_v = -1$ solo para un número finito de primos v;*
2) *se cumple*

$$\prod_v (a,b)_v = 1,$$

donde el producto es sobre todos los primos, incluso ∞, y este tiene sentido gracias a 1).

Podemos pensar en la fórmula $\prod_v (a,b)_v = 1$ como en un análogo multiplicativo de la fórmula $\sum_z \operatorname{Res}_z(f) = 0$ de análisis complejo.

miércoles, 11 de julio

Para calcular los símbolos de Hilbert se puede usar el lema de Hensel. Sin entrar en detalles, voy a formular la respuesta.

[*] No lo vamos a probar, pero es algo evidente y conocido en el caso de $v = \infty$: tenemos $\mathbb{R} = \mathbb{Q}_\infty$ con la única extensión $\mathbb{C} = \mathbb{R}(\sqrt{-1})$. La norma viene dada por

$$N_{\mathbb{C}/\mathbb{R}} \colon x + y\sqrt{-1} \mapsto x^2 + y^2.$$

Las normas de los números complejos no nulos forman el grupo $\mathbb{R}_{>0}$ que tiene índice 2 en $\mathbb{R}^\times$.

4.9. Lema. *Si p es un primo impar, entonces*

$$(u,u')_p = 1, \quad (u,p)_p = \left(\frac{u}{p}\right), \quad (p,p)_p = (-1)^{\frac{p-1}{2}},$$

para cualesquiera $u,u' \in \mathbb{Z}_p^\times$.

Si $p=2$, entonces

$$(u,u')_2 = \begin{cases} +1, & \text{si } u \text{ o } u' \equiv 1 \pmod 4, \\ -1, & \text{si } u \text{ y } u' \equiv 3 \pmod 4; \end{cases}$$

$$(u,2)_2 = \begin{cases} +1, & \text{si } u \equiv 1,7 \pmod 8, \\ -1, & \text{si } u \equiv 3,5 \pmod 8; \end{cases}$$

para cualesquiera $u,u' \in \mathbb{Z}_p^\times$, y además

$$(2,2)_2 = 1.$$

(La última fórmula es obvia: la ecuación $2x^2+2y^2=1$ tiene una solución $x=y=\frac{1}{2}$.)

Bosquejo de la demostración de la ley de reciprocidad de Hilbert. Puesto que $a,b \in \mathbb{Z}_p^\times$ para todo p, excepto un número finito, tenemos $(a,b)_p = 1$ casi para todo p, y el producto $\prod_v (a,b)_v$ es finito. Para comprobar que es igual a 1, notamos que gracias a la multiplicatividad y la simetría del símbolo de Hilbert, sería suficiente analizar los siguientes casos.

1) $a=-1$, $b=-1$. En este caso

$$(-1,-1)_\infty = -1,$$
$$(-1,-1)_2 = -1, \text{ ya que } -1 \equiv 3 \pmod 4,$$
$$(-1,-1)_p = +1 \text{ para } 2 < p < \infty, \text{ ya que } -1 \in \mathbb{Z}_p^\times.$$

2) $a=-1$, $b=2$.

$$(-1,2)_\infty = +1,$$
$$(-1,2)_2 = +1, \text{ ya que } -1 \in \mathbb{Z}_2^\times \text{ y } -1 \equiv 3 \pmod 4,$$
$$(-1,2)_p = +1 \text{ para } 2 < p < \infty, \text{ ya que } -1,2 \in \mathbb{Z}_p^\times.$$

3) $a=2$, $b=2$.

$$(2,2)_\infty = +1,$$
$$(2,2)_2 = +1,$$
$$(2,2)_p = +1 \text{ para } 2 < p < \infty, \text{ ya que } 2 \in \mathbb{Z}_p^\times.$$

4) $a=b=p$ impar.

$$(p,p)_\infty = +1,$$
$$(p,p)_2 = (p,p)_p = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4, \end{cases}$$
$$(p,p)_q = +1 \text{ para } 2 < q < \infty, q \neq p, \text{ ya que } p \in \mathbb{Z}_q^\times.$$

5) $a = -1$, $b = p$ impar.

$$(-1,p)_\infty = +1,$$
$$(-1,p)_2 = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4, \end{cases}$$
$$(-1,p)_p = \left(\frac{-1}{p}\right),$$
$$(-1,p)_q = +1.$$

6) $a = 2$, $b = p$ impar.

$$(2,p)_\infty = +1,$$
$$(2,p)_2 = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv 1,7 \pmod 8, \\ -1, & \text{si } p \equiv 3,5 \pmod 8, \end{cases}$$
$$(2,p)_p = \left(\frac{2}{p}\right),$$
$$(2,p)_q = +1.$$

7) $a = p$ y $b = q$ son primos impares diferentes.

$$(p,q)_\infty = +1,$$
$$(p,q)_2 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1, & \text{si } p \text{ o } q \equiv 1 \pmod 4, \\ -1, & \text{si } p \text{ y } q \equiv 3 \pmod 4, \end{cases}$$
$$(p,q)_p = \left(\frac{q}{p}\right),$$
$$(p,q)_q = \left(\frac{p}{q}\right).$$

En todos los casos la fórmula del producto se cumple. En el caso 5) esto sigue de la ley de reciprocidad suplementaria

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

En el caso 6) esto sigue de

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Finalmente, el último caso corresponde a la ley principal

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

■

5 Generalización a los cuerpos de números

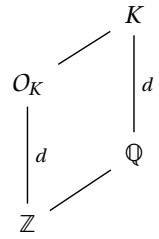
Notamos que los casos no triviales en la última prueba corresponden a la reciprocidad cuadrática. ¿A qué sirve entonces la reciprocidad de Hilbert, si es equivalente a la reciprocidad cuadrática de Gauss? Bueno, primero, es una fórmula muy bonita, donde todos los primos, incluso 2 y el primo infinito, juegan el mismo papel. Pero no es simplemente una cuestión de estética: gracias a esto, a diferencia de la ley de reciprocidad en la forma clásica, la fórmula $\prod_v (a,b)_v = 1$ admite generalizaciones directas.

5.1. Definición. Sea K una extensión finita de $\mathbb{Q}$. En este caso se dice que K es un **cuerpo de números**. Definamos O_K como el conjunto de los elementos de K que satisfacen una ecuación polinomial mónica

$$\alpha^n + c_{n-1}\,\alpha^{n-1} + \cdots + c_1\,\alpha + c_0 = 0,$$

donde $c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z}$. Resulta que O_K es un anillo[*] y este recibe el nombre del **anillo de los enteros** en K.

Si $[K:\mathbb{Q}] = d$, entonces O_K es un $\mathbb{Z}$-módulo libre de rango d.



5.2. Ejemplo. Tenemos

$$O_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}], \quad O_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right], \quad O_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}].$$

En general, para un entero libre de cuadrados d se tiene

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{si } d \equiv 2,3 \mod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{si } d \equiv 1 \mod 4. \end{cases}$$

▲

El cuerpo de fracciones de O_K coincide con K. Para todo ideal primo $\mathfrak{p} \subset O_K$ y $\alpha \in O_K$ la valuación $\mathfrak{p}$-ádica de α se define mediante

$$\alpha\, O_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)}$$

—el anillo O_K no necesariamente admite descomposición única: por ejemplo, en $\mathbb{Z}[\sqrt{-5}]$ se tiene $6 = 2\cdot 3 = (1+\sqrt{-5})\,(1-\sqrt{-5})$. Sin embargo, lo que se puede hacer es factorizar el ideal generado por α en ideales primos.

A partir de $\nu_{\mathfrak{p}}(\alpha)$ se define una norma $|\cdot|_{\mathfrak{p}}$. Además, K admite un número finito de normas arquimedianas que vienen de encajamientos $K \hookrightarrow \mathbb{R}$ y $K \hookrightarrow \mathbb{C}$. Sea entonces $v = \mathfrak{p}$, o uno de los "primos infinitos" que corresponden a las normas arquimedianas. Denotemos por K_v la completación correspondiente.

El símbolo de Hilbert para $a, b \in K_v^\times$ se define de la misma manera:

$$(a,b)_v := \begin{cases} +1, & ax^2 + by^2 = 1 \text{ tiene una solución en } K_v, \\ -1, & \text{en el caso contrario.} \end{cases}$$

Tenemos la misma reciprocidad.

5.3. Teorema. *Para cualesquiera $a, b \in K^\times$ se cumple*

$$\prod_v (a,b)_v = 1.$$

[*] No es tan inmediato.

6 Álgebras centrales con división

Para ver otra encarnación de la reciprocidad, necesitamos revisar la teoría de álgebras con división. En este contexto una F**-álgebra** es un espacio vectorial A sobre cuál también está definida una multiplicación bilineal

$$\cdot\colon A \times A \to A.$$

Vamos a asumir que existe la identidad $1 \in A$ y que la multiplicación es asociativa. Sin embargo, para nosotros será importante considerar álgebras con multiplicación no conmutativa. Si los únicos elementos que conmutan con todos los elementos de A son los escalares:

$$Z(A) := \{a \in A \mid ab = ba \text{ para todo } b \in A\} = F,$$

entonces se dice que A es **central**. Cuando todos los elementos no nulos de A son invertibles, se dice que A es un **álgebra con división**. Nos van a interesar álgebras centrales con división.

6.1. Ejemplo. Un ejemplo de $\mathbb{R}$-álgebras conocido a todo el mundo son los números complejos. Es un espacio vectorial

$$\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i$$

con la multiplicación definida por la relación $i^2 = -1$. Todo elemento no nulo de $\mathbb{C}$ es invertible: para $z = x + yi$ se define

$$\overline{z} := x - yi, \quad N(z) := z\overline{z} = x^2 + y^2,$$

y luego

$$z^{-1} = \frac{1}{N(z)}\,\overline{z}.$$

Entonces, $\mathbb{C}$ es una $\mathbb{R}$-álgebra con división. Sin embargo, no es un álgebra central: la multiplicación compleja es conmutativa. ▲

6.2. Ejemplo. Otro ejemplo clásico son los **cuaterniones de Hamilton** que se definen como el espacio vectorial de dimensión 4

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

con la multiplicación definida por las relaciones

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.$$

De aquí se deduce que

$$ji = -k, \quad kj = -i, \quad ik = -j.$$

Entonces, los cuaterniones no son conmutativos: se ve que el centro consiste solamente en los escalares:

$$Z(\mathbb{H}) = \mathbb{R}.$$

Para ver que todo cuaternión no nulo

$$q = x + yi + zj + wk$$

es invertible, se introduce la norma

$$\overline{q} = x - yi - zj - wk, \quad N(q) := q\,\overline{q} = \overline{q}\,q = x^2 + y^2 + z^2 + w^2.$$

Luego, si $q \neq 0$, se tiene

$$q^{-1} = \frac{1}{N(q)}\,\overline{q}.$$

Entonces, $\mathbb{H}$ es una $\mathbb{R}$-álgebra central con división. ▲

La construcción de los cuaterniones puede ser generalizada: se puede reemplazar $\mathbb{R}$ por otro cuerpo y también se puede ajustar las relaciones sobre i, j, k.

6.3. Definición. Sea F un cuerpo de característica diferente de 2. Para $a, b \in F^\times$ pongamos

$$\left(\frac{a,b}{F}\right) := F1 \oplus Fi \oplus Fj \oplus Fk$$

con la multiplicación definida por las relaciones

$$i^2 = a, \quad j^2 = b, \quad ij = k = -ji.$$

6.4. Ejemplo. La construcción de Hamilton corresponde a $\left(\frac{-1,-1}{\mathbb{R}}\right)$. ▲

De nuevo, $\left(\frac{a,b}{F}\right)$ es un álgebra central de dimensión 4. Sin embargo, los elementos no nulos no son necesariamente invertibles. Si definamos la norma de la misma manera, llegamos a la fórmula

$$\overline{q} := x - yi - zj - wk, \quad N(q) = q\overline{q} = \overline{q}q = x^2 - ay^2 - bz^2 + abw^2 \in F.$$

Si $N(q) \neq 0$, entonces q es invertible. Sin embargo, puede pasar que para $q \neq 0$ se tiene $N(q) = 0$.

6.5. Proposición. *Para $a, b \in F^\times$ supongamos que a no es un cuadrado en F y $b \notin N_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)$. Entonces, $\left(\frac{a,b}{F}\right)$ es un álgebra central con división.*

Demostración. Supongamos que para $q \in \left(\frac{a,b}{F}\right)$ se cumple $N(q) = 0$. Bastaría probar que $q = 0$. Tenemos

$$N(q) = 0 \iff x^2 - ay^2 = b(z^2 - aw^2).$$

Supongamos que las partes de esta ecuación no son nulas. Entonces, son normas de algunos elementos de $F(\sqrt{a})^\times$. Las normas forman un grupo, y por lo tanto

$$b = \frac{x^2 - ay^2}{z^2 - aw^2} \in N_{F(\sqrt{a})/F}(F(\sqrt{a})^\times),$$

pero esto no se cumple por la hipótesis. Entonces, tenemos un sistema de ecuaciones

$$x^2 - ay^2 = b(z^2 - aw^2) = 0.$$

Ya que $b \neq 0$ y a no es un cuadrado, se sigue que $x = y = z = w = 0$. ■

De hecho, cuando la división en $\left(\frac{a,b}{F}\right)$ no es posible, es necesariamente el álgebra de matrices.

6.6. Teorema. *Si $\left(\frac{a,b}{F}\right)$ no es un álgebra con división, entonces $\left(\frac{a,b}{F}\right) \cong M_2(F)$.*

6.7. Ejemplo. Sea p un primo impar y sea a un número que no es un cuadrado módulo p. Entonces, $p \neq r^2 - as^2$ para ningún $r, s \in \mathbb{Q}$. Se sigue que $\left(\frac{a,p}{\mathbb{Q}}\right)$ es una F-álgebra central con división. A priori, algunas de estas álgebras pueden ser isomorfas. En efecto, cuando a no es un cuadrado, tenemos

$$\left(\frac{a,b}{\mathbb{Q}}\right) \cong \left(\frac{a,c}{\mathbb{Q}}\right) \iff \frac{b}{c} \in N_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\mathbb{Q}(\sqrt{a})^\times).$$

Ahora si tomamos dos primos diferentes $p, q \equiv 3 \pmod 4$ (hay un número infinito de ellos), entonces $p/q \neq x^2 + y^2$ para ningún $x, y \in \mathbb{Q}$. Se sigue que

$$\left(\frac{-1,p}{\mathbb{Q}}\right) \ncong \left(\frac{-1,q}{\mathbb{Q}}\right).$$

▲

El ejemplo de arriba nos da una familia infinita de álgebras centrales con división sobre $\mathbb{Q}$. Esto no sucede sobre $\mathbb{R}$.

6.8. Teorema (Frobenius, 1898). *Salvo isomorfismo, las únicas álgebras centrales con división sobre $\mathbb{R}$ son los mismos números reales $\mathbb{R}$ y los cuaterniones $\mathbb{H}$.*

Para construir álgebras centrales con división en dimensiones mayores que 4, se puede generalizar la construcción de los cuaterniones de Hamilton, pero de diferente manera. Notamos que $\mathbb{H}$ puede ser visto como un espacio vectorial sobre $\mathbb{C}$:

$$\mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k = (\mathbb{R}1 \oplus \mathbb{R}i) \oplus (\mathbb{R}1 \oplus \mathbb{R}i)\, j = \mathbb{C} \oplus \mathbb{C}\, j,$$

donde $j^2 = -1$, y la multiplicación de un número complejo por j satisface

$$jz = \overline{z}\, j.$$

Esta reinterpretación de los cuaterniones motiva la siguiente construcción.

6.9. Definición (Dickson, 1905). Sea E/F una extensión de Galois cíclica de grado n; es decir, una extensión de cuerpos con el grupo $\mathrm{Gal}(E/F)$ cíclico. Sea σ un generador de $\mathrm{Gal}(E/F)$ y $c \in F^\times$. Definamos

$$(E/F, \sigma, c) := E1 \oplus E\,u \oplus E\,u^2 \oplus \cdots \oplus E\,u^{n-1}$$

con la multiplicación definida por

$$u^n := c, \quad u\alpha := \sigma(\alpha)\, u \text{ para todo } \alpha \in E.$$

6.10. Proposición.

1) *Tenemos*
$$\dim_F (E/F, \sigma, c) = n^2,$$
donde $n = [E : F]$ es el grado de la extensión.

2) *Las álgebras $(E/F, \sigma, c)$ son centrales; es decir, $Z((E/F, \sigma, c)) = F$.*

3) *Las álgebras $(E/F, \sigma, c)$ son **simples**; es decir, no tienen ideales bilaterales no triviales.*

4) *Si el grado $[E : F]$ es primo y $c \notin N_{E/F}(E^\times)$, entonces $(E/F, \sigma, c)$ es un álgebra con división.*

6.11. Ejemplo. Tenemos $\mathbb{H} = (\mathbb{C}/\mathbb{R}, \sigma, -1)$, donde $\sigma : z \mapsto \overline{z}$ es la multiplicación compleja, y en general

$$\left(\frac{a, b}{F}\right) = (F(\sqrt{a})/F, \sigma, b),$$

donde $\sigma : \sqrt{a} \mapsto -\sqrt{a}$. ▲

jueves,
12 de julio

6.12. Teorema (Artin–Wedderburn). *Si A es una F-álgebra central simple de dimensión finita, entonces $A \cong M_r(D)$ donde $r \geq 1$ y D es una álgebra con división con $Z(D) = F$. Además, r y D están definidos de modo único (salvo isomorfismo).*

6.13. Proposición. *Las F-álgebras centrales simples tienen las siguientes propiedades.*

1) *Si A_1 y A_2 son F-álgebras centrales simples, entonces $A_1 \otimes_F A_2$ es una F-álgebra central simple.*

2) *$M_r(D) \otimes_F M_s(F) \cong M_{rs}(D)$.*

3) $A \otimes_F A^{op} \cong M_d(F)$*, donde* A^{op} *es el* ***álgebra opuesta*** *con la multiplicación definida por* $a \cdot b := ba$ y $d := \dim_F A$.

Las propiedades de arriba nos llevan a la siguiente construcción.

6.14. Definición (Brauer, 1929). Para dos F-álgebras centrales simples de dimensión finita $A_1 \cong M_{r_1}(D_1)$ y $A_2 \cong M_{r_2}(D_2)$ definamos la relación de equivalencia

$$A_1 \sim A_2 \iff D_1 \cong D_2$$

y la multiplicación sobre las clases de equivalencia

$$[A_1] \cdot [A_2] := [A_1 \otimes_F A_2].$$

Respecto esta operación, las clases de equivalencia de F-álgebras centrales simples de dimensión finita forman un grupo abeliano $\mathrm{Br}(F)$, llamado el **grupo de Brauer**[*] **de** F.

El elemento neutro en $\mathrm{Br}(F)$ es la clase de equivalencia $[F]$. Los inversos vienen dados por $[A]^{-1} = [A^{op}]$. Notamos que toda clase de equivalencia es de la forma $[D]$, donde D es un álgebra central con división. Sin embargo, los productos tensoriales $D_1 \otimes_F D_2$ no suelen tener división y es necesario trabajar con las álgebras centrales simples.

6.15. Ejemplo. Según el teorema de Frobenius (6.8), tenemos

$$\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}.$$

El producto tensorial nos da $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$. ▲

6.16. Ejemplo. Para todo primo finito p tenemos

$$\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}.$$

A saber, resulta que todo elemento $[A] \in \mathrm{Br}(\mathbb{Q}_p)$ está representado por un álgebra $(F/\mathbb{Q}_p, \mathrm{Frob}, p^k)$, donde $F/\mathbb{Q}_p$ es la extensión no ramificada de grado n (es única para cada n) y $\mathrm{Frob} \in \mathrm{Gal}(F/\mathbb{Q}_p)$ es el automorfismo de Frobenius. El número

$$\mathrm{inv}[A] := [k/n] \in \mathbb{Q}/\mathbb{Z}$$

se llama el **invariante de Hasse** de A y nos da un isomorfismo entre $\mathrm{Br}(\mathbb{Q}_p)$ y $\mathbb{Q}/\mathbb{Z}$. ▲

Sea v un primo finito o ∞. A partir de una $\mathbb{Q}$-álgebra central simple A, se puede obtener una $\mathbb{Q}_v$-álgebra central simple, tomando el producto tensorial con $\mathbb{Q}_v$. Esto nos da un homomorfismo de grupos

$$\begin{aligned} \mathrm{Br}(\mathbb{Q}) &\to \mathrm{Br}(\mathbb{Q}_v), \\ [A] &\mapsto [A \otimes_{\mathbb{Q}} \mathbb{Q}_v]. \end{aligned}$$

Podemos hacerlo para todo v, y de esta manera se obtiene un homomorfismo

$$\begin{aligned} \mathrm{Br}(\mathbb{Q}) &\to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v), \\ [A] &\mapsto ([A \otimes_{\mathbb{Q}} \mathbb{Q}_v])_v. \end{aligned}$$

La clase de equivalencia $[A \otimes_{\mathbb{Q}} \mathbb{Q}_v]$ es trivial en $\mathrm{Br}(\mathbb{Q}_v)$ casi para todo v, y por esto la imagen está en la *suma* directa. Este homomorfismo es inyectivo. Su imagen puede ser descrita mediante el siguiente resultado importante.

[*] No confundir el algebrista y teórico de números alemán Richard Brauer (1901–1977) con el matemático holandés L.E.J. Brouwer (1881–1966), conocido por su teorema del punto fijo.

6.17. Teorema. *Hay una sucesión exacta corta de grupos*

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0 \tag{1}$$

Aquí el homomorfismo $\bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$ viene dado por la suma: tenemos $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ mediante el invariante de Hasse y $\mathrm{Br}(\mathbb{Q}_\infty) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, y dada una sucesión $([A_v])_v$, se puede tomar $\sum_v \mathrm{inv}[A_v]$. Las palabras **sucesión exacta corta** significan que

- el homomorfismo $\mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v)$ es inyectivo,
- el homomorfismo $\bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$ es sobreyectivo,
- $\mathrm{im}(\mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v)) = \ker(\mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z})$.

La sucesión exacta corta (1) nos da una descripción del grupo $\mathrm{Br}(\mathbb{Q})$ en términos de grupos $\mathrm{Br}(\mathbb{Q}_v)$, cuya estructura es más fácil.

Ahora si consideramos la 2-torsión, tenemos una sucesión exacta corta

$$0 \to \mathrm{Br}(\mathbb{Q})[2] \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v)[2] \to \frac{1}{2}/\mathbb{Z} \to 0 \tag{2}$$

En general, para las álgebras de cuaterniones $A = \left(\frac{a,b}{F}\right)$ hay un isomorfismo $A \cong A^{op}$ dado por la conjugación $q \mapsto \overline{q}$. Esto significa que las álgebras de cuaterniones son elementos de 2-torsión en el grupo de Brauer:

$$\left(\frac{a,b}{F}\right) \in \mathrm{Br}(F)[2] := \{[A] \in \mathrm{Br}(F) \mid [A] \cdot [A] = [F]\}.$$

Además, para $F = \mathbb{R}$ o $\mathbb{Q}_p$, *todos* los elementos de $\mathrm{Br}(F)[2]$ están representados por las álgebras de cuaterniones. Tenemos

$$\left(\frac{a,b}{\mathbb{Q}}\right) \otimes_{\mathbb{Q}} \mathbb{Q}_v = \left(\frac{a,b}{\mathbb{Q}_v}\right),$$

y luego,

- si $(a,b)_v = +1$, entonces $\left(\frac{a,b}{\mathbb{Q}_v}\right) \cong M_2(\mathbb{Q}_v)$ es trivial en $\mathrm{Br}(\mathbb{Q}_v)$;
- si $(a,b)_v = -1$, entonces $\left(\frac{a,b}{\mathbb{Q}_v}\right)$ es un álgebra con división que no es trivial en $\mathrm{Br}(\mathbb{Q}_v)$.

La exactitud de la sucesión (2) en el medio nos da

$$\sum_v \mathrm{inv}\left[\left(\frac{a,b}{\mathbb{Q}_v}\right)\right] = 0,$$

y esto es equivalente a la reciprocidad de Hilbert

$$\prod_v (a,b)_v = 1.$$

Todo esto se generaliza a los cuerpos de números: para toda extensión finita $K/\mathbb{Q}$ hay una sucesión exacta corta

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0$$

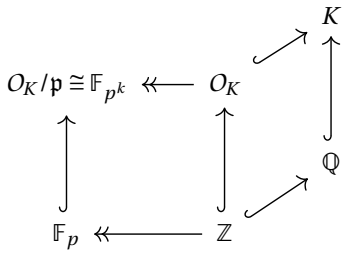
7 La ley de reciprocidad de Artin

Vamos a terminar nuestra historia por un caso especial de la ley de reciprocidad de Artin. Primero necesitamos revisar algunas nociones de la teoría de números algebraica. Sea $K/\mathbb{Q}$ un cuerpo de números y O_K su anillo de enteros. Todo ideal primo no nulo $\mathfrak{p} \subset O_K$ es automáticamente maximal y el cuerpo $O_K/\mathfrak{p}$ es finito y tiene característica p; es decir, es isomorfo a $\mathbb{F}_{p^k}$ para algún k.

Para un número primo $p \in \mathbb{Z}$, el ideal generado por p en O_K se factoriza en ideales primos:

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

En este caso escribimos $\mathfrak{p} \mid p$. Si en la factorización se tiene $e_i > 1$ para algún i, entonces se dice que p **se ramifica** en O_K. Para un cuerpo de números K fijo, hay un número finito de primos que se ramifican.



7.1. Ejemplo. Para ejemplos específicos de cuerpos de números el lector puede consultar la base de datos http://www.lmfdb.org/NumberField/. También muchos cálculos explícitos se pueden hacer en el programa PARI/GP (http://pari.math.u-bordeaux.fr/). Aquí vamos a revisar un ejemplo bien conocido a todo el mundo: $K = \mathbb{Q}(\sqrt{-1})$ y $O_K = \mathbb{Z}[\sqrt{-1}]$, los enteros de Gauss.

Para $p = 2$ se tiene $2 = -\sqrt{-1}\,(1+\sqrt{-1})^2$, donde $-\sqrt{-1}$ es invertible y $1+\sqrt{-1}$ es primo en $\mathbb{Z}[\sqrt{-1}]$. Entonces, en $\mathbb{Z}[\sqrt{-1}]$ hay una factorización en ideales primos

$$(2) = (1+\sqrt{-1})^2.$$

Esto significa que 2 se ramifica en $\mathbb{Z}[\sqrt{-1}]$. Tenemos

$$\mathbb{Z}[\sqrt{-1}]/(1+\sqrt{-1}) \cong \mathbb{F}_2.$$

Otros primos no se ramifican en $\mathbb{Z}[\sqrt{-1}]$. Por ejemplo,

$$\begin{aligned}
(3) &= (3),\\
(5) &= (2+\sqrt{-1})\,(1+2\sqrt{-1}),\\
(7) &= (7),\\
(11) &= (11),\\
(13) &= (2+3\sqrt{-1})\,(3+2\sqrt{-1}),\\
&\cdots
\end{aligned}$$

Luego,

$$\mathbb{Z}[\sqrt{-1}]/(3) \cong \mathbb{F}_9, \quad \mathbb{Z}[\sqrt{-1}]/(2+\sqrt{-1}) \cong \mathbb{Z}[\sqrt{-1}]/(1+2\sqrt{-1}) \cong \mathbb{F}_3,$$
$$\mathbb{Z}[\sqrt{-1}]/(7) \cong \mathbb{F}_9, \quad \mathbb{Z}[\sqrt{-1}]/(11) \cong \mathbb{F}_9, \quad \mathbb{Z}[\sqrt{-1}]/(2+3\sqrt{-1}) \cong \mathbb{Z}[\sqrt{-1}]/(3+2\sqrt{-1}) \cong \mathbb{F}_3.$$

▲

7.2. Ejemplo. En general, si d es un entero libre de cuadrados, para $K = \mathbb{Q}(\sqrt{d})$, hay dos posibilidades:

- si $d \equiv 1 \pmod 4$, entonces en O_K se ramifican precisamente los factores de d;
- si $d \equiv 2,3 \pmod 4$, entonces en O_K se ramifican los factores de d y además el primo 2.

▲

7.3. Teorema. *Sea $K/\mathbb{Q}$ un cuerpo de números tal que el grupo $\mathrm{Gal}(K/\mathbb{Q})$ es abeliano. Luego, para todo primo $p \in \mathbb{Z}$ que no se ramifica en O_K existe un elemento único $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$, llamado el **elemento de Frobenius**, que satisface*

$$\mathrm{Frob}_p(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$$

para cualesquiera $\alpha \in O_K$ y $\mathfrak{p} \mid p$.

En la teoría de cuerpos finitos, el automorfismo de Frobenius de $\mathbb{F}_{p^k}$ viene dado por $x \mapsto x^p$. Aquí se trata de un automorfismo de K que actúa como $x \mapsto x^p$ sobre $O_K/\mathfrak{p}$.

7.4. Ejemplo. Para $K = \mathbb{Q}(\sqrt{-1})$ y $p = 3$ tenemos

$$(x + y\sqrt{-1})^3 \equiv x^3 + y^3(\sqrt{-1})^3 \equiv x - y\sqrt{-1} \pmod 3.$$

Entonces, Frob_3 es la conjugación $\sqrt{-1} \mapsto -\sqrt{-1}$. Notamos que para $p = 2$ y $(1 + \sqrt{-1}) \mid 2$ se tiene

$$(x + y\sqrt{-1})^2 \equiv x \pm y\sqrt{-1} \pmod{1 + \sqrt{-1}}.$$

Esto significa que ambos elementos $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$ satisfacen la condición $\sigma(\alpha) \equiv \alpha^2$. Pero 2 se ramifica, y por esto el elemento de Frobenius no está definido. ▲

Estamos listos para formular un caso particular de la ley de reciprocidad de Artin. La verdadera ley de Artin se formula para extensiones de cuerpos de números L/K, pero nos contentaremos con $K/\mathbb{Q}$.

7.5. Teorema (Emil Artin, 1927). *Sea $K/\mathbb{Q}$ un cuerpo de números tal que el grupo $\mathrm{Gal}(K/\mathbb{Q})$ es abeliano. Sea $n = p_1 \cdots p_s \in \mathbb{Z}$ un entero positivo cuyos factores primos p_i no se ramifican en O_K. Definamos el **símbolo de Artin** mediante*

$$\left(\frac{K/\mathbb{Q}}{n}\right) := \mathrm{Frob}_{p_1} \circ \cdots \circ \mathrm{Frob}_{p_s} \in \mathrm{Gal}(K/\mathbb{Q}).$$

Luego, existe un entero positivo m_K tal que para todo

$$n \equiv 1 \pmod{m_K} \Longrightarrow \left(\frac{K/\mathbb{Q}}{n}\right) = 1.$$

Los factores primos de m_K son precisamente los primos que no se ramifican en O_K.

7.6. Ejemplo. Sea d un entero libre de cuadrados. Consideremos el cuerpo de números $K = \mathbb{Q}(\sqrt{d})$. Tenemos $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, donde σ es la conjugación $\sqrt{d} \mapsto -\sqrt{d}$.

Sea p un número primo que no se ramifica en O_K. Esto significa que $p \nmid d$, y además, 2 también se ramifica cuando $d \equiv 2,3 \pmod 4$. Por esto vamos a asumir que p es impar.

1) Si $\mathrm{Frob}_p = \mathrm{id}$, entonces

$$\sqrt{d}^p \equiv \sqrt{d} \pmod{\mathfrak{p}},$$

lo que nos da

$$\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \equiv +1 \pmod p$$

(recuerde la congruencia de Euler).

2) De la misma manera, si $\mathrm{Frob}_p = \sigma$, entonces

$$\sqrt{d}^{\,p} \equiv -\sqrt{d} \pmod{\mathfrak{p}},$$

y

$$\left(\frac{d}{p}\right) = -1.$$

Gracias a esto, podemos identificar el elemento de Frobenius con el símbolo de Legendre:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong \{\pm 1\}, \quad \mathrm{Frob}_p = \left(\frac{d}{p}\right).$$

Ahora si $n = p_1 \cdots p_s$ es un entero tal que $\mathrm{mcd}(n, 2d) = 1$, el símbolo de Artin correspondiente es el símbolo de Jacobi

$$\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{n}\right) := \mathrm{Frob}_{p_1} \cdots \mathrm{Frob}_{p_s} = \left(\frac{d}{p_1}\right) \cdots \left(\frac{d}{p_s}\right) =: \left(\frac{d}{n}\right).$$

Sea p un primo impar. Consideremos

$$p^* := (-1)^{\frac{p-1}{2}} p$$

y $K = \mathbb{Q}(\sqrt{p^*})$. Tenemos $p^* \equiv 1 \pmod 4$, y el único primo que se ramifica en O_K es p. Gracias a esto, el número m_K en la Ley de Artin 7.5 es igual a p^r para algún r (si 2 se ramificara, m_K tendría también una potencia 2, lo que no es deseable).

Entonces, la reciprocidad de Artin nos dice que

$$n \equiv 1 \pmod{p^r} \Longrightarrow \left(\frac{p^*}{n}\right) = 1.$$

De aquí se sigue que si n_1, n_2 son invertibles en $\mathbb{Z}/p^r\mathbb{Z}$, entonces $n_1 \equiv n_2 \pmod{p^r}$ implica[*]

$$\left(\frac{p^*}{n_1}\right) = \left(\frac{p^*}{n_2}\right).$$

Podemos concluir que existe un homomorfismo no trivial

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \to \{\pm 1\},$$
$$[n] \mapsto \left(\frac{p^*}{n}\right).$$

Además, conocemos otro homomorfismo no trivial dado por el símbolo de Legendre

$$[n] \mapsto \left(\frac{n}{p}\right).$$

[*] En efecto, si $n_1 n_1' \equiv 1 \pmod{p^r}$, entonces

$$\left(\frac{p^*}{n_1}\right)\left(\frac{p^*}{n_1'}\right) = \left(\frac{p^*}{n_1 n_1'}\right) = 1,$$

así que

$$\left(\frac{p^*}{n_1}\right) = \left(\frac{p^*}{n_1'}\right).$$

Ahora si $n_1 \equiv n_2 \pmod{p^r}$ y $n_2 n_2' \equiv 1 \pmod{p^r}$, entonces $n_2 n_1' \equiv 1 \pmod r$ y

$$\left(\frac{p^*}{n_2}\right) = \left(\frac{p^*}{n_1'}\right) = \left(\frac{p^*}{n_1}\right).$$

El grupo $(\mathbb{Z}/p^r\mathbb{Z})^\times$ es cíclico para p impar, y por ende dos homomorfismos no triviales $(\mathbb{Z}/p^r\mathbb{Z})^\times \to \{\pm 1\}$ necesariamente coinciden. Podemos concluir que

$$\left(\frac{n}{p}\right) = \left(\frac{p^*}{n}\right)$$

para $p \nmid n$. En particular, si $n = q$ es otro primo impar diferente de p,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) := \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

Aquí la última igualdad es una de las leyes suplementarias de reciprocidad cuadrática (que es un cálculo fácil), y la fórmula que hemos deducido es precisamente la ley principal de reciprocidad cuadrática (que no es fácil). ▲

Entonces, la ley de Gauss es un caso muy especial de la ley de Artin. El ejemplo de arriba por fin nos explica el significado del símbolo de Jacobi: es nada más un caso especial del símbolo de Artin.

8 Conclusión

Empezamos por la reciprocidad cuadrática de Gauss y vimos sus diferentes generalizaciones: la reciprocidad de Hilbert $\prod_v (a,b)_v = 1$, la sucesión exacta $0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z} \to 0$ y la reciprocidad de Artin. En el camino hemos visto muchos conceptos importantes: números p-ádicos, lema de Hensel, símbolos de Hilbert, álgebras con división, cuaterniones, álgebras centrales simples, grupos de Brauer, cuerpos de números, ramificación, grupos de Galois, etc. Mi objetivo no era presentar todos los detalles, sino mencionar ciertas palabras clave.

He aquí una lista de libros de texto sobre los temas que han aparecido en nuestro minicurso. Los principiantes pueden empezar por los primeros tres.

1. Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Numer Theory*.
   Pruebas de la reciprocidad cuadrática de Gauss.
2. Kazuya Kato, Nobushige Kurokawa, Takeshi Saito, *Number Theory 1: Fermat's Dream*.
   El capítulo 2 introduce los números p-ádicos y el símbolo de Hilbert. El capítulo 4 está dedicado a los cuerpos de números.
3. Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*.
   El capítulo I contiene una buena introducción a los números p-ádicos. El capítulo III está dedicado a las extensiones de $\mathbb{Q}_p$.
4. Richard S. Pierce, *Associative Algebras*.
   Pruebas de los resultados sobre los grupos de Brauer.
5. Philippe Gille, Tamás Szamuely, *Central Simple Algebras and Galois Cohomology*.
   Otro libro de texto, más reciente.
6. Jürgen Neukirch, *Algebraic Number Theory*.
   El capítulo I está dedicado a los cuerpos de números y el capítulo II a los cuerpos p-ádicos. La reciprocidad de Hilbert y Artin aparecen el los capítulos V y VI en un contexto mucho más general y abstracto.
7. J.W.S. Kassels, A. Fröhlich, *Algebraic Number Theory*.
   La biblia de la teoría de números algebraica.