Teoría de números

José Cuevas Barrientos

7 de mayo de 2024

Índice general

Introducción

La teoría de números es tal vez una de las dos más antiguas ramas de las matemáticas, junto con la geometría son aquellas que conforman la totalidad de los Elementos de Euclides; asimismo, varias civilizaciones llegaron a una serie de resultados de teoría de números que abarcan las ternas pitagóricas y los números primos. Los números primos son el principal foco de la teoría de números, y si bien sabemos de su existencia hace más de 300 a.C. (publicación aproximada de los Elementos), no fue hasta finales del siglo XVIII que se conjeturó el teorema de los números primos (independientemente por Legendre y Gauss), uno de los primeros significativos patrones en la distribución de ellos y no fue hasta 1848-'50 que Pafnuty Chebyshev publicó una demostración del teorema. Hoy en día el consenso general es que la teoría de números, a pesar de que es fácil de leer, es imposible de estudiar sin técnicas más avanzadas importadas desde otros campos de las matemáticas como la combinatoria, el álgebra, el análisis entre otras. Así, éste libro va incluyendo al inicio de cada capítulo una tabla de dependencias en relación a mis otros libros de *Álgebra* [A], *Topología y Análisis* [T] y a éste libro cómo *Teoría de Números* [N].

0.1 Historia clásica de la teoría de números

En algún lugar de Grecia de cuyo nombre no quiero acordarme, en el siglo III d.C. el matemático **Diofanto de Alejandría** escribiría trece libros, de los que se conservan sólo seis, que conformarían su obra *Arithmetica* que marcarían el inicio de la *teoría de números*. Trazar un origen (cualquiera) a la teoría es una imposibilidad: desde que el hombre tiene memoria que

le gustan los deportes, las artes, las ciencias y los números; naturalmente identidades relacionadas a la adición y multiplicación eran conocidas desde Egipto Antiguo, y **Euclides** también incluye un tratamiento primitivo en los *Elementos*, pero no considero osado tomar a Diofanto como una piedra angular.

Los números tienen un atractivo bien particular, esconden tras de sí un halo de magia y misterio, una serie de intrincados patrones que resultan todo un deleite por ser un juego sin inicio ni fin, y porque representan un absoluto desafío a la inteligencia humana. El término «juego» aquí no puede tener mejor uso, puesto que los primeros registros de patrones numéricos (e.g., tabletas de ternas pitagóricas entre los egipcios) no responden a ningún impulso lógico más que el de probar a ensayo y error, pero con el pasar de los años, éstos patrones han requerido más atención y más ingenio por parte de sus autores. La teoría de números es entonces inmensamente llamativa, puesto que siquiera encontrar un patrón lo suficientemente convincente para no tacharse de trivial requiere de un gran ingenio; resolverlo aún más, y quizá lo más alucinante de todo es que sus conjeturas, que abundan como peces en el mar, suelen estar escritas en la más simple de las jergas; no es arriesgada la frase de que hasta un niño entendería *qué* dicen ésta clase de problemas, aunque la solución no podría considerarse igualmente «accesible» a los hombres comunes.

Desde Euclides, hasta Pitágoras y Platón, todos han alabado una cierta idea de perfección o pureza entre los números. En sus *Elementos*, Euclides desarrolla la misma teoría con la que abrimos el libro y que luego sería generalizada mediante el lenguaje de anillos en el siglo xviii, y culmina ésta obra con la clasificación de los números pares perfectos (§3.1.1).

En 1636, y siguiendo la tradición de los niños en los charcos de barro, un abogado francés llamado **Pierre de Fermat** habría comprado y comenzado el intensivo estudio de la *Arithmetica* de Diofanto, en una edición comentada por Bachet de Méziriac. Ensimismado en sus rompecabezas aritméticos, Fermat trató de convencer a otros matemáticos a subirse al tren de los números sin tanto éxito. Había contactado a Pascal con el propósito de comenzar un tratado en conjunto, pero fue rechazado. En 1670, cinco años después de su fallecimiento, su hijo Samuel publicaría la copia de la *Arithmetica* de Fermat junto con comentarios de un padre jesuita, y el año anterior habría logrado la publicación de varias de las cartas de Fermat. Tendría que esperar un par de siglos para que la huella de Fermat atravesara toda clase de épocas históricas hasta que penetrará en la posteridad como uno de los grandes visionarios de las matemáticas.

Específicamente, tendría que esperar 59 años (1729) hasta que en medio

de la correspondencia de un joven de ascendencia rusa y otro austriaco se reavivase aquél dragón dormido. Los jóvenes se llamaban **Leonhard Euler** y **Christian Goldbach** respectivamente; de entre esa colección de cartas, Goldbach le presenta la famosa conjetura homónima y le insta a leer los trabajos de Fermat; particularmente, le pregunta acerca de los llamados primos de Fermat (aquellos de la forma $F_n := 2^{2^n} + 1$) y Euler se cuestiona la hipótesis de Fermat de que todos éstos números sean primos en una carta de diciembre de dicho año. Para junio del año siguiente, Euler habría encontrado la respuesta, el primer número no verificado por Fermat ($F_5 = 4294967297$) no era primo (cf. §2.3.1); y en conjunto había revisado (no demostrado) varias de las otras afirmaciones hechas por Fermat, como que todo número es suma de cuatro cuadrados (teo. 2.9), que todo número es suma de tres triangulares (teo. 10.35), que todo número es suma de cinco pentagonales, etc. La pasión de Euler se contagio a Lagrange, que a su vez la contagió a Legendre, que a su vez la contagió a Gauss.

Parte I.

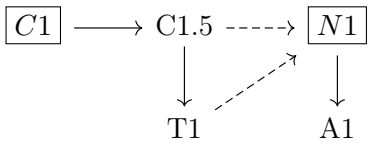
Teoría elemental de números

1

Divisibilidad

Comenzaremos el capítulo con dar una breve introducción a la teoría de números, la cual servirá tanto para ilustrar como para poder definir ciertos conceptos que nos serán útiles.

La lectura adecuada con respecto a mis libros sería la siguiente:



La simbología es la siguiente: *Teoría de* [C]*onjuntos*, [T]*opología y Análisis*, [A]*lgebra* y *Teoría de* [N]*úmeros*. Las flechas puntuadas se leen como "complementario pero opcional".

1.1 La aritmética de Peano

Comencemos desde cero: En éste momento no tenemos números, así que siguiendo los axiomas de Peano construiremos los números desde los naturales hasta los racionales. Los números reales y los números complejos son todo un tema distinto.

Definición 1.1: Se denota por $\mathbb{N}$ al conjunto dotado de un elemento «0» y una función s (léase ***sucesor***), tales que:

1. No existe $n \in \mathbb{N}$ tal que $s(n) = 0$ (el cero no posee antecesor).
2. s es inyectiva, i.e., si $n, m \in \mathbb{N}$ son tales que $s(n) = s(m)$, entonces $n = m$ (dos números con mismo sucesor son iguales).
3. Si $A \subseteq \mathbb{N}$ es tal que $0 \in A$ y para todo $n \in A$ se cumple que $s(n) \in A$, entonces $A = \mathbb{N}$ (principio de inducción).

A los elementos de $\mathbb{N}$ les llamamos *números naturales* y se definen:

$$\begin{array}{lll} 1 := s(0) & 4 := s(3) & 7 := s(6) \\ 2 := s(1) & 5 := s(4) & 8 := s(7) \\ 3 := s(2) & 6 := s(5) & 9 := s(8) \end{array}$$
$$\vdots$$

El principio de inducción debe interpretarse con dos propósitos: el primero es decir que $\mathbb{N}$ es el conjunto «más pequeño» que cumple los primeros dos axiomas, y el segundo es el decir que $\mathbb{N}$ posee un orden natural que sigue de aplicar s al 0 que no está «desconectado». Evidentemente, nótese que $\mathbb{N} \cup \frac{1}{2}\mathbb{N} = \{n + \frac{m}{2} \in \mathbb{Q} : n, m \in \mathbb{N}\}$ también cumple los dos primeros axiomas, pero no solo es más grande sino que aquí s va «saltandose números». Otro ejemplo sería tomar $\{0, 1\} \times \mathbb{N}$, donde el $0 := (0, 0)$, claro que éste conjunto cumple los dos axiomas, pero corresponde a dos copias «desconectadas» de $\mathbb{N}$.

Proposición 1.2: Para todo $n \in \mathbb{N}$ distinto del 0, existe $m \in \mathbb{N}$ tal que $s(m) = n$.

Demostración: Sea A el conjunto formado por todos los elementos que hacen cumplir el enunciado, incluyendo al 0, luego probaremos que $A = \mathbb{N}$ mediante el principio de inducción:

Por definición $0 \in A$. Si $n \in A$, entonces existe $m \in A$ tal que $s(m) = n$ ó $n = 0$, luego n es tal que $s(n) = s(n) \in A$. En conclusión $A = \mathbb{N}$, y todo elemento distinto del 0 cumple lo pedido. □

Teorema 1.3 – *Principio de recursión*: Dados $a \in A$ y $g : \mathbb{N} \times A \to A$, existe una única función $f : \mathbb{N} \to A$ tal que para todo $n \in \mathbb{N}$ se

cumple:

$$f(0) = a, \quad f(s(n)) = g(n, f(n)).$$

Demostración: Antes de considerar la función f como tal, diremos que una función $h\colon X \to A$ es una *aproximación* si:

1. $X \subseteq \mathbb{N}$, $0 \in X$ y para todo $n \in X_{\neq 0}$ se cumple que existe un $m \in X$ tal que $n = s(m)$.
2. h hace cumplir el enunciado (al menos respecto de los elementos que posee).

Ahora probaremos que las aproximaciones concuerdan en los valores: En concreto construyendo:

$$P := \{n \in \mathbb{N} : \forall h\colon X \to A, h'\colon Y \to A \text{ aprox.}(n \in X \cap Y \implies h(n) = h'(n))\}$$

probaremos por inducción que $P = \mathbb{N}$.

Claramente $0 \in P$, pues todas las aproximaciones toman a en el valor 0. Si h, h' son aproximaciones definidas en $s(n)$, entonces también están definidas en n (pues su dominio incluye los antecesores de todos) y cómo $n \in P$ entonces se concluye que $h(n) = h'(n)$ (por definición de P), luego $h(s(n)) = g(n, h(h)) = g(n, h'(n)) = h'(s(n))$, como se quería probar.

Ahora hemos de probar que existen aproximaciones definidas para cualquier elemento de $\mathbb{N}$, lo cual también se hace por inducción (ejercicio para el lector).

Finalmente f se define para todo $n \in \mathbb{N}$ como el valor que toma cualquier aproximación definida en n.

Por último queda la unicidad, que se hace también por inducción y es análogo a cómo se demuestra que las aproximaciones concuerdan en los valores. □

Definición 1.4: Dado un natural m se define por recursión la función $(m+) : \mathbb{N} \to \mathbb{N}$ tal que

$$\begin{aligned} m + 0 &= m & m \cdot 0 &= 0 \\ m + s(n) &= s(m + n) & m \cdot s(n) &= m \cdot n + m \end{aligned}$$

Por ejemplo,

$$\begin{aligned} 2 + 2 &= 2 + s(1) = s(2 + 1) = s(2 + s(0)) \\ &= s(s(2 + 0)) = s(s(2)) = s(3) = 4. \end{aligned}$$

Inmediatamente notemos que $s(n) = n + 1$.

Teorema 1.5: Para todo $n, m, p \in \mathbb{N}$ se cumple que $(n + m) + p = n + (m + p)$ (asociatividad).

Demostración: Se realiza por inducción sobre p:
Si $p = 0$:

$$(n + m) + 0 = n + m = n + (m + 0).$$

Si se cumple para p, entonces

$$\begin{aligned}(n + m) + (p + 1) &= ((n + m) + p) + 1 = (n + (m + p)) + 1 \\ &= n + ((m + p) + 1) = n + (m + (p + 1)).\end{aligned}$$ □

En general todas las demostraciones respecto de propiedades de la adición se hacen por medio de inducción.

Lema 1.6: Para todo $n \in \mathbb{N}$ se cumple

$$n + 0 = 0 + n = n, \quad 1 + n = n + 1.$$

Teorema 1.7: Para todo $n, m \in \mathbb{N}$ se cumple que $n + m = m + n$ (conmutatividad).

Definición 1.8: Dado un natural m se define por recursión la función $(m\cdot) : \mathbb{N} \to \mathbb{N}$ tal que

$$(m\cdot)(0) = 0, \quad (m\cdot)(n + 1) = (m\cdot)(n) + m.$$

Al igual que con la suma, escribimos $(m\cdot)(n) = m \cdot n$. En algunos casos incluso obviamos el "$\cdot$" y escribimos $mn = m \cdot n$

Teorema 1.9: Para todo $n, m, p \in \mathbb{N}$ se cumple:

1. $n(m + p) = nm + np$ (distributividad por la izquierda).
2. $(n + m)p = np + mp$ (distributividad por la derecha).
3. $n(mp) = (nm)p$ (asociatividad).
4. $n \cdot 0 = 0 \cdot n = 0$ y $n \cdot 1 = 1 \cdot n = n$.
5. $nm = mn$ (conmutatividad).

Pista: Todas las demostraciones son por inducción y/o utilizan propiedades anteriores. □

Teorema 1.10: Si $n, m \in \mathbb{N}$ son tales que existe $p \in \mathbb{N}$ tal que $n + p = m + p$, entonces $n = m$ (cancelación).

Teorema 1.11: Se cumple:

1. Si $n + m = 0$, entonces $n = m = 0$.
2. Si $nm = 0$, entonces o $n = 0$ o $m = 0$

Demostración:

1. Supongamos que $n \neq 0$, luego posee antecesor p tal que $n = p + 1$, luego $n + m = (p + m) + 1$, pero como 0 no es el sucesor de nadie, entonces $n + m \neq 0$.
2. Supongamos que $n = n' + 1$ y $m = m' + 1$, entonces

$$nm = (n' + 1)m = n'm + m = (n'm + m') + 1 \neq 0. \qquad \square$$

Definición 1.12 (Relación de orden lineal): Se dice que una relación $\leq$ sobre un conjunto A es de ***orden lineal*** si para todo $a, b, c \in A$ se cumplen:

1. $a \leq a$ (reflexividad).
2. Si $a \leq b$ y $b \leq c$ entonces $a \leq c$ (transitividad).
3. Si $a \leq b$ y $b \leq a$ entonces $a = b$ (antisimetría).
4. Se cumple que $a \leq b$ ó que $b \leq a$ (conexión).

En general si «$\leq$» es un orden lineal, entonces $a < b$ significa «$a \leq b$ y $a \neq b$».

Teorema 1.13: Se dice que un natural n es menor o igual que otro m, denotado $n \leq m$, si existe un $p \in \mathbb{N}$ tal que $n + p = m$. $\leq$ es una relación de orden lineal.

Demostración: Con $p = 0$ es claro que $\leq$ es reflexiva, la asociatividad comprueba que $\leq$ es transitiva. Si $n \leq m$ y $m \leq n$, entonces existen $p, q \in \mathbb{N}$ tales que $n + p = m$ y $m + q = n$, luego

$$n + 0 = n = m + q = n + (p + q),$$

luego por cancelación se cumple que $p + q = 0$, con lo que $p = q = 0$ y $n = m$, probando que $\leq$ es antisimétrica.

La conexión de $\leq$ se deduce por inducción. $\square$

1.2 Cardinalidad finita y buen orden

En ésta sección querremos formalizar la noción de «un conjunto de n elementos». El conjunto $I_n := \{m \in \mathbb{N} : m < n\}$ será nuestro candidato, pero formalicemos primero el por qué.

Primero necesitaremos unas propiedades con $\leq$:

Teorema 1.14: Se cumplen las siguientes:

1. El 0 es el mínimo de $\mathbb{N}$ bajo $\leq$, es decir, $0 \leq n$ para todo $n \in \mathbb{N}$. Equivalentemente si $n \leq 0$, entonces $n = 0$.
2. Para todo $n \in \mathbb{N}$ se cumple que no existe m tal que $n < m < n + 1$. Equivalentemente si $m > n$, entonces $m \geq n + 1$, o que si $m < n + 1$, entonces $m \leq n$.
3. $I_0 = \varnothing$ y para todo $n \in \mathbb{N}$ se cumplen que $n \notin I_n$ y $I_{n+1} = I_n \cup \{n\}$.

Demostración:

1. Basta notar que $0 + n = n$ para concluir que $0 \leq n$. Si $n \leq 0$, entonces como $0 \leq n$, por antisimetría se concluye que $0 = n$.
2. Si $m > n$, entonces $m = n + p$ con $p \neq 0$, así que basta probar que todo natural p o es igual a 0 o $p \geq 1$.

   Ello lo probaremos por inducción sobre p: Claramente si $p = 0$ o $p = 1$ se cumple el enunciado. Si se cumple para $p \neq 0$, entonces nótese que $1 \leq p \leq p + 1$, por lo que, por transitividad $1 \leq p + 1$.

   Más aún, si $m < n + 1$, entonces, por la proposición anterior $m + 1 \leq n + 1$, es decir, $n + 1 = (m + 1) + p$ para algún $p \in \mathbb{N}$, pero nótese que

   $$n + 1 = (m + 1) + p = m + (1 + p) = m + (p + 1) = (m + p) + 1$$

   y por cancelación del 1 se obtiene que $n = m + p$, luego $n \geq m$.
3. Son consecuencia del inciso anterior. □

De ésta forma hemos probado que

$$I_0 = \{\} \qquad I_3 = \{0, 1, 2\}$$
$$I_1 = \{0\} \qquad I_4 = \{0, 1, 2, 3\}$$
$$I_2 = \{0, 1\} \qquad \ddots$$

Éstamos listos para introducir el concepto de finitud, pero primero una noción preliminar:

Definición 1.15: Se denota que $A \lesssim B$ si existe una función $f\colon A \to B$ que sea inyectiva. Se denota que $A \approx B$ si existe una función $f\colon A \to B$ que sea biyectiva.

Proposición 1.16: Sean A, B, C conjuntos, entonces:

1. $A \approx A$.
2. $A \approx B$ syss $B \approx A$.
3. Si $A \approx B$ y $B \approx C$, entonces $A \approx C$.
4. $A \lesssim A$.
5. Si $A \lesssim B$ y $B \lesssim C$, entonces $A \lesssim C$.

Lema 1.17: Para todo $n \in \mathbb{N}$ no existe $A \subset I_n$ tal que $A \approx I_n$.

Demostración: Lo haremos por inducción sobre n:

- Caso base $n = 0$: Como $I_0 = \varnothing$ notemos que no existe $A \subset \varnothing$, así que listo.
- Caso inductivo: Supongamos que I_n cumple el enunciado. Si I_{n+1} no lo cumpliera, entonces fuera $A \subset I_{n+1}$ y $f : I_{n+1} \to A$. Si $n \notin A$, entonces $f' : I_n \to A \setminus \{f(n)\}$ es una biyección entre I_n y un subconjunto propio, lo cuál es imposible por hipótesis de inducción.

  Si $n \in A$, entonces haremos algo similar: sea $k := f^{-1}(n)$, luego sea $g : I_n \to A \setminus \{n\}$ tal que

$$g(m) := \begin{cases} f(m), & m \neq k \\ f(n), & m = k \end{cases}$$

  entonces g es una biyección entre I_n y un subconjunto propio de él (¿por qué?). □

Corolario 1.17.1: Si $A \approx I_n$ y $A \approx I_m$, entonces $n = m$.

Definición 1.18: Un conjunto A se dice ***finito*** si existe algún $n \in \mathbb{N}$ tal que $A \approx I_n$, en cuyo caso, llamamos su ***cardinal***, denotado por $|A|$, a dicho n que es único por el corolario anterior. De lo contrario se dice que A es ***infinito***.

Teorema 1.19: Se cumplen los siguientes:

1. Todo subconjunto de un conjunto finito es finito.
2. Si $A \lesssim B$ y B es finito, entonces A también y $|A| \leq |B|$.
3. Si A es infinito y $A \lesssim B$, entonces B también.
4. Si $|B| > |A|$, entonces toda función $f : B \to A$ **no** es inyectiva, es decir, hay algún elemento de A con más de una preimagen (principio del palomar).
5. $\mathbb{N}$ es infinito.

Demostración:

1. Demostraremos por inducción sobre n que todo subconjunto de I_n es finito:
   - Caso base $n = 0$: Es claro, puesto que el único subconjunto de $\varnothing$ es $\varnothing$.
   - Caso inductivo: Sea $A \subseteq I_{n+1}$. Si $n \notin A$, entonces $A \subseteq I_n$ y es finito por hipótesis inductiva. Si $n \in A$, entonces $A \setminus \{n\} \subseteq I_n$ y es finito también por hipótesis inductiva, luego existe $f\colon I_m \to A \setminus \{n\}$ biyección. Por ende $g\colon I_{m+1} \to A$ definido como
   $$g(k) := \begin{cases} f(k), & k \neq m \\ n, & k = m \end{cases}$$
   es una biyección y por ende A es finito.
2. Ejercicio para el lector.
3. Ejercicio para el lector.
4. Sean $g\colon I_m \to B$ y $h\colon A \to I_n$ biyecciones con $m > n$, entonces $F := (g \circ f \circ h)\colon I_m \to I_n$ es una inyección. Sea $S := \operatorname{Img}(F)$, entonces $S \subseteq I_n \subset I_m$, así que F es una biyección entre I_m y un subconjunto propio de él, lo cual es una contradicción.

5. Supongamos que $\mathbb{N}$ fuera finito y de cardinal n. Entonces existiría una biyección $f\colon \mathbb{N} \to I_n$. Luego la retricción $f'\colon I_{n+1} \to I_n$ es inyectiva, lo que contradice el principio del palomar. □

Una de las ventajas de introducir la noción de finitud es una caracterización muy útil de $\mathbb{N}$. Para ello definamos:

Definición 1.20: Si $(A, \leq)$ es un conjunto linealmente ordenado y $S \subseteq A$, entonces se dice que $x \in S$ es el mínimo (resp. máximo) de S, denotado mín S (resp. máx S), si para todo $s \in S$ se cumple que $x \leq s$ (resp. $x \geq s$).

Teorema 1.21: Se cumplen:

1. Todo subconjunto finito de un conjunto linealmente ordenado posee mínimo y máximo.
2. **Principio del buen orden:** Todo subconjunto S no vacío de $\mathbb{N}$ posee mínimo.
3. **Principio de inducción fuerte:** Sea $S \subseteq \mathbb{N}$ tal que si para todo $m < n$ se cumple que $m \in S$, entonces $n \in S$. Entonces $S = \mathbb{N}$.

Demostración:

1. Ejercicio para el lector (pista: emplee inducción).

2. Sea $S \subseteq \mathbb{N}$ no vacío, de modo que $n \in S$. Luego $I_{n+1} \cap S$ es un subconjunto no vacío y finito de S, por lo que posee mínimo m, veamos que $m = \text{mín}\, S$: En efecto, si $k \in S$, entonces o $k \leq n$, en cuyo caso $k \in I_{n+1} \cap S$ y $m \leq k$ por definición de mínimo; o $k > n$, en cuyo caso $m \leq n < k$, por lo que $m \leq k$.

3. Supongamos, por contradicción que $S \neq \mathbb{N}$, entonces $\mathbb{N} \setminus S$ es no vacío y por principio del buen orden tiene un mínimo n. Pero para todo $m < n$ se cumple que $m \notin \mathbb{N} \setminus S$, es decir, $m \in S$ y por construcción se ha de cumplir que $n \in S$. Contradicción. □

Definición 1.22: Sea X un conjunto linealmente ordenado, entonces una función $f\colon X \to X$ se dice ***creciente*** si $x \leq y$ implica $f(x) \leq f(y)$; si f es además inyectiva se le dice ***estrictamente creciente*** (en este caso $x < y$ implica $f(x) < f(y)$).

Teorema 1.23: Sea $f\colon \mathbb{N} \to \mathbb{N}$. Entonces:

1. f es estrictamente creciente syss para todo $n \in \mathbb{N}$ se cumple que $f(n) < f(n+1)$.
2. Si f es estrictamente creciente, entonces $n \leq f(n)$.
3. Si f es estrictamente creciente, entonces para todo $n \geq f(0)$ existe un único k natural tal que $f(k) \leq n < f(k+1)$.

Pista: Demuéstrelo por inducción. □

Proposición 1.24: Son funciones estrictamente crecientes:

1. La función identidad, $n \mapsto n$.
2. La suma por una constante, $n \mapsto n + c$.
3. El producto por una constante, $n \mapsto n \cdot c$, donde $c \neq 0$.

Definición 1.25: Si $n \leq m$ son naturales, entonces existe $p \in \mathbb{N}$ tal que $n + p = m$ y por cancelación dicho p es único, luego denotamos $p := m - n$. A esta operación la llamamos ***resta***.

Observe que la resta **no** está definida sobre todos los naturales. Una propiedad que emplearemos, y que no es difícil de probar es que $(n+1)-1 = n$.

Ésta es una variante del principio de inducción que puede resultar útil en ciertos contextos:

Teorema 1.26 (Principio de inducción regresiva o de Cauchy): Sea $S \subseteq \mathbb{N}$ y $f\colon \mathbb{N} \to \mathbb{N}$, tales que S es no vacío y f es estrictamente creciente. Si:

1. Para todo $n \in \mathbb{N}$ se cumple que $f(n) \in S$.
2. Para todo $m \in S$ tal que $1 \leq m$, se cumple que $m - 1 \in S$.

entonces $S = \mathbb{N}$.

Demostración: Supongamos que $S \neq \mathbb{N}$, entonces por el principio del buen orden se cumple que existe un N mínimo que no está en S. Entonces probaremos que para todo $m := N + k \geq N$ se cumple que $m \notin S$ por

inducción sobre k: Claramente $N+0 = N \notin S$ y si $m \notin S$, entonces $m+1 \notin S$ puesto que si $m+1 \in S$, entonces $m = (m+1)-1 \in S$ lo que contradice la hipótesis de inducción.

Sin embargo, obsérvese que $f(N) \in S$ y que $n \leq f(N)$, por ser estrictamente creciente, así que no puede existir dicho N y $\mathbb{N} = S$. □

Se le suele decir «inducción de Cauchy» cuando $f(n) = 2^n$ (demuestre que esta función es estrictamente creciente).

1.3 El algoritmo de división

Comenzaremos por una aplicación directa del principio del buen orden de $\mathbb{N}$:

Teorema 1.27 – *Algoritmo de la división*: Dados cualesquiera $a, b \in \mathbb{Z}$ con $a > 0$, existen unos únicos números $q, r \in \mathbb{Z}$ tales que

$$b = aq + r, \quad 0 \leq r < a$$

Demostración: Vamos a definir un conjunto

$$S = \{x \in \mathbb{N} : x = b - an, \quad n \in \mathbb{Z}\}$$

y veremos que es no vacío.

Si $b \geq 0$ entonces para $n = 0$ se obtiene $x = b - a \cdot 0 = b \geq 0$ luego $b \in S$.

Si $b < 0$ entonces, como a es entero positivo, luego $a \geq 1$, multiplicando por $-b$ obtenemos

$$-ab \geq -b \implies x = b - ab \geq 0,$$

finalmente $x \in S$, es decir, S es siempre no vacío.

Por principio del buen orden, S posee mínimo al que denotaremos como

$$r = b - aq.$$

Ahora hemos de probar la desigualdad con r. Supongamos que (como r es natural) por contradicción $r \geq a$, luego $r - a = b - aq - a = b - a(q+1) \geq 0$, por lo tanto, $r - a \in S$, lo que contradice el que nuestro r sea el mínimo elemento.

Finalmente probaremos la unicidad suponiendo que existen múltiples r_1, r_2 y q_1, q_2 que satisfacen, la ecuación, luego

$$aq_1 + r_1 = aq_2 + r_2,$$

supongamos que $r_2 \geq r_1$ es positivo, luego

$$r_2 - r_1 = a(q_1 - q_2)$$

como a es positivo y entero, $q_1 - q_2$ debe ser también entero positivo. Luego $r_2 - r_1$ debe ser múltiplo de a, sin embargo, como

$$0 \leq r_1 \leq r_2 < a,$$

entonces debe ser cero; con lo cual se concluye que $q_1 = q_2$. □

A tal q en el algoritmo se le dice «cociente», mientras que a r se le denomina «resto».

Definición 1.28 – *Divisibilidad*: Sean $a, b \in \mathbb{Z}$, escribiremos $a \mid b$ (léase «a divide a b», «b es múltiplo de a» o «a es un divisor de b») si existe un entero q tal que $b = aq$.

Teorema 1.29: La divisibilidad en los naturales es una relación de orden parcial.

Demostración: Es claro que es reflexiva. La transitividad es sencilla, pues

$$a \mid b \wedge b \mid c \iff b = aq_1 \wedge c = bq_2 \implies c = (aq_1)q_2 = a(q_1q_2) \implies a \mid c.$$

La antisimetría es la más difícil, pero nótese que si $b = aq_1$ con $q_1 \in \mathbb{N}$, entonces $b \geq a$ y $\leq$ ($\geq$ también) es una relación de orden total, lo que significa que es antisimétrica.

También podemos ver que no es de orden total puesto que $2 \nmid 3$ y $3 \nmid 2$. □

Por ejemplo $2 \mid 10$ o $3 \mid 6$.

Teorema 1.30: Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0$ entonces:

1. $a \mid 0$, $a \mid ka$ y $1 \mid a$ para todo $k \in \mathbb{Z}$.
2. $a \mid b$ y $c \mid d$ implican $ac \mid bd$.
3. $a \mid b$ y $b \mid c$ implican $a \mid c$.
4. $a \mid b$ y $a \mid c$ implican $a \mid ub + vc$, donde $u, v \in \mathbb{Z}$.
5. $a \mid b$ con a, b positivos implica $a \leq b$.

6. $a \mid b$ y $b \mid a$ implican $|a| = |b|$.

Demostración: Probaremos el 4:
Por construcción existen $q_1, q_2 \in \mathbb{Z}$ tales que $b = aq_1$ y $c = aq_2$, finalmente $ub + vc = uaq_1 + vaq_2 = a(uq_1 + vq_2)$. □

Definición 1.31: Dados $a, b \in \mathbb{Z}$ definimos el *máximo común divisor* como el número natural $M = (a; b)$ (a veces denotado como $\text{mcd}(a, b)$) como aquel que satisface:

MCD1. $M \mid a$ y $M \mid b$.

MCD2. Si $c \in \mathbb{N}$, $c \mid a$ y $c \mid b$, entonces $c \leq M$.

Análogamente, definimos el *mínimo común múltiplo* $m = \text{mcm}(a, b)$ como el número natural que satisface:

MCM1. $a \mid m$ y $b \mid m$.

MCM2. Si $c \in \mathbb{N}$, $a \mid c$ y $a \mid c$, entonces $m \leq c$

Cabe destacar que el máximo común divisor no es una *función ordenada*, es decir, $(a; b) = (b; a)$.

Proposición 1.32: Para todo $a, b \in \mathbb{N}$ se cumple que $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = ab$.

Teorema 1.33: Sean $a, b, k \in \mathbb{Z}$ no nulos, entonces

1. $(a; b) = (-a; b) = (-a; -b) = (|a|; |b|)$.

2. $(ak; bk) = |k|(a; b)$.

3. $(a; b) = d$ syss $(a/d; b/d) = 1$.

Lema 1.34: Sean $a, b \in \mathbb{Z}$ tales que $b = aq + r$, entonces $(a; b) = (a; r)$.

Demostración: Sean $k = (a; b)$ y $l = (a; r)$. Es fácil ver que como $r = b - aq$, entonces $k \mid r$ por definición $k \leq l$. Asimismo, se deduce que $k \geq l$; con lo cual $k = l$. □

Teorema 1.35 (Algoritmo de Euclides): Sean $a, b \in \mathbb{Z}$, una forma de calcular $(a; b)$ es a través del siguiente método:

$$\begin{aligned} b &= aq_1 + r_1, & 0 < r_1 < a \\ a &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_n &= r_{n+1}q_{n+2}, \end{aligned}$$

dónde $r_{n+1} = (a; b)$.

Tomemos dos números cualesquiera: 288 y 560, e intentemos aplicar al método de Euclides:

$$\begin{aligned} 560 &= 288 \cdot 1 + 272 \\ 288 &= 272 \cdot 1 + 16 \\ 272 &= 16 \cdot 17 \end{aligned}$$

por lo tanto $16 = (288; 560)$.

Teorema 1.36 – *Identidad de Bézout*: Para todo $a, b \in \mathbb{Z}$ existen $x, y \in \mathbb{Z}$ tales que $(a; b) = ax + by$.

Demostración: Definamos el conjunto

$$S = \{z > 0 : z = ax + by, \quad x, y \in \mathbb{Z}\}$$

veamos que no es vacío. Pues $a^2 + b^2 \in S$. Por principio del buen ordenamiento posee mínimo $g = ax_0 + by_0$.

Podemos ver que g divide a a y a b pues

$$a = qg + r, \quad 0 \leq r < g$$

con lo cual

$$\begin{aligned} r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + by_0 \in S \end{aligned}$$

Si $r \neq 0$ entonces se contradice con que g era el menor.

Como g es un divisor común de a, b se concluye que $g \leq d = (a; b)$.

Como $d \mid a$, $d \mid b$, entonces $d \mid ax_0 + by_0 = g$. Al ser ambos positivos, $d \leq g$. Por antisimetría $d = g$. □

Definición 1.37 – *Números coprimos y primos*: Decimos que $a, b \in \mathbb{Z}$ son *coprimos* syss $(a; b) = 1$. Un número primo p es aquel que es positivo y sólo posee dos divisores naturales: el 1 y p. Los números que son el producto de números primos son llamados *compuestos*.

Nótese que como los números primos por definición poseen dos divisores, el 1 no es primo, pero tampoco cumple con la condición para ser compuesto. Más adelante veremos que es el único natural que posee esta propiedad.

Teorema 1.38: Sea p un número primo tal que $p \nmid a$ entonces p, a son coprimos.

Demostración: Por definición $d = (p; a)$ cumple $d \mid p$, luego $d \mid 1$ o $d \mid p$. Como $d \mid a$ y $p \nmid a$ entonces $d \nmid p$, es decir, $d \mid 1$. □

Esto podríamos haberlo utilizado como definición auxiliar de *primo*.

Teorema 1.39: Si se encuentran $u, v \in \mathbb{Z}$ tales que

$$ua + vb = 1,$$

entonces a, b son coprimos.

Demostración: Considere la prueba anterior, demostramos que el mínimo del conjunto equivale al máximo común divisor, como dicho conjunto admite únicamente valores positivos, el mínimo valor posible es 1, de ser obtenido, es inmediato que equivale al mcd. □

Teorema 1.40 – *Lema de Euclides*: Sea $a \mid bc$ con a, b coprimos; entonces $a \mid c$.

Demostración: Por identidad de Bézout, $1 = ax_0 + by_0$, por lo tanto, $c = ax_0c + by_0c$. Evidentemente $a \mid ax_0c$ y por construcción $a \mid y_0bc$, luego $a \mid ax_0c + by_0c = c$. □

Más adelante nos referiremos a esta propiedad como "ley de cancelación".

Teorema 1.41: Sea $(a; b) = 1$ y $(a; c) = 1$, entonces $(a; bc) = 1$.

Demostración: Digamos que $d = (a; bc)$. Como $d \mid a$ y $(a; b) = 1$, se obtiene que $(d; b) = 1$. Por lema de Euclides $d \mid c$. Y como $(a; c) = 1$ entonces $d = 1$. □

Teorema 1.42: Sea p primo tal que $p \mid ab$ entonces $p \mid a$ o $p \mid b$. Más aún, si $p \mid a_1 \cdots a_n$, entonces divide a por lo menos uno de los a_i.

Demostración: Probaremos la primera proposición. Si $p \mid ab$ pero $p \nmid a$, lo que implica $(p; a) = 1$, por lema de Euclides, $p \mid b$. El resto es por inducción. □

Teorema 1.43 – *Teorema fundamental de la aritmética*: Todo número natural mayor que 1 es o primo o compuesto y puede escribirse como un único producto de números de primos (descomposición prima).

Demostración: Primero probaremos que todo número o es primo o es compuesto. Supongamos que tenemos el siguiente conjunto

$$S = \{n \in \mathbb{N} : n > 1 \text{ y } n \text{ es primo o compuesto}\},$$

probaremos que contiene a todo $n > 1$ por inducción. Evidentemente $2 \in S$. Si $n+1$ es primo entonces pertenece a S, sino, puede escribirse como $n+1 = ab$ donde como $a \mid n+1$ se cumple que $a \leq n+1$ y $b \leq n+1$, luego $a, b \in S$; es decir, a, b o son primos o son producto de primos, por lo tanto, $n+1$ es compuesto.

Ahora probaremos que la descomposición prima es única. Supongamos que no lo fuese y hubiesen dos posibles descomposiciones primas:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell.$$

Luego $p_1 \mid q_1 q_2 \cdots q_k$. Por ser primo, $p_1 \mid q_i$ para algún $1 \leq i \leq \ell$, y por ser q_i primo se cumple que $p_1 = q_i$, reordenemos tal que dicho índice $i = 1$. Luego podemos aplicar el mismo método sobre

$$\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_\ell$$

para ver que, por inducción, $p_1 = q_1, p_2 = q_2, \ldots, p_k = q_\ell$ y $k = \ell$. Es decir, la factorización es única. □

Corolario 1.43.1: Todo número entero es: ± 1, primo o un múltiplo de un primo (el 0 cae en este último grupo).

Éste teorema tiene varias razones para considerarse «fundamental»: en primer lugar ilustra la importancia de los números primos, y en segundo, ofrece una herramienta universal (la descomposición prima) para comprender la divisibilidad entre números. He aquí dos ejemplos concretos:

Teorema 1.44: Sean n, m dos números cuya descomposición prima es la siguiente:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

donde los p_i's son primos distintos y los α_i, β_i's pueden ser nulos. Entonces $n \mid m$ syss $\alpha_i \leq \beta_i$ para todo $i \in \{1, 2, \ldots, k\}$.

Teorema 1.45: Sean n, m dos números cuya descomposición prima es la siguiente:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

donde los p_i's son primos distintos y los α_i, β_i's pueden ser nulos. Definiendo $\gamma_i := \text{mín}\{\alpha_i, \beta_i\}$ y $\delta_i := \text{máx}\{\alpha_i, \beta_i\}$ se cumple que

$$\text{mcd}(n, m) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}, \quad \text{mcm}(n, m) = p_1^{\delta_1} \cdots p_k^{\delta_k}.$$

Éste ejercicio nos dice que si conocemos la descomposición prima de dos números, entonces su mcd y mcm es fácil de calcular. El problema, implícito aquí, está en que computacionalmente es muy ineficiente calcular la descomposición prima de números (excepto cuando éstos son pequeños, o tienen patrones muy definidos), por ello el algoritmo de Euclides es tan relevante.

Ejercicio 1.46 (AIME 1988): ¿Cuál es la probabilidad de que un divisor de 10^{99} sea un múltiplo de 10^{88}?

Solución: Sabemos que la factorización prima de 10 es $2 \cdot 5$, luego $10^{99} = 2^{99} \cdot 5^{99}$, por lo que sus divisores son de la forma $2^n \cdot 5^m$ con $0 \leq n, m \leq 99$, lo que da 100 posibilidades para n y m, ergo, hay $100^2 = 10000$ divisores de 10^{99}. Para que un número $2^n \cdot 5^m$ sea múltiplo de 10^{88} ha de cumplirse que $88 \leq n, m \leq 99$ lo que nos da 12 posibilidades para n y m, ergo hay $12^2 = 144$ divisores de 10^{99} que son múltiplos de 10^{88}. Luego la probabilidad buscada es:

$$\frac{144}{10000} = \frac{9}{625} = 14{,}4\,\%. \qquad \square$$

Teorema 1.47: Los números primos son infinitos.

Demostración(Euclides): Sean $p_1 < p_2 < \cdots < p_r$ primos. Sea $N := p_1 \cdots p_r \geq 2$. Como c y $c+1$ son coprimos cuando $c \geq 2$, entonces $p_i \mid N$, pero $p_i \nmid N+1$, por lo que N posee algún factor primo que no estaba en nuestra lista. □

Es usual que la prueba de Euclides se presente como una demostración por contradicción, pero es absolutamente constructiva. Se puede variar un poco la demostración en las siguientes:

Demostración(Kummer): Sean $p_1 < p_2 < \cdots < p_r$ primos. Sea $N := p_1 \cdots p_r > 2$ (puesto que sabemos que el 2 y el 3 son primos), si existiese i tal que $p_i \mid N-1$, entonces $p_i \mid N-(N-1) = 1$ lo cual es absurdo. □

Demostración(Stieltjes): Sean $p_1 < p_2 < \cdots < p_r$ primos y sea $N := p_1 \cdots p_r$. Podemos factorizar $N = mn$ y notar que cada p_i o bien divide a m o bien divide a n, pero no a ambos. Luego $m+n \geq 2$ no posee a ningún p_i por factor. □

También, suele ser necesario tener que confirmar si un número es primo, por lo cual, hay varias formas, la primera es **la criba de Eratóstenes** que consiste en denotar los números de 2 hasta n y comenzar tachando los múltiplos de los primos, los no tachados resultan ser primos:

		2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~
~~10~~	**11**	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**
~~20~~	~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**
~~30~~	**31**	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~
~~40~~	**41**	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	**53**	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	**59**
~~60~~	**61**	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	**67**	~~68~~	~~69~~
~~70~~	**71**	~~72~~	**73**	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	**79**
~~80~~	~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**
~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~

pero considera que si queremos ver si n es primo debemos comprobar que no sea divisible por ningún número entre 2 y $n-1$ (lo cuál es un proceso terriblemente ineficiente). Por lo cuál, el truco está en probar **sólo** los números primos, del 2 hasta $\sqrt{n}$.

Definición 1.48: Una ***ecuación diofántica*** es una expresión del estilo $f(x_1, \ldots, x_n) = 0$ donde $f \in \mathbb{Z}[x_1, \ldots, x_n]$. La ecuación se dice ***homogénea*** si f es homogéneo, i.e., si todos los monomios de f tienen

el mismo grado.

Las ecuaciones diofánticas usualmente conllevan a dos clases de preguntas: las soluciones racionales (en $\mathbb{Q}$) y las soluciones enteras (en $\mathbb{Z}$).

Toda ecuación diofántica homogénea admite la solución trivial $(0, 0, \ldots, 0)$ así que nos enfocamos en las soluciones no triviales. Nótese que la existencia de soluciones racionales no triviales implica la de soluciones enteras: en efecto, si $(p_1/q_1, \ldots, p_n/q_n)$ es una solución de f de grado d, entonces existe un entero N tal que $N \mid q_i$ para todo i y luego

$$f(Np_1/q_1, \ldots, Np_n/q_n) = N^d f(p_1/q_1, \ldots, p_n/q_n) = 0.$$

Las ecuaciones diofánticas son protagonistas en la teoría de números. No obstante, es notorio el hecho de que, pese a ser algunas bastante simples, no es para nada fácil encontrar sus soluciones.

Tomemos como ejemplo la ecuación diofántica lineal. De la identidad de Bézout se sigue lo siguiente:

Teorema 1.49: Una ecuación de la forma $ax + by = n$, donde $a, b, n \in \mathbb{Z}$ tiene soluciones enteras syss $(a; b) \mid n$.

Teorema 1.50: Sean x_0, y_0 soluciones enteras de la ecuación

$$ax + by = n \tag{1.1}$$

entonces el resto de soluciones son exactamente los de la forma

$$x = x_0 + bt, \quad y = y_0 - at; \qquad t \in \mathbb{Z}.$$

1.4 El álgebra de la escuela

En la escuela básica se nos enseñan varias cosas bastante concretas de los números, como por ejemplo que todo número se puede expresar en base diez así como «13» o «452». También se nos enseñan métodos para calcular la multiplicación y división. A pesar de que es algo tan fundamental es curioso como casi nunca se justifican éstos métodos, como ¿por qué la multiplicación funciona como tal? Aquí daremos razones para ello.

Primero comencemos con las bases viendo lo siguiente:

Lema 1.51: Para todo $b \geq 2$, la función $n \mapsto b^n$ es estrictamente creciente.

Teorema 1.52: Dado un $b \geq 2$, entonces todo número natural $n \neq 0$ se puede expresar como

$$n = d_k b^k + \cdots + d_2 b^2 + d_1 b^1 + d_0$$

si $b^k \leq n < b^{k+1}$, donde para todo i se da que $d_i < b$ y $d_k \neq 0$. Más aún, ésta representación es única, es decir, los d_i's lo son.

Demostración: Aquí hay que probar dos cosas, que cada número admite dicha representación y que es única.

i) Cada natural admite una representación: Procedamos por contradicción: de no cumplirse sea n el mínimo natural que lo cumple. Claramente $n \neq 0$ por definición, así que existe un único k natural tal que $b^k \leq n < b^{k+1}$, y por definición $m := (n - b^k)$ si admite una representación.

   Si $m = 0$, entonces $n = 1 \cdot b^k$. Si $m < b^k$, entonces admite una representación con dígitos d'_i y n se representa con los mismos dígitos, donde $d_i = d'_i$ si existe, $d_k = 1$ y $d_i = 0$ en otro caso. Si $b^k \leq m$, entonces $m = d'_k b^k + \cdots + d'_0$ y $0 < d'_k < b$; pero $d'_k + 1 < b$, de lo contrario $n \geq b^{k+1}$, así que definiendo $d_i := d'_i$ para todo $i < k$ y $d_k := d'_k + 1$ se obtiene una representación para n.

ii) Dicha representación es única: Supongamos que

$$n = d_k b^k + \cdots + d_1 b^1 + d_0 = e_k b^k + \cdots + e_1 b^1 + e_0$$

   entonces consideremos su resta que está bien definida en $\mathbb{Z}$:

$$(d_k - e_k) b^k + \cdots + (d_1 - e_1) b^1 + (d_0 - e_0) = 0 \tag{1.2}$$

   así pues, como $b \mid 0$ se concluye que $b \mid (d_0 - e_0)$ y como $0 \leq d_0 < b$ y $0 \geq e_0 > -b$ nos queda que $b > d_0 - e_0 > -b$ y así pues $d_0 - e_0 = 0$, osea $d_0 = e_0$. Luego dividimos (1.2) por b^1 y obtenemos que

$$(d_k - e_k) b^{k-1} + \cdots + (d_2 - e_2) b^1 + (d_1 - e_1) = 0$$

   y procedemos del mismo modo para concluir que $d_1 = e_1$, y así sucesivamente. □

Definición 1.53: Dado $b \geq 2$, entonces para todo $n \geq 1$ se denota

$$n = (d_k d_{k-1} \cdots d_1 d_0)_b \iff n = d_k b^k + \cdots + d_1 b^1 + d_0$$

a la que se le llama *representación de n en base b* o b-aria. A los d_i's se les llama *dígitos* de la representación.

Cuando no se especifica la base se asume que es base $9+1$ (anotamos eso en lugar de «10», pues para toda base b se cumple que $(10)_b = b$). Otras representaciones comúnes son la base 2 o binaria, donde

$$11010_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 = 34;$$

y la base 16 o hexadecimal, donde se identifican $\mathrm{A} = 10, \mathrm{B} = 11, \ldots, \mathrm{F} = 15$ y donde

$$\mathrm{D56B}_{16} = 13 \cdot 16^3 + 5 \cdot 16^2 + 6 \cdot 16^1 + 11 = 54635,$$

ésta última se emplea en contextos informáticos.

1.5 El lenguaje de anillos

Ahora que tenemos introducido la noción básica de números naturales, enteros y racionales, conviene ampliar esta definición al contexto más general de los *anillos* y los *cuerpos*. Hay tratamientos más profundos de los anillos en mi libro de álgebra **[1],** pero nos contentaremos con dar un resumen orientado a la teoría de la divisibilidad.

Definición 1.54: Un ***anillo*** es una quíntupla $(A, +, \cdot, 0, 1)$ tal que para todo $a, b, c \in A$ se satisface:

1. $(a+b)+c = a+(b+c)$ (asociatividad).
2. $0+a = a+0 = a$ (neutro aditivo).
3. Existe $-a \in A$ tal que $a+(-a) = (-a)+a = 0$ (inverso aditivo).
4. $a+b = b+a$ (conmutatividad).
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociatividad).
6. $1 \cdot a = a \cdot 1 = a$ (neutro multiplicativo).
7. $(a+b) \cdot c = a \cdot c + b \cdot c$ (distributividad).

De no haber ambigüedad diremos que A es un anillo.

Un anillo se dice ***conmutativo*** si la multiplicación es conmutativa, i.e., si $a \cdot b = b \cdot a$ para todo $a, b \in A$. Un ***dominio*** es un anillo conmutativo donde $1 \neq 0$. Un ***cuerpo*** k es un dominio que posee inversos

multiplicativos, i.e., si para todo $a \in k_{\neq 0}$ se cumple que existe $a^{-1} \in k$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Ejemplo.
- El anillo nulo $A := \{0\}$ donde $0 + 0 := 0$ y $0 \cdot 0 = 0$ es un anillo donde $1 = 0$. Recíprocamente, si en un anillo se satisface que $1 = 0$, entonces corresponde al anillo nulo.
- $\mathbb{Z}$ es un anillo.
- $\mathbb{Q}$ es un cuerpo.

Ahora queremos formalizar las ideas de *divisor*, *número primo*, etc., en contexto de los anillos:

Definición 1.55: Sea A un anillo. Un elemento no nulo $a \in A_{\neq 0}$ se dice ***invertible*** si existe $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$; el conjunto de los invertibles de A se denota por $A^\times$ (e.g., $1 \in A^\times$).

Sean $a, b \in A$, se denota $a \mid b$ si existe $c \in A$ tal que $ac = b$; en cuyo caso se dice que a es un ***divisor*** de b. Se dice que $a, b \in A$ son ***asociados*** si existe $u \in A^\times$ tal que $a = ub$. Un divisor de $b \in A$ se dice un ***divisor propio*** si no es asociado a b ni es invertible. Un elemento que no es nulo ni invertible se dice ***irreducible*** si no posee divisores propios, de lo contrario se dice ***reducible***.

Hay un tipo especial de divisores, llamados los ***divisores de cero*** que son los $a \in A_{\neq 0}$ tales que existe $b \in A_{\neq 0}$ con $ab = 0$. Un anillo se dice un ***dominio íntegro*** si es conmutativo y no posee divisores de cero.

Un elemento $p \in A$ que no es nulo ni invertible se dice un ***primo*** si para todo $a, b \in A$ tal que $p \mid ab$ se cumple que $p \mid a$ o que $p \mid b$.

Así pues, los elementos de un anillo se dividen entre: el 0, los invertibles, los reducibles y los irreducibles. No es cierto en general que los primos coincidan con los irreducibles, pero:

Proposición 1.56: En un dominio íntegro, todo elemento primo es irreducible.

Demostración: Sea $p \in A$ primo y sea $a \in A$ un divisor de p, vale decir, existe $b \in A$ tal que $p = ab$, luego $p \mid ab$ y por definición de primo se concluye que $p \mid a$ o que $p \mid b$. Sin perdida de generalidad supongamos que $p \mid a$, es decir, existe $c \in A$ tal que $pc = a$ y $p = p(cb)$, luego $p(cb - 1) = 0$, pero como

A no posee divisores de cero y $p \neq 0$, entonces $cb = 1$, luego $b, c \in A^\times$ y se comprueba que a está asociado a p. □

Definición 1.57: Sea A un dominio. Un ***ideal*** $\mathfrak{a}$ de A, denotado $\mathfrak{a} \trianglelefteq A$, es un subconjunto $\mathfrak{a} \subseteq A$ no vacío tal que para todo $a, b \in \mathfrak{a}$ se cumple que $a + b, a \cdot b \in \mathfrak{a}$ y para todo $c \in A$ se cumple que $ac \in \mathfrak{a}$.

Un ideal $\mathfrak{p} \lhd A$ se dice ***primo*** si para todo $a, b \in A$ tales que $ab \in \mathfrak{p}$ se concluye que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Un ideal $\mathfrak{m} \lhd A$ se dice ***maximal*** si es $\subseteq$-maximal entre los ideales impropios, i.e., si para todo $\mathfrak{a} \trianglelefteq A$ con $\mathfrak{m} \subset \mathfrak{a}$ se cumple que $\mathfrak{a} = A$.

Ejemplo.
1. En un dominio arbitrario A se cumple que $\{0\}$ y A son ideales de A, llamados ***ideales impropios***.
2. En $\mathbb{Z}$, el conjunto $n \cdot \mathbb{Z} := \{na : a \in \mathbb{Z}\}$ para todo $n \in \mathbb{Z}$ es un ideal.

Lema 1.58: La intersección de ideales es un ideal.

Demostración: Sean $\{\mathfrak{a}_i\}_{i \in I}$ un conjunto de ideales, y sea $\mathfrak{b} := \bigcap_{i \in I} \mathfrak{a}_i$, veremos que se trata de un ideal. Sea $a, b \in \mathfrak{b}$, esto quiere decir que $a, b \in \mathfrak{a}_i$ para todo $i \in I$, luego para todo $c \in A$ y todo $i \in I$ se cumple que $a + b, ab, ca \in \mathfrak{a}_i$ (por definición de ideales), luego $a + b, ab, ca \in \mathfrak{b}$. □

Corolario 1.58.1: Sea $S \subseteq A$ un subconjunto de un dominio A, entonces

$$\bigcap \{\mathfrak{a} : S \subseteq \mathfrak{a} \trianglelefteq A\},$$

es un ideal y es de hecho el más pequeño que contiene a S.

Definición 1.59: Denotamos

$$(S) := \bigcap \{\mathfrak{a} : S \subseteq \mathfrak{a} \trianglelefteq A\},$$

y si $S = \{a_1, \ldots, a_n\}$, entonces $(a_1, \ldots, a_n) := (S)$. Si $\mathfrak{a}$ es un ideal, se dice que un conjunto S es un ***generador*** si $(S) = \mathfrak{a}$. Un ideal se dice ***finitamente generado*** si posee un conjunto generador finito, y se dice ***principal*** si está generado por un sólo elemento.

Corolario 1.59.1: Un elemento $a \in A$ es primo syss el ideal (a) es primo.

Proposición 1.60: Todo ideal maximal es un ideal primo.

Definición 1.61: Sea A un dominio íntegro. Una ***norma euclídea*** es una aplicación $\phi\colon A_{\neq 0} \to \mathbb{N}$ que satisface lo siguiente: dados $a \in A$ y $b \in A_{\neq 0}$, entonces existen $q, r \in A$ tales que

$$a = qb + r,$$

donde $r = 0$ o $\phi(r) < \phi(a)$ (algoritmo de la división).

Un dominio íntegro A se dice un:

Dominio euclídeo Si posee alguna norma euclídea.

Dominio de ideales principales (abrev., DIP) Si todos sus ideales son principales.

Dominio de factorización única (abrev., DFU) Si todo elemento no nulo ni invertible $a \in A$ se escribe de forma $a = p_1 \cdots p_n$ con cada p_i primo; y si se escribe de otra manera $a = q_1 \cdots q_m$, entonces $n = m$ y tras una permutación se cumple que cada p_i está asociado a q_i.

Teorema 1.62: Todo dominio euclídeo es un DIP.

Demostración: Sea $\mathfrak{a} \trianglelefteq A$, si $\mathfrak{a} = \{0\}$ entonces es principal (generado por 0). Si no, entonces posee elementos no nulos y podemos elegir $a \in \mathfrak{a}$ con norma mínima, luego $(a) \subseteq \mathfrak{a}$. Sea $b \in \mathfrak{a}$, entonces por algoritmo de la división se cumple que $b = aq + r$ con $r = 0$ o $\phi(r) < \phi(a)$. Si $r \neq 0$ entonces $r = b - aq \in \mathfrak{a}$ tiene norma menor que a lo que contradice la elección de a. Así que $r = 0$ y $b = aq \in (a)$. □

Teorema 1.63 (lema de Euclides): Sea A un DIP. Entonces un elemento a es irreducible syss (a) es maximal. En consecuencia, todo irreducible es primo.

1.6 Problemas clásicos en la teoría elemental

§1.6.1 El problema de Basilea, irracionalidad de π y otra demostración de la infinitud de primos. Ésto es muy curioso, pero no deja de ser una demostración genial:

Teorema 1.64 (Problema de Basilea): Se cumple que

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Demostración: Ésta demostración se le atribuye a Cauchy. Nótese que la fórmula de Euler induce

$$(\cos x + \mathrm{i}\sin x)^n = e^{\mathrm{i}nx} = \cos(nx) + \mathrm{i}\sin(nx).$$

A la izquierda tenemos la potencia de un binomio que iguala a

$$(\cos x + \mathrm{i}\sin x)^n = \sum_{k=0}^{n} \binom{n}{k} \mathrm{i}^k \sin^k x \cos^{n-k} x,$$

en particular, si $k = 2r+1$ se tiene que $\mathrm{i}^k = (-1)^r\mathrm{i}$. Por igualdad de las coordenadas complejas se tiene:

$$\sin(nx) = \binom{n}{1} \sin x \cos^{n-1} x - \binom{n}{3} \sin^3 x \cos^{n-3} x + \cdots \tag{1.3}$$

Lo que querremos es emplear la expresión de la derecha para construir un polinomio, así que elijamos primero que $n = 2m+1$ sea impar para que su último término sea de la forma $(-1)^m \sin^n x$ y elijamos los siguientes valores para el x:

$$\alpha_k := \frac{k\pi}{2m+1}, \quad k \in \{1, \ldots, m\}$$

de modo que $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_m < \pi/2$ y que $n\alpha_k = \pi$, luego $\sin(n\alpha_k) = 0$ y así dividiendo por $\sin^n(\alpha_k)$ en (1.3) se obtiene:

$$\begin{aligned} 0 &= \binom{n}{1} \left(\frac{\cos(\alpha_k)}{\sin(\alpha_k)}\right)^{n-1} - \binom{n}{3} \left(\frac{\cos(\alpha_k)}{\sin(\alpha_k)}\right)^{n-3} + \cdots \\ &= \binom{2m+1}{1} \tan^{-2m}(\alpha_k) - \binom{2m+1}{3} \tan^{-2(m-1)}(\alpha_k) + \cdots \end{aligned}$$

Luego podemos considerar el siguiente polinomio:

$$p(x) = \binom{2m+1}{1} x^m - \binom{2m+1}{3} x^{m-1} + \cdots$$

que tiene grado m luego tiene a lo más m raíces. Nótese sin embargo que cada $\beta_k := \tan^{-2}(\alpha_k)$ es raíz de $p(x)$ y son distintas puesto que, empleando la identidad trigonométrica,

$$1+\tan^{-2}(x) = \sin^{-2}(x) \implies \tan^{-2}(x) = \tan^{-2}(y) \implies \sin^{-2}(x) = \sin^{-2}(y),$$

sin embargo cada α_k está en $(0, \pi/2)$, en donde la función sin es positiva e inyectiva.

Como las raíces de $p(x)$ son $\beta_1, \ldots, \beta_m$ y su coeficiente lider es $\binom{2m+1}{1} = (2m+1)$ se factoriza así:

$$p(x) = (2m+1)(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m).$$

De modo que el coeficiente que acompaña al término x^{m-1} es:

$$(2m+1)(\beta_1+\beta_2+\cdots+\beta_m) = \binom{2m+1}{3} = \frac{(2m+1)2m(2m-1)}{6}$$

cancelando en ambos lados el $(2m+1)$ se obtiene que

$$\tan^{-2}(\alpha_1)+\cdots+\tan^{-2}(\alpha_m) = \frac{2m(2m-1)}{6}, \tag{1.4}$$

Podemos volver a emplear la identidad trigonométrica para notar que $\tan^{-2}(\alpha_k) = \sin^{-2}(\alpha_k) - 1$ y así

$$\sin^{-2}(\alpha_1)+\cdots+\sin^{-2}(\alpha_m) = \frac{2m(2m-1)}{6} + m = \frac{2m(2m+2)}{6}. \tag{1.5}$$

Ya estamos casi listos, sólo falta hacer la siguiente observación, válida para todo $x \in (0, \pi/2)$:

$$0 \le \sin x \le x \le \tan x,$$

como son todos positivos, podemos dar vuelta las desigualdades elevando a (-1)

$$0 \le \frac{1}{\tan x} \le \frac{1}{x} \le \frac{1}{\sin x},$$

y se conserva si elevamos a 2:

$$0 \le \tan^{-2}(x) \le x^{-2} \le \sin^{-2} x.$$

Finalmente sumamos sobre todos los valores de α_k, empleando las ecuaciones (1.4) y (1.5):

$$\frac{2m(2m-1)}{6} \le \sum_{k=1}^{m} \left(\frac{2m+1}{k\pi}\right)^2 \le \frac{2m(2m+2)}{6}$$

y multiplicamos por $(\pi/2m+1)^2$ para obtener:

$$\frac{2m(2m-1)}{(2m+1)^2}\frac{\pi}{6} \le \sum_{k=1}^{m} \frac{1}{k^2} \le \frac{2m(2m+2)}{(2m+1)^2}\frac{\pi}{6}$$

donde se termina el problema, pues los términos en azul y rojo convergen a 1 cuando $m \to \infty$ y se concluye empleando el teorema del sandwich. □

Ahora probaremos que π^2 es irracional, según la prueba de [**101,** pp. 19–21].

Lema 1.65: Si $g(x) \in \mathbb{Z}[x]$ y $h(x) := x^n g(x)/n!$, entonces $h^{(k)}(0)$ es entero para todo k. Más aún si $k \neq n$, entonces $n+1 \mid h^{(k)}(0)$ y si $g(0) = 0$, entonces $n+1 \mid h^{(n)}(0)$.

Demostración: Basta notar que $f(x) := x^n g(x)$ es un polinomio de coeficientes enteros, luego si c_j son los coeficientes de f se cumple que

$$h^{(k)}(x) = \frac{c_k \cdot (k!)}{n!}.$$

Nótese que $c_0 = c_1 = \cdots = c_{n-1} = 0$ y si $k > n$ claramente se cumple el enunciado. Más aún $g(0) = 0$ se traduce en que $c_n = 0$ así que también se cumple, tal como se quería probar. □

Teorema 1.66: π y π^2 son irracionales.

Demostración: Nótese que si π^2 es irracional, entonces π también lo es (pues toda potencia natural de un racional es racional). Comencemos por definir

$$f(x) := \frac{x^n(1-x)^n}{n!},$$

que por el lema anterior tiene derivadas enteras en 0 y de hecho, como $f(1-x) = f(x)$, también tiene derivadas enteras en 1. Además satisface la siguiente desigualdad:

$$0 < f(x) < \frac{1}{n!}, \quad x \in (0,1).$$

Supongamos que $\pi^2 = a/b$ con $a, b \in \mathbb{N}_{\neq 0}$, entonces

$$F(x) := b^n\big(\pi^{2n} f(x) - \pi^{2(n-1)} f^{(2)}(x) + \cdots + (-1)^n f^{(2n)}(x)\big)$$

satisface que $F(0)$ y $F(1)$ son enteros (por la observación de las derivadas de f). Ahora nótese que

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}x}(F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)) &= F''(x)\sin(\pi x) + \cancel{\pi F'(x)\cos(\pi x)} \\ &\quad - \cancel{\pi F'(x)\cos(\pi x)} + \pi^2 F(x)\sin(\pi x) \\ &= (F''(x) + \pi^2 F(x))\sin(\pi x) \\ &= b^n \pi^{2n+2} f(x)\sin(\pi x) = a^n \pi^2 f(x)\sin(\pi x).\end{aligned}$$

Es decir, por el teorema fundamental del cálculo, que

$$a^n\pi \int_0^1 f(x)\sin(\pi x)\,\mathrm{d}x = \left[\frac{F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)}{\pi}\right]_0^1 = F(1)+F(0).$$

(Empleando que $\sin(\pi) = \sin(0) = 0$ y que $-\cos(\pi) = \cos(0) = 1$.) El cual es un número entero y, de hecho, es estrictamente positivo puesto que $f(x)\sin(\pi x)$ lo es en el intervalo $(0, 1)$. Pero

$$0 < a^n\pi \int_0^1 f(x)\sin(\pi x)\,\mathrm{d}x < a^n\pi \int_0^1 \frac{1}{n!}\,\mathrm{d}x = \frac{a^n\pi}{n!}$$

lo cual no es entero para un n suficientemente grande. Contradicción. □

Ahora una demostración absolutamente ilegal de la infinitud de primos: nótese que

$$\prod_p (1+p^{-2})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

donde el término de la derecha es irracional. Pero si hubieran finitos primos, claramente el producto de la izquierda sería racional. Contradicción.

Notas históricas

Los números son tan antiguos como la civilización misma lo permite. Sistemas numéricos acompañan históricamente a los registros más antiguos y precarios de escritura, posiblemente empleados con el propósito de llevar cuentas de, por ejemplo, la cantidad de recursos a disposición, o bien como una forma primitiva de economía.

Los registros más antiguos datan de tablillas empleadas por los egipcios, pero los trabajos de los babilonios nos son mucho más familiares. Los babilinios desarrollaron métodos de representación en expansiones en serie.[1] Los babilonios también conocían el método de «completación de cuadrados» para resolver ecuaciones cuadráticas y mediante tablas de $x^2(x+1)$ eran capaces de resolver algunas cúbicas. Los griegos mantienen un sistema decimal con ciertas limitaciones,[2] y trabajaban también con fracciones.

[1] Explícitamente, los babilinios escribían los números en base 60 con subexpansiones de la forma $10 \cdot 60^n$.

[2] Por ejemplo, para los griegos $\alpha = 1$ y $\iota = 10$, de modo que $\iota\alpha = 11$. Por la longitud de su alfabeto, tenían la limitación de que los milenios los denotaban con una comilla, como $,\alpha = 1000$ y las decenas de mil las denotaban con una M (μ mayúscula) con un superíndice, como $\mathrm{M}^\beta = 20000$.

Entre los griegos, destaca la corriente de los pitagóricos, que recibe su nombre del geométra Pitágoras. Los pitagóricos ahondaban en la filosofía tras de los números, y naturalmente la pregunta acerca de cómo definir un número. **Euclides** define un número como «una multitud compuesta de unidades», donde una unidad es «aquello cuya existencia es llamada, por virtud, uno»; de manera que ni pitagóricos ni euclídeos consideran al 1 como un número. Aristóteles dice: «aquello que es divisible en partes discretas se dice *multitud*, y su multiplicidad acotada (finita) se dice *número*.»

Entre 300 a.C. y 600 d.C., en India bajo influencia babilónica surge la notación decimal con el cero que, además de representar los números, prioriza la idea de su posición en la recta numérica. Los indios, y más tarde los arábigos, adoptaron la idea de *positividad* y *negatividad* entre cantidades, aunque las cantidades negativas eran consideradas como meras soluciones algebraicas y no como «números» *per se* (Descartes mismo les llamaba «*falsos* números»), o como una dirección en situaciones físicas. El símbolo del 0 surge probablemente como la primera letra de ' (gr., 'vacío'); los arábigos empleaban el término «al-sifr» para el cero, del que deriva la palabra «cifra». La aritmética indoarábica se difundió en occidente entre los siglos XIII y XVI.

La pregunta acerca de los números también fue esencial para el desarrollo de los fundamentos lógicos de las matemáticas a finales del siglo XIX e inicios del siglo XX. La definición presente de *número natural* (que es la base para la definición del resto de números) fue propuesta por **Richard Dedekind [22]** (escrito entre 1872-1878, publ. 1888). Para Dedekind, los naturales son un sistema en el que uno puede formular el teorema de recursión, el cual luego inspiró la axiomatización de Peano. Otras definiciones, como «cardinalidades finitas» son propuestas por Frege y Cantor.

Referencias

65. Andreescu, T., Andrica, D. y Feng, Z. *104 number theory problems: from the training of the USA IMO team* (Springer Science & Business Media, 2007).

83. Gauss, C. F. *Disquisitiones Arithmeticae* trad. por Ruiz Zúñiga, A. `https://archive.org/details/disquisitiones-arithmeticae-carl-f.-gauss-espanol` (Universidad de Costa Rica, 1801).

100. Nathanson, M. B. *Elementary Methods in Number Theory* (Springer-Verlag New York, 2000).

101. Niven, I. *Irrational Numbers* (Mathematical Association of America, 1956).

Otros recursos.

1. CUEVAS, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).
2. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).
3. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
4. LIU, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).
5. WILSON, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. BRIESKORN, E. y KNORRER, H. *Plane Algebraic Curves* trad. por STILLWELL, J. (Birkhäuser Verlag, 1981).
7. DICKSON, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).
8. NEWTON, I. *The Correspondence of Isaac Newton* (ed. TURNBULL, H. W.) (Cambridge University Press, 1960).
9. ROQUETTE, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).
10. WILLIAMS, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. BENNETT, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. ALFORD, W. R., GRANVILLE, A. y POMERANCE, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).
12. APÉRY, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. BARNES, E. S. y SWINNERTON-DYER, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. BEUKERS, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).
15. BOMBIERI, E. y VAALER, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).

16. Cassels, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).

17. Catalan, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).

18. Chao, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).

19. Chatland, H. y Davenport, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).

20. Clark, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).

21. De Bessy, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).

22. Dedekind, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).

23. Dickson, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).

24. Dirichlet, G. L. en *G. Lejeune Dirichlet's Werke* (ed. Kronecker, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.

25. Euler, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).

26. Euler, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).

27. Euler, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).

28. Gauss, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.

29. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

30. Hensel, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).

31. Hensel, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. Hyyrö, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. INKERI, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. INKERI, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. KAUSLER, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. KELLER, W. y RICHSTEIN, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. KÜRSCHÁK, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. LANG, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. LEGENDRE, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. LEHMER, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. MAHLER, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. MIGNOTTE, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. MINKOWSKI, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. MOTZKIN, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. NAGELL, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. NORTHCOTT, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. OCHEM, P. y RAO, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. OSTROWSKI, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. OSTROWSKI, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. OSTROWSKI, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. Ostrowski, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. Ostrowski, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. Perron, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. Rédei, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. Rella, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. Remak, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. Roth, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. Rychlík, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. Rychlík, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. Siegel, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. Tate, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 305-347.

63. Verger-Gaugry, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

2

Congruencias

2.1 Introducción a las congruencias

Lema 2.1: Sea $m > 1$. Entonces la relación sobre $\mathbb{Z}$ dada por

$$a \equiv b \pmod{m} \iff m \mid a - b$$

es una relación de equivalencia.

Definición 2.2 – *Congruencia modular.* Se dice que dos enteros a, b son congruentes en módulo $m \geq 2$ natural syss $m \mid a - b$, en cuyo caso demotaremos $a \equiv b \pmod{m}$. En general escribiremos $\mathbb{Z}/m\mathbb{Z}$ al conjunto cociente dado por la congruencia en módulo m.

Teorema 2.3: Sean $a \equiv b, c \equiv d \pmod{m}$ entonces:

1. $a + c \equiv b + d \pmod{m}$.
2. $ac \equiv bd \pmod{m}$.
3. Para todo $k \in \mathbb{N}$ se cumple $a^k \equiv b^k \pmod{m}$.
4. Si $(a; m) = 1$, entonces existe b tal que $ab \equiv 1$.

En consecuencia, $\mathbb{Z}/m\mathbb{Z}$ es un dominio y si $m = p$, entonces es un cuerpo.

Pista: El último sale con la identidad de Bézout. □

La ventaja de las congruencias modulares es que nos permiten estudiar mejor las ecuaciones diofánticas, puesto que si $f(x) = 0$, entonces $f(x) \equiv 0$ (mód m) para todo m. Veamos un ejemplo:

Ejercicio 2.4: La ecuación diofántica $x^2+y^2 = 4z+3$ no tiene soluciones enteras.

Solución: Si tuviera alguna solución entera, entonces podríamos estudiar dicha solución módulo 4, luego $x^2 + y^2 \equiv 3$ (mód 4). Ahora bien, los cuadrados módulo cuatro son los siguientes:

n	0	1	2	3
$n^2 \quad (4)$	0	1	$4 \equiv 0$	$9 \equiv 1$

Luego $x^2 + y^2$ puede ser 0, 1 o 2, pero no 3. □

Ejercicio 2.5: La ecuación diofántica homogénea

$$x^2 + y^2 = (4a + 3)z^2,$$

no tiene soluciones no triviales.

Solución: Si $a < 0$, entonces el lado derecho con $z \neq 0$ es negativo por lo que es claro. Si $a \geq 0$ volvemos a hacer reducción módulo 4 y obtenemos que $x^2 + y^3 \equiv 3z^2$ (mód 4) lo cual sólo tiene solución si $z^2 \equiv 0$ (4), en cuyo caso z es par. La ecuación $x^2 + y^2 \equiv 0$ (mód 4) sólo tiene solución si $x^2 \equiv y^2 \equiv 0$ (4), en cuyo caso x, y son pares. Luego si (x, y, z) fuera una solución no trivial, podemos dividir por 2 hasta que alguno sea impar, lo cual es imposible. □

También traduzcamos algunas de las propiedades de divisibilidad a congruencias modulares. Ésto es consecuencia del lema de Euclides:

Teorema 2.6: Sean $m > 1$, $a, b \in \mathbb{Z}$ y $(c; m) = 1$. Entonces

$$ac \equiv bc \pmod{m} \implies a \equiv b \pmod{m}.$$

El que c sea coprimo a m es fundamental: observe que $2 \cdot 3 \equiv 0 \cdot 3$ (mód 6).

Las congruencias son una herramienta increiblemente potente, veamos ejemplos:

Ejercicio 2.7: Demuestre que $2222^{5555} + 5555^{2222}$ es múltiplo de 7.

Solución: Podemos comprobar que $2222 = 317 \cdot 7 + 3$ y $5555 = 793 \cdot 7 + 4$. Luego queremos estudiar sus potencias en módulo 7:

n		1	2	3	4	5	6
3^n	(mód 7)	3	$9 \equiv 2$	$6 \equiv -1$	-3	-2	1
4^n	(mód 7)	4	$16 \equiv 2$	$8 \equiv 1$	4	2	1

Así, sabemos que $2222^6 \equiv 5555^6 \equiv 1 \pmod 7$.

Por algoritmo de la división, $2222 = 370 \cdot 6 + 2$ y $5555 = 925 \cdot 6 + 5$. Luego se cumple:

$$\begin{aligned} 2222^{925 \cdot 6 + 5} &= (2222^6)^{925} \cdot (2222)^5 \equiv 2222^5 \\ &\equiv 3^5 = 9^2 \cdot 3 \equiv 2^2 \cdot 3 = 12 \equiv 5 \pmod 7 \\ 5555^{370 \cdot 6 + 2} &\equiv 5555^2 \equiv 3^2 = 9 \equiv 2 \pmod 7. \end{aligned}$$

Y claramente $5 + 2 \equiv 0 \pmod 7$. □

Las congruencias tienen una infinitud de aplicaciones, veamos algunas:

Teorema 2.8 (Gersónides): Las únicas potencias consecutivas de 2 y 3 son 1, 2, 3, 4 y 8, 9.

Demostración: El enunciado se reduce a encontrar las soluciones enteras a la ecuación $2^n = 3^m \pm 1$. En el enunciado ya se ven los casos $n \leq 3$ y $m \leq 2$, y las exponenciales son estrictamente crecientes, así que podemos asumir $n > 3$ y $m > 2$. En éste caso $2^n = 8 \cdot 2^{n-3}$, por lo que $2^n \equiv 0 \pmod 8$, y además, en módulo 8 se nota que las potencias de 3 son:

m		1	2	3	4	
3^m	(mód 8)	3	$9 \equiv 1$	3	1	$\cdots$

por lo que vemos que $3^m + 1 \equiv 2, 4 \pmod 8$ y que $3^m - 1 \equiv 0, 2 \pmod 8$. Nótese que $3^m \equiv 1 \pmod 8$ syss $m = 2k$, luego nótese que si se diese que $2^n = 3^{2k} - 1$, entonces

$$2^n = 3^{2k} - 1 = (3^k - 1)(3^k + 1)$$

donde, por el teorema fundamental del álgebra se ha de dar que $3^k - 1 = 2^u$ y $3^k + 1 = 2^v$. Pero

$$3^k + 1 = (3^k - 1) + 1 = 2^u + 2 = 2(2^{u-1} + 1) = 2^v.$$

Luego como $2^{u-1}+1$ es impar cuando $u>1$, ha de darse que

$$2^v = 4 = 3^k + 1 \iff k = 1$$

por lo que la ecuación no es válida para $k>1$. □

Teorema 2.9 – *Teorema de los cuadrados de Lagrange*: Todo número natural puede escribirse como suma de cuatro cuadrados.

Demostración: En primer lugar enunciaremos y emplearemos la identidad de los cuatro cuadrados de Euler,[1] vale decir:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) &= (-aw+bx+cy+dz)^2 \\ &+ (ax+bw+cz-dy)^2 + (ay-bz+cw+dx)^2 + (az+by-cx+dw)^2\end{aligned} \tag{2.1}$$

de modo que si n, m satisfacen el enunciado, entonces $n\cdot m$ también. Luego vale demostrarlo para el $0, 1$ y todo número primo. Claramente

$$0 = 0^2+0^2+0^2+0^2, \quad 1 = 1^2+0^2+0^2+0^2, \quad 2 = 1^2+1^2+0^2+0^2.$$

Luego basta ver que vale para p primo impar: En primer lugar, nótese que para $0 \le x \le \frac{1}{2}(p-1)$, se cumple que los números x^2 son distintos módulo p. (Esto pues, si $x^2 \equiv y^2$, entonces $p \mid x-y$ o $p \mid x+y$, pero $0 < x+y \le p-1 < p$, así que $p \mid x-y$, y luego $x = y$.) En segundo lugar, los números $-1-y^2$ son distintos módulo p para $0 \le y \le \frac{1}{2}(p-1)$ dado que los y^2 lo son. Nótese que hay $p+1$ congruencias de x^2 y $-1-y^2$ en conjunto, así que, como $\mathbb{Z}/p\mathbb{Z}$ sólo tiene p elementos alguno se ha de repetir y, en consecuente,

$$x^2+y^2+1 \equiv 0 \pmod{p}$$

Es decir, $x^2+y^2+1^2+0^2 = mp < 1+2\left(\frac{p}{2}\right)^2 < p^2$. Definamos r como el mínimo natural no nulo tal que $rp = a^2+b^2+c^2+d^2$, claramente $r \le m < p$. Nótese que si r es par, entonces del conjunto $\{a,b,c,d\}$ hay 0, 2 o 4 pares. Como

$$\text{impar} \pm \text{impar} = \text{par} \pm \text{par} = \text{par},$$

[1] El lector más avanzado puede comprobar la identidad, notando que se deriva del hecho de que, para α, β cuaterniones, se tiene $|\alpha|^2\,|\beta|^2 = |\alpha\beta|^2$. El problema de encontrar otras identidades, parecidas a las de Euler, se conoce como el *problema de Hurwitz* y lo desarrollamos en mi libro de álgebra **[1],** §10.3.

entonces podemos reordenar los términos para exigir que $a+b, a-b, c+d, c-d$ sean pares. Luego

$$\frac{r}{2}p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

lo que contradiciría la minimalidad de r.

Queremos concluir que $r = 1$: Para ello, supongamos que $r > 1$, entonces sean w, x, y, z los restos módulo r de a, b, c, d resp., tales que sean menores que $r/2$ y mayores que $-r/2$ (podemos exigirlo, puesto que r es impar), luego sea

$$n := w^2 + x^2 + y^2 + z^2 \equiv a^2 + b^2 + c^2 + d^2 = rp \equiv 0 \pmod{r}.$$

Si $n = 0$, entonces $r \mid a, b, c, d$ y $r^2 \mid a^2 + b^2 + c^2 + d^2 = rp$, y como r, p son coprimos, se tiene que $r \mid p$ y $r = 1$, lo que es absurdo por hipótesis. Si $n > 0$, entonces $n = kr$ puesto que $n \equiv 0 \pmod{r}$, y por elección de los sumandos se obtiene que $n < 4(r/2)^2 = r^2$, por lo que $0 < k < r$.

Recordemos la identidad (2.1) y reemplacemos a por $-a$, para obtener:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) = (aw+bx+cy+dz)^2+(-ax+bw+cz-dy)^2 \\ + (-ay - bz + cw + dx)^2 + (-az + by - cx + dw)^2\end{aligned}$$

de modo que

$$krpr = t_1^2 + t_2^2 + t_3^2 + t_4^2$$

donde, además, cada uno es múltiplo de r ($t_2 = -ax + bw + cz - dy \equiv -ab + ab + cd - cd \equiv 0 \pmod{r}$). Luego sea $t_i = c_i r$ y cancelando por r^2 se obtiene que

$$kp = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

lo que contradice la minimalidad de r. □

Una observación es que en la demostración hemos empleado la identidad de Euler (2.1); a lo largo de este libro aparecerán varias identidades, para las cuales emplearemos el ***principio de Littlewood***:

> *Todas las identidades algebraicas son triviales de probar, pero no de encontrar.*

No obstante, en varios casos daremos pequeños indicios en pies de página del cómo se deducen, para un lector con suficientes conocimientos en álgebra.

Ahora veamos un famoso resultado de las olimpiadas de las matemáticas, conocido por sus siglas en inglés como el LTE (eng. *Lifting-the-Exponent*, «elevando el exponente»):

Teorema 2.10: Sean x, y enteros tales que $x \equiv y \not\equiv 0 \pmod{p}$ y sea $n \geq 1$. Entonces:

1. Si $p \neq 2$ o $p = 2$ y $4 \mid x - y$. Entonces
$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$
2. Si $p = 2$ y n es par, entonces
$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(n) - 1.$$

Demostración: Veremos la demostración por casos:

a) $\underline{p \nmid n}$: Entonces $\nu_p(n) = 0$, y podemos realizar la siguiente factorización
$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \tag{2.2}$$
donde el segundo término es congruente en módulo p a $nx^{n-1} \not\equiv 0$. Luego todas las potencias de p en $(x^n - y^n)$ están en $(x - y)$.

b) $\underline{n = p \text{ y } p \neq 2}$: Sea $y = x + pq$. Primero nótese que, en módulo p^2,
$$\begin{aligned} x^{p-1-t}y^t = x^{p-1-t}(x + pq)^t &= x^{p-1-t}(x^t + tx^{t-1}pq + (pq)^2(\cdots)) \\ &\equiv x^{p-1-t}(x^t + tx^{t-1}pq) = x^{p-1} + tx^{p-2}pq \pmod{p^2}. \end{aligned}$$
Enfocándose en el segundo término de (2.2) y mirándolo en módulo p^2 se obtiene que
$$\begin{aligned} x^{p-1} + x^{p-2}y + \cdots &\equiv x^{p-1} + (x^{p-1} + x^{p-2}pq) + (x^{p-2} + 2x^{p-2}pq) + \cdots \\ &= px^{p-1} + (1 + 2 + \cdots + (p-1))x^{p-2}pq \\ &= px^{p-1} + \frac{p(p-1)}{2}x^{p-2}pq \equiv px^{p-1} \pmod{p^2}. \end{aligned}$$
Luego se concluye el enunciado.

c) $\underline{n = p^\alpha m \text{ con } p \nmid m \text{ y } p \neq 2}$: Luego, por el caso (a):
$$\nu_p(x^n - y^n) = \nu_p\big((x^{p^\alpha})^m - y_m^{p^\alpha}\big) = \nu_p(x^{p^\alpha} - y^{p^\alpha})$$
Por la ecuación (2.2) se cumple que $p \mid x^k - y^k$ para todo k, luego podemos emplear recursivamente el caso (b):
$$\nu_p(x^{p^\alpha} - y^{p^\alpha}) = \nu_p\big((x^{p^{\alpha-1}})^p - (y^{p^{\alpha-1}})^p\big) = \nu_p(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}) + 1$$
y así sucesivamente.

d) $\underline{p = 2}$: Al igual que antes, por el caso (a) se concluye que si $n = 2^\alpha m$, entonces

$$\nu_2(x^n - y^n) = \nu_2(x^{2^\alpha} - y^{2^\alpha}).$$

Luego nótese la siguiente factorización

$$x^{2^\alpha} - y^{2^\alpha} = (x^{2^{\alpha-1}} + y^{2^{\alpha-1}})(x^{2^{\alpha-2}} + y^{2^{\alpha-2}}) \cdots (x+y)(x-y).$$

Como $2 \mid x-y$ se sigue que $x^2 \equiv y^2 \equiv 1 \pmod 4$. Luego $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$, y si $\alpha \geq 1$ entonces

$$\nu_\alpha(x^{2^\alpha} - y^{2^\alpha}) = \alpha - 1 + \nu_2(x+y) + \nu_2(x-y).$$

Si $4 \mid x-y$, entonces $x \equiv y \equiv \pm 1 \pmod 4$, así que $x+y \equiv \pm 2 \pmod 4$ y se obtiene la fórmula del inciso 1. □

2.2 Las unidades de $\mathbb{Z}/n\mathbb{Z}$

En primer lugar conviene recordar la definición de grupo (cf. [**1,** Def. 1.1]):

Definición 2.11: Se dice que un par $(G, \cdot)$ es un ***grupo***, si $\cdot\colon G \times G \to G$ satisface lo siguiente:

1. Para todos $a, b, c \in G$ se cumple que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociatividad).
2. Existe e tal que para todo $a \in G$ se cumple que $a \cdot e = e \cdot a = e$; en cuyo caso a e se le dice un elemento neutro.
3. Para todo $a \in G$ existe un $b \in G$ tal que $a \cdot b = b \cdot a = e$, donde e es un neutro; en cuyo caso a b se le dice una inversa.

Un grupo se dice ***abeliano*** si además cumple que $a \cdot b = b \cdot a$ (conmutatividad) para todo $a, b \in G$.

Inmediatamente se prueba que el neutro de un grupo es único, por lo que le denotamos 1, y la inversa de a también es única, por lo que le denotamos a^{-1} (cfr. [**1,** teo. 1.2]).

En particular, nos enfocaremos en el siguiente grupo:

Definición 2.12: Sea $m > 1$. Entonces $U_m := \{[k]_m : (k; m) = 1\} \subseteq \mathbb{Z}/m\mathbb{Z}$, que es finito.

Proposición 2.13: Para todo $m > 1$ se cumple que $(U_m, \cdot)$ es un grupo y, de hecho, U_m es el conjunto de los $\overline{a}$'s en $\mathbb{Z}/m\mathbb{Z}$ que poseen inversa.

Pista: Basta aplicar la identidad de Bézout. □

Siguiendo con otras definiciones de teoría de grupos (cfr. [**1,** def. 1.14]):

Definición 2.14: Dado un grupo G y $g \in G$, para todo $n \in \mathbb{Z}$ se define:

$$g^n := \begin{cases} 1, & n = 0 \\ \underbrace{g \cdot g \cdots g}_{n \text{ veces}}, & n > 0 \\ (g^{-1})^{-n}, & n < 0 \end{cases}$$

Más aún, se le llama el ***orden*** de g, denotado por $\operatorname{ord} g$, al mínimo $n > 0$ tal que $g^n = 1$ si existe, o ∞ si no.

Para enfatizar que que el orden de un entero a es el de su clase de residuos módulo m, lo anotaremos por $\operatorname{ord}_m a$.

Nótese que el neutro es el único elemento de orden 1.

Teorema 2.15 (Wilson): Sea p primo, entonces

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración: Nótese que $(2-1)! = 1$, así que vale para $p = 2$.

Para $p > 2$, se tiene que

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1).$$

Proponemos que todos los términos del medio se cancelan dejando así solo al 1 y al $p-1 \equiv -1$. Para ello nótese que como la inversa es única se cumple que a todo x le corresponde su x^{-1}, pero aún así podría darse que $x \equiv x^{-1}$. Observe que $x \equiv x^{-1}$ syss $x^2 \equiv 1$. Así que se reduce a encontrar las raíces del polinomio $p(x) = x^2 - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$. Nótese que $p(x) = (x-1)(x+1)$, por lo que sus raíces son 1 y -1. Así que:

$$(p-1)! \equiv 1 \cdot \cancel{2 \cdot 3 \cdots (p-2)} \cdot (p-1) \equiv 1 \cdot -1 = -1 \pmod{p}. \qquad \square$$

Proposición 2.16: La aplicación $n \mapsto g^n$ de dominio $\mathbb{Z}$ es un homomorfismo de grupos; vale decir, que las siguientes se cumplen:

1. $g^0 = 1$.
2. $g^{n+m} = g^n g^m$.
3. $g^{-n} = (g^n)^{-1}$.
4. $g^{nm} = (g^n)^m$.

Además, $1^n = 1$ para todo $n \in \mathbb{Z}$.

Teorema 2.17: Se cumplen las siguientes:

1. Si $\operatorname{ord} g = d < \infty$, entonces $g^n = g^m$ syss $n \equiv m \pmod{d}$.
2. Si $\operatorname{ord} g = \infty$, entonces $g^n = g^m$ syss $n = m$.

Demostración:

1. $\Longleftarrow$. Si $n \equiv m \pmod{d}$, entonces $n = m + dq$ para algún $q \in \mathbb{Z}$, luego
$$g^n = g^{dq+m} = g^{dq} g^m = (g^d)^q g^m = 1^q g^m = g^m.$$
$\Longrightarrow$. Si $g^n = g^m$, entonces $1 = g^{-n} g^m = g^{m-n}$. Luego, por algoritmo de la división se cumple que $m - n = dq + r$ donde $0 \leq r < d$, así que
$$1 = g^{m-n} = g^{dq+r} = g^{dq} g^r = 1^q g^r = g^r.$$
Pero, como $r < d$ y d es el mínimo entero positivo que $g^d = 1$, entonces necesariamente $r = 0$. Así que $m - n = dq$ y $m \equiv n \pmod{d}$ como se quería probar.
2. Si $g^n = g^m$, entonces $g^{n-m} = 1$. Claramente la ecuación es falsa si $n - m > 0$ (de lo contrario tendría orden finito) y si $n - m < 0$, entonces $1 = 1^{-1} = (g^{n-m})^{-1} = g^{m-n}$ con lo que el argumento anterior vale. Por ende, necesariamente $n - m = 0$. □

Teorema 2.18: Si G es un grupo abeliano finito y $g \in G$, entonces $\operatorname{ord} g \mid |G|$.

Demostración: Primero veamos que la aplicación $x \mapsto gx$ es una permutación de G. Dado que G es finito, basta notar que es inyectiva; para demostrarlo sean $x, y \in G$ tales que $gx = gy$, luego multiplicando por g^{-1} por la izquierda se obtiene que
$$x = 1x = (g^{-1}g)x = (g^{-1}g)y = 1y = y.$$

Luego si $G = \{g_1, g_2, \ldots, g_n\}$, entonces

$$g_1 g_2 \cdots g_n = (gg_1)(gg_2)\cdots(gg_n) = g^n(g_1 g_2 \cdots g_n)$$

podemos cancelar a ambos lados para obtener que $g^n = 1$. Luego, por el teorema anterior, se tiene que $n \equiv 0 \pmod{d}$, donde $d := \operatorname{ord} g$, por lo que $d \mid n$ como se quería probar. □

El teorema anterior también puede verse como una simple consecuencia del teorema de Lagrange (cfr. [**1,** teo. 1.24]).

Proposición 2.19: Sean $a, b \in G$ un grupo abeliano finito y sea $n \neq 0$. Entonces:

1. $\operatorname{ord}(a^n) = \dfrac{\operatorname{ord} a}{\operatorname{mcd}(n, \operatorname{ord} a)} = \dfrac{\operatorname{mcm}(n, \operatorname{ord} a)}{n}$.
2. $\operatorname{ord}(ab) = \operatorname{mcm}(\operatorname{ord} a, \operatorname{ord} b)$.

Teorema 2.20: En todo grupo abeliano finito, existe un elemento cuyo orden es divisible por el orden de todos los otros elementos.

Demostración: Sea g el elemento de orden máximo de G, y sea $h \in G$ cualquiera; sea $m := \operatorname{ord} g$ y $n := \operatorname{ord} h$, queremos probar que $n \mid m$. Sean $p_1, \ldots, p_k$ todos los primos que dividen a m o a n, de modo que por el teorema fundamental de la aritmética se cumple que

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad n = \prod_{i=1}^{k} p_i^{\beta_i}.$$

Ahora, definamos u como el producto de los $p_i^{\alpha_i}$'s con $\alpha_i \geq \beta_i$, y sea v el producto de los $p_i^{\beta_i}$'s con $\alpha_i < \beta_i$. De éste modo $u \mid m$, $v \mid n$ y $(u; v) = 1$.

Definamos $g' := g^{m/u}$ y $h' := h^{n/v}$, nótese que $\operatorname{ord}(g') = u$ y $\operatorname{ord}(h') = v$ con órdenes coprimos, luego $\operatorname{ord}(g'h') = \operatorname{mcm}(u, v) = uv$, de modo que $m \mid \operatorname{ord}(g'h')$, por lo que $uv \geq m$. Como m es el orden máximo, se cumple que $uv = m$ y, luego, $v = 1$, con lo que $n \mid m$. □

Definición 2.21: Se define la función ϕ o indicatriz de Euler (ver fig. 2.1) como $\phi\colon \mathbb{N}_{\neq 0} \to \mathbb{N}$ dada por

$$\phi(m) := \begin{cases} |U_m|, & m \neq 1 \\ 1, & m = 1 \end{cases}$$

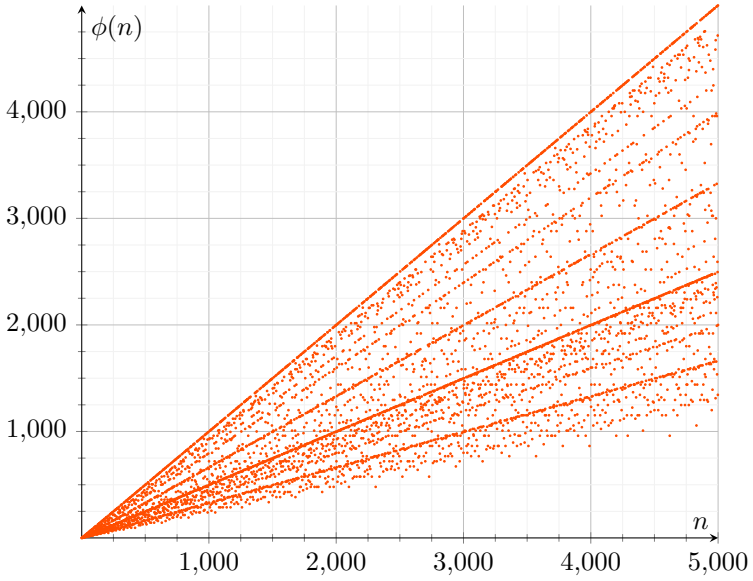


Figura 2.1. Función ϕ de Euler.

En primera instancia la función ϕ de Euler parece tremendamente misteriosa, pero aún así el lector debería ser capaz de identificar unas ciertas «ramas», ya veremos a qué corresponden (ver fig. 3.1).

Teorema 2.22 (de Euler-Fermat): Si $m > 1$, entonces para todo $(a; m) = 1$ se cumple que $\text{ord}_m(a) \mid \phi(m)$. En consecuente,

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Demostración: Basta notar que $|U_m| = \phi(m)$ por definición y aplicar el teorema 2.18. □

Y como caso particular:

Teorema 2.23 (pequeño teorema de Fermat): Sea p primo y a tal que $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

Gracias al pequeño teorema de Fermat tenemos otra demostración del teorema de Wilson:

Demostración(Teo. 2.15): Para $p = 2$ es trivial. Considere el siguiente polinomio para $p > 2$:

$$f(x) := (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1).$$

Ahora veamos reducción módulo p. Si $f(x) \not\equiv 0 \pmod{p}$, entonces tendría grado $p-2$, pero es claro que $f(a) \equiv 0 \ (p)$ para todo $a \not\equiv 0 \ (p)$ por el pequeño teorema de Fermat, por tanto $f(x)$ tiene $p-1$ raíces distintas. Como f tiene más raíces que grado, necesariamente $f(x) \equiv 0 \ (p)$, así que

$$\begin{aligned} 0 \equiv f(0) &= (-1)(-2)\cdots(p-1) - (-1) \pmod{p} \\ &= (-1)^{p-1}(p-1)! + 1 = (p-1)! + 1 \pmod{p}. \end{aligned}$$ □

El polinomio en la demostración anterior es bastante curioso, y un mejor estudio da el siguiente resultado:

Teorema 2.24 (Wolstenholme): Sea $p \geq 5$ primo. Entonces:

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}.$$

Recuerde que si $1 \leq a < p$, entonces a es coprimo con p^2 y, por lo tanto, es invertible en $\mathbb{Z}/p^2\mathbb{Z}$.

Demostración: Consideremos nuevamente el polinomio:

$$f(x) := (x-1)\cdots(x-(p-1)) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0.$$

Ya vimos que $f(x) \equiv x^{p-1} - 1 \pmod{p}$, de modo que p divide a cada coeficiente a_j con $j \neq 0$. Nótese que podemos evaluar el polinomio en 0 y p, y obtener la igualdad $f(0) = (p-1)! = f(p)$, o equivalentemente $f(p) - a_0 = 0$, lo que cancelando p nos da:

$$p^{p-2} + a_{p-2}x^{p-3} + \cdots + a_1 = 0.$$

Mirando módulo p^2 obtenemos que $a_1 \equiv 0 \pmod{p^2}$ y, expandiendo la definición de a_1, obtenemos

$$p^2 \mid (p-1)!\left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right),$$

como $p^2 \nmid (p-1)!$ obtenemos el enunciado. □

Otra consecuencia que nos será útil más adelante es la siguiente, que sigue del teorema chino del resto:

Corolario 2.24.1: Sean $(n; m) = 1$, entonces $\phi(nm) = \phi(n)\phi(m)$.

Algo que nos será útil más adelante, en la discusión sobre el teorema de Dirichlet, es que los U_m's sean cíclicos[2] o en éste caso que satisfagan la siguiente definición:

Definición 2.25: Una ***raíz primitiva módulo*** m es un entero a coprimo a m, tal que $\text{ord}_m(a) = \phi(m)$; es decir, es un generador (como grupo) de U_m.

EjemploUn grupo de unidades sin raíz primitiva. Considere U_{12}, como $12 = 2^2 \cdot 3$ sus elementos son los que no son ni divisibles por 2 ni por 3. Así, pues, $U_{12} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Y nótese que $5^2 = 25 = 2 \cdot 12 + 1 \equiv 1$ (mód 12), y ésto sucede también con el 7 y el 11. Es decir, todo elemento distinto de $\overline{1}$ tiene orden 2, luego no existen raíces primitivas módulo 12.

Así notamos que no todo U_m tiene raíz primitiva, pero U_p sí:

Teorema 2.26: Si k es un cuerpo finito, entonces $k^\times$ es un grupo cíclico. En consecuencia, U_p tiene raíces primitivas.

Demostración: Sea $G := k^\times$ y sea g el elemento cuyo orden es divisible por el orden de todos los otros elementos (teorema 2.20). Luego $g^m = 1$, es decir, g es raíz de $p(x) := x^m - 1 \in k[x]$, además, como todo otro elemento tiene un orden que divide a m, entonces para todo $h \in G$ se cumple que $h^m = 1$, es decir, es raíz de $p(x)$.

El polinomio $p(x)$ tiene a lo sumo m raíces, por tener grado m, y tiene como mínimo m raíces (las potencias de g), luego tiene exactamente m raíces. Y las raíces de $p(x)$ son los elementos de G, luego g es un generador de G. □

Teorema 2.27: Si p es un primo y g es una raíz primitiva módulo p. Entonces g o $g + p$ es una raíz primitiva módulo p^2.

Demostración: Lo separaremos por casos:

a) $\underline{p = 2}$: Se cumple que $U_2 = \{\overline{1}\}$ y $U_4 = \{\overline{1}, \overline{3}\}$. Nótese que 1 es raíz

[2]Un grupo se dice ***cíclico*** si está generado por un elemento (cfr. **[1,** def. 1.14]).

primitiva módulo 2 y que $3 = 1 + 2$ es raíz primitiva módulo $4 = 2^2$.

b) $\underline{p \neq 2}$: Sea $m := \mathrm{ord}_{p^2}(g)$. Como $g^m \equiv 1 \pmod{p}^2$, entonces $p^2 \mid g^m - 1$ y $g^m \equiv 1 \pmod{p}$, es decir, $\phi(p) = p - 1 \mid m \mid p(p-1)$. Luego o $m = p - 1$ o $m = p(p-1)$, y en el segundo caso g es raíz primitiva módulo p^2.

Como $g + p \equiv g \pmod{p}$, entonces lo mismo ocurre para g. Luego basta probar que no se puede dar que $\mathrm{ord}_{p^2}(g) = \mathrm{ord}_{p^2}(g+p) = p-1$, lo que haremos por contradicción: Ésto es equivalente a que $g^p \equiv g$ y $(g+p)^p \equiv g + p \pmod{p^2}$, pero

$$g + p \equiv (g+p)^p = g^p + p \cdot g^{p-1}p + p^2 \cancelto{0}{\sum_{k=2}^{p} \binom{p}{k} g^{p-k} p^{k-2}} \pmod{p^2}$$
$$\equiv g^p \equiv g \pmod{p^2}$$

luego $p \equiv 0 \pmod{p^2}$. Contradicción. □

Teorema 2.28: Sea p un primo impar. Si g es una raíz primitiva módulo p^2, entonces es una raíz primitiva módulo p^n para todo n.

Demostración: Lo veremos por inducción sobre n: Claramente aplica para $n \in \{1, 2\}$. Supongamos que $n > 2$, entonces, por el resultado anterior, tenemos que

$$g^{p-1} \equiv 1 \pmod{p}, \quad g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Luego $\nu_p(g^{p-1} - 1) = 1$. Sea g una raíz primitiva módulo p^n (hipótesis inductiva), luego sea $m := \mathrm{ord}_{p^{n+1}}(g)$, se cumple que $g^m \equiv 1 \pmod{p^{n+1}}$, por lo que $g^m \equiv 1 \pmod{p^n}$. Por el teorema 2.18 se cumple que $m \mid p^n(p-1)$ y como $\mathrm{ord}_{p^n}(g) = p^{n-1}(p-1)$, se tiene que $p^{n-1}(p-1) \mid m$, lo que nos reduce a dos posibilidades. Nótese que, por el teorema 2.10,

$$\nu_p(g^{p^{n-1}(p-1)} - 1) = \nu_p(g^{p-1} - 1) + (n-1) = n$$

luego $p^{n+1} \nmid g^{p^{p-1}(p-1)} - 1$ y $g^{p^{p-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$, por lo que $m = p^n(p-1)$ como se quería probar. □

Éste teorema será vital más adelante para demostrar el teorema de Dirichlet (véase §3.4). Nótese que la condición de primo impar es necesaria pues U_8 no tiene raíces primitivas y, en consecuente, U_{2^r} tampoco para $r \geq 3$.

Teorema 2.29: Un número $m > 0$ tiene raíces primitivas módulo m syss es de la forma $2, 4, p^n$ o $2p^n$, donde p es un primo impar y $n > 0$ es un entero.

Demostración: Esto es una mera aplicación del teorema chino del resto, notando que el producto de grupos cíclicos es cíclico syss sus cardinalidades son coprimas, y que $\phi(p_1^{n_1}), \phi(p_2^{n_2})$ son pares cuando p_1, p_2 son primos distintos impares. □

2.3 Residuos cuadráticos

Definición 2.30: Sean $m > 1$ y a enteros. Se dice que a es un ***resto potencial n-esimo*** módulo m si la congruencia

$$x^n \equiv a \pmod{m}$$

tiene soluciones. A los restos potenciales n-ésimos con $n = 2, 3, 4$ se les dicen ***residuo cuadrático***, ***cúbico*** y ***bicuadrático*** resp.

La definición es absolutamente general, pero podemos hacer bastante más si tenemos alguna raíz primitiva:

Definición 2.31: Si g es una raíz primitiva módulo m, entonces para todo $h \in U_m$ se denota $\text{índ}_g(h)$ al mínimo $k > 0$ tal que $g^k = h$.

Teorema 2.32: Sea $m > 1$ natural con una raíz primitiva g módulo m y sea a coprimo con m. Definiendo $d := (n; \phi(m))$ donde $n > 1$ arbitrario, entonces la congruencia

$$x^n \equiv a \pmod{m}$$

tiene solución syss $a^{\phi(m)/d} \equiv 1 \pmod{m}$, en cuyo caso posee exactamente d soluciones.

Demostración: Sea $r := \text{índ}_g(a)$. Nótese que toda potencial solución debe ser necesariamente coprima con m, de modo que es alguna potencia de g; luego la ecuación se reescribe a $g^{kn} \equiv g^r \pmod{m}$, o equivalentemente, $\phi(m) \mid kn - r$. Escribamos $n = du$ y $\phi(m) = dv$ con u, v coprimos (por definición de mcd), luego si $\phi(m) \mid kn - r$, entonces $d \mid kn - r$ y como $d \mid n$, entonces necesariamente $d \mid r$. Ésto prueba $\implies$.

Recíprocamente, si $a^{\phi(m)/d} = a^v \equiv 1 \pmod{m}$, entonces $\text{ord}(a) \mid v$ y $g^{r \cdot \text{ord}(a)} \equiv 1 \pmod{m}$, es decir, $\phi(m) \mid r$ y $d \mid r$. Para encontrar una solución

notamos que se busca que $dv \mid kdu - r$, equivalentemente, $ku \equiv r/d \pmod{v}$. Pero como $(u; v) = 1$, entonces $u \in (\mathbb{Z}/v\mathbb{Z})^\times$ y buscamos $k \equiv r/n \pmod{v}$ lo cual siempre existe. Finalmente, hay tantas soluciones como $0 \leq k < \phi(m) = dv$ que me satisfagan lo anterior, y es claro que hay exactamente d exponentes k que lo satisfacen. □

Ahora nos enfocamos casi exclusivamente en residuos cuadráticos.

Lema 2.33: Sea $m > 2$, y g_1, g_2 son raíces primitivas módulo m y $h \in U_m$, entonces

$$\text{índ}_{g_1}(h) \equiv \text{índ}_{g_2}(h) \pmod{2}.$$

Demostración: Sea $k := \text{índ}_{g_1}(g_2)$. Nótese que como $\phi(m) = \text{ord}_m(g_1) = \text{ord}_m(g_2) = \text{ord}_m(g_1^k)$, entonces necesariamente $(k; \phi(m)) = 1$. Además nótese que si $m > 2$, entonces $(m; m-1) = 1$ y $(m-1)^2 \equiv 1 \pmod{m}$, luego $2 \mid \phi(m)$, por lo que $2 \nmid k$ y $k \equiv 1 \pmod{2}$. Finalmente $h = g_1^\alpha = g_2^\beta = g_1^{k\beta}$, por lo que $2 \mid \phi(m) \mid \alpha - \beta k$; es decir $\alpha \equiv \beta k \equiv \beta \pmod{2}$. □

Definición 2.34: Sea g una raíz primitiva módulo p, luego se define el ***símbolo de Legendre*** así:

$$\left(\frac{x}{p}\right) := \begin{cases} (-1)^{\text{índ}_g(x)} & x \in U_p \\ 0 & p \mid x \end{cases}$$

es decir, $\left(\frac{x}{p}\right)$ es 1 si x es una potencia cuadrada de g o -1 si no, y 0 si $x \notin U_p$.

De la definición es claro que el valor de $\left(\frac{x}{p}\right)$ es invariante salvo congruencias módulo p.

Ejercicio 2.35: Empleando el teorema de Wilson, demuestre que -1 es un residuo cuadrático módulo p si $p \equiv 1 \pmod{4}$.

Pista: Emplee que $p - j \equiv (-1)j \ (p)$. □

Teorema 2.36 – *Criterio de Euler*: Sea $p > 2$ primo, entonces para

todo $a \in \mathbb{Z}$ se cumple que

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

Demostración: Es claro que $a \equiv 0 \pmod{p}$ syss $\left(\frac{a}{p}\right) = 0$.

Si $\left(\frac{a}{p}\right) = 1$, entonces $a = g^{2k}$ para g raíz primitiva módulo p. Luego

$$(g^{2k})^{\frac{1}{2}(p-1)} = (g^{p-1})^k \equiv 1 \pmod{p}$$

Y conversamente, si $a = g^{2k+1}$, entonces

$$(g^{2k+1})^{\frac{1}{2}(p-1)} = (g^{2k}g)^{\frac{1}{2}(p-1)} = g^{\frac{1}{2}(p-1)} =: h \pmod{p}$$

Ahora bien, nótese que por el pequeño teorema de Fermat se cumple que $h^2 \equiv 1$, pero $h \not\equiv 1$ por definición de raíz primitiva, luego necesariamente $h \equiv -1$. □

Corolario 2.36.1: Sea $p > 2$ primo y a, b, entonces

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

Otra consecuencia del criterio de Euler:

Teorema 2.37: Sea $p > 2$ primo. Entonces:

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

Es decir, -1 es un cuadrado módulo p syss $p \equiv 1 \pmod{4}$.

Definición 2.38: Sea $p > 2$ primo y consideremos U_p (que sabemos tiene cardinalidad par). Luego $S \subseteq U_p$ se dice un ***conjunto gaussiano módulo*** p si para todo $g \in U_p$ se cumple que g o $-g \in S$ (pero no ambos). Equivalentemente, para todo $g \in U_p$ existe un único $s \in S$ y un único $\epsilon \in \{\pm 1\}$ tal que $g = s\epsilon$.

Ejemplos de conjuntos gaussianos módulo p lo son $\{1, 2, \ldots, \frac{1}{2}(p-1)\}$, $\{\frac{1}{2}(p-1), \frac{1}{2}(p+1), \ldots, p-1\}$, $\{2, 4, \ldots, p-1\}$, etc.

Teorema 2.39 (lema aritmético de Gauss): Sea $p > 2$ primo, $(a;p) = 1$ y S un conjunto gaussiano módulo p. Para todo $s \in S$ existe un único $\epsilon_a(s) \in \{\pm 1\}$ y $u_a(s) \in S$ tales que

$$as \equiv \epsilon_a(s)u_a(s) \pmod{p},$$

de modo que u_a es una permutación de S. Más aún,

$$\left(\frac{a}{p}\right) = \prod_{s\in S} \epsilon_a(s) = (-1)^m$$

donde m es la cantidad de $s \in S$ tales que $\epsilon_a(s) = -1$.

Demostración: Sean $s, s' \in S$, si $u_a(s) = u_a(s')$, entonces se cumple que

$$as \equiv \epsilon_a(s)u_a(s) \equiv \epsilon_a(s)u_a(s') = \pm as' \pmod{p},$$

como $(a;p) = 1$, por cancelación se tiene que $s = \pm s'$. Pero como solo hay un $t \in S$ tal que $s = \pm t$ y $s' = \pm t$, entonces $s = s'$.

Ahora bien:

$$\begin{aligned} a^{\frac{1}{2}(p-1)} \prod_{s\in S} s &= \prod_{s\in S} as \equiv \prod_{s\in S} \epsilon_a(s)u_a(s) \\ &\equiv \prod_{s\in S} \epsilon_a(s) \prod_{s\in S} u_a(s) \equiv \prod_{s\in S} s \pmod{p} \end{aligned}$$

donde en el último paso empleamos que $u_a \colon S \to S$ es una permutación. Luego cancelando e invocando el criterio de Euler se tiene que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \equiv \prod_{s\in S} \epsilon_a(s) \pmod{p}. \qquad \square$$

Teorema 2.40: Para todo $p > 2$ se cumple que:

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

Demostración: Considere el conjunto gaussiano $S := \{1, 2, \ldots, \frac{1}{2}(p-1)\}$, luego por el lema de Gauss se tiene que

$$\left(\frac{2}{p}\right) = \prod_{s\in S} \epsilon_2(s) = (-1)^m.$$

Nótese que si $1 \leq 2s \leq \frac{1}{2}(p-1)$, entonces $2s \in S$ y $\epsilon_2(s) = 1$. En cambio si $\frac{1}{2}(p+1) \leq 2s \leq p-1$, entonces $1 \leq p - 2s \leq \frac{1}{2}(p-1)$ y

$$2s \equiv -(p-2s) \pmod{p};$$

en conclusión $\epsilon_2(s) = -1$ syss

$$\frac{p+1}{4} \leq s \leq \frac{p-1}{2}.$$

Aquí dividimos por casos:

a) $p \equiv \pm 1 \pmod 8$: Entonces o $p = 8k+1$ y

$$2k + \frac{1}{2} \leq s \leq 4k.$$

O $p = 8k-1$ y

$$2k \leq s \leq 4k - 1.$$

Pero en ambos casos $m = 2k$.

b) $p \equiv \pm 3 \pmod 8$: Entonces o $p = 8k+3$ y

$$2k + 1 \leq s \leq 4k + 1,$$

por lo que $m = 2k+1$.

O $p = 8k-3$ y

$$2k - \frac{1}{2} \leq s \leq 4k - 2,$$

por lo que $m = 2k-1$. Pero en ambos casos m es impar.

Finalmente queda al lector comprobar que la ecuación sintetiza las dos congruencias módulo 8. □

Teorema 2.41 – *Ley de reciprocidad cuadrática*: Sean $p, q > 2$ primos, entonces

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

Demostración: Sean $S := \{1, 2, \ldots, \frac{1}{2}(p-1)\}$ y $T := \{1, 2, \ldots, \frac{1}{2}(q-1)\}$. Luego consideramos el conjunto de puntos en el plano $S \times T$. Por el lema de Gauss se tiene que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\prod_{s\in S} \epsilon_q(s)\right) \cdot \left(\prod_{t\in T} \epsilon_p(t)\right) = (-1)^m(-1)^n.$$

Así nos preguntamos los valores de m y n. Consideremos los puntos $(s,t) \in S \times T$ que satisfacen la siguiente desigualdad:

$$1 \leq pt - qs \leq \frac{p-1}{2}. \tag{2.3}$$

Si (s,t_1) y (s,t_2) son puntos que la satisfacen, entonces:

$$p|t_1 - t_2| = |(pt_1 - qs) - (pt_2 - qs)| < \frac{p-1}{2} < p,$$

de modo que $t_1 = t_2$. Así pues, de cumplirse, lo hace para un único t. Sea (s,t) un punto que satisface la ec. (2.3), entonces, por definición, $pt - qs =: s' \in S$ por lo que

$$qs \equiv -s' \pmod{p},$$

o lo que es equivalente, $u_q(s) = s'$ y $\epsilon_q(s) = -1$.

Recíprocamente, si $s \in S$ y $\epsilon_q(s) = -1$, entonces, por definición, $qs \equiv -u_q(s) \pmod{p}$, o lo que es equivalente, existe un $t > 0$ tal que $qs = pt - u_q(s)$. Como

$$0 < pt = qs + u_q(s) \leq q \cdot \frac{p-1}{2} + \frac{p-1}{2} = \frac{(q+1)(p-1)}{2},$$

de modo que

$$0 < t \leq \frac{q+1}{2} \cdot \frac{p-1}{p} < \frac{q+1}{2}.$$

Como q es impar, podemos aseverar que $t \leq \frac{q-1}{2}$.

De modo que m corresponde a la cantidad de puntos de $S \times T$ que satisfacen la ec. (2.3). Y análogamente, n corresponde a la cantidad de puntos de $S \times T$ que satisfacen:

$$1 \leq qs - pt \leq \frac{q-1}{2} \iff -\frac{q-1}{2} \leq pt - qs \leq -1.$$

Ésto último nos permite notar que los subconjuntos dados por las restricciones son de hecho disjuntos. Como $pt - qs \neq 0$ (de lo contrario $q \mid t$ y $p \mid s$), entonces $n + m$ corresponde a la cantidad de puntos que cumplen:

$$-\frac{q-1}{2} \leq pt - qs \leq \frac{p-1}{2}.$$

Sea M la cantidad de puntos que satisface:

$$pt - qs > \frac{p-1}{2}, \tag{2.4}$$

y N la cantidad de puntos que satisface:

$$pt - qs < -\frac{q-1}{2}.$$

Entonces, se ha de cumplir que

$$m + n + M + N = |S \times N| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Probaremos que $M = N$: Para ello, construyamos la siguiente aplicación:

$$\begin{aligned} \psi\colon S \times T &\longrightarrow S \times T \\ (s,t) &\longmapsto \Big(\underbrace{\frac{p+1}{2} - s}_{=:s'}, \underbrace{\frac{q+1}{2} - t}_{=:t'} \Big) \end{aligned}$$

la cual es una biyección, puesto que $\psi \circ \psi = \mathrm{Id}$. Si (s,t) satisface la condición (2.4), entonces

$$\begin{aligned} pt' - qs' &= p\left(\frac{q+1}{2} - t\right) - q\left(\frac{p+1}{2} - s\right) \\ &= \frac{p(q+1) - q(p+1)}{2} - (pt - qs) < \frac{p-q}{2} - \frac{p-1}{2} = -\frac{q-1}{2}. \end{aligned}$$

De modo que ψ establece una biyección entre los conjuntos y $M = N$. Finalmente

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{m+n} = (-1)^{m+n+2M} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \qquad \square$$

La ley posee una infinitud de demostraciones, algunas radicalmente distintas, más adelante veremos otra empleando extensiones de cuerpo.

La ley de reciprocidad cuadrática ofrece un método muy eficaz de calcular los símbolos de Legendre:

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Así, con la ley de reciprocidad cuadrática tenemos un criterio para saber si un determinado residuo módulo p es un cuadrado o no, pero el método no nos ofrece un candidato a cuadrado. Presentamos un par de métodos, dependiendo de $p > 2$:

(a) Caso $p \equiv 3 \pmod 4$: Como existe x tal que $x^2 \equiv n \pmod p$, entonces, por el pequeño teorema de Fermat:

$$n^{\frac{1}{2}(p-1)} \equiv (x^2)^{\frac{1}{2}(p-1)} = x^{p-1} \equiv 1 \pmod p,$$

en consecuente,

$$\left(n^{\frac{1}{4}(p+1)}\right)^2 = n^{\frac{1}{2}(p+1)} \equiv n \pmod p.$$

(b) Caso $p \equiv 5 \pmod 8$: Por el mismo razonamiento vemos que $n^{\frac{1}{2}(p-1)} \equiv 1 \pmod p$, de modo que $n^{\frac{1}{4}(p-1)}$ es ± 1.

Si $n^{\frac{1}{4}(p-1)} \equiv 1$, entonces

$$\left(n^{\frac{1}{8}(p+3)}\right)^2 = n^{\frac{1}{4}(p+3)} \equiv n \pmod p.$$

Si $n^{\frac{1}{4}(p-1)} \equiv -1$, entonces primero buscamos una raíz para -1 empleando el teorema de Wilson:

$$\begin{aligned} -1 \equiv (p-1)! &= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(p - \frac{p-1}{2}\right) \cdots (p-2)(p-1) \\ &\equiv \left(1 \cdot 2 \cdots \frac{1}{2}(p-1)\right)^2 = \left(\frac{p-1}{2}\right)!^2 \pmod p. \end{aligned}$$

de modo que podemos concluir que

$$\left(n^{\frac{1}{8}(p+3)} \cdot \left(\frac{p-1}{2}\right)!\right)^2 \equiv n \pmod p.$$

(c) Caso $p \equiv 1 \pmod 8$: Aquí no se presenta un método algorítmico sino mero «ensayo y error». Para agilizar un poco las cosas, $x^2 \equiv n \pmod p$ equivale a resolver la ecuación diofantina $x^2 = n + pq$. Podemos suponer que $0 < n < p$ y que $0 < x < p/2$, de modo que $x < p^2/4$ y $0 < q < p/4$. Sea $e > 2$ con $p \nmid e$ y sean $n_1, n_2, \ldots$ residuos *no*-cuadráticos; como x^2 *sí* es un cuadrado, entonces denotando por $s_1, s_2, \ldots$ las soluciones respectivas (para q) de

$$n + pq \equiv n_1, \quad n + pq \equiv n_2, \quad \ldots \pmod e$$

entonces $[q]_e \notin \{s_1, s_2, \ldots\}$. Así podemos ir reduciendo los candidatos para q.

Ahora, nos gustaría poder pasar de los primos al caso general. Para ello, en primer lugar:

Teorema 2.42: Sea $n = p_1^{e_1} \cdots p_r^{e_r}$ donde los p_i's son primos distintos y $e_i \geq 1$. Se cumple que a es un residuo cuadrático módulo n syss es un residuo cuadrático módulo $p_i^{e_i}$ para cada i.

DEMOSTRACIÓN: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Si $a \equiv r_i^2 \pmod{p_i^{e_i}}$ para cada i, entonces, por el teorema chino del resto, existe r tal que $r \equiv r_i \pmod{p_i^{e_i}}$ para todo i. Luego $a \equiv r^2 \pmod{p_i^{e_i}}$, es decir, $p_i^{e_i} \mid a - r^2$ para todo i, luego $n \mid a - r^2$. □

Así que, basta poder tener un criterio para verificar si un número es un residuo cuadrático, sería necesario tener criterios para las potencias de primos:

Teorema 2.43: Sea p un primo impar y sea a no divisible por p. Entonces a es un residuo cuadrático módulo p^k para todo $k \geq 1$ syss es un residuo cuadrático módulo p.

DEMOSTRACIÓN: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Demostraremos por inducción sobre k que si a es un residuo cuadrático módulo p^k, entonces lo es módulo p^{k+1}. Sea $a = r^2 + mp^k$, entonces

$$(r + np^k)^2 = r^2 + 2rnp^k + n^2p^{2k} \equiv a + (2rn - m)p^k \pmod{p^{k+1}},$$

sabemos que $p \nmid r$ y $p \nmid 2$ luego podemos elegir $n \equiv m/2r \pmod{p}$, de modo que $a \equiv (r + np^k) \pmod{p^{k+1}}$ para dicho n. □

Teorema 2.44: Un número impar a es un residuo cuadrático módulo 2^k para todo $k \geq 3$ syss $a \equiv 1 \pmod{8}$.

DEMOSTRACIÓN: Al igual que antes, la implicancia $\Longrightarrow$ es trivial y la recíproca es por inducción. Si $a = r^2 + m2^k$, entonces

$$(r + m2^{k-1})^2 = r^2 + rm2^k + m^2 2^{2k-2} \equiv a + (r-1)m2^k \pmod{2^{k+1}}$$

donde empleamos que $2k - 2 \geq k + 1$ si $k \geq 3$. Nótese que $r - 1$ ha de ser par así que ese término también se anula. De ésto se concluye el enunciado, porque el 1 es el único residuo cuadrático impar módulo 8. □

Definición 2.45: Dado un $n > 1$ entero, podemos extender la definición del símbolo de Legendre al ***símbolo de Jacobi*** así: Si $n = p_1 \cdots p_m$, donde p_j son primos no necesariamente distintos, entonces:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right).$$

Ejemplo. Cabe destacar que el símbolo de Jacobi da espacio para confusión: Si $\left(\frac{a}{n}\right) = 1$, entonces *no* necesariamente se cumple que a es un residuo cuadrático módulo n. Considere $n = 55$ y $a = 2$. Luego

$$\left(\frac{2}{55}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{11}\right) = (-1)^2 = 1.$$

No obstante, por el teorema chino del resto, 2 no puede ser un residuo cuadrático módulo 55 pues equivale a serlo para 5 y 11 simultáneamente.

Teorema 2.46 (Thue): Sea $n \in \mathbb{N}_{\neq 0}$. Para todo a coprimo con n existen $0 < x, y \leq \sqrt{n}$ tales que:

$$ay \equiv x \quad \text{o} \quad ay \equiv -x \pmod{n}.$$

Demostración: Sean $ay + x$ todas las combinaciones con $0 \leq x, y \leq \sqrt{n}$. Como hay una cantidad $(\lfloor\sqrt{n}\rfloor + 1)^2 > n$ de tales combinaciones se satisface, por el principio del palomar, que $ay_1 + x_1 \equiv ay_2 + x_2$ para $(x_1, y_1) \neq (x_2, y_2)$. Nótese que como $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ entonces debe cumplirse que $x_1 \neq x_2$ e $y_1 \neq y_2$, y luego

$$a(y_1 - y_2) \equiv x_2 - x_1 \pmod{n}$$

con $0 < |y_1 - y_2| < \sqrt{n}$ y $0 < |x_1 - x_2| < \sqrt{n}$. Podemos suponer, sin perdida de generalidad, que $y_1 > y_2$ y definir $y := y_1 - y_2$ y $x := |x_2 - x_1|$, y así obtener el enunciado. □

Con una modificación a la prueba se obtiene el siguiente resultado, un poco más general:

Teorema 2.47 (Scholz): Sea $n \in \mathbb{N}_{>1}$ y sean e, f tales que $ef > n$, $e > 1$ y $f \leq n$. Para todo a coprimo con n existen $0 < x < e$ y $0 < y < f$ tales que:

$$ay \equiv x \quad \text{o} \quad ay \equiv -x \pmod{n}.$$

§2.3.1 Primos de Fermat.

Lema 2.48: Si $2^m + 1$ es primo, entonces $m = 2^n$ para algún $n \geq 0$.

Demostración: Lo probaremos por contrarrecíproca. Sea $m = 2^n q$ con $q > 1$ impar. Definamos el polinomio $f(t) := t^q + 1$, luego posee a -1 como raíz, es decir, $x + 1 \mid f(x)$. Definiendo el otro polinomio $g(x) := f(x^{2^n}) = x^m + 1$ se concluye que $x^{2^n} + 1 \mid g(x)$ y, en particular, $2^{2^n} + 1 \mid 2^m + 1$, por lo que el número no es primo. □

Definición 2.49: Se define la siguiente sucesión

$$F_n := 2^{2^n} + 1,$$

cuyos valores son conocidos como los ***números de Fermat***. Un primo que es un número de Fermat se dice un ***primo de Fermat***.

Fermat observo que

n	0	1	2	3	4
F_n	3	5	17	257	65537

donde todos los términos aquí presentes son primos y conjeturó que todos los números de la sucesión debían de serlo. Quizá comprobar el caso de 257 no es tan laborioso, pero ya F_4 presenta problemas a menos que dispongamos de un ordenador; Euler descubrió que F_5 no es primo lo que resultó en uno de los más famosos casos de falsa intuición en las matemáticas.

Teorema 2.50: Sea p un primo tal que $p \mid F_n$, entonces p es de la forma $p = 2^{n+2}k + 1$.

Demostración: Si $p \mid F_n = 2^{2^n} + 1$, entonces $2^{2^n} \equiv -1 \pmod{p}$ y $2^{2^{n+1}} \equiv 1 \ (p)$ de modo que $\mathrm{ord}_p(2) \mid 2^{n+1}$ pero $\mathrm{ord}_p(2) \nmid 2^n$ con lo que se concluye que $\mathrm{ord}_p(2) = 2^{n+1}$.

Por el teorema de Lagrange se tiene que $\mathrm{ord}_p(2) = 2^{n+1} \mid p - 1$ de modo que $p = 2^{n+1}r + 1$. Si $n < 2$ entonces F_n es primo y no posee divisores por lo que el enunciado es cierto, y si $n \geq 2$, entonces se tiene que $p \equiv 1 \pmod{8}$, luego $\left(\frac{2}{p}\right) = 1$ y por ende la ecuación $x^2 \equiv 2 \pmod{p}$ tiene solución. Se concluye que $\mathrm{ord}_p(x) = 2^{n+2}$ y nuevamente por Lagrange se tiene que $p = 2^{n+2}k + 1$. □

Así pues, el 257 tiene por posible divisores a números de la forma $32k+1$, pero $\sqrt{257} < \sqrt{400} = 20$ así que debe ser primo. Para el 65537 tenemos que sus divisores son de la forma $64k+1$ y $\sqrt{65537} = \sqrt{256^2+1} < 257$ luego habría que verificarlo para los números $\{65, 129, 193\}$ de entre los cuales solo el 193 es primo.

Ejercicio 2.51: Verificar que $F_5 = 4\,294\,967\,297$ no es primo. F_5 no es primo

Solución: Se cumple que $\sqrt{F_5} < F_4$ luego hay varios candidatos:

$$129, \mathbf{257}, 385, 513, \mathbf{641}, \mathbf{769}, 897, 1025, \mathbf{1153}, 1281, \ldots$$

Resolveremos si $p \mid F_5$ notando si $F_5 = 2^{2^5}+1 \equiv 0 \pmod{p}$. Para el caso de $257 = 2^8+1$ notamos que

$$2^{32}+1 = (2^8)^4+1 \equiv (-1)^4+1 = 2 \pmod{257}.$$

Para 641 podemos hacer una tabla con las potencias de dos:

m		1	2	4	8	16	32
2^m	(mód 641)	2	4	16	256	$65536 \equiv 154$	$154^2 = 23716 \equiv -1$

Y así concluir que $641 \mid F_5$. □

Una última propiedad:

Proposición 2.52: Los números de Fermat F_n son coprimos dos a dos.

Demostración: Si $d \mid F_n$ y $d \mid F_m$, entonces $d \mid F_n - F_m = 2^{2^n} - 2^{2^m}$ el cual es par, por lo que d es par. Pero F_n, F_m son impares, así que no pueden tener divisores pares. □

Podemos emplear éste hecho para otorgar otra demostración de la infinitud de los primos:

Demostración(Goldbach 1.47): Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de números naturales > 1 tales que son coprimos dos a dos. Entonces las factores primos de los a_n's serán todos distintos, lo que nos otorgará una sucesión infinita de números primos. En particular, por la proposición anterior se cumple que $(F_n)_{n\in\mathbb{N}}$ es un ejemplo de ese tipo de sucesiones. □

Demostración(Schorn 1.47): Sea $n > 1$ y sean $1 \leq i < j \leq n$, entonces veamos que $(n!)i+1$ y $(n!)j+1$ son coprimos: Para ello, nótese que $d := j-i$ es tal que $1 \leq d < n$, $j = i + d$ y

$$\big((n!)i + 1; (n!)j + 1\big) = \big((n!)i + 1; (n!)d\big) = 1.$$

Luego, para todo n se cumple que la sucesión finita $(n!)i + 1$ con $1 \leq i \leq n$ nos da n naturales > 1 coprimos dos a dos, lo que nos otorga, por parte baja, n primos distintos. □

Teorema 2.53 (criterio de Pépin): F_n es primo, con $n > 0$ syss

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Demostración: $\Longrightarrow$. En primer lugar:

$$F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1 \equiv 2 \equiv -1 \pmod 3, \qquad 2^{2^n} + 1 \equiv 1 \pmod 4.$$

Luego, por reciprocidad cuadrática, vemos que:

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Por lo que, por criterio de Euler:

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

$\Longleftarrow$. Si F_n no fuese primo, entonces existiría $q \mid F_n$ primo con $q^2 \leq F_n$ y claramente $3^{(F_n-1)/2} \equiv -1 \pmod q$ y por el pequeño teorema de Fermat, vemos que $\mathrm{ord}_q(3) = F_n - 1 \mid q - 1$, luego $F_n \leq q < q^2 \leq F_n$ lo que es absurdo. □

§2.3.2 Números de Carmichael. En éste capítulo vimos dos ecuaciones que nos entregan criterios para cuando un número es primo: el teorema de Wilson $(n-1)! \equiv -1 \pmod n$ y el pequeño teorema de Fermat $a^{n-1} \equiv 1 \pmod n$. Ambos fallan si n es compuesto por razones triviales: -1 es coprimo con n, pero si $n = uv$, entonces u aparece en $(n-1)!$, el cual no es coprimo con n; 1 también es coprimo con n y u^{n-1} no puede dar un número coprimo con n. No obstante, el pequeño teorema de Fermat igual da un test probabilístico bueno, ya que es de poca potencia computacional calcular potencias de primos; con ello llegamos a:

Definición 2.54: Un ***número de Carmichael*** es un entero compuesto $n > 1$ tal que para todo a coprimo con n se satisface que $a^{n-1} \equiv 1 \pmod{n}$.

Es decir, en nuestro test, los números de Carmichael son los principales obstáculos; por ello algunos se refieren a éstos números como *pseudoprimos*.

Teorema 2.55 (criterio de Korselt): Un número compuesto $n > 2$ es de Carmichael syss es libre de cuadrados y para todo primo $p \mid n$ se cumple que $(p-1) \mid (n-1)$.

Demostración: $\Longrightarrow$. Sea n un número de Carmichael y escribamos $n = p^r m$ con $r \geq 1$ y $p \nmid m$. Si $r \geq 2$, entonces por el teorema chino del resto existe $a \in \mathbb{Z}$ tal que $a \equiv 1 + p \pmod{p^r}$ y $a \equiv 1 \pmod{m}$. Así, a es coprimo con n, de modo que $a^{n-1} \equiv 1 \pmod{n}$. Reduciendo módulo p^2 obtenemos que

$$\begin{aligned} 1 \equiv (1+p)^{n-1} &= 1 + (n-1)p + p^2 \sum_{i=2}^{n} \binom{n}{i} p^{i-2} \pmod{p^2} \\ &\equiv 1 + (n-1)p \equiv 1 - p \pmod{p^2}, \end{aligned}$$

lo que es absurdo, por lo que $a = 1$.

Sea $p \mid n$ primo. Como n es libre de cuadrados, entonces $p, n/p$ son coprimos. Sea g una raíz primitiva módulo p, por el teorema chino del resto existe $a \in \mathbb{Z}$ tal que $a \equiv g \pmod{p}$ y $a \equiv 1 \pmod{n/p}$, de modo que a es coprimo con n, por lo que $a^{n-1} \equiv 1 \pmod{n}$. Reduciendo módulo p, esto induce que $g^{n-1} \equiv 1 \pmod{p}$, por lo que $(p-1) \mid (n-1)$ como se quería ver.

$\Longleftarrow$. Sea n libre de cuadrados y tal que $(p-1) \mid (n-1)$ para todo $p \mid n$ primo. Dado a coprimo con n, vemos que a es coprimo con cada factor primo p de n, por lo que $a^{p-1} \equiv 1 \pmod{p}$ y, como $(p-1) \mid (n-1)$, también $a^{n-1} \equiv 1 \pmod{p}$. Así, por el teorema chino del resto, concluimos que $a^{n-1} \equiv 1 \pmod{n}$. □

Ejemplo. Empleando el criterio de Korselt uno puede verificar el siguiente método algorítmico para construir números de Carmichael: supongamos que para $m > 1$ entero se satisface que $6m+1, 12m+1$ y $18m+1$ son todos primos; entonces su producto $(6m+1)(12m+1)(18m+1)$ es un número de Carmichael. Si además $36m+1$ también es primo, entonces $(6m+1)(12m+1)(18m+1)(36m+1)$ es un número de Carmichael.

Ejemplos de cuando ésto sucede son:

m	1	2	3	4	5	6	7
$6m+1$	**7**	**13**	**19**	25	**31**	**37**	**43**
$12m+1$	**13**	25	**37**	49	**61**	**73**	85
$18m+1$	**19**	**37**	55	**73**	91	**109**	**127**
	1729	-	-	-	-	**294409**	-

Conjetura 2.56: Se cree que hay infinitos números de Carmichael de la forma $(6m+1)(12m+1)(18m+1)$, donde cada uno de los tres factores es primo.

También era conjetural la infinitud de los números de Carmichael, pero fue resuelta en Alford *et al.* [**11**] (1994).

Corolario 2.56.1: Un número compuesto n es de Carmichael syss para todo a se cumple que $a^n \equiv a \pmod{n}$.

Demostración: Esto es una aplicación del teorema chino del resto sabiendo que los números de Carmichael son libres de cuadrados. □

Teorema 2.57: Un número de Carmichael n es impar y posee al menos tres factores primos distintos, cada uno $< \sqrt{n}$.

Demostración: Nótese que $n-1$ es coprimo con n, luego $(-1)^{n-1} \equiv (n-1)^{n-1} \equiv 1 \pmod{n}$, de modo que $n-1$ es par.

Si $n = pq$ supongamos sin perdida de generalidad que $p > q$. Sabemos que $(p-1) \mid (n-1)$, por lo que

$$\frac{n-1}{p-1} = \frac{pq-1}{p-1} = \frac{(p-1)q+q-1}{p-1} = q + \frac{q-1}{p-1},$$

de modo que $(p-1) \mid (q-1)$, con lo que $p \leq q$ lo que es absurdo.

Si $p \mid n$, entonces

$$\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+(n/p)-1}{p-1} = (n/p) + \frac{(n/p)-1}{p-1},$$

con lo que $(p-1) \mid (n/p-1)$ y, por tanto, $p < n/p$, o equivalentemente, $p < \sqrt{n}$. □

§2.3.3 Ecuaciones de Mordell I. Las ecuaciones diofánticas de la forma $y^2 = x^3 + k$ son llamadas ***ecuaciones de Mordell*** por su particular estudio (cf. [**98,** págs. 41, 48, 135, 218, 238-254]), aquí veremos algunos ejemplos.

Ejercicio 2.58: Las únicas soluciones de $y^2 = x^3 + 16$ son $(x, y) = (0, \pm 4)$.

Solución: Nótese que la ecuación puede reescribirse a $x^3 = y^2 - 16 = (y-4)(y+4)$.

(a) Si y es impar: Entonces podemos notar que $(y-4; y+4) = (8; y-4) = 1$. Luego debe cumplirse que $y - 4 = u^3$ e $y + 4 = v^3$ sean cubos y una solución satisface que $v^3 - u^3 = 8$. La mínima distancia entre cubos es aquella entre dos cubos consecutivos:

$$(w+1)^3 - w^3 = 3w^2 + 3w + 1,$$

el cual es > 8 si $w > 1$. Si $w = 0$ entonces la distancia es 1 y si $w = 1$ entonces la distancia es 7.

(b) Si y es par: Empleando congruencias mód 2 vemos que x debe ser par. Así pues, notamos que $8 \mid x^3 + 16$ luego $4 \mid y$, y por ello $16 \mid x^3 + 16$ con lo que $4 \mid x$. Definamos $x = 4x'$ e $y = 4y'$, la ecuación se reduce a

$$4x'^3 = y'^2 - 1.$$

Nuevamente empleando congruencias mód 2 se obtiene que y' es impar, ergo, $y' = 2m + 1$ con lo que

$$4x'^3 = 4m^2 + 4m + 1 - 1 \iff x'^3 = m(m+1),$$

y $(m; m+1) = 1$ así que ambos deben ser cubos. Pero los únicos cubos consecutivos son $-1, 0, 1$, lo que nos da las soluciones $(0, \pm 4)$. □

Ésta técnica de factorizar la ecuación como $x^3 = (y - \sqrt{k})(y + \sqrt{k})$ cuando k es un cuadrado es muy usual. Más adelante, veremos que será útil extender $\mathbb{Z}$ para incluir raíces cuadradas de k para resolver algunas ecuaciones de Mordell, lo cual ilustra la necesidad de anillos algebraicos para la teoría clásica.

Ejercicio 2.59: Las únicas soluciones de $y^2 = x^3 + 1$ son

$$(x, y) \in \{(-1, 0), (0, \pm 1), (2, \pm 3)\}.$$

Solución:

(a) Si y es par: Entonces $(y+1; y-1) = (2; y+1) = 1$. Luego ambos factores son cubos $y-1 = u^3$ e $y+1 = v^3$ y no existen cubos a distancia 2 exceptuando $u^3 = -1$ y $v^3 = 1$, lo cual induce la solución $(-1, 0)$.

(b) Si y es impar: Entonces $(y+1; y-1) = 2$. Sustituyendo y por $-y$ de ser necesario podemos suponer que $y \equiv 1 \pmod 4$ con lo que $y+1 \equiv 2$ e $y-1 \equiv 0 \pmod 4$. Así pues:

$$\left(\frac{x}{2}\right)^3 = \frac{y+1}{2}\frac{y-1}{4},$$

donde los dos factores de la derecha son coprimos y, por tanto, son cubos. Definiendo $\frac{y+1}{2} =: a^3$ y $\frac{y-1}{4} = b^3$ se concluye que $2a^3 - 1 = y = 4b^3 + 1$, y reordenando y dividiendo por 2 se obtiene:

$$a^3 - 2b^3 = 1.$$

Por el argumento de la distancia entre los cubos podemos concluir que la única solución es $a = \pm 1$ y $b = 0$, por lo que $y \in \{1, -3\}$. Recordando la sustitución $-y$ se obtiene que, en general, $y \in \{\pm 1, \pm 3\}$. □

Ejercicio 2.60: La ecuación $y^2 = x^3 - 5$ no tiene soluciones enteras.

Solución: Veamos todas las posibles congruencias módulo 4:

y	y^2	x	$x^3 - 1$
0	**0**	0	3
1	1	1	**0**
2	**0**	2	3
3	1	3	2

De modo que debe darse que y es par y $x \equiv 1 \pmod 4$. Reescribamos:

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2 + x + 1),$$

nótese que $x^2 + x + 1 \equiv 1 + 1 + 1 = 3 \pmod 4$, así que $x^2 + x + 1$ posee algún factor primo $p \equiv 3 \pmod 4$ (¿por qué?). Luego $p \mid y^2 + 4$ e $y^2 \equiv -4 \pmod p$. Como $y = 2k$ se obtiene que $k^2 \equiv -1 \pmod p$, es decir, -1 es un residuo cuadrático módulo p, lo que es absurdo. □

Proseguimos a emplear varias veces el hecho de que los residuos cuadráticos módulo 8 son $0, 1, 4$.

Ejercicio 2.61: La ecuación $y^2 = x^3 - 6$ no tiene soluciones enteras.

Demostración: Si x fuera par, entonces $y^2 \equiv 2 \pmod 8$ y 2 no es un residuo cuadrático. Así que x es impar e y también, de hecho, podemos precisar que $x \equiv x^3 \equiv -1 \pmod 8$ e $y \equiv 1 \pmod 8$. Reescribamos la ecuación como

$$y^2 - 2 = x^3 - 8 = (x-2)(x^2+2x+4).$$

Nótese que $x^2 + 2x + 4 \equiv 3 \pmod 8$ y $x^2 + 2x + 4 = (x+1)^2 + 3 > 0$, luego éste factor tiene algún factor primo $p \equiv \pm 3 \pmod 8$, de modo que $p \mid y^2 - 2$ o que $2 = y^2 \pmod p$, luego 2 es resto cuadrático módulo p, pero $(2/p) = -1$ lo cual es absurdo. □

Ejercicio 2.62: La ecuación $y^2 = x^3 + 6$ no tiene soluciones enteras.

Demostración: Análogamente x no puede ser par, así que x e y son impares. Luego

$$1 \equiv y^2 = x^3 + 6 \equiv x + 6 \pmod 8,$$

luego $x \equiv 3 \pmod 8$. Reescribimos la ecuación como

$$y^2 + 2 = x^3 + 8 = (x-2)(x^2-2x+4).$$

Nótese que $x^2 + 2x + 4 \equiv -1 \pmod 8$. Luego, si $p \mid x^2 + 2x + 4$, entonces $y^2 \equiv -2 \pmod p$, por lo que $(-2/p) = 1$ con lo que $p \mod 8 \in \{1, 3\}$, pero el producto de dichos primos también es $\equiv 1, 3 \pmod 8$ con lo que x^2+2x+4 mód $8 \in \{1, 3\}$ lo cual es absurdo. □

Ejercicio 2.63: La ecuación $y^2 = x^3 - 24$ no tiene soluciones enteras.

Demostración: Reescribamos:

$$y^2 + 16 = x^3 - 8 = (x-2)(x^2+2x+4),$$

donde $x^2 + 2x + 4 = (x+1)^2 + 3 > 0$.

Si x fuese impar, entonces $x^2+2x+4 \equiv 3 \pmod 4$, luego posee un factor primo $p \equiv 3 \ (4)$, pero $y^2 \equiv -16 \pmod p$, luego $\left(\frac{-1}{p}\right) = 1$ lo cual es absurdo.

Por ende, x es par, y de hecho $8 \mid y$ de la ecuación. Luego, sean $x = 2x'$ e $y = 8y'$:

$$8y'^2 = x'^3 - 3.$$

Luego $x' \equiv x'^3 \equiv 3 \pmod 8$ y:

$$8y'^2 + 2 = x'^3 - 1 = (x' + 1)(x'^2 - x' + 1),$$

y $x'^2 - x' + 1 \equiv -1 \ (8)$. Luego si p es un factor primo suyo, debe satisfacer que es impar y que $2(4y'^2+1) \equiv 0 \pmod p$, ergo $(2y')^2 \equiv -1 \ (p)$, por lo que, $\left(\frac{-1}{p}\right) = 1$ y, por tanto, $p \equiv 1 \pmod 4$, luego $p \bmod 8 \in \{1, 3\}$, pero nótese que como $3^2 \equiv 1 \ (8)$, entonces tendríamos que $x'^2 - x' + 1 \bmod 8 \in \{1, 3\}$ lo cual es absurdo. □

§2.3.4 Primos de la forma $x^2 + ny^2$. La idea de ésta subsección es aplicar nuestro conocimiento sobre reciprocidad cuadrática para poder concluir criterios para determinar si un primo p es de la forma x^2+ny^2 para un $n \geq 1$ fijo. Ésta sigue la sección §1.1 de Cox **[78].**

Comenzamos con el caso $n = 1$, el cual puede lograrse completamente con métodos elementales:

Lema 2.64: Sea $N = a^2 + b^2$ con $a, b \in \mathbb{Z}$ coprimos y sea $q = x^2 + y^2$ un divisor primo de N. Entonces $N/q = c^2 + d^2$ para algunos $c, d \in \mathbb{Z}$ coprimos.

Demostración: Nótese que q divide a

$$\begin{aligned} x^2N - a^2q &= x^2(\cancel{a^2} + b^2) - a^2(\cancel{x^2} + y^2) \\ &= x^2b^2 - a^2y^2 = (xb - ay)(xb + ay). \end{aligned}$$

De modo que se tiene que $q \mid xb - ay$, donde sustituimos a por $-a$ de ser necesario. Es decir, $xb - ay = dq$ para algún $d \in \mathbb{Z}$.

Afirmamos que $x \mid a + dy$: Como x, y son coprimos, ésto equivale a que $x \mid (a + dy)y$, lo cual

$$(a + dy)y = ay + dy^2 = (xb - dq) + dy^2 = xb - dx^2. \tag{2.5}$$

Así pues, digamos que $a + dy = cx$. Reemplazando en (2.5), obtenemos que $b = cy + dx$ y sabemos que $a = cx - dy$. Luego invocamos la siguiente identidad:

$$(x^2 + y^2)(c^2 + d^2) = (cx \pm dy)^2 + (cy \mp dx)^2, \tag{2.6}$$

para concluir que $N = a^2 + b^2 = q(c^2 + d^2)$. □

Lema 2.65: Si $p \equiv 1 \pmod 4$, entonces $p \mid x^2 + y^2$ para algunos $x, y \in \mathbb{Z}$ coprimos.

Demostración: La ecuación $p \mid x^2 + y^2$ queda como $x^2 + y^2 \equiv 0 \pmod{p}$. Como x, y son coprimos no pueden ser ambos $\equiv 0 \ (p)$, luego son no nulos y reescribiendo tenemos que

$$x^2 \equiv -y^2 \iff -1 \equiv \left(\frac{x}{y}\right)^2 \pmod{p},$$

es decir, -1 es un cuadrado módulo p y ésto es el teorema 2.37. □

Teorema 2.66: Un primo $p > 2$ es de la forma $x^2 + y^2$ syss $p \equiv 1 \pmod{4}$.

Demostración: $\Longrightarrow$. Aplicando congruencias módulo 4 uno obtiene que los cuadrados son $0, 1$ luego la suma es $0, 1$ o 2. Si fuera $p \bmod 4 \in \{0, 2\}$, entonces p sería par lo que es absurdo. Por ello, $p \equiv 1 \ (4)$.

$\Longleftarrow$. Supongamos, por contradicción, que existe $p \equiv 1 \ (4)$ que no es de la forma $x^2 + y^2$. Por el lema anterior, $p \mid a^2 + b^2 =: N$ con $a, b \in \mathbb{Z}$ coprimos. Nótese que la congruencia $a^2 + b^2 \equiv 0 \pmod{p}$ es válida siempre que reemplacemos a por $a + np$, así que podemos suponer que $|a| < p/2$ y $|b| < p/2$ de modo que $p < N < p^2/2$. Sea $q \neq p$ un divisor primo de N, luego $q \leq N/p < p$.

Si $q \equiv 3 \ (4)$, entonces $a^2 + b^2 \equiv 0 \ (q)$ de lo que se concluye que $(a/b)^2 \equiv -1 \ (q)$ lo cual es absurdo. Luego todos los divisores q son $\equiv 1 \ (4)$, y como $q < p$ entonces son de la forma $x^2 + y^2$, y así aplicando el lema 2.69 repetidas veces podemos concluir que p es de la forma $x^2 + y^2$ lo cual es absurdo. □

Ahora, a uno le gustaría poder generalizar la demostración anterior a otros casos. Mejoraremos ambos lemas:

Lema 2.67: Sea $n > 0$ natural, $p > 2$ primo con $p \nmid n$. Entonces $p \mid x^2 + ny^2$ para algunos $x, y \in \mathbb{Z}$ coprimos syss $-n$ es un cuadrado módulo p.

En particular, nótese que:

Ejercicio 2.68: Para $p > 2$ primo, se tiene que:

1. $(-2/p) = 1$ syss $p \equiv 1, 3 \pmod{8}$.

2. Si $p > 3$, entonces $(-3/p) = 1$ syss $p \equiv 1, 7 \pmod{12}$.

También podemos mejorar (2.6) a[3]

$$(x^2 + ny^2)(z^2 + nw^2) = (xz \pm nyw)^2 + n(xw \mp yz)^2. \tag{2.7}$$

Con lo cual, podemos mejorar el lema 2.69:

Lema 2.69: Sea $n > 0$ un natural fijo. Dado $N = a^2 + nb^2$ con $a, b \in \mathbb{Z}$ coprimos con un divisor $q = x^2 + ny^2 \nmid n$ primo de N. Entonces $N/q = c^2 + nd^2$ para algunos $c, d \in \mathbb{Z}$ coprimos.

Pero he aquí la sutileza del asunto, parte de la demostración consiste en que construido el N vemos que todos los divisores no caen en casos anómalos.

Teorema 2.70: Un primo $p > 2$ es de la forma $x^2 + 2y^2$ syss $p \equiv 1, 3$ (mód 8).

Teorema 2.71: Un primo $p > 3$ es de la forma $x^2 + 3y^2$ syss $p \equiv 1, 7$ (mód 12).

Demostración: $\Longrightarrow$. Basta notar que los cuadrados mód 12 son $0, 1, 4, -3$ cuyas sumas dan $0, 1, 3, 4, 7, 9$; y descartamos las congruencias $0, 3, 4, 9$ puesto que no dan números primos (exceptuando al $p = 3$).

$\Longleftarrow$. ... □

Notas históricas

El criterio de Korselt fue probado en 1899, once años antes de que Carmichael en 1910 redescubriera el criterio, por lo que algunos argumentan que deberían llamarse «números de Korselt» en su lugar. El contra-argumento podría ser que Korselt no llegó a encontrar ejemplos de números de Carmichael, en cambio éste último sí; pero, de ser ese el caso, deberían llamarse «números de Šimerka», pues éste matemático checo encontró siete ejemplos en 1885, antes que Korselt y Carmichael.

Tras el artículo de Alford *et al.* **[11],** el estudio de los números de Carmichael ha sido mucho más fructífero y agudo. En primer lugar, en el artículo prueban algo mucho mejor que infinitud: que la distribución de números de Carmichael entre 1 a n es $\sim n^{2/7}$. En 2013, T. Wright demostró que hay

[3] Otra manera de verificarlo es empleando el *álgebra de duplicación* (cfr. Jacobson **[3,** vol. 1, pág. 445]) con la involución Id y $c = -n$. Un caso particular son las álgebras cuaterniónicas.

infinitos números de Carmichael en progresiones aritméticas, haciendo un simil con el teorema de Dirichlet y en 2022, D. Larsen demostró que hay un simil del postulado de Bertrand para números de Carmichael.

3

Funciones aritméticas

3.1 Funciones multiplicativas

Definición 3.1: Se dice que una función f es ***aritmética*** cuando su dominio es $\mathbb{N}_{\neq 0}$ y cuando su codominio es $\mathbb{C}$ (puede ser un subconjunto de $\mathbb{C}$, como $\mathbb{Z}$ o $\mathbb{R}$). Una función aritmética f es ***multiplicativa*** (resp. ***completamente multiplicativa***) si es no nula y $f(ab) = f(a)f(b)$ cuando a y b son coprimos (resp. para todos a, b).

Proposición 3.2: Se cumplen:

1. Toda función completamente multiplicativa es multiplicativa.
2. Las potencias $n \mapsto n^k$ para k entero fijo son completamente multiplicativas. En particular, la identidad lo es.
3. Si f es multiplicativa, entonces $f(1) = 1$.

Demostración: Probaremos la 3: Basta notar que todo n es coprimo con 1, luego $f(n) = f(n)f(1)$. Además, como f no es nula, existe un n donde no lo es y se concluye que $f(1) = 1$. □

Una aplicación inmediata del teorema fundamental de la aritmética es el siguiente:

Teorema 3.3: Se cumplen:

1. Sea f una función definida sobre las potencias de los números primos de codominio $\mathbb{C}$, entonces existe una única función f^* multiplicativa que extiende a f. Y de hecho, f^* está dada por:

$$f^*(p_1^{k_1} \cdots p_n^{k_n}) = f(p_1^{k_1}) \cdots f(p_n^{k_n}),$$

donde los p_i's son primos distintos y donde los k_i's son naturales no nulos.

2. Así mismo, si f está definida sobre los números primos con codominio $\mathbb{C}$, entonces existe una única función f^* completamente multiplicativa que extiende a f. Y de hecho, f^* está dada por:

$$f^*(p_1^{k_1} \cdots p_n^{k_n}) = f(p_1)^{k_1} \cdots f(p_n)^{k_n},$$

donde los p_i's son primos distintos y donde los k_i's son naturales no nulos.

En §2.2 ya definimos a la función ϕ de Euler y vimos que es multiplicativa (teorema 2.24.1), por lo que el teorema anterior induce lo siguiente:

Proposición 3.4: Si p es primo y $k \neq 0$, entonces

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right),$$

por lo que, para todo $n > 1$ se da que

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Ésto permite entender mejor el gráfico que habíamos visto de la función ϕ y nos debería permitir reconocer las siguientes rectas (ver fig. 3.1).

Proposición 3.5: Para todo $n \in \mathbb{N}_{\neq 0}$ se cumple

$$n = \sum_{d|n} \phi(d).$$

Demostración: Sabemos que

$$S := \{1, 2, \ldots, n\}$$

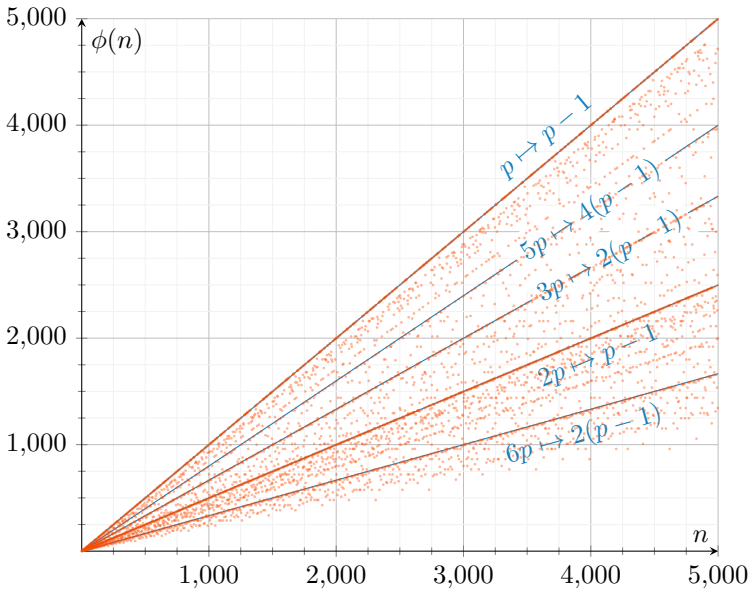


Figura 3.1. Función ϕ de Euler (con rectas de apoyo).

tiene cardinalidad n, y definamos

$$C_x := \{m : m \leq x \wedge (m; x) = 1\},$$

claramente $\phi(x) := |C_x|$.

Sea $k \in S$, veremos que existe una biyección entre S y $\coprod_{d|n} C_d$ (la unión disjunta de los C_d's). Para ello, sea $d := (k; n)$, entonces $(k/d; n/d) = 1$ con $n/d \mid n$, así que $k \mapsto k/d \in C_{n/d}$. Claramente ésta aplicación es intectiva y queda al lector ver que es suprayectiva. □

Definición 3.6: Se define la función de Möbius μ como la única función multiplicativa tal que

$$\mu(p^k) := \begin{cases} -1, & k = 1 \\ 0, & k > 1 \end{cases}$$

Nótese que si $n = p_1 \cdots p_m$ con $p_1, \ldots, p_m$ primos distintos, entonces $\mu(n) = (-1)^m$, pero μ es nula si n es divisible por el cuadrado de un primo.

Se define la función unitaria ε como

$$\varepsilon(n) := \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$$

Proposición 3.7: Para todo $n \in \mathbb{N}_{\neq 0}$ se cumple que

$$\sum_{d|n} \mu(d) = \varepsilon(n)$$

Demostración: Lo demostraremos por inducción fuerte, donde el caso base ($n = 1$) es trivial.

Si $n = p^k$, entonces sus divisores son $\{1, p, p^2, \ldots, p^k\}$ y claramente satisface el enunciado.

Si $n = ab$ con $a = p_1^{k_1} \cdots p_m^{k_m}$ y $b = p_{m+1}^{k_{m+1}}$, de modo que a, b son coprimos. Luego si $d \mid n$, entonces tenemos tres posibilidades: $d \mid a$; $d \mid b$; o $d = d_1 d_2$ con $d_1 \mid a$ y $d_2 \mid b$, con $d_1 \neq 1 \neq d_2$. Éstas son casi disjuntas dos a dos, sin embargo si $d = 1$ cabe en las dos primeras. Así pues

$$\sum_{d|n} \mu(d) = \cancelto{0}{\sum_{d|a} \mu(d)} + \cancelto{0}{\sum_{d|b} \mu(b)} - \mu(1) + \sum_{\substack{1<d_1|a \\ 1<d_2|b}} \mu(d_1)\mu(d_2).$$

Nótese que si $d_2 = p_{m+1}^{\eta}$ con $\eta \geq 2$, entonces su valor, bajo μ, será nulo. Luego podemos asumir que $d_2 = p_{m+1}$ y

$$\begin{aligned} \sum_{d|n} \mu(d) &= -1 + \sum_{1<d_1|a} \mu(d_1)\mu(p_{m+1}) \\ &= -1 - \left(\sum_{d_1|a} \mu(d_1) - \mu(1) \right) = \sum_{d_1|a} \mu(d_1) = 0, \end{aligned}$$

donde hemos aplicado la hipótesis de inducción al cancelar las sumatorias. □

He aquí una relación curiosa:

Teorema 3.8: Para todo $n \in \mathbb{N}_{\neq 0}$ se cumple que

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

Demostración: Nótese que

$$\phi(n) = \sum_{(k;n)=1} 1 = \sum_{k=1}^{n} \varepsilon\big((n;k)\big)$$

y empleando la proposición anterior:

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n;k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Analicemos bien la sumatoria. Se satisface que $d \mid n$ en todo caso, y si $d \mid k$, entonces $k = qd$ con $1 \leq k \leq n$ se ha de cumplir que $1 \leq q \leq n/d$. Es decir:

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d) \frac{n}{d}. \qquad \square$$

Ésto motiva la siguiente definición:

Definición 3.9: Sean f, g funciones aritméticas. Entonces se le dice *convolución* o *producto de Dirichlet* a la función

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a) g(b).$$

Se denota por 1 (en contexto de funciones) a la constante $1(n) = 1$, que claramente es multiplicativa.

Así pues, el teorema anterior se formula como $\phi = \mu * \mathrm{Id}$, y la proposición 3.7 como $\mu * 1 = \varepsilon$. Pero la gran importancia radica en lo siguiente:

Teorema 3.10: Sea $\mathcal{M}$ el conjunto de las funciones aritméticas. Entonces $(\mathcal{M}, *)$ es un grupo abeliano, cuyo neutro es ε, es decir, para todas las funciones multiplicativas f, g, h se cumple:

1. $f * g$ es multiplicativa (clausura).
2. $f * g = g * f$ (conmutatividad).
3. $f * (g * h) = (f * g) * h$ (asociatividad).
4. $f * \varepsilon = \varepsilon * f = f$ (elemento neutro).
5. Para todo f existe una función multiplicativa g tal que $f * g = g * f = \varepsilon$ (inverso).

Demostración:

1. Definamos $h := f * g$. Claramente

$$h(1) = (f * g)(1) = f(1)g(1) = 1.$$

Y si $(n; m) = 1$, entonces

$$h(nm) = \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right).$$

Como $d \mid nm$, podemos elegir que $d = ab$ con $a \mid n$ y $b \mid m$, de modo que

$$\begin{aligned} h(nm) &= \sum_{a|n}\sum_{b|m} f(ab)g\left(\frac{n}{a}\frac{m}{b}\right) = \sum_{a|n}\sum_{b|m} f(a)f(b)g\left(\frac{n}{a}\right)g\left(\frac{m}{b}\right), \\ &= \sum_{a|n} f(a)g\left(\frac{n}{a}\right)\sum_{b|m} f(b)g\left(\frac{m}{b}\right), \\ &= h(n)h(m). \end{aligned}$$

2. Para ésto basta notar que $d \mid n$ syss $n/d \mid n$, y que $d \mapsto n/d$ es una biyección entre los divisores de n.

3. Para todo $n \in \mathbb{N}_{\neq 0}$ sea

$$\begin{aligned} \big(f * (g * h)\big)(n) &= \sum_{ab=n} f(a)(g * h)(b) = \sum_{ab=n} f(a) \sum_{cd=b} g(c)h(d) \\ &= \sum_{acd=n} f(a)g(c)h(d) = \sum_{md=n} \left(\sum_{uv=m} f(u)g(v)\right) h(d) \\ &= \sum_{md=n} (f * g)(m)h(d) = \big((f * g) * h\big)(n). \end{aligned}$$

4. Para todo $n \in \mathbb{N}_{\neq 0}$ se cumple

$$\sum_{ab=n} f(a)\varepsilon(b) = f(n) + \sum_{\substack{ab=n \\ n\neq 1}} f(a)\cancelto{0}{\varepsilon(b)} = f(n).$$

5. Vamos a usar el teorema fundamental de la aritmética para construir g a partir de sus valores en p^n. Primero $g(p^0) = g(1) := 1$. Y por recursión, sobre un mismo p primo, se define:

$$g(p^n) := -\sum_{k=1}^{n} f(p^k)g(p^{n-k}).$$

De éste modo se satisface que

$$(f*g)(p^n) = \sum_{ab=p^n} f(a)g(b) = \sum_{k=1}^{n} f(p^k)g(p^{n-k}) + \cancel{f(1)}^{1}g(p^n) = 0.$$

Es decir, $f*g$ es una función multiplicativa (por clausura) que toma 1 en el 1 y 0 en toda otra potencia de un primo. Pero como toda función multiplicativa viene únicamente determinada por sus valores en las potencias de los primos y ε también cumple lo mismo, entonces se concluye que $f*g=\varepsilon$. □

En teoría de grupos se demuestra que en un grupo el inverso es único, lo que nos permite definir lo siguiente:

Definición 3.11: Dada una función multiplicativa f, se dice que g es su *inversa de Dirichlet*, denotada $g = f^{-1}$, si $f*g=\varepsilon$.

Teorema 3.12 (fórmula de inversión de Möbius): Dadas f, g multiplicativas. Entonces $f = g*1$ syss $g = f*\mu$.

Demostración: Ésto es una reformulación de la proposición 3.7, puesto que $\mu*1=\varepsilon$. □

Teorema 3.13: Sea f una función multiplicativa. Entonces f es completamente multiplicativa syss su inversa de Dirichlet

$$f^{-1}(n) = \mu(n)f(n).$$

Demostración: $\Longrightarrow$. Sea $g(n) := \mu(n)f(n)$, entonces

$$(g*f)(n) = \sum_{d|n} g(d)f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d|n}\mu(d) = f(n)\varepsilon(n)$$

que es igual a ε, puesto que si $n=1$ entonces da $f(1)=1$ y de lo contrario da 0.

$\Longleftarrow$. Basta probar que $f(p^n) = f(p)^n$, lo que probaremos por inducción sobre $n \geq 1$: El caso base es claro y si se cumple para n, entonces

$$(f^{-1}*f)(p^{n+1}) = 0 = \sum_{k=0}^{n+1} f(p^k)\mu(p^k)f(p^{n+1-k})$$

$$= f(1)\mu(1)f(p^{n+1}) + f(p)\mu(p)f(p^n) + \cancelto{0}{\sum_{k=2}^{n+1} f(p^k)\mu(p^k)f(p^{n+1-k})}$$
$$= f(p^{n+1}) - f(p)f(p)^n,$$

de lo que se deduce el caso inductivo (los términos cancelados lo están por tener un factor de $\mu(p^{2+j})$). □

La fórmula de Möbius puede generalizarse involucrando el siguiente concepto:

Definición 3.14: Sea $F\colon (0,\infty) \to \mathbb{C}$ con $F \restriction (0,1) \equiv 0$, y sea $\alpha(n)$ una función aritmética. Entonces se denota

$$(\alpha *' F)(x) := \sum_{n\leq x} \alpha(n) F\left(\frac{x}{n}\right),$$

donde $(\alpha *' F)\colon (0,\infty) \to \mathbb{C}$.

Nótese que si m es natural no nulo, entonces $(\alpha *' F)(m) = (\alpha * F)(m)$.

Lema 3.15: Sean α, β funciones aritméticas y $F\colon (0,\infty) \to \mathbb{C}$ con $F \restriction (0,1) \equiv 0$. Entonces

$$\alpha *'(\beta *' F) = (\alpha * \beta) *' F.$$

Demostración: Basta seguir el siguiente razonamiento:

$$\begin{aligned}
\alpha *'(\beta *' F)(x) &= \sum_{n\leq x} \alpha(n)(\beta *' F)\left(\frac{x}{n}\right) \\
&= \sum_{n\leq x} \alpha(n) \sum_{m\leq x/n} \beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{mn\leq x} \sum_{n\leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{r\leq x} (\alpha * \beta)(r) F\left(\frac{x}{r}\right) = \big((\alpha * \beta) *' F\big)(x)
\end{aligned}$$ □

Teorema 3.16 (fórmula de inversión generalizada de Möbius): Sea α una función multiplicativa con inversa de Dirichlet α^{-1}, luego

$$G(x) = (\alpha *' F)(x) \iff F(x) = (\alpha^{-1} *' G)(x).$$

El ejemplo común es $\alpha = 1$ y $\alpha^{-1} = \mu$.

Finalmente veamos el siguiente resultado que nos será útil más adelante:

Teorema 3.17: Si f es aritmética, entonces

$$\sum_{n\leq x}(f*1)(n)=\sum_{d\leq x}f(d)\left\lfloor\frac{x}{d}\right\rfloor.$$

§3.1.1 Primos de Mersenne y números perfectos. Definamos la función

$$\sigma_s(n):=\sum_{d|n}d^s,$$

la cual es la convolución de 1 con $n\mapsto n^s$, las cuales son multiplicativas, de modo que σ_s también lo es. En particular denotamos $\tau(n):=\sigma_0(s)$, la función que cuenta la cantidad de divisores de n, y $\sigma(n):=\sigma_1(n)$, la función suma de los divisores de n (incluyendo a n mismo). Como ambas funciones son multiplicativas, es fácil calcular sus valores, puesto que en potencias de primos valen:

$$\tau(p^r)=r+1,\qquad \sigma(p^r)=1+p+\cdots+p^r=\frac{p^{r+1}-1}{p-1}.$$

Definición 3.18: Un número n se dice ***perfecto*** si es la suma de sus divisores impropios.

Por ejemplo, el 6 es perfecto pues $6=1+2+3$. En lenguaje de σ: n es perfecto syss $\sigma(n)=2n$.

Teorema 3.19 (Euclides-Euler): Un número par es perfecto syss es de la forma $2^{n-1}(2^n-1)$ donde 2^n-1 es un número primo.

Demostración: $\Longleftarrow$. Ésto es un mero calculo empleando que

$$1+2+\cdots+2^n=2^{n+1}-1,$$

luego si $M_n=2^n-1$ es un primo de Mersenne, entonces

$$\sigma\big(2^{n-1}(2^n-1)\big)=\sigma(2^{n-1})\sigma(M_n)=(2^n-1)2^n=2\big(2^{n-1}(2^n-1)\big).$$

$\Longrightarrow$. Sea 2^nm con m impar un número par perfecto, luego

$$2^{n+1}m=\sigma(2^nm)=(2^{n+1}-1)\sigma(m).$$

Como $2^{n+1}-1$ es impar, se concluye que $\sigma(m) = 2^{n+1}a$ para cierto a impar y luego, despejando se tiene que $m = (2^{n+1}-1)a$ y luego $\sigma(m) = 2^{n+1}a = m+a$. Si $a > 1$, entonces a, m son divisores distintos de m y $\sigma(m) \geq 1+a+m$ lo cual es absurdo. □

Para el caso impar no se sabe mucho, pero se tiene lo siguiente:

Teorema 3.20 (Euler-De Souza): Si n es un número perfecto impar, entonces $n = pm^2$ donde $p \equiv 1 \pmod 4$ y $p \nmid m$. En consecuente, $n \equiv 1 \pmod 4$.

Euler demostró que $n = p^r m^2$ con $p \equiv r \equiv 1 \pmod 4$, mientras que de Souza [**79**] probó que necesariamente $r = 1$ y seguimos su demostración.

Demostración: Escribamos $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ donde cada p_i es primo e impar. Como n es impar, entonces $n \equiv \pm 1 \pmod 4$ y, por tanto, $\sigma(n) = 2n \equiv 2 \ (4)$ y

$$2n = \sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdots \sigma(p_m^{\alpha_m}).$$

Así pues, se tiene que $\sigma(p_i^{\alpha_i}) \equiv 2 \ (4)$ para exactamente un índice i.

Como los primos p_i's son impares, tenemos dos casos para $p := p_i$ y $\alpha := \alpha_i$:

(a) $\underline{p \equiv -1 \pmod 4}$: Entonces

$$\begin{aligned}\sigma(p^\alpha) &= 1 + p + p^2 + \cdots + p^\alpha \equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^\alpha \\ &\equiv \begin{cases} 0 & (4), \quad 2 \nmid \alpha \\ 1 & (4), \quad 2 \mid \alpha \end{cases}\end{aligned}$$

Así pues, se sigue que α_i es par.

(b) $\underline{p \equiv 1 \pmod 4}$: Entonces

$$\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha \equiv 1 + 1 + 1^2 + \cdots + 1^\alpha = \alpha + 1 \quad (4).$$

Como $\sigma(p_i^{\alpha_i}) \equiv 2 \ (4)$ para algún i, entonces $\alpha_i \equiv 1 \ (4)$.

Así pues, ya vimos que todos los primos $\equiv 3 \ (4)$ aparecen al cuadrado. Para los primos $\equiv 1 \ (4)$, se cumple que alguno aparece con potencia $\alpha_i \equiv 1 \ (4)$ para que $\sigma(p_i^{\alpha_i}) \equiv 2 \ (4)$; mientras que para el resto, es necesario que $\sigma(p_i^{\alpha_i}) \equiv \pm 1 \ (4)$, de modo que $\alpha_i \equiv 0$ o $\alpha_i \equiv 2 \ (4)$ y, en ambos casos, aparecen al cuadrado.

Ahora, sea $n = p^r m^2$ con $p \equiv r \equiv 1 \ (4)$ y $p \nmid m$. Defínase $a := \sigma(m^2)$ y $b := 2m^2$, tenemos que

$$a(1 + p + \cdots + p^r) = (1 + p + \cdots + p^r)\sigma(m^2) = \sigma(n) = 2n = 2p^r m^2 = bp^r,$$

así que p es raíz del polinomio

$$f(x) := \left(1 - \frac{b}{a}\right) x^r + x^{r-1} + \cdots + 1 \in \mathbb{Q}[x],$$

y, como m^2 no es perfecto (¿por qué?), tenemos que $b/a \neq 1$. Nótese que $\sigma(m^2) < 2m^2$ puesto que, de lo contrario, los coeficientes de $f(x)$ son positivos y p no puede ser raíz. Así que, como $m^2 < \sigma(m^2) < 2m^2$, tenemos que $1 < b/a < 2$. Definiendo $d := (a; b)$, $a_1 := a/d$ y $b_1 := b/d$, vemos que una raíz entera s de $f(x)$ tiene que satisfacer que $a_1 \mid s$ y, como b_1/a_1 no puede ser entero, entonces $a_1 > 1$ y necesariamente $a_1 = p$. Finalmente si, por contradicción, r fuese mayor que 1, tendríamos que

$$f(a_1) = (a_1 - b_1)a_1^{r-1} + a_1^{r-1} + \cdots + a_1 + 1 = 0,$$

y, por tanto, $a_1 \mid 1$ lo cual es absurdo. □

Si bien el caso de los números perfectos pares es fácilmente soluble, el caso de los impares es otra historia.

Conjetura 3.21: No existen números perfectos impares.

Se ha comprobado que no existen impares perfectos menores que $\leq 10^{1500}$ (cfr. Ochem y Rao [**47**]).

Volviendo al caso par, ¿cuando es $2^n - 1$ primo? Nótese que:

Proposición 3.22: Sean $a > 0$ y $n \geq 2$. Si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

Demostración: En primer lugar, podemos factorizar

$$a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \cdots + a + 1),$$

donde

$$a^{k-1} + a^{k-2} + \cdots + a + 1 \geq a + 1 > a - 1 > 0.$$

De modo que $a - 1 = 1$ y $a = 2$.

Ahora procedemos por contrarrecíproca. Si n no es primo, tenemos que $n = qd$ con $q, d > 1$. Luego $2^d \equiv 1 \pmod{2^d - 1}$ y

$$2^n - 1 = (2^d)^q - 1 \equiv 1^q - 1 = 0 \pmod{2^d - 1},$$

de modo que $2^d - 1 \mid 2^n - 1$, por lo que $2^n - 1$ no es primo. □

Ejercicio 3.23: Un número perfecto par n tiene por últimos dígitos 6 u 8; equivalentemente, $n \equiv 6 \pmod{10}$ o $n \equiv 8 \pmod{10}$.

Solución: Por el teorema de Euclides-Euler tenemos que $n = 2^{p-1}(2^p - 1)$ y, por el lema anterior, p es primo. Luego tenemos dos casos:

(a) $p \equiv 1 \pmod 4$: Entonces $p = 4m + 1$ y

$$n = 2^{4m}(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m.$$

Y como $16 \equiv 6 \pmod{10}$ y $6^2 = 36 \equiv 6 \pmod{10}$, entonces $16^m \equiv 6 \pmod{10}$ para todo $m > 1$, así que $n \equiv 2 \cdot 6 - 6 = 6 \pmod{10}$.

(b) $p \equiv 3 \pmod 4$: Entonces $p = 4m + 3$ y

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) = 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m \\ &\equiv 2 \cdot 6 - 4 \cdot 6 = -12 \equiv 8 \pmod{10}. \end{aligned}$$

□

Definición 3.24: Los ***números de Mersenne*** son aquellos de la forma $M_p := 2^p - 1$ con p primo. Los primos que son números de Mersenne se dicen ***primos de Mersenne***.

Conjetura 3.25: Existen infinitos primos de Mersenne, o equivalentemente, existen infinitos números pares perfectos.

Proposición 3.26: Si p es un número primo impar, entonces todo divisor primo de M_p es de la forma $2pk + 1$.

Demostración: Basta notar que $q \mid M_p$ syss $2^p \equiv 1 \pmod q$, luego $d := \mathrm{ord}_q(2) \mid p$ y $d \mid q - 1$, por lo que $d = p$ y $p \mid q - 1$, con lo que $q = pr + 1$. Finalmente, nótese que M_p es impar, luego sus divisores son impares por lo que $q = 2pk + 1$. □

Definición 3.27: Se dice que un número p es un ***primo de Sophie Germain*** si p y $2p+1$ son primos.

Teorema 3.28: Si $p \equiv 3 \pmod 4$ es un primo de Sophie Germain, entonces $2p+1 \mid M_p$. En consecuencia, M_p no es primo, exeptuando por $p=3$ en cuyo caso $2 \cdot 3 + 1 = 7 = M_3$.

Demostración: Definamos $q := 2p+1$ el cual es primo. Por el pequeño teorema de Fermat vemos que $2^{2p} \equiv 1 \pmod q$, por lo que $2^p \equiv \pm 1 \pmod q$. Si $2^p \equiv -1$, entonces se tendría que

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

pero nótese que si $p = 4k-1$, entonces $q = 2p+1 = 8k+1$, por lo que $(-2/q) = -1$ lo cual es absurdo. □

Proposición 3.29: Si p, q son primos impares tales que $q \mid 2^p - 1$, entonces $q \equiv \pm 1 \pmod 8$.

Demostración: Por hipótesis tenemos que $2^p \equiv 1 \pmod q$, y luego, por el pequeño teorema de Fermat, se cumple que $\operatorname{ord}(2) = p \mid q-1$. Como p y q son impares, entonces $p \mid \frac{q-1}{2}$ por lo que

$$2^{\frac{q-1}{2}} \equiv 1 \pmod q,$$

pero por el criterio de Euler se cumple que $(2/q) = 1$, luego $q \equiv \pm 1 \pmod 8$. □

§3.1.2 El producto de Euler y la infinitud de primos. Terminamos ésta sección con una aplicación del producto de Cauchy a las funciones multiplicativas:

Teorema 3.30 (producto de Euler): Sea f una función multiplicativa, entonces si alguna de las siguientes se cumplen:

a) $\sum_{n=1}^{\infty} |f(n)|$ converge.

b) $\prod_p (1 + |f(p)| + |f(p^2)| + \cdots)$ converge.

Entonces ambas se cumplen y de hecho

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \cdots)$$

Demostración: Supongamos que se cumple la condición a), entonces definamos $L := \sum_{n=1}^{\infty} |f(n)|$. También definamos

$$P(x) := \prod_{p \leq x} (1 + f(p) + f(p^2) + \cdots)$$

que está bien definido pues es un producto finito de una serie absolutamente convergente. Más aún, nótese que en el caso de $P(3)$, por el producto de Cauchy de series absolutamente convergentes, se da que

$$P(3) = f(1) + (f(2) + f(3)) + (f(2^2) + f(2 \cdot 3) + f(3^2)) + \cdots$$

donde los paréntesis rodean los términos formales de la serie producto. Ésto se generaliza a notar que

$$P(x) = \sum_{\forall p \leq x \; p|n} f(n).$$

Por convergencia absoluta se concluye que

$$S := \sum_{n=1}^{\infty} f(n)$$

existe y luego

$$S - P(x) = \sum_{\exists p > x : p|n} f(n),$$

en particular,

$$|S - P(x)| \leq \sum_{n > x} |f(n)| \leq L$$

pero por convergencia de L se cumple que el término del medio converge a 0 cuando $x \to \infty$, que es justamente lo que se quería probar.

Supongamos ahora que se cumple la condición b), entonces sea

$$L := \prod_{p} (1 + |f(p)| + |f(p^2)| + \cdots)$$

luego, sea

$$L(x) := \prod_{p \leq x} (1 + |f(p)| + |f(p^2)| + \cdots)$$

que claramente satisface $\lim_n L(n) = L$. Además, nótese que por las observaciones anteriores

$$L(x) = \sum_{\forall p \leq x \; p|n} |f(n)| \geq \sum_{n \leq x} |f(x)| =: S(x)$$

es decir, $S(x) \leq L(x) \leq L$, de modo que $S(x)$ está acotada superiormente y es una suma de términos positivos, así que converge absultamente y nos remitimos a la situación a). □

Corolario 3.30.1: Si f es completamente multiplicativa, entonces dadas las condiciones del teorema anterior se cumple que

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \frac{1}{1 - f(p)}.$$

Demostración: Basta notar que

$$1 + f(p) + f(p^2) + \cdots = 1 + f(p) + f(p)^2 + \cdots = \frac{1}{1 - f(p)}$$

por ser serie geométrica. □

Corolario 3.30.2: Para todo $s > 1$ se satisface

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

Éstos resultados por sí solos ya son bastante fuertes, pero Euler ofrece dos aplicaciones curiosas. La primera, otra demostración de la infinitud de números primos:

Demostración(Euler 1.47): Considerese la función multiplicativa $f(n) := 1/n$, por los corolarios anteriores se tiene que

$$\prod_{p} \frac{1}{1 - p^{-1}} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

luego no pueden haber finitos primos pues claramente el término de la izquierda convergería. □

La segunda que es una afirmación más fuerte que la anterior:

Teorema 3.31: La serie $\sum_p \frac{1}{p}$ diverge.

Demostración: Supongamos, por el contrario, que converge a un valor C. Entonces, siguiendo el argumento anterior nótese que

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

Luego, recordemos que $e^x = 1 + x + x^2/2! + x^3/3! + \cdots$, es decir,

$$\prod_{p\leq x}\left(1+\frac{2}{p}\right) \leq \prod_{p\leq x} e^{2/p} = \exp\left(\sum_{p\leq x}\frac{2}{p}\right) \leq \exp(2C).$$

Pero entonces se daría que

$$\prod_{p\leq x}\frac{1}{1-p^{-1}} = \sum_{n\leq x}\frac{1}{n} \leq \exp(2C),$$

de modo que $\sum_{n=1}^{\infty}\frac{1}{n}$ convergería, lo que es absurdo. □

3.2 Promedios de funciones aritméticas

Definición 3.32: Se denota la ***parte fraccionaria*** de un real x como:

$$\{x\} := x - \lfloor x \rfloor .$$

En general se subentenderá que la notación representa ésta función si está contenida en una fórmula.

Teorema 3.33 (fórmula de Abel): Sean $a(n)$ una función aritmética con

$$A(x) := \sum_{n\leq x} a(n)$$

y sea $f \in C^1\big([y,x]\big)$. Entonces

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_x^y A(t)f'(t)\,\mathrm{d}t.$$

Demostración: Sean $m := \lfloor y \rfloor$, y $k := \lfloor x \rfloor$. Nótese que si n es tal que $y \leq n-1 \leq n \leq x$, entonces

$$\begin{aligned}\int_{n-1}^{n} A(t)f'(t)\,\mathrm{d}t &= A(n-1)\big(f(n)-f(n-1)\big)\\ &= \big(A(n)f(n) - A(n-1)f(n-1)\big) - a(n)f(n).\end{aligned}$$

Luego

$$\int_{m+1}^{k} A(t)f'(t)\,\mathrm{d}t = A(k)f(k) - A(m+1)f(m+1) - \sum_{y<n\leq x} a(n)f(n).$$

Finalmente basta refinar que

$$\int_k^x A(t)f'(t)\,\mathrm{d}t = A(k)\big(f(x)-f(k)\big)$$

y que

$$\int_y^m A(t)f'(t)\,\mathrm{d}t = A(m-1)\big(f(m)-f(y)\big) = A(y)\big(f(m)-f(y)\big). \qquad \square$$

Teorema 3.34 – *Fórmula de Euler-Maclaurin*: Sean $y < x$ reales, $f \in C^1\big([y,x]\big)$ y. Entonces

$$\sum_{y<n\leq x} f(n) = -\{x\}f(x) + \{y\}f(y) + \int_y^x f(t)\,\mathrm{d}t + \int_y^x \{t\}f'(t)\,\mathrm{d}t.$$

Demostración: Basta aplicar el teorema anterior con $a(n) = 1$ y notar que $A(x) = \lfloor x \rfloor$. Así se obtiene

$$\begin{aligned}
\sum_{y<n\leq x} f(n) &= \lfloor x \rfloor f(x) - \lfloor y \rfloor f(y) - \int_y^x \lfloor t \rfloor f'(t)\,\mathrm{d}t \\
&= xf(x) - \{x\}f(x) + \{y\}f(y) - yf(y) - \int_y^x (t-\{t\})f'(t)\,\mathrm{d}t \\
&= -\{x\}f(x) + \{y\}f(y) + \int_y^x \{t\}f'(t)\,\mathrm{d}t + xf(x) - yf(y) - \int_y^x tf'(t)\,\mathrm{d}t \\
&= -\{x\}f(x) + \{y\}f(y) + \int_y^x \{t\}f'(t)\,\mathrm{d}t + \int_x^y f(t)\,\mathrm{d}t,
\end{aligned}$$

donde el último paso fue integración por partes. $\square$

Definición 3.35 – *Notación de Bachmann-Landau*: Se denota $f(x) = O(g(x))$ si $\limsup_{x\to\infty} |f(x)|/g(x) < \infty$, es decir, una función que está eventualmente acotada por $g(x)$. Se denota $f(x) = o(g(x))$ si $\limsup_{x\to\infty} |f(x)/g(x)| = 0$. De éste modo $O(1)$ representa cualquier función acotada y $o(1)$ representa cualquier función que converja a 0 cuando $x \to \infty$.

Más aún se denota $f(x) \sim g(x)$ cuando $\lim_{x\to\infty} f(x)/g(x) = 1$, en cuyo caso se dice que f y g son ***asintóticamente equivalentes***.

Para acostumbrarnos un poco a la notación de Bachmann-Landau, unas propiedades elementales:

Proposición 3.36: Sean f, g, h funciones[1] de codominio $\mathbb{R}$. Entonces:

1. Para todo $\lambda \in \mathbb{R}$ se cumple que $f = O(g)$ implica $\lambda f = O(g)$.
2. $O(f) \cdot O(g) = O(fg)$.
3. $O(f) + O(g) = O\big(|f| + |g|\big)$.
4. Si $f = O(g)$, entonces $O(f) + O(g) = O(g)$.
5. Si $f = O(g)$ y $g = O(h)$, entonces $f = O(h)$.
6. Si $f \sim g$ y $g \sim h$, entonces $f \sim h$.

Justificar convergencia con referencia al libro de *Análisis*.

Definición 3.37: Se define la constante de Euler-Mascheroni

$$\gamma := \lim_n \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right) = 0{,}5772156649...$$

Éstas herramientas nos permiten refinar varias series divergentes:

Teorema 3.38: Si $x \geq 1$, entonces:

1. $\displaystyle\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$.
2. Si $s > 0$ y $s \neq 1$, entonces

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s})$$

$$C(s) = \begin{cases} \zeta(s), & s > 1 \\ \lim\limits_{x \to \infty} \left(\displaystyle\sum_{n \leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right), & s < 1 \end{cases}$$

3. Si $s > 1$, entonces $\displaystyle\sum_{n \leq x} \frac{1}{n^s} = O(x^{1-s})$.

[1] No especificamos dominio pues dependiendo del contexto se puede hablar de $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$.

4. Si $\alpha \geq 0$, entonces $\displaystyle\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$.

5. $\displaystyle\sum_{n\leq x} \log n = x\log x - x + O(\log x)$.

Demostración:

1. Empleamos $f(n) = 1/n$ en la fórmula de Euler-Maclaurin:

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n} &= -\frac{\{x\}}{x} + 1 + \int_1^x \frac{\mathrm{d}t}{t} - \int_1^x \frac{\{t\}}{t^2}\,\mathrm{d}t \\ &= O\left(\frac{1}{x}\right) + 1 + \log x - \int_1^x \frac{\{t\}}{t^2}\,\mathrm{d}t \\ &= \log x + 1 - \int_1^{\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t + \int_x^{\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t + O\left(\frac{1}{x}\right)\end{aligned}$$

   Nótese que

$$0 \leq \int_x^{\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t \leq \int_x^{\infty}\frac{1}{t^2}\,\mathrm{d}t = \frac{1}{x}.$$

   Reemplazando en la fórmula se tiene que

$$\sum_{n\leq x}\frac{1}{n} = \log x + 1 - \int_1^{\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t + O\left(\frac{1}{x}\right)$$

   así pues reordenando los términos y considerando el límite cuando $x \to \infty$ se obtiene que

$$1 - \int_1^{\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t = \lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n} - \log x\right) = \gamma.$$

2. Proseguimos de manera análoga al inciso anterior:

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n^s} &= -\frac{\{x\}}{x^s} + 1 + \int_1^x \frac{\mathrm{d}t}{t^s} - s\int_1^x \frac{\{t\}}{t^{s-1}}\,\mathrm{d}t \\ &= O(x^{-s}) + 1 + \frac{x^{1-s}}{1-s} - \frac{1}{1-s} - s\int_1^x \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t.\end{aligned}$$

   Luego se cumple que

$$0 \leq \int_x^{\infty}\frac{\{t\}}{t^{s+1}}\,\mathrm{d}t \leq \int_x^{\infty}\frac{1}{t^{s+1}}\,\mathrm{d}t \leq \frac{s}{x^s}.$$

Igualando las constantes se tiene que

$$C(s) := 1 - \frac{1}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t = \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right).$$

Si $s > 1$, entonces $x^{1-s} \to 0$ y la serie converge a $\zeta(s)$ por definición de tal.

5. Por Euler-Maclaurin:

$$\begin{aligned}\sum_{n\le x}\log n &= \int_1^x \log t\,\mathrm{d}t + \int_1^x \frac{\{t\}}{t}\,\mathrm{d}t - \{x\}\log x \\ &= x\log x - x + \theta\log x - \{x\}\log x = x\log x - x + O(\log x).\end{aligned}$$

Aquí el $\theta \in [0,1]$ viene inducido del hecho de que

$$0 \le \int_1^x \frac{\{t\}}{t}\,\mathrm{d}t \le \int_1^x \frac{1}{t}\,\mathrm{d}t = \log x. \qquad \square$$

Lema 3.39: Sea f una función multiplicativa. Si $\lim_{p^m} f(p^m) = 0$, donde el subíndice recorre todas las potencias de todos los primos, entonces $\lim_n f(n) = 0$.

Demostración: Como $f(p^m) \to 0$, entonces existe A tal que $|f(p^m)| \le A$ para toda potencia de primos p^m. También existe $B \in \mathbb{N}$ tal que si $p^m \ge B$, entonces $|f(p^m)| \le 1$.

Para todo $\epsilon > 0$ existe $C \in \mathbb{N}$ tal que si $p^m \ge C$, entonces

$$|f(p^m)| \le \frac{\epsilon}{A^B}.$$

Sea $n \ge 1$ con factorización prima $n = p_1^{e_1}\cdots p_r^{e_r}$. Si cada $p_i^{e_i} < C$, entonces $n < C^C$ (pues como los p_i's son crecientes, necesariamente $r < C$); por lo tanto, si $n \ge C^C$ entonces existe $p_i^{e_i} \mid n$ con $p_i^{e_i} \ge C$. Luego

$$\begin{aligned}f(n) &= \prod_{p_i^{e_i}<B} |f(p_i^{e_i})| \cdot \prod_{B\le p_i^{e_i}<C} |f(p_i^{e_i})| \cdot \prod_{C\le p_i^{e_i}} |f(p_i^{e_i})| \\ &\le \prod_{p_i^{e_i}<B} A \cdot \prod_{B\le p_i^{e_i}<C} 1 \cdot \prod_{C\le p_i^{e_i}} \frac{\epsilon}{A^B} \\ &< A^B \cdot 1 \cdot \frac{\epsilon}{A^B} = \epsilon. \qquad \square\end{aligned}$$

El enunciado es bien específico, nótese que si cambiamos la hipótesis a que $\lim_r f(p^r) = 0$ para todo primo p, la conclusión es falsa. En efecto, la función multiplicativa dada por $f(p^r) := p^{2-r}$ satisface que $\lim_r f(p^r) = 0$, pero $\lim_n f(n) \neq 0$ pues la sucesión $\{f(n)\}_{n=1}^{\infty}$ posee la subsucesión $f(p) = p$ que es divergente. Otro ejemplo es la función de Möbius.

Proposición 3.40: Se cumplen:

1. Para todo $\epsilon > 0$ se tiene que $\tau(n) = o(n^{\epsilon})$.
2. $\phi(n) = O(n)$.
3. Para todo $\epsilon > 0$ se tiene que $n^{1-\epsilon} = o(\phi(n))$.
4. $n = O(\sigma(n))$.
5. Para todo $\epsilon > 0$ se tiene que $\sigma(n) = O(n^{1+\epsilon})$.

Demostración:

1. Definamos $f(n) := \tau(n)/n^{\epsilon}$, la cual es una función multiplicativa. Por el lema anterior, basta probar que

$$\lim_{p^m} f(p^m) = \lim_{p^m} \frac{\tau(p^m)}{p^{\epsilon m}} = \lim_{p^m} \frac{m+1}{p^{\epsilon m}} = 0$$

   lo que se sigue de que

$$\frac{m+1}{p^{\epsilon m}} \leq \frac{2m}{p^{\epsilon m}} = \frac{2\log(p^m)}{p^{\epsilon m}\log p} \leq \frac{2}{\log 2} \cdot \frac{\log(p^m)}{p^{\epsilon m}}.$$

2. Basta notar que trivialmente $\varphi(n)/n \leq 1$ y que

$$\frac{\phi(p^m)}{p^m} = 1 - \frac{1}{p} \to 1,$$

   de modo que $\limsup_n \phi(n)/n = 1$.

3. Definamos $f(n) := n^{1-\epsilon}/\phi(n)$, la cual es una función multiplicativa. Basta notar que

$$f(p^m) = \frac{p^{m(1-\epsilon)}}{p^m(1-1/p)} = \frac{p^{-m\epsilon}}{1-1/p} \leq 2p^{-m\epsilon}$$

   la cual converge a 0, por lo que, aplicando el lema anterior vemos que $\lim_n n^{1-\epsilon}/\phi(n) = 0$.

4. Como $n < 1 + n \leq \sigma(n)$ y $\sigma(p) = p + 1$ se tiene que

$$\limsup_n \frac{n}{\sigma(n)} = 1.$$

5. Definamos $f(n) := \sigma(n)/n^{1+\epsilon}$, la cual es una función multiplicativa. Nótese que

$$f(p^m) = \frac{p^{m+1} - 1}{p - 1} \cdot \frac{1}{p^{m(1+\epsilon)}} = \frac{1}{p^{m\epsilon}} \cdot \frac{1 - 1/p^{m+1}}{1 - p}$$

el cual converge a 0 para todo $\epsilon > 0$. □

Proposición 3.41: Para $s > 1$ se tiene la siguiente identidad:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.$$

Demostración: Basta notar que

$$\begin{aligned}\left(\sum_{k=1}^{\infty} \frac{1}{k^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) &= \sum_{k\geq 1}\sum_{n\geq 1} \frac{\mu(n)}{(kn)^s} = \sum_{n=1}^{\infty}\sum_{d|n} \frac{\mu(d)}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s}\left(\sum_{d|n} \mu(d)\right) = 1.\end{aligned}$$

Donde aquí empleamos el que la s-serie $\sum_{k=1}^{\infty} 1/k^s$ converge absolutamente, así como la serie de Möbius (puesto que $|\mu(n)| \leq 1$ aplicando comparación de series). □

Lema 3.42: Sean f, g funciones aritméticas, entonces sean F, G sus funciones sumatorias, es decir

$$F(x) := \sum_{n\leq x} f(n), \qquad G(x) := \sum_{n\leq x} g(n).$$

Entonces, para todo $1 \leq y \leq x$ se cumple que

$$\sum_{n\leq x}(f * g)(n) = \sum_{n\leq y} F\left(\frac{x}{n}\right) g(n) + \sum_{m\leq x/y} f(m)G\left(\frac{x}{m}\right) - F\left(\frac{x}{y}\right) G(y).$$

Demostración: Basta ver que

$$\begin{aligned}\sum_{n\leq x}(f*g)(n) &= \sum_{md\leq x} f(m)g(d)\\ &= \sum_{\substack{md\leq x\\ d\leq y}} f(m)g(d) + \sum_{\substack{md\leq x\\ d>y}} f(m)g(d)\\ &= \sum_{d\leq y} g(d) \sum_{m\leq x/d} f(m) + \sum_{m\leq x/y} f(m) \sum_{y<d\leq x/m} g(d)\\ &= \sum_{d\leq y} g(d) F\left(\frac{x}{d}\right) + \sum_{m\leq x/y} f(m)\left(G\left(\frac{x}{m}\right) - G(y)\right). \qquad \square\end{aligned}$$

Definición 3.43: Sea $r(n) := |\{(a,b)\in\mathbb{Z}^2 : a^2+b^2 = n\}$, la función que cuenta la cantidad de formas de representar a un natural n como suma de cuadrados.

Teorema 3.44: Se cumplen:

1. $\dfrac{1}{x}\displaystyle\sum_{n\leq x}\tau(n) = \log x + (2\gamma - 1) + O\left(\frac{1}{\sqrt{x}}\right).$
2. (Problema del círculo de Gauss) $\dfrac{1}{x}\displaystyle\sum_{n\leq x} r(n) = \pi + O\left(\frac{1}{\sqrt{x}}\right).$
3. $\dfrac{1}{x}\displaystyle\sum_{n\leq x}\phi(n) = \frac{3}{\pi^2}x + O(\log x).$

Demostración:

1. Nótese que la función contadora de divisores $\tau(n)$ se puede escribir como la convolución $\tau = 1*1$. Basta emplear el resultado anterior con $f = g = 1$, y con $y = \sqrt{x}$, en cuyo caso nótese que $F(x) = G(x) = \lfloor x\rfloor$ y que:

$$\begin{aligned}\sum_{n\leq x}\tau(n) &= \sum_{n\leq\sqrt{x}}\left\lfloor\frac{x}{n}\right\rfloor + \sum_{m\leq\sqrt{x}}\left\lfloor\frac{x}{m}\right\rfloor - \left\lfloor\sqrt{x}\right\rfloor^2\\ &= 2x\sum_{n\leq\sqrt{x}}\frac{1}{n} - x + O(\sqrt{x}) = 2x(\log\sqrt{x} + \gamma + O(x^{-1/2})) - x + O(\sqrt{x}).\end{aligned}$$

   que reordenando términos concluye el enunciado.

2. Nótese que $r(n)$ puede verse como la cantidad de puntos del reticulado $\mathbb{Z}^2$ en la esfera $S(\sqrt{n}) := \{(x,y) \in \mathbb{R}^2 : \|(x,y)\| = \sqrt{n}\}$. Así que, para un entero N la cantidad total de puntos del reticulado $\mathbb{Z}^2$ en la bola cerrada $\overline{B}_N(0)$ es

$$R(N) := 1 + \sum_{n \leq N} r(n).$$

Podemos asociar a cada punto de dicho reticulado, un cuadrado de 1×1 (ver fig. 3.2) y así notar que $R(N)$ está incluido en la bola cerrada de radio $\sqrt{N} + \sqrt{2}$ (donde el $+\sqrt{2}$ viene de que los cuadrados que se «salen» tienen una diagonal de $\sqrt{2}$) y a su vez incluyen la bola cerrada de radio $\sqrt{N} - \sqrt{2}$.

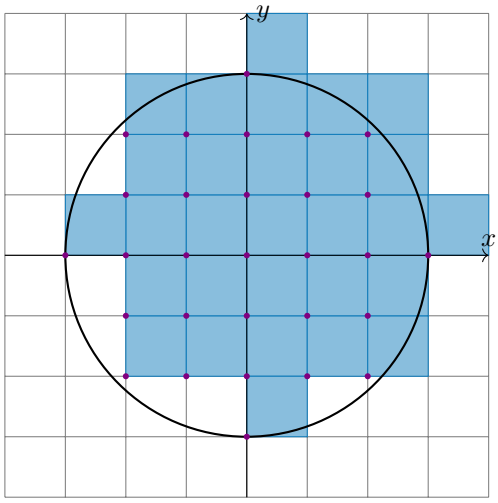


Figura 3.2

Así vemos que

$$\pi\left(\sqrt{N} - \sqrt{2}\right)^2 \leq 1 + \sum_{n \leq N} r(n) \leq \pi\left(\sqrt{N} + \sqrt{2}\right)^2,$$

de modo que $R(N) \leq \pi N + 2\pi\sqrt{2N} + 2\pi$ y $R(N) \geq \pi N - 2\pi\sqrt{2N} + 2\pi$.

3. Ya sabemos que $\phi(n) = \sum_{d|n} \mu(d) n/d$, por lo que

$$\frac{1}{x}\sum_{n \leq x} \phi(n) = \frac{1}{x}\sum_{n \leq x}\sum_{ab=n} a\mu(b) = \frac{1}{x}\sum_{a}\sum_{b \leq x/a} a\mu(b)$$

$$= \frac{1}{x}\sum_{b\leq x}\mu(b)\cdot\sum_{a\leq x/b}a = \frac{1}{x}\sum_{b\leq x}\mu(b)\frac{\lfloor x/b\rfloor(\lfloor x/b\rfloor+1)}{2}$$
$$= \frac{1}{2x}\sum_{n\leq x}\mu(n)\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}\right)\left(\frac{x}{n}-\left\{\frac{x}{n}\right\}+1\right)$$
$$= \frac{x}{2}\sum_{n\leq x}\frac{\mu(n)}{n^2}+\frac{1}{2}\sum_{n\leq x}\frac{\mu(n)(1-2\{x/n\})}{n}$$
$$+\frac{1}{2x}\sum_{n\leq x}\mu(n)\left\{\frac{x}{n}\right\}\left(1-\left\{\frac{x}{n}\right\}\right)$$

Por las proposiciones anteriores tenemos que

$$\frac{1}{2}\left|\sum_{n\leq x}\frac{\mu(n)(1-2\{x/n\})}{n}\right| \leq \frac{1}{2}\sum_{n\leq x}\frac{1}{n} = O(\log x),$$
$$\frac{1}{2x}\sum_{n\leq x}\mu(n)\left\{\frac{x}{n}\right\}\left(1-\left\{\frac{x}{n}\right\}\right) = O(1).$$

Y finalmente, acotamos el término restante:

$$\sum_{n\leq x}\frac{\mu(n)}{n^2} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^2} - \sum_{n=\lfloor x\rfloor+1}^{\infty}\frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)}+O\left(\frac{1}{x}\right). \qquad \square$$

Más adelante veremos que podemos agudizar la cota del problema del círculo de Gauss. Se conjetura lo siguiente:

Conjetura 3.45: Se creen:

1. Es cierto que $\sum_{n\leq x} r(n) = \pi x + O(x^{1/4+\epsilon})$.
2. Es falso que $\sum_{n\leq x} r(n) = \pi x + O(x^{1/4-\epsilon})$.

3.3 Distribución de números primos

El objetivo principal es llegar a probar uno de los resultados más importantes de la teoría analítica de números, primero veamos las funciones involucradas:

Definición 3.46: Se definen las siguientes funciones:

$$\pi(x) := |\{p \in \mathbb{N} : p \text{ primo} \wedge p \leq x\}| = \sum_{p \leq x} 1,$$

$$\mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t},$$

a π se le dice ***función contadora de primos*** y a Li se le conoce como ***función logaritmo integral***.

Así la observación empírica a la que llego Gauss fue a ver que éstas dos funciones «se parecían mucho cuando x era muy grande» (ver fig. 3.3), o más rigurosamente que daba la impresión de que eran asintoticamente equivalentes. A éste resultado se le conoce como el *teorema de números primos* (abrev., TNP) y uno de los objetivos fundamentales de éste texto será probarlo.

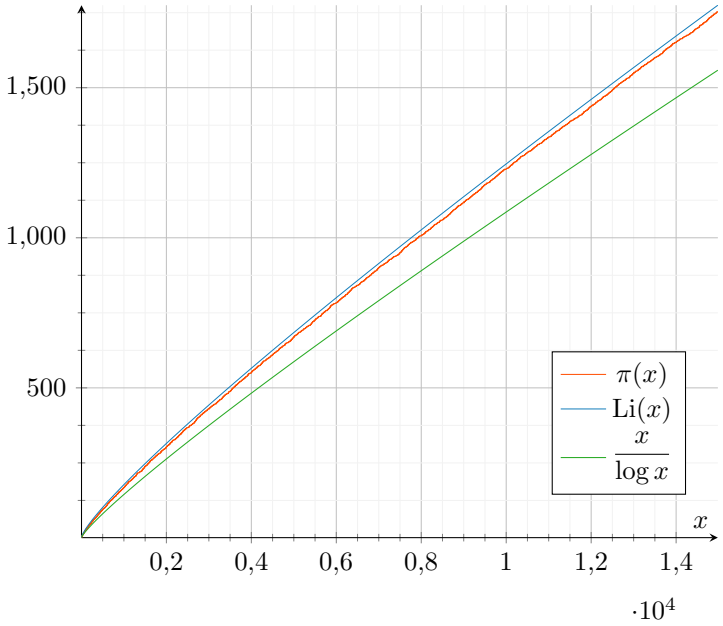


Figura 3.3. Teorema de los números primos.

En primer lugar veamos como deducir un par de cotas iniciales para $\pi(x)$. La primera se sigue inmediata de la demostración de Euclides:

Proposición 3.47: Para $x \geq 2$ se cumple que $\pi(x) \geq \log\log x$.

Demostración: Sea $p_n\colon \mathbb{N} \to \mathbb{N}$ la enumeración creciente de los números primos, de modo que $p_0 = 2$, $p_1 = 3$, etc. Veamos que $p_n \leq 2^{2^n}$ por inducción sobre n: El caso base $p_0 = 2 \leq 2^{2^0}$, y la demostración de Euclides induce que

$$p_{n+1} \leq p_0 \cdots p_n + 1 \leq 2^{2^0} \cdots 2^{2^n} + 1 = 2^{2^{n+1}-1} + 1,$$

y, considerando $x = 2^{2^{n+1}}$, vemos que $\frac{x}{2} + 1 \leq x$ syss $2 \leq x$. Ésto nos permite concluir que $\pi(2^{2^n}) \geq n + 1$. Así pues, si $x \geq 2$ podemos encontrar un único n tal que $2^{2^n} \leq x < 2^{2^{n+1}}$, o lo que es equivalente, $n \leq \log_2 \log_2 x < n + 1$ y luego

$$\pi(x) \geq \pi(2^{2^n}) \geq n + 1 > \log_2 \log_2 x;$$

finalmente, como $0 < \log 2 < 1$ vemos que $\log_2 x = (\log x)/(\log 2) > \log x$ de lo que se concluye la demostración. □

Curiosamente, podemos sacar una mucho mejor cota con incluso menos trabajo. Vamos a requerir la siguiente definición:

Definición 3.48: Un entero n se dice ***libre de cuadrados*** si no existe otro $m > 1$ tal que $m^2 \mid n$.

El 1 es el único número que es un cuadrado y está libre de cuadrados.

Por el teorema fundamental de la aritmética, notamos que un natural libre de cuadrados es un producto de primos distintos (con exponente 1), de hecho, la totalidad de números libres de cuadrados está en biyección con los subconjuntos finitos de números primos (donde al vacío $\varnothing$ se le asocia el 1), de modo que bastaría probar que hay infinitos números libres de cuadrados para probar la infinitud de los primos. Con ésto otorgamos dos demostraciones y cotas (en simultáneo):

Demostración(Perott 1.47): Considere el conjunto $S_N := \{1, 2, \ldots, N\}$ que posee exactamente N elementos. Nótese que podemos acotar la cantidad de números libres de cuadrados $A(N)$ en S_N, mediante la siguiente criba: eliminamos a los múltiplos de 2^2, a los de 3^2, a los de 4^2 y así:

$$\sum_{k=2}^{\infty} \lfloor N/k^2 \rfloor \leq N \sum_{k=2}^{\infty} \frac{1}{k^2} = N(\zeta(2) - 1),$$

de modo que:

$$A(N) \geq N - N(\zeta(2) - 1) = N(2 - \zeta(2)).$$

Ahora, nótese que $\zeta(2) < 2$ puesto que

$$\zeta(2) = 1 + \sum_{k=2}^{\infty} \frac{1}{k^2} < 1 + \sum_{k=2}^{\infty} \int_{k-1}^{k} \frac{1}{t^2}\,\mathrm{d}t = 1 + \int_{1}^{\infty} \frac{1}{t^2}\,\mathrm{d}t = 2.$$

Luego tenemos que $A(N)/N \to 2 - \zeta(2)$ el cual es > 0, de modo que $A(N)$ es infinito. □

Y de la misma demostración se sigue que:

Corolario 3.48.1: Se satisface que $\pi(N) \geq \log N/\log 2 + O(1)$.

Demostración: Basta notar que $A(N) \leq 2^{\pi(N)}$ pues, como dijimos, los enteros libres de cuadrados están en biyección con los subconjuntos finitos de los primos. □

Otra demostración, y más sencilla es la siguiente:

Demostración(Erdős 1.47): Considere el conjunto $S_N := \{1, 2, \ldots, N\}$ que posee exactamente N elementos. Nótese que hay a lo más $2^{\pi(N)}$ números libres de cuadrados en S_N y que hay a lo más $\sqrt{N}$ cuadrados en S_N. Finalmente, todo elemento puede expresarse como un número cuadrado por un número libre de cuadrados, de modo que

$$N = S_N \leq \sqrt{N} \cdot 2^{\pi(N)} \implies \pi(N) \geq \log_2(\sqrt{N}) = c \cdot \log N,$$

donde $c = \frac{1}{2}\log(2)^{-1} \approx 0{,}72$. Como $\log N \to \infty$ cuando $N \to \infty$, entonces se concluye que $\pi(N) \to \infty$. □

Definición 3.49: Dada una función aritmética f, se define la ***función sumatoria de*** F como

$$F(n) := \sum_{n \leq x} f(n).$$

Y vamos a definir varias funciones aritméticas:

$$\Lambda(x) := \begin{cases} \log p & x = p^k, k \geq 1 \\ 0 & \text{en otro caso} \end{cases}$$

$$\vartheta(x) := \sum_{p \leq x} \log p,$$

$$\psi(x) := \sum_{p^k \leq x} \log p = \sum_{n \leq x} \Lambda(n),$$

$$T(x) := \sum_{n \leq x} \log n.$$

A Λ se le conoce como la ***función de von Mangoldt***, a ϑ y ψ se le conocen como ***primera*** y ***segunda función de Chebyshev*** resp., y T es simplemente la función sumatoria de logaritmo. Nótese que ψ es la función sumatoria de Λ, sin embargo, Λ no es una función multiplicativa.

Uno de los descubrimientos vitales de la teoría analítica de números es que los primos se «llevan bien con la función log», lo cual tiene cierto sentido si pensamos que están definidos a partir de una propiedad del producto.

En general veremos que resolver el TNP de forma elemental es difícil, por lo que debemos cambiar ligeramente el problema, y el siguiente teorema caracteriza la necesidad de las funciones de Chebyshev:

Teorema 3.50: Son equivalentes:

1. $\pi(x) \sim \mathrm{Li}(x)$.
2. $\pi(x) \sim \dfrac{x}{\log x}$.
3. $\vartheta(x) \sim x$.
4. $\psi(x) \sim x$.

Demostración: Ver que $1 \iff 2$ se reduce a notar que $\mathrm{Li}(x) \sim \frac{x}{\log x}$ por regla de L'Hôpital.

Ahora definamos la función aritmética:

$$a(n) := \begin{cases} 1, & n \text{ primo} \\ 0, & n \text{ no primo} \end{cases}$$

Nótese que $\sum_{n \leq x} a(n) = \pi(x)$. Por fórmula de Abel se tiene que

$$\vartheta(x) = \sum_{n \leq x} a(n) \log n = \pi(x) \log x - \int_1^x \frac{\pi(t)}{t} \, \mathrm{d}t,$$

y viceversa, si $b(n) := a(n) \log n$, nótese que $\sum_{n \leq x} b(n) = \vartheta(x)$, por lo que

$$\pi(x) = \sum_{n \leq x} b(n) \frac{1}{\log n} = \frac{\vartheta(x)}{\log x} - \int_1^x \frac{\vartheta(t)}{t \log^2 t} \, \mathrm{d}t. \tag{3.1}$$

Luego para probar que $2 \implies 3$ basta demostrar que

$$\lim_{x\to\infty} \frac{1}{x}\int_1^x \frac{\pi(t)}{t}\,\mathrm{d}t = 0,$$

para ello, nótese que 2 se traduce en que $\pi(t)/t = O(1/\log t)$ cuando $t \geq 2$, luego

$$\frac{1}{x}\int_2^x O\left(\frac{1}{\log t}\right)\mathrm{d}t = O\left(\frac{1}{x}\int_2^x \frac{\mathrm{d}t}{\log t}\right)$$

Y nótese que

$$\int_2^x \frac{\mathrm{d}t}{\log t} \leq \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{\log t} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{\log t} \leq \frac{\sqrt{x}-2}{\log 2} + \frac{x-\sqrt{x}}{\log(\sqrt{x})}.$$

Luego al multiplicar por $1/x$ se comprueba que

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\mathrm{d}t}{\log t} = 0.$$

Para probar que $3 \implies 2$, notamos que mirando la fórmula (3.1) y multiplicando por $\frac{\log x}{x}$ se nota que basta demostrar que

$$\lim_{x\to\infty} \frac{\log x}{x}\int_1^x \frac{\vartheta(t)}{t\log^2 t}\,\mathrm{d}t.$$

Igual que antes, por 3, sea $\vartheta(t) = O(t)$, luego

$$\frac{\log x}{x}\int_1^x \frac{O(t)}{t\log^2 t}\,\mathrm{d}t = O\left(\frac{\log x}{x}\int_1^x \frac{1}{\log^2 t}\,\mathrm{d}t\right).$$

Y nótese que

$$\int_2^x \frac{\mathrm{d}t}{\log^2 t} \leq \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{\log^2 t} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{\log^2 t} \leq \frac{\sqrt{x}-2}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2(\sqrt{x})}.$$

Luego se concluye análogamente.

Veamos que $3 \iff 4$. Así pues, comencemos por notar que

$$\begin{aligned}\psi(x) &= \sum_{p^k\leq x} \log p = \sum_{k\leq x}\sum_{p\leq x^{1/k}} \log p = \sum_{k\leq x} \vartheta(x^{1/k}) \\ &= \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \cdots \end{aligned} \tag{3.2}$$

nótese que la suma es finita, dado que $\vartheta(x^{1/m}) = 0$ si $x^{1/m} < 2$ para $m > \log_2 x$. Luego

$$0 \leq \psi(x) - \vartheta(x) = \sum_{m \leq \log_2 x} \vartheta(x^{1/m}).$$

Además, notemos que

$$\vartheta(x) \leq \sum_{n \leq x} \log n \leq x \log x.$$

Por lo que

$$\begin{aligned} 0 \leq \psi(x) - \vartheta(x) &\leq \sum_{m \leq \log_2 x} x^{1/m} \log(x^{1/m}) \leq \log_2 x x^{1/2} \log(x^{1/2}) \\ &= \frac{\log x}{\log 2} \frac{\sqrt{x}}{2} \log x = \frac{\sqrt{x}(\log x)^2}{2 \log 2}. \end{aligned}$$

Finalmente, dividiendo por x se puede comprobar que el límite converge a 0. Es decir, hemos probado que $\psi(x)/x \sim \vartheta(x)/x$. □

Uno de los incisos del teorema 3.38 se se traduce en que

$$T(x) = x \log x - x + O(\log x). \tag{3.3}$$

Teorema 3.51 (Shapiro): Sea $\{a(n)\}_{n=1}^{\infty}$ una sucesión de reales positivos tales que

$$\sum_{n \leq x} a(n) \left\lfloor \frac{x}{n} \right\rfloor = x \log x + O(x).$$

Entonces:

1. Para $x \geq 1$ se cumple que

$$\sum_{n \leq x} \frac{a(n)}{n} = \log x + O(1).$$

2. Existen $0 < c_1 < c_2$ tales que para x suficientemente grande

$$c_1 x \leq \sum_{n \leq x} a(n) \leq c_2 x.$$

Demostración: Definamos

$$S_1(x) := \sum_{n\leq x} a(n), \quad S_2(x) := \sum_{n\leq x} a(n)\left\lfloor \frac{x}{n}\right\rfloor.$$

Primero notemos que

$$\begin{aligned} S_2(x) - 2S_2\left(\frac{x}{2}\right) &\geq \sum_{n\leq x} a(n)\left\lfloor\frac{x}{n}\right\rfloor - 2\sum_{n\leq x/2} a(n)\left\lfloor\frac{x}{2n}\right\rfloor \\ &\geq \sum_{n\leq x} \underbrace{\left(\left\lfloor\frac{x}{n}\right\rfloor - 2\left\lfloor\frac{x}{2n}\right\rfloor\right)}_{\geq 0} a(n) + \sum_{x/2<n\leq x} a(n)\left\lfloor\frac{x}{n}\right\rfloor \\ &\geq \sum_{x/2<n\leq x} a(n)\left\lfloor\frac{x}{n}\right\rfloor \geq \sum_{x/2<n\leq x} a(n) = S_1(x) - S_1(x/2). \end{aligned}$$

Luego, por construcción se tiene que

$$S_2(x) - 2S_2\left(\frac{x}{2}\right) = x\log x + O(x) - 2\left(\frac{x}{2}\log\left(\frac{x}{2}\right) + O(x)\right) = O(x).$$

En consecuencia, se tiene que

$$S_1(x) - S_1\left(\frac{x}{2}\right) \leq Kx$$

luego, sustituyendo x por $x/2^j$ se obtiene que

$$S_1\left(\frac{x}{2^j}\right) - S_1\left(\frac{x}{2^{j+1}}\right) \leq Kx\frac{1}{2^j}$$

y por ende

$$S_1(x) \leq Kx\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) = 2Kx$$

por lo que $c_2 := 2K$ aplica.

Para el inciso 1., basta notar que $\lfloor x/n\rfloor = x/n + O(1)$ para notar que

$$\begin{aligned} S_2(x) &= \sum_{n\leq x} a(n)\left(\frac{x}{n} + O(1)\right) = x\sum_{n\leq x}\frac{a(n)}{n} + O\left(\sum_{n\leq x} a(n)\right) \\ &= x\sum_{n\leq x}\frac{a(n)}{n} + O(x) \end{aligned}$$

donde la última igualdad sale de la conclusión anterior. Luego

$$\sum_{n\leq x}\frac{a(n)}{n} = \frac{1}{x}(S_2(x) + O(x)) = \log x + O(1).$$

Para completar la última desigualdad definamos

$$A(x) := \sum_{n\leq x} \frac{a(n)}{n} = \log x + R(x)$$

donde $R(x)$ es el término error y sabemos que $|R(x)| \leq M$ para algún $M > 0$, por ser de orden $O(1)$.

Para todo $x \geq 1$ y todo α tal que $\alpha x \geq 1$ se satisface que

$$\begin{aligned} A(x) - A(\alpha x) &= \log x + R(x) - \big(\log(\alpha x) + R(\alpha x)\big) = -\log\alpha + R(x) - R(\alpha x) \\ &\geq -\log\alpha - |R(x)| - |R(\alpha x)| \geq -\log\alpha - 2M. \end{aligned}$$

Luego definamos α tal que $-\log\alpha - 2M = 1$, es decir, $\alpha = \exp(-1-2M)$ y por tanto $\alpha \in (0,1)$. Es decir $A(x) - A(\alpha x) \geq 1$ para todo $x \geq 1/\alpha$. Pero

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leq x} \frac{a(n)}{n} \leq \frac{1}{\alpha x} \sum_{n\leq x} a(n) = \frac{S_1(x)}{\alpha x}.$$

Así pues

$$S_1(x) \geq \alpha x$$

para $x \geq 1/\alpha$, que completa el inciso 2. □

Corolario 3.51.1: Se cumplen las siguientes:

1. $(\Lambda * 1)(n) = \log n$.
2. $\displaystyle\sum_{n\leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor = \log x + O(1)$.
3. $c_1 x \leq \psi(x) \leq c_2 x$. En consecuente, $\psi(x)/x = O(1)$.

Demostración: La primera es trivial y la tercera se demuestra de la segunda, que es la que probaremos: Nótese que

$$\begin{aligned} \sum_{n\leq x} \Lambda(n) \left\lfloor \frac{x}{n} \right\rfloor &= \sum_{d\leq x} \Lambda(d) \sum_{m\leq x/d} 1 = \sum_{d\leq x} (\Lambda * 1)(d) \\ &= \sum_{d\leq x} \log d = T(x) \qquad (3.4) \\ &= x\log x - x + O(\log x) = x\log x + O(x). \end{aligned}$$

□

Teorema 3.52 – *Primer teorema de Mertens*:

$$\sum_{p\leq x}\frac{\log p}{p}=\log x+O(1).$$

Demostración: Primero nótese que

$$\begin{aligned}\sum_{n\leq x}\frac{\Lambda(n)}{n}&=\sum_{n\leq x}\Lambda(n)\frac{1}{x}\left(\left\lfloor\frac{x}{n}\right\rfloor+O(1)\right)\\&=\frac{1}{x}\sum_{n\leq x}\Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor+O\left(\frac{1}{x}\sum_{n\leq x}\Lambda(n)\right)\\&=\frac{1}{x}(x\log x+O(1))+O\left(\frac{\psi(x)}{x}\right)=\log x+O(1).\end{aligned}\tag{3.5}$$

Ahora hay que ver que la diferencia entre ésta suma y el enunciado está acotada, para ello nótese que

$$\sum_{n\leq x}\frac{\Lambda(n)}{n}=\sum_{p\leq x}\frac{\log p}{p}+\sum_{p^{k+1}\leq x}\frac{\log p}{p^{k+1}},$$

y que

$$\begin{aligned}\sum_{p^{k+1}\leq x}\frac{\log p}{p^{k+1}}&=\sum_{p\leq\sqrt{x}}\log p\sum_{m=2}^{\lfloor\log x/\log p\rfloor}\frac{1}{p^m}\\&\leq\sum_{p\leq\sqrt{x}}\frac{\log p}{p^2-p}\leq\sum_{p\leq\sqrt{x}}\frac{\log p}{p^2}\leq\sum_{n=1}^{\infty}\frac{\log n}{n^2},\end{aligned}$$

sin embargo, el último término es una serie convergente, así se concluye el enunciado. □

Teorema 3.53 – *Segundo teorema de Mertens*:

$$\sum_{p\leq x}\frac{1}{p}=\log\log p+M+O\left(\frac{1}{\log x}\right),$$

donde M es una constante, llamada la ***constante de Mertens***.

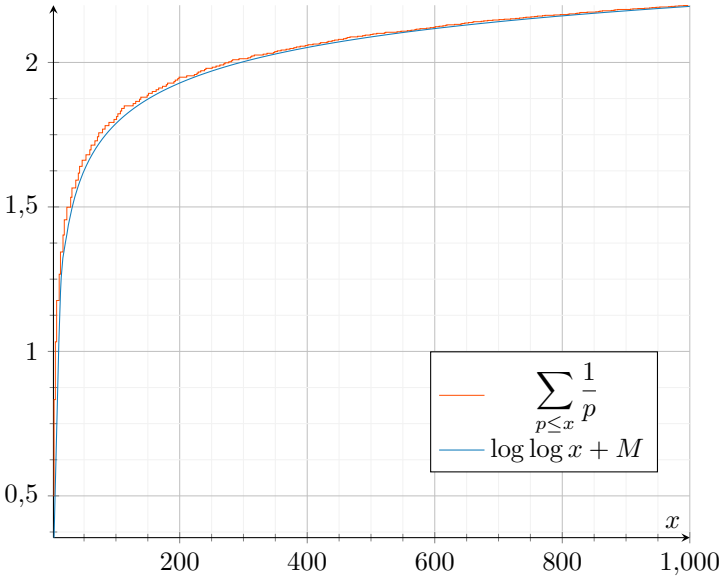


Figura 3.4. Segundo teorema de Mertens.

Demostración: Definamos las siguientes:

$$a(n) := \begin{cases} 1, & n \text{ primo} \\ 0, & n \text{ no primo} \end{cases} \qquad A(n) := \sum_{n\leq x} a(n)\frac{\log n}{n} = \sum_{p\leq x} \frac{\log p}{p}.$$

Así pues, empleando $f(t) = 1/\log t$ en la fórmula de Abel nos queda que

$$\sum_{n\leq x} \frac{1}{p} = \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t\log^2 t}\,\mathrm{d}t.$$

Como $A(x) = \log x + R(x)$, donde $R(x) = O(1)$, por el primer teorema de Mertens, se obtiene que

$$\begin{aligned} \sum_{n\leq x} \frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{\log t + R(t)}{t\log^2 t}\,\mathrm{d}t \\ &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}\,\mathrm{d}t + \int_2^x \frac{R(t)}{t\log^2 t}\,\mathrm{d}t. \end{aligned}$$

Sin embargo, nótese que

$$\frac{\mathrm{d}}{\mathrm{d}t}\log\log t = \frac{1}{t\log t}$$

y de que

$$\int_2^x \frac{R(t)}{t\log^2 t}\,\mathrm{d}t = \int_2^\infty \frac{R(t)}{t\log^2 t}\,\mathrm{d}t - \int_x^\infty \frac{R(t)}{t\log^2 t}\,\mathrm{d}t.$$

El primer término es una constante, y el segundo

$$0 \le \int_x^\infty \frac{R(x)}{x\log^2 x}\,\mathrm{d}t \le \int_x^\infty \frac{K}{x\log^2 x}\,\mathrm{d}t = -\frac{K}{\log x} = O\left(\frac{1}{\log x}\right)$$

Reuniendo todo se obtiene que

$$\sum_{n\le x}\frac{1}{p} = \log\log x + \underbrace{1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t\log^2 t}\,\mathrm{d}t}_{M} + O\left(\frac{1}{\log x}\right). \qquad \square$$

§3.3.1 El postulado de Bertrand.

Teorema 3.54 – *Postulado de Bertrand*: Para todo $n \ge 2$ existe un primo p tal que $n < p \le 2n$.

Demostración: Comenzamos con la siguiente fórmula:

$$\begin{aligned}\sum_{k\ge 1}\psi\left(\frac{x}{k}\right) &= \sum_{k\ge 1}\sum_{n\le x/k}\Lambda(n) = \sum_{\substack{kn\le x\\ k\ge 1}}\Lambda(n)\\ &= \sum_{n\le x}\sum_{k\le x/n}\Lambda(n) = \sum_{n\le x}\Lambda(n)\left\lfloor\frac{x}{n}\right\rfloor = T(x)\end{aligned}$$

donde la última igualdad corresponde a la ecuación (3.4). De modo que

$$T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \cdots$$

Luego se obtiene que

$$T(x) - 2T\left(\frac{x}{2}\right) = \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) - \cdots$$

Ahora, la fórmula (3.3) nos permite notar que

$$\begin{aligned}T(x) - 2T(x/2) &= x\log x - x - 2\left(\frac{x}{2}\log\frac{x}{2} - \frac{x}{2}\right) + O(\log x)\\ &= x\log 2 - \frac{x}{2} + O(\log x)\end{aligned}$$

Y como ψ es monótona se tiene que

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right) \leq \psi(x)$$

En definitiva

$$\psi(x) - \psi(x/2) \leq x\log 2 - \frac{x}{2} + O(\log x) \leq \psi(x).$$

Por otro lado:

$$\begin{aligned}\psi(x) &= \big(\psi(x) - \psi(x/2)\big) + \big(\psi(x/2) - \psi(x/4)\big) + \cdots \\ &\leq \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right)\big(x\log 2 - x/2 + O(\log x)\big) \\ &= x\log 4 - x + O(\log x).\end{aligned}$$

Luego como $\psi(x/2) \geq x\log(2^{1/2}) - x/4 + O(\log x)$, entonces

$$\psi(x) - \psi(x/2) \geq \frac{3x}{2}\big(\log(2) - 1\big) + O(\log x)$$

□

Ahora incluimos la demostración de Ramanujan mediante la modificación de Erdős.

Teorema 3.55: Para todo $n \geq 2$ se cumple que

$$\prod_{p\leq n} p \leq 4^n \iff \vartheta(x) \leq 2x\log 2.$$

Demostración: Ésto se realiza por inducción: Primero, podemos notar que la relación se cumple trivialmente para $n = 2$, así que podremos asumir n más grande.

Si n es par, entonces no es primo, luego

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-1} \leq 4^n.$$

Si $n = 2m + 1$, entonces, considere primero al coeficiente binomial:

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m+1}$$

y nótese que todos los primos $> m+1$ no están en el denominador, de modo que

$$\prod_{m+1<p\leq n} p \mid \binom{2m+1}{m} = \frac{1}{2}\left(\binom{2m+1}{m} + \binom{2m+1}{m+1}\right) \leq \frac{1}{2}(1+1)^{2m+1} = 4^m.$$

Luego, por hipótesis inductiva se concluye que

$$\prod_{p\leq n} p = \left(\prod_{p\leq m+1} p\right)\cdot\left(\prod_{m+1<p\leq n} p\right) \leq 4^{m+1}\cdot 4^m = 4^n. \qquad \square$$

Lema 3.56: Para todo $n \geq 1$ tenemos que

$$\binom{n}{\lfloor n/2\rfloor} \geq \frac{2^n}{n}, \qquad \binom{2n}{n} \geq \frac{4^n}{2n}.$$

Demostración: En efecto, basta notar que, por el binomio de Newton

$$2^n = (1+1)^n = \sum_{j=0}^{n}\binom{n}{j},$$

luego los coeficientes binomiales suman 2^n y agrupando $\binom{n}{0}+\binom{n}{n}, \binom{n}{1}, \ldots, \binom{n}{n-1}$ tenemos n sumandos. Finalmente, basta notar que $\binom{2n}{\lfloor n/2\rfloor}$ es el máximo valor en la lista (esto se puede comprobar analizando el triángulo de Pascal-Tartaglia). $\square$

Demostración(Erdős-Ramanujan): En primer lugar, nótese que el coeficiente binomial $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ incluye al primo p exactamente

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right).$$

Nótese que cada sumando es ≤ 1 pues es entero y

$$\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2.$$

Además, cada sumando es cero cuando $p^k > 2n$, de modo que tenemos

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \leq \text{máx}\{r : p^r \leq 2n\}, \tag{3.6}$$

en consecuencia, los primos $p > \sqrt{2n}$ aparecen a lo más una vez.

Además, para todo primo p entre $\frac{2}{3}n < p \leq n$ tenemos que $p \nmid \binom{2n}{n}$: en efecto, como $3p > 2n$ entonces los múltiplos de p menores que $2n$ son p y $2p$, ambos de los cuales aparecen en el denominador de $\binom{2n}{n}$. Empleando toda esta información podemos sacar la siguiente cota:

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p.$$

El primer producto no tiene más de $\sqrt{2n}$ términos y, denotando $P(n) := \sum_{n<p\leq 2n} 1$, tenemos:

$$\frac{4^n}{2n} < (2n)^{\sqrt{2n}} \cdot 4^{2/3n} \cdot (2n)^{P(n)} \iff 4^{n/3} < (2n)^{\sqrt{2n}+1+P(n)}.$$

Aplicando $\log_2$ a ambos lados tenemos:

$$P(n) > \frac{2n}{3\log_2(2n)} - (\sqrt{2n}+1).$$

Basta ver que la función de la derecha es positiva para un n suficientemente grande. Así

$$\frac{2n}{3\log_2(2n)} > \sqrt{2n}+1 \iff (\sqrt{2n}-1)(\sqrt{2n}+1) = 2n-1 > 3\log_2(2n)(\sqrt{2n}+1)-1,$$

por lo que basta probar que $3\log_2(2n) < \sqrt{2n} - 1$. Para $n = 2^9$ tenemos $3\log_2(2n) = 30 < 31 = \sqrt{2n} - 1$ y la función $\sqrt{2n} - 1 - 3\log_2(2n)$ es creciente (en un intervalo apropiado) pues su derivada es

$$(\sqrt{x} - 1 - 3\log_2(x))' = \frac{1}{2\sqrt{x}} - \frac{3}{x\log 2},$$

y $6\sqrt{x} < x\log 2$ para $x > (6/\log 2)^2 \approx 75$.

Así pues, vemos que el postulado de Bertrand vale para $n \geq 2^9 = 512$ y para $n < 512$ también por la siguiente lista de primos:

$$3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631. \qquad \square$$

Un problema abierto, con el mismo espíritu del postulado de Bertrand pero severamente más estricto es el siguiente:

Conjetura 3.57: Para todo $n \geq 1$ existe un primo entre n^2 y $(n+1)^2$.

El lector podrá notar que a medida que n es grande, el postulado de Bertrand se puede traducir en que hay un primo a menos de n unidades; y la conjetura anterior a que hay uno a menos de $2\sqrt{n}+1$ unidades. En teoría de números hay matemáticos trabajando en un problema relativamente opuesto: ¿qué tan frecuentemente se dan primos a distancias cortas? En su forma más extrema está la siguiente conjetura:

Conjetura de los primos gemelos 3.58: Hay infinitos pares de primos de la forma $\{p, p+2\}$.

Finalmente incluimos el siguiente resultado vinculado al postulado de Bertrand. Si pensamos los números en base 2, entonces el postulado de Bertrand se traduce en que existe un primo entre $(d_m d_{m-1} \dots d_1)_2$ y $(d_m \dots d_1 0)_2$; más en particular, si elegimos $d_m = 1$ y $d_j = 0$ para $j \neq m$, esto corresponde a encontrar un primo con m dígitos en base 2. Así pues, llegamos al siguiente problema:

Teorema 3.59: Sea k un cuerpo finito. Para todo natural $n \geq 1$ existe un polinomio $f(x) \in k[x]$ irreducible (equivalentemente primo) de grado n.

Demostración: Sea $q := |k|$ la cardinalidad del cuerpo. Para todo n, denotamos por $F_n(x)$ al producto de todos los polinomios mónicos de grado n en $k[x]$. Nótese que hay q^n polinomios mónicos de grado n, de modo que $\deg(F_n) = nq^n$. Si $g(x)$ es mónico de grado $n-1$, entonces $(x-a)g(x)$ con $a \in k$ corresponden a q polinomios de grado n, por lo que, $F_{n-1}(x)^q \mid F_n(x)$ y así sea $Q_n(x) := F_n(x)/F_{n-1}(x)^q$.

Sea $p(x)$ un polinomio mónico irreducible de grado d, y considere el máximo r tal que $p^r \mid F_n$, lo que equivale al número de polinomios mónicos de grado n divisibles por p, más el número de polinomios mónicos de grado n divisibles por p^2, más los divisibles por p^3 y así. La cantidad de polinomios mónicos de grado n divisbles por p^e es q^{n-de} si $n-de \geq 0$ y 0 de lo contrario; en forma cerrada queda $\lfloor q^{n-de} \rfloor$. En resumen:

$$r = \sum_{e=1}^{\infty} \lfloor q^{n-de} \rfloor.$$

Aplicando ésta fórmula, podemos ver que la potencia de $p(x)$ que divide a

$Q_n(x)$ es exactamente:

$$\sum_{e=1}^{\infty}(\lfloor q^{n-de}\rfloor - q\lfloor q^{n-1-de}\rfloor).$$

Si $de \leq n-1$ o si $de \geq n+1$, entonces $\lfloor q^{n-de}\rfloor - q\lfloor q^{n-1-de}\rfloor = 0$. Si $de = n$, o equivalentemente si $d \mid n$, entonces $\lfloor q^{n-de}\rfloor - q\lfloor q^{n-1-de}\rfloor = 1$; por lo tanto

$$\frac{F_n(x)}{F_{n-1}(x)^q} = Q_n(x) = \prod_{\deg P \mid n} P,$$

donde el producto recorre polinomios mónicos irreducibles.

Ahora bien, si $n = 1$, entonces claramente x es un ejemplo de un polinomio irreducible de grado n. Si $n \geq 2$, entonces $\deg(Q_n) = nq^n - q((n-1)q^{n-1}) = q^n$. Sea $\pi(n,k)$ la cantidad de polinomios irreducibles mónicos de grado n, entonces lo anterior nos da que

$$\sum_{d\mid n} d\pi(d,k) = q^n. \tag{3.7}$$

Si $\pi(n,k) = 0$, entonces podemos hacer la suma sobre el resto de divisores de n los cuales son $\leq \lfloor n/2\rfloor$:

$$\begin{aligned} q^n &\leq \sum_{1\leq q\leq \lfloor n/2\rfloor} d\pi(d,k) \leq \lfloor n/2\rfloor \sum_{1\leq q\leq \lfloor n/2\rfloor} q^d = \lfloor n/2\rfloor \cdot \frac{q^{\lfloor n/2\rfloor+1}-q}{q-1} \\ &< \lfloor n/2\rfloor \cdot \frac{q}{q-1} q^{\lfloor n/2\rfloor} \leq 2\lfloor n/2\rfloor q^{\lfloor n/2\rfloor}, \end{aligned}$$

pero esto es imposible puesto que $q^n \geq q^{\lfloor n/2\rfloor}2^{\lfloor n/2\rfloor} \geq 2\lfloor n/2\rfloor q^{\lfloor n/2\rfloor}$ para todo $\lfloor n/2\rfloor \geq 1$ (vale decir, todo $n \geq 2$). □

Esta última demostración es original de Soundararajan **[106].** La identidad (3.7) en la demostración se conoce como *relación de Gauss.*

§3.3.2 El teorema de Sylvester-Schur. Con un poco más de trabajo y estudio de los coeficientes binomiales, uno puede mejorar el postulado de Bertrand.

Lema 3.60: Supongamos que, para $n \geq j \geq 1$, tenemos

$$\binom{n+j}{j} > (n+j)^{\pi(j)}. \tag{3.8}$$

Entonces alguno de los enteros $n+1, n+2, \ldots, n+j$ es divisible por un primo $p > j$. Además, si se satisface (3.8) para $n = n_1(j)$, entonces se satisface para todo $n \geq n_1(j)$.

Demostración: Si, por contradicción, todos los factores primos de $n+1, \ldots, n+j$ son $\leq j$, entonces todos los factores primos de $\binom{n+j}{j}$ son $\leq j$ y, por (3.6), vemos que si $p^r \mid \binom{n+j}{j}$ y $p^{r+1} \nmid \binom{n+j}{j}$, entonces

$$\binom{n+j}{j} \leq \prod_{p \leq j} (n+j) = (n+j)^{\pi(j)},$$

lo que contradice el enunciado.

Por inducción, podemos probar que

$$\forall x \geq j \geq 1 \qquad \left(1 + \frac{1}{x+j}\right)^j \leq 1 + \frac{j}{x+j}.$$

Así, probaremos que (3.8) para $n \geq n_1(j)$ por inducción:

$$\begin{aligned}\binom{n+1+j}{j} &= \left(1 + \frac{j}{n+1}\right)\binom{n+j}{j} > \left(1 + \frac{1}{n+j}\right)^j (n+j)^{\pi(j)} \\ &> (n+1+j)^{\pi(j)},\end{aligned}$$

que es lo que se quería probar. □

Teorema 3.61 (Sylvester-Schur): Dados enteros $n \geq j \geq 1$. Al menos uno de los enteros $n+1, n+2, \ldots, n+j$ es divisible por un primo $p > j$.

Nótese que con $n = j$ se obtiene el postulado de Bertrand usual.

Demostración: Por el lema anterior, basta demostrar que $n_1(j) = j$ en (3.8), lo cual es cierto para $202 \leq j \leq 1500$. También es fácil comprobar que $j \leq n_1(j) \leq j + 17$ para $j \leq 201$; por lo que comprobamos mediante un ordenador que el enunciado es cierto con $j \leq 201$ y $j \leq n \leq j + 17$.

Para $j > 1500$ supongamos que (3.8) no se cumple para $n_1(j) = j$. Ahora, es fácil comprobar que $\pi(j) < j/3$ por inducción desde un j suficientemente grande y $\frac{n+j-i}{j-i} > \frac{n+j}{j}$ para $0 \leq i < j$, de modo que $\binom{n+j}{j} \geq \left(\frac{n+j}{j}\right)^j$, con lo que concluimos que

$$\left(\frac{n+j}{j}\right)^j \leq \binom{n+j}{j} \leq (n+j)^{\pi(j)} < (n+j)^{j/3},$$

cancelando el exponente j y reordenando obtenemos que

$$n + j \leq j^{3/2} \iff n \leq j^{3/2} - j.$$

Ahora bien, si $p > \sqrt{n+j}$ y $p^r \mid \binom{n+j}{j}$ (de modo que, $p^r \leq n + j$), entonces $r \in \{0, 1\}$. Así que

$$\binom{n+j}{j} \leq \prod_{p \leq \sqrt{n+j}} (n+j) \prod_{p \leq j} p \leq j^{\frac{1}{3} j^{3/4}} 4^{j-1},$$

donde empleamos que $\pi(\sqrt{n+j}) \leq \frac{1}{3}(n+j)^{1/2} \leq \frac{1}{3} j^{3/4}$ y el teorema 3.55.

Por ello, de darse $n_1(j) \geq 3j$, entonces

Justificar Granville **[84,** Ex. 4.14.1].

$$\frac{(4^4/3^3)^j}{ej} \leq \binom{4j}{j} \leq \binom{n+j}{j} \leq j^{\frac{1}{3} j^{3/4}} 4^{j-1},$$

lo cual es falso para todo $j \geq 1$. Por ello, $n_1(j) + j \leq 4j$. Si $n_1(j) + j > \frac{5}{2} j$, entonces

$$\frac{(5^5/3^3 2^2)^{j/2}}{ej} \leq \binom{5j/2}{j} \leq \binom{n+j}{j} \leq (4j)^{j^{1/2}} 4^{j-1},$$

lo cual es absurdo para $j \geq 780$ (convierta lado derecho menos izquierdo en una función, estudie derivadas y haga el cálculo).

□

§3.3.3 Cotas de Chebyshev.

Definición 3.62: Sean

$$H(x) := \sum_{1 \leq n \leq x} \frac{1}{n},$$

los ***números harmónicos***.

Ya sabemos que $H(x) = \log x + \gamma + O(1/x)$ y, por tanto, $H(x) \sim \log x$.

Lema 3.63: Para todo entero $m > 0$ se tiene que $\frac{m}{2} \leq H(2^m) \leq m$.

Pista: Esto es parte de la demostración usual de que la serie harmónica diverge (cfr. **[2],** ej. 1.54). □

Lema 3.64: Para todo entero $m > 0$ se tiene que $\pi(2^{m+1}) \leq 2^m$.

Demostración: Para $x \geq 3$ entonces $\pi(x) - 1 \leq \frac{x-2}{2}$ porque en el conjunto $\{3, 4, \ldots, \lfloor x \rfloor\}$ la mitad de números son pares. Para el resto funciona por inspección. □

Teorema 3.65: $\dfrac{1}{8} \leq \dfrac{\pi(x)}{x/H(x)} \leq 6.$

Demostración: Nos ponemos en contexto de la demostración de Erdős-Ramanujan del postulado de Bertrand.

Nótese que, por (3.6), tenemos:

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} \leq \binom{2n}{n} \leq \prod_{p^r \leq 2n < p^{r+1}} p^r \leq (2n)^{\pi(2n)}$$

Además, podemos sacar la siguiente cota:

$$\begin{aligned}\binom{2n}{n} &= \frac{2n(2n-1)(2n-2)\cdots(n+1)}{n(n-1)(n-2)\cdots 1} \\ &= 2 \cdot \left(2 + \frac{1}{n-1}\right)\left(2 + \frac{2}{n-2}\right)\cdots\left(2 + \frac{n-1}{1}\right) \geq 2^n.\end{aligned}$$

Así, empleando que $\binom{2n}{n} \leq 4^n$ obtenemos que

$$n^{\pi(2n)-\pi(n)} < 2^{2n}, \qquad 2^n \leq (2n)^{\pi(2n)}, \qquad n \geq 1.$$

Reemplazando $n = 2^j$ obtenemos que

$$2^{j(\pi(2^{j+1})-\pi(2^j))} < 2^{2^{j+1}}, \qquad 2^{2^j} \leq 2^{(j+1)\pi(2^{j+1})}, \tag{3.9}$$

o equivalentemente

$$j(\pi(2^{j+1}) - \pi(2^j)) < 2^{j+1}, \qquad 2^j \leq (j+1)\pi(2^{j+1}),$$

sumando $\pi(2^{j+1})$ a ambos lados y aplicando el lema anterior tenemos que

$$(j+1)\pi(2^{j+1}) - j\pi(2^j) < 2^{j+1} + \pi(2^{j+1}) \leq 3 \cdot 2^j.$$

Realizando la suma telescópica con $j = 0$ hasta j:

$$(j+1)\pi(2^{j+1}) < 3(2^0 + 2^1 + \cdots + 2^j) < 3 \cdot 2^{j+1}.$$

Juntando esto con (3.9), entonces tenemos

$$\frac{1}{2}\frac{2^{j+1}}{j+1}\pi(2^{j+1}) < 3\cdot\frac{2^{j+1}}{j+1}.$$

Sea $x \geq 2$ y elijamos j tal que $2^{j+1} \leq x < 2^{j+2}$, finalmente

$$\pi(x) \leq \pi(2^{j+2}) < 3\cdot\frac{2^{j+2}}{j+2} \leq 6\cdot\frac{2^{j+1}}{H(2^{j+2})} \leq 6\cdot\frac{x}{H(x)}$$

y por otro lado

$$\pi(x) \geq \pi(2^{j+1}) \geq \frac{1}{2}\frac{2^{j+1}}{j+1} \geq \frac{1}{8}\frac{2^{j+2}}{\frac{1}{2}(j+2)} \geq \frac{1}{8}\frac{x}{H(x)}. \qquad \square$$

Teorema 3.66: $\dfrac{1}{8} \leq \dfrac{\pi(x)}{x/\log x} \leq 6, \qquad n \geq 2.$

Demostración: Basta aproximar

$$\log\left(\frac{n}{2}\right) = \int_2^n \frac{1}{t}\,\mathrm{d}t \leq \frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n} = H(n)-1 < \int_1^n \frac{1}{t}\,\mathrm{d}t = \log t,$$

y notar que para $n \geq 4$ se tiene $\frac{1}{2}\log n \leq \log(n/2)$. $\square$

3.4 El teorema de Dirichlet

El teorema de Dirichlet demuestra una versión mucho más fuerte de la infinitud de primos, formalmente demuestra que si $(m;k) = 1$ [son coprimos], entonces hay infinitos primos de la forma $mn+k$.

Definición 3.67: Los elementos formales de $\mathbb{Z}/n\mathbb{Z}$, es decir, las clases de equivalencia $[a]_n := \{b : n \mid b-a\}$, se le llaman *clases de residuos módulo* n.

Las clases cuyo resto es coprimo, son las clases de $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$.

Los naturales se reparten entre las clases de residuos módulo n, sin embargo, la clase $[a]_n$ cuando a, n no son coprimos, sólo puede tener como máximo un número primo: en efecto, al no ser coprimos sea $m := (a;n)$, luego $m \mid nk+a$. Aún así, puede darse que $a = p$ primo y $p \mid n\cdot 0+p = p$, sin embargo, si $k > 1$, entonces m es un divisor propio y el término no es primo. El teorema de Dirichlet pues se enunciaría así: una clase de residuos módulo n que no esté en U_n tiene a lo más un primo y las de U_n tienen infinitos.

Un ejemplo para visualizar ésto reside en el siguiente gráfico de puntos de la forma $n \mapsto (n \cos n, n \sin n)$ (ver fig. 3.5), donde las clases de equivalencia módulo 6 están marcadas. En rojo son las clases de resto no coprimo, en azul los que sí. Los puntos en azúl son números primos.[2]

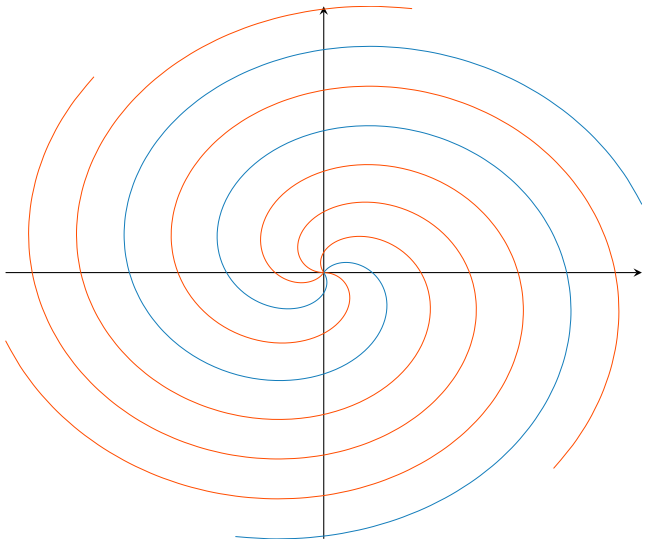


Figura 3.5

Antes de empezar con la demostración, cabe observar un hecho notable:

Teorema 3.68: Las expresiones siguientes son equivalentes:

1. **Teorema de Dirichlet:** Para todo a, n coprimos, existen infinitos números primos p tales que $p \equiv a \mod n$.
2. Para todo a, n coprimos, existe *al menos un* número primo p tal que $p \equiv a \mod n$.

Ojo, el uso de cuantificadores puede ser engañoso: el teorema no dice que saber que existe $p \equiv 4 \pmod 5$ (en este caso $p = 19$) implica la infinitud de los primos en $[4]_5$; sino que hay que saberlo para todo par a, n coprimos.

Demostración: Es claro que $1 \implies 2$, veamos el recíproco: Sean a, m coprimos, de modo que $m > 1$ y podemos exigir que $0 < a \leq m$. Por

[2] La idea fue original de un video expositorio de 3Blue1Brown: `https://www.youtube.com/watch?v=EK32jo7i5LQ`.

hipótesis se tiene que existe un primo p tal que $p \equiv a \pmod{m}$. Luego, sean $p_1, \ldots, p_r$ primos tales que $p \equiv a \pmod{m}$ y elijamos un natural k de modo que $m^k > p_1 \cdots p_r$. Nótese que

$$0 < a < a + m^k \leq m + m^k = m(1 + m^{k-1}) \leq m^{k+1},$$

donde empleamos que $1 + x \leq mx$ syss $\frac{1}{m-1} < 1 \leq x$. Es fácil notar que $(a + m^k; m^{k+1}) = 1$, de modo que existe un primo p que satisface $p \equiv a + m^k \pmod{m^{k+1}}$. Finalmente, $p \geq a + m^k > p_j$ para todo j, de modo que es un nuevo primo en nuestra lista. □

Primero vamos a tener que definir las siguientes funciones:

Definición 3.69 – *Carácter de Dirichlet*: Dado un natural $m > 1$, se dice que una función $\chi \colon \mathbb{Z} \to \mathbb{C}$ es un *carácter de Dirichlet módulo* m si no es idénticamente nula y satisface lo siguiente:

i) Si $a \equiv b \pmod{m}$, entonces $\chi(a) = \chi(b)$.

ii) Si a, m no son coprimos, entonces $\chi(a) = 0$.

iii) $\chi(ab) = \chi(a)\chi(b)$.

Traduciendo las propiedades: la primera dice que un carácter módulo m está bien definido sobre $\mathbb{Z}_m$, la segunda que se anula fuera de U_m y la tercera es que las funciones son completamente multiplicativas y, por ende, un morfismo de grupos (multiplicativo).

Un ejemplo trivial es el siguiente:

Definición 3.70: Se le llama carácter *principal* de Dirichlet módulo m a aquella tal que $\chi(c) = 1$ si $c \in U_m$ y $\chi(c) = 0$ si $c \notin U_m$.

Proposición 3.71: Sea $\chi \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ un carácter de Dirichlet:

1. χ está completamente determinado por su valor en U_m.
2. $\chi(1) = 1$.
3. $\chi|_{U_m} \colon U_m \to \mathbb{C}_{\neq 0}$ es un morfismo (multiplicativo) de grupos. En consecuente, $\chi(c) \neq 0$ para todo $c \in U_m$ y $\chi(c^k) = \chi(c)^k$ para todo $k \in \mathbb{Z}$.
4. Para todo $c \in U_m$ se cumple que $\chi(c)$ es una $\phi(m)$-ésima raíz de la unidad.

5. Los caracteres de Dirichlet módulo m forman un grupo con el producto puntual.

Demostración: La primera se deduce de la propiedad (ii). La segunda del hecho de que χ es completamente multiplicativa. La tercera sale del hecho de que $\chi(c)\chi(c^{-1}) = \chi(1) = 1$, luego $\chi(c)$ es no nula y por ser completamente multiplicativa se deduce que es morfismo de grupos.

La cuarta es consecuencia del teorema de Euler-Fermat puesto que $c^{\phi(m)} \equiv 1$, luego $\chi(c^{\phi(m)}) = \chi(c)^{\phi(m)} = 1$.

Para la quinta basta comprobar que se cumplen los axiomas de grupo. La asociatividad y conmutatividad son heredados del producto complejo. Sea χ_0 el carácter principal, es claro que éste juega el rol del neutro. Sólo basta notar que si $\chi\colon U_m \to \mathbb{C}$ es un carácter de Dirichlet, entonces χ' dado por $\chi'(a) = \chi(a)^{-1}$ (puesto que el dominio es U_m) es también un carácter de Dirichlet y es de hecho su inversa. □

La quinta propiedad es ya por sí sola curiosa, pero se puede refinar bastante:

Teorema 3.72: Para todo $m > 1$ se cumple que el grupo de los caracteres de Dirichlet módulo m es isomorfo a U_m. En consecuencia hay exactamente $\phi(m)$ caracteres de Dirichlet módulo m.

Demostración: La demostración será por casos:

a) $\underline{m = p^n}$: Por el teorema 2.28 se cumple que U_m está generado por un solo elemento, digamos a. Sea ζ la $\phi(m)$-ésima raíz de la unidad, es decir, tal que $\operatorname{ord}\zeta = \phi(m)$ en el grupo $\mathbb{C}^\times$. Y sea χ la función determinada por $\chi(a^j) = \zeta^j$. Luego la aplicación $a^j \mapsto \chi^j$ es de hecho un isomorfismo de grupos.

b) <u>En otro caso:</u> Entonces $m = p_n^{\alpha_1} \cdots p_n^{\alpha_n}$ y basta aplicar el teorema chino del resto. □

Teorema 3.73: Sea $m \geq 2$. Entonces:

1. Para todo carácter χ de Dirichlet módulo m se cumple:

$$\sum_{k=1}^{m} \chi(k) = \begin{cases} \phi(m), & \chi \text{ es principal} \\ 0, & \chi \text{ no es principal} \end{cases}$$

2. Si k es un entero fijo, entonces:

$$\sum_{\chi} \chi(k) = \begin{cases} \phi(m), & k \equiv 1 \pmod{k} \\ 0, & k \not\equiv 1 \pmod{k} \end{cases}$$

donde χ recorre todos los caracteres de Dirichlet módulo m.

Demostración:

1. Claramente si χ es principal se cumple la relación, puesto que $\chi(c) = 1$ para $c \in U_m$ y hay $\phi(m)$ elementos en U_m.

   Si χ no es principal, entonces elijamos $\bar{k}_0$ tal que $\chi(\bar{k}_0) \neq 1$. Como U_m es un grupo, se cumple que $x \mapsto \bar{k}_0 \cdot x$ es una permutación, luego

$$\sum_{k=1}^{m} \chi(k) = \sum_{k=1}^{m} \chi(k_0 k) = \chi(k_0) \sum_{k=1}^{m} \chi(k).$$

   Por lo que

$$(1 - \chi(k_0)) \sum_{k=1}^{m} \chi(k) = 0$$

   donde el primer término es no nulo.

2. Es trivial si $k \equiv 1 \pmod{m}$ o si $(k; m) \neq 1$. Para el caso restante sean $\chi_1, \ldots, \chi_n$ todos los caracteres de Dirichlet, entonces veamos que si $\psi(k)$ es el valor de algún $\chi_i(k) \neq 1$, entonces $\psi(k)\chi_1(k), \ldots, \psi(k)\chi_n(k)$ es una mera permutación de los valores originales. Ésto se cumple dado que $\chi \mapsto \chi \cdot \chi_j$ es una permutación en el grupo de caracteres de Dirichlet módulo m. Luego

$$\sum_{\chi} \chi(k) = \sum_{\chi} \psi(k)\chi(k) = \psi(k) \sum_{\chi} \chi(k)$$

   y procediendo igual que antes se concluye el teorema. □

Teorema 3.74: Sea $C \in U_m$, entonces para todo $k \in \mathbb{Z}$ se cumple que

$$\frac{1}{\phi(m)} \sum_{\chi} \overline{\chi}(C)\chi(k) = \begin{cases} 1, & k \in C \\ 0, & k \notin C \end{cases}$$

Demostración: Nótese que $\overline{\chi}(C) = \chi(C)^{-1}$ y luego basta aplicar el teorema anterior, ya que si $k \in C$, entonces $C^{-1}\overline{k} = \overline{1}$ y la suma vale $\phi(m)$; y en otro caso vale 0. □

Estamos ya a punto de ver el teorema de Dirichlet, pero aún son necesarias algunas herramientas adicionales. Para ello, primero veamos el siguiente teorema:

Teorema 3.75: Sea $f\colon (0,\infty) \to \mathbb{R}$ una función decreciente tal que $\lim_{x\to\infty} f(x) = 0$, y sea χ un carácter de Dirichlet módulo $m > 1$ no principal. Entonces, la serie $\sum_{n=1}^{\infty} \chi(n)f(n)$ converge y

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)).$$

Demostración: Sea $A(x) := \sum_{n\leq x} \chi(n)$. Nótese que $\chi(n)$ es m-periódica y que por el teorema 3.73 se cumple que $A(m) = 0$. Luego $|A(x)| \leq K$ para algún K.

Por fórmula de suma por partes se tiene que

$$\begin{aligned}\sum_{x<n\leq y} \chi(n)f(n) &= \sum_{n=\lfloor x\rfloor+1}^{\lfloor y\rfloor} \chi(n)f(n) \\ &= A(\lfloor y\rfloor)f(\lfloor y\rfloor) - A(\lfloor x\rfloor)f(\lfloor x\rfloor) + \sum_{n=\lfloor x\rfloor+1}^{\lfloor y\rfloor-1} A(n)\big(f(n) - f(n+1)\big).\end{aligned}$$

Luego nótese que

$$\begin{aligned}\left|\sum_{n=\lfloor x\rfloor+1}^{\lfloor y\rfloor-1} A(n)\big(f(n) - f(n+1)\big)\right| &\leq K \sum_{n=\lfloor x\rfloor+1}^{\lfloor y\rfloor-1} \big(f(n) - f(n+1)\big) \\ &= K\big(f(\lfloor x\rfloor+1) - f(\lfloor y\rfloor-1)\big) \leq Kf(\lfloor x\rfloor+1).\end{aligned}$$

De modo que

$$\sum_{x<n\leq y} \chi(n)f(n) \leq Kf(\lfloor x\rfloor+1) \leq Kf(x) = O(f(x))$$

por lo que, la sumatoria converge y

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) - \sum_{n>x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x))$$

□

El teorema anterior nos permite definir las dos siguientes funciones para un carácter de Dirichlet χ no principal:

$$L_0(\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \quad L_1(\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}.$$

Ahora estamos listos para ver el teorema, el cuál saldrá como una consecuencia de una versión de los teoremas de Mertens para progresiones aritméticas.

Teorema 3.76: Para todo $m > 1$ y todo $C \in U_m$ se cumple que

$$\sum_{\substack{p \leq x \\ p \in C}} \frac{\log p}{p} = \frac{1}{\phi(m)} \log x + O(1).$$

Demostración: Primero nótese que, al igual que con el primer teorema de Mertens, primero introducimos la función de von Mangoldt:

$$\sum_{\substack{n \leq x \\ n \in C}} \frac{\Lambda(n)}{n} = \sum_{\substack{p \leq x \\ p \in C}} \frac{\log p}{p} + \sum_{\substack{p^{k+1} \leq x \\ p^{k+1} \in C}} \frac{\log p}{p^{k+1}}$$

y se nota que

$$0 \leq \sum_{\substack{p^{k+1} \leq x \\ p^{k+1} \in C}} \frac{\log p}{p^{k+1}} \leq \sum_{n=1}^{\infty} \frac{\log n}{n^2}$$

donde el último término converge, por lo que basta probar el enunciado para $\Lambda(n)/n$.

Nótese que por el teorema 3.74 se tiene que

$$\begin{aligned} \sum_{\substack{n \leq x \\ n \in C}} \frac{\Lambda(n)}{n} &= \frac{1}{\phi(m)} \sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \overline{\chi}(C)\chi(n) \\ &= \frac{1}{\phi(m)} \sum_{\chi} \overline{\chi}(C) \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} \end{aligned}$$

Separemos la última suma entre el carácter principal y los no principales y notemos que si χ es no principal entonces

$$\left| \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} \right| \leq \left| \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} \right| = |L_1(\chi)|.$$

Luego el problema se reduce a estudiar el caso de χ_0:

$$\sum_{n\leq x}\frac{\chi_0(n)\Lambda(n)}{n}=\sum_{\substack{n\leq x\\(n;m)=1}}\frac{\Lambda(n)}{n}=\sum_{n\leq x}\frac{\Lambda(n)}{n}-\sum_{\substack{p^k\leq x\\p|m}}\frac{\log p}{p^k}.$$

Pero

$$\sum_{\substack{p^k\leq x\\p|m}}\frac{\log p}{p^k}\leq\sum_{p|m}\sum_{k=1}^{\infty}\frac{\log p}{p^k}=\sum_{p|m}\frac{\log p}{p(p-1)},$$

que por ser suma finita de términos es también finita y acotada. Finalmente basta recordar la variación del primer teorema de Mertens (3.5):

$$\sum_{n\leq x}\frac{\Lambda(n)}{n}=\log x+O(1).$$ □

Teorema 3.77 – *Teorema de Dirichlet*: Para todo $m>1$ y todo $C\in U_m$, existen infinitos primos en C.

Y el complementario:

Teorema 3.78: Para todo $m>1$ y todo $C\in U_m$ se cumple que

$$\sum_{\substack{p\leq x\\p\in C}}\frac{1}{p}=\frac{1}{\phi(m)}\log\log x+M_C+O\left(\frac{1}{\log x}\right),$$

donde M_C es una constante que depende de C.

Demostración: Definamos

$$a(n):=\begin{cases}1, & n \text{ primo en } C\\ 0, & \text{otro caso}\end{cases}\qquad A(x):=\sum_{n\leq x}a(n)\frac{\log n}{n}=\frac{1}{\phi(m)}\log x+R(x)$$

donde $|R(x)|\leq K$. Con $f(t):=1/\log t$ por fórmula de Abel se cumple que

$$\sum_{\substack{p\leq x\\p\in C}}\frac{1}{p}=\frac{A(x)}{\log x}+\int_2^x\frac{A(t)}{t\log^2 t}\,\mathrm{d}t$$

Luego basta seguir al pie de la letra la demostración del segundo teorema de Mertens para llegar a la conclusión del enunciado. □

Referencias

79. De Souza, A. N. *Where do odd perfect numbers live?* 2018. arXiv: 1801.06182 [math.NT].

84. Granville, A. *Number Theory Revealed. A Masterclass* (American Mathematical Society, 2020).

85. Hlawka, E., Schoissengeier, J. y Taschner, R. *Geometric and Analytic Number Theory* (Springer-Verlag, 1991).

106. Soundararajan, K. *Bertrand's postulate and the existence of finite fields* 2020. arXiv: 2007.01389 [math.NT].

Otros recursos.

1. Cuevas, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).

2. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

3. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).

4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

5. Wilson, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. Brieskorn, E. y Knorrer, H. *Plane Algebraic Curves* trad. por Stillwell, J. (Birkhäuser Verlag, 1981).

7. Dickson, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

8. Newton, I. *The Correspondence of Isaac Newton* (ed. Turnbull, H. W.) (Cambridge University Press, 1960).

9. Roquette, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

10. Williams, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. Bennett, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. Alford, W. R., Granville, A. y Pomerance, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).

12. APÉRY, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. BARNES, E. S. y SWINNERTON-DYER, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. BEUKERS, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).
15. BOMBIERI, E. y VAALER, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).
16. CASSELS, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).
17. CATALAN, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).
18. CHAO, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).
19. CHATLAND, H. y DAVENPORT, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).
20. CLARK, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).
21. De BESSY, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
22. DEDEKIND, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).
23. DICKSON, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).
24. DIRICHLET, G. L. en *G. Lejeune Dirichlet's Werke* (ed. KRONECKER, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.
25. EULER, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).
26. EULER, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).
27. EULER, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).
28. GAUSS, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.

29. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

30. Hensel, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).

31. Hensel, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. Hyyrö, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. Inkeri, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. Inkeri, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. Kausler, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. Keller, W. y Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. Kürschák, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. Lang, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. Legendre, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. Lehmer, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. Mahler, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. Mignotte, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. Minkowski, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. Motzkin, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. Nagell, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. Northcott, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. Ochem, P. y Rao, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. OSTROWSKI, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. OSTROWSKI, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. OSTROWSKI, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. OSTROWSKI, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. OSTROWSKI, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. PERRON, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. RÉDEI, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. RELLA, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. REMAK, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. ROTH, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. RYCHLÍK, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. RYCHLÍK, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. SIEGEL, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. TATE, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. CASSELS, J. W. S. y FRÖHLICH, A.) (Academic Press, 1967), 305-347.

63. VERGER-GAUGRY, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

4

Enteros algebraicos

Es natural que de tratarse de la teoría *algebraica* de números sean necesarios una serie de resultados algebraicos. Varias referencias se dedican a probar éstos resultados de manera previa a la parte exclusivamente numérica, pero yo en cambio opto por citar los preliminares desde mi libro de álgebra [**1**]**;** principalmente del capítulo 4 de extensiones de cuerpo, del capítulo 6 de álgebra conmutativa y del capítulo 10 de teoría de la valuación.

4.1* Preliminares del álgebra

Módulos noetherianos.

Proposición 4.1: Sea A un dominio, M un A-módulo y $N \leq M$ un submódulo. Entonces M es noetheriano syss N y M/N lo son. (Cf. [**1,** Teo. 6.61])

Corolario 4.1.1: La suma directa de A-módulos noetherianos es también un A-módulo noetheriano. (Cf. [**1,** Cor. 6.62])

Corolario 4.1.2: Sea A un dominio noetheriano, entonces todo A-módulo finitamente generado es también noetheriano. (Cf. [**1,** Prop. 6.66])

Norma y traza.

Definición 4.2: Sea K/k una extensión finita de cuerpos. Sea N la clausura normal[1] de K y $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, N)$ (los k-monomorfismos de K en N). Para todo $\alpha \in K$ se definen su *traza* y su *norma* como

$$\mathrm{Tr}_{K/k}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Nm}_{K/k}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha).$$

En el texto original definimos la traza y la norma de otra manera, pero probamos que ambas definiciones coinciden **[1,** Teo. 4.59**]**.

El uso de los monomorfismos es fundamental: los $\sigma_i(\alpha)$ son los k-conjugados de α contando multiplicidad.

Las propiedades básicas son las siguientes:

Proposición 4.3: Sea K/k una extensión finita de cuerpos. Para todo $\alpha, \beta \in K$ se cumplen:

1. $\mathrm{Tr}_{K/k}(\alpha + \beta) = \mathrm{Tr}_{K/k}(\alpha) + \mathrm{Tr}_{K/k}(\beta)$.
2. $\mathrm{Nm}_{K/k}(\alpha \cdot \beta) = \mathrm{Nm}_{K/k}(\alpha) \cdot \mathrm{Nm}_{K/k}(\beta)$. (Cf. **[1,** Prop. 4.58**]**)
3. $\mathrm{Tr}_{K/k}(\alpha), \mathrm{Nm}_{K/k}(\alpha) \in k$.[2]
4. Si L/K es una extensión finita de cuerpos, entonces

$$\mathrm{Tr}_{L/k} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{K/k}, \qquad \mathrm{Nm}_{L/k} = \mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{K/k}\,.$$

(Cf. **[1,** Teo. 4.60**]**)

Extensiones íntegramente cerradas.

Lema 4.4: Sea B una A-álgebra y $\alpha \in B$. Son equivalentes:

1. α es raíz de un polinomio mónico $p(x) \in A[x]$ no constante.
2. El subálgebra $A[\alpha]$ es un A-módulo finitamente generado.
3. $A[\alpha]$ está contenido en un subálgebra C que es un A-módulo finitamente generado.

[1] La mínima extensión N/K tal que N/k es normal. (Cf. **[1,** Def. 4.25-Prop. 4.26**]**)

[2] En **[1]** se sigue de la propia definición alternativa.

4. Existe un $A[\alpha]$-módulo fiel sobre que es un A-módulo finitamente generado.

(Cf. [**1,** Lema 10.15])

Definición 4.5: Sea B una A-álgebra. Un elemento $\alpha \in B$ se dice *entero* sobre A. B se dice una A-álgebra *entera* si todo elemento de B es entero.

Proposición 4.6: Sea B/A una extensión de anillos, y sea C el conjunto de elementos enteros de B. Entonces C/A es una extensión de anillos. (Cf. [**1,** Prop. 10.24])

Definición 4.7: El subanillo C construido en la proposición anterior se le dice la *clausura íntegra* de B. Si $C = A$, entonces se dice que A es *íntegramente cerrado* sobre B. En particular, decimos que un dominio íntegro A es *íntegramente cerrado* (a secas) si lo es sobre $\mathrm{Frac}(A)$.

Proposición 4.8: Sea A un dominio íntegro y un DFU, entonces A es íntegramente cerrado. (Cf. [**1,** Prop. 10.26])

Proposición 4.9: Sean B/A una extensión entera de dominios íntegros. Entonces A es un cuerpo syss B es un cuerpo. (Cf. [**1,** Prop. 10.28])

Proposición 4.10: Sea A un dominio íntegro, $k := \mathrm{Frac}\, A$ y sea K/k una extensión finita de cuerpos. Sea $\alpha \in K$ un elemento entero de K/A, y sea $\beta \in K$ un k-conjugado de α; entonces β es entero. En consecuencia, $\mathrm{Tr}_{K/k}(\alpha)$ y $\mathrm{Nm}_{K/k}(\alpha)$ son también enteros.

Demostración: Si α es entero, entonces es raíz de un polinomio $p(x) \in A[x]$ mónico. Como K/k es finita, entonces α es algebraico y es raíz de un polinomio minimal $q(x) \in k[x]$. Por definición de polinomio minimal se debe cumplir que $q(x) \mid p(x)$. Por definición de k-conjugado β es raíz de $q(x)$ y, por tanto, también es raíz de $p(x)$, de modo que efectivamente es entero. □

4.2 Enteros algebraicos y cuadráticos

Comenzaremos estudiando un famoso teorema de Lagrange que dice que un primo se puede escribir como suma de cuadrados syss es $\equiv 1 \pmod 4$. Una

implicancia es clara, pero la conversa requiere introducir un nuevo objeto que, entre otras cosas, ilustrará la clase de resultados y métodos que emplearemos a lo largo del libro.

En primer lugar, una definición fundamental:

Definición 4.11: Se dice que un cuerpo k es un ***cuerpo numérico***[a] si es una extensión finita de $\mathbb{Q}$. Un cuerpo k se dice ***cuadrático*** si es un cuerpo numérico de grado $[k:\mathbb{Q}] = 2$.

Dado un cuerpo numérico k se le llama su ***anillo de enteros***, denotado $\mathcal{O}_k$, a los elementos que sean enteros sobre $\mathbb{Z}$.

[a] Otros textos emplean *cuerpo de números algebraicos* o *cuerpo de números*.

Será útil recordar que todo cuerpo numérico se puede extender a uno normal y que los cuerpos cuadráticos ya son normales.

Veamos un par de propiedades generales de los anillos de enteros:

Proposición 4.12: Sea k un cuerpo numérico. Entonces:

1. Los conjugados de los enteros de k son también enteros.
2. Para todo $\alpha \in \mathcal{O}_k$ se cumple que $\mathrm{Tr}_{k/\mathbb{Q}}(\alpha), \mathrm{Nm}_{k/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.
3. Si $k/\mathbb{Q}$ es una extensión normal, entonces para $\alpha \in \mathcal{O}_k$ se cumple que α es invertible (en $\mathcal{O}_k$) syss $\mathrm{Nm}_{k/\mathbb{Q}}(\alpha) = \pm 1$.

Demostración:

1. Si $\alpha \in k$ es entero, entonces se anula en un polinomio $f(x) \in \mathbb{Z}[x]$ mónico, luego si $g(x)$ es el polinomio irreducible de α debe cumplirse que $g(x) \mid f(x)$ y por ello se cumple que si β es un conjugado de α entonces $f(\beta) = 0$.
2. Como $\mathcal{O}_k$ es cerrado bajo conjugación, entonces se concluye que $\mathrm{Tr}_{k/\mathbb{Q}}(\alpha), \mathrm{Nm}_{k/\mathbb{Q}}(\alpha)$ son enteros y además están en $\mathbb{Q}$, luego están en $\mathbb{Z}$ puesto que es íntegramente cerrado.
3. $\Longrightarrow$. Si α es invertible, entonces

$$1 = \mathrm{Nm}(1) = \mathrm{Nm}(\alpha \cdot \alpha^{-1}) = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\alpha^{-1}),$$

luego $\mathrm{Nm}(\alpha) \in \mathbb{Z}$ es invertible en $\mathbb{Z}$.

$\Longleftarrow$. Conversamente, si $\mathrm{Nm}(\alpha) = \pm 1$, entonces, por definición

$$\mathrm{Nm}(\alpha) = \alpha \cdot \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha) = \pm 1,$$

Donde σ recorre los $\mathbb{Q}$-monomorfismos de k en su clausura normal N. Luego $\beta := \mathrm{Nm}(\alpha) \cdot \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha)$ es claramente entero y satisface que $\alpha \cdot \beta = 1$. □

Por la fórmula cuadrática se puede deducir lo siguiente:

Proposición 4.13: Todo cuerpo numérico cuadrático es de la forma $\mathbb{Q}[\sqrt{d}]$, donde d es un entero libre de cuadrados.

Teorema 4.14: Sea $K = \mathbb{Q}(\sqrt{d})$, donde $d \in \mathbb{Z}$ está libre de cuadrados. Se satisface que $\mathcal{O}_K = \mathbb{Z}[\omega]$, donde

$$\omega = \begin{cases} \sqrt{d}, & d \not\equiv 1 \pmod 4 \\ \frac{1}{2}(1+\sqrt{d}), & d \equiv 1 \pmod 4 \end{cases}.$$

Demostración: Nótese que si $x \in K$ es entero, entonces como sus conjugados $\sigma(x)$ son raíces del mismo polinomio en $\mathbb{Q}[x]$, entonces también son enteros en K; i.e., $\sigma(x) \in A$. Por consiguiente, $x + \sigma(x), x \cdot \sigma(x) \in A$. Como $x = a + b\sqrt{d} \in K$ para algunos $a, b \in \mathbb{Q}$, se sigue que

$$x + \sigma(x) = 2a \in A, \qquad x \cdot \sigma(x) = a^2 - db^2 \in A, \tag{4.1}$$

luego deben ser elementos de $\mathbb{Z}$. Conversamente, si $2a, a^2 - db^2 \in \mathbb{Z}$, entonces x debe pertenecer a A, puesto que es raíz del polinomio mónico

$$t^2 - 2at + a^2 - db^2 \in \mathbb{Z}[t].$$

- Si $d \not\equiv 1 \pmod 4$: Si $2a \in \mathbb{Z}$, pero $a \notin \mathbb{Z}$, entonces $a = c/2$ con $c \in \mathbb{Z}$ impar; para que $c^2/4 - db^2 \in \mathbb{Z}$ debe darse que $b = e/2$ con $e \in \mathbb{Z}$ y que se satisfaga que $c^2 - de^2$ sea múltiplo de 4, i.e., que $c^2 \equiv de^2 \pmod 4$. Pero ésto es imposible, pues e no puede ser par ya que $de^2 \equiv 0$ y tampoco impar pues $de^2 \equiv d \not\equiv 1 \equiv c^2$.

- Si $d \equiv 1 \pmod 4$: Como $2x \in A$ (por ser anillo), entonces por las condiciones de la ec. (4.1) se debe dar que $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ y luego que $d(2b)^2 \in \mathbb{Z}$. Si $2b \notin \mathbb{Z}$, entonces es de la forma $2b = c/e$ donde $c, e \in \mathbb{Z}$ coprimos y $e \in \mathbb{Z} \setminus \{0, \pm 1\}$, de modo que $p \mid e$. Así, $(2b)^2$ es un racional

que posee un p^2 en el denominador, y luego necesariamente $p^2 \mid d$ para que $d(2b)^2 \in \mathbb{Z}$, lo cual es absurdo ya que d está libre de cuadrados.

Definamos $u := 2a, v := 2b \in \mathbb{Z}$, se tiene que $x \in A$ syss

$$u^2 - dv^2 \equiv 0 \pmod 4.$$

Si v es par, entonces clarmante u también debe serlo. Si v es impar, entonces $v^2 \equiv 1$ y $u^2 \equiv d \equiv 1$; lo que concluye el enunciado. □

Así, hemos visto que la norma tiene una serie de ventajas para el estudio de los cuerpos numéricos. Pero aún queda una herramienta por introducir. Comencemos con una observación:

Proposición 4.15: Sea K/k una extensión finita de cuerpos. Entonces, la siguiente aplicación:

$$\begin{aligned} \psi\colon K \times K &\longrightarrow k \\ (x, y) &\longmapsto \mathrm{Tr}_{K/k}(xy) \end{aligned}$$

es una forma bilineal simétrica.

Definición 4.16: Sea K/k una extensión finita separable de cuerpos, sea $B := (\alpha_1, \ldots, \alpha_n)$ una base ordenada de K como k-espacio vectorial y sean $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, N)$, donde N es la clausura normal de K. Se define el ***discriminante*** de la base como:

$$\mathfrak{d}_B(K/k) = \det\left([\sigma_i\alpha_j]_{ij}\right)^2 \in k.$$

Proposición 4.17: Sea K/k una extensión finita separable y sea $B := (\alpha_1, \ldots, \alpha_n)$ una base ordenada de K como k-espacio vectorial. Entonces

$$\mathfrak{d}_B(K/k) = \det\left([\mathrm{Tr}_{K/k}(\alpha_i\alpha_j)]_{ij}\right) \neq 0.$$

Es decir, $\psi(x, y)$ es una forma bilineal no degenerada.

Demostración: Sean $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_k(K, N)$, donde N es la clausura normal de K, entonces:

$$\mathrm{Tr}_{K/k}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} (\sigma_k\alpha_i)(\sigma_k\alpha_j),$$

de modo que $[\mathrm{Tr}_{K/k}(\alpha_i\alpha_j)]_{ij} = [\sigma_k\alpha_i]_{ik}^t \cdot [\sigma_k\alpha_j]_{kj}$.

Como K/k es finita y separable, entonces por el teorema de las raíces primitivas[3] existe $\theta \in K$ tal que $K = k(\theta)$ y $\{1, \theta, \ldots, \theta^{n-1}\}$ es una base. Definamos $\theta_k := \sigma_k\theta$, entonces nos queda que $\mathfrak{d}(1, \ldots, \theta^{n-1})$ es el determinante al cuadrado de la matriz:

$$\begin{bmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \theta_n^2 & \cdots & \theta_n^{n-1} \end{bmatrix},$$

la cual, el lector reconocerá como una matriz de Vandermonde [**1,** Prop. 3.58], de modo que

$$\mathfrak{d}(1, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_j - \theta_i)^2,$$

el cual es no nulo pues $\theta_j \neq \theta_i$ dado que θ es elemento primitivo.

Finalmente, si el discriminante es no nulo en una base, lo es en todas ellas. □ Insertar referencia.

Lema 4.18: Sea A un dominio íntegro, K su cuerpo de fracciones, L/K una extensión separable finita de cuerpos y B la clausura íntegra de L/A. Sea $C := (\alpha_1, \ldots, \alpha_n)$ una base de L como K-espacio vectorial de elementos enteros y sea $d := \mathfrak{d}_C(K/k)$. Entonces, se cumple que

$$dB \subseteq \alpha_1 A + \cdots + \alpha_n A.$$

Demostración: Sea $\beta \in B \subseteq L$. Por definición de base, se cumple que $\beta = \sum_{i=1}^n \lambda_j \alpha_j$ con $\lambda_j \in K$. Los λ_j's satisfacen ser la solución al sistema de ecuaciones:

$$\operatorname{Tr}(\alpha_i\beta) = \operatorname{Tr}\left(\alpha_i \cdot \sum_{j=1}^n \lambda_j \alpha_j\right) = \sum_{j=1}^n \lambda_j \operatorname{Tr}(\alpha_i\alpha_j),$$

lo cual podemos describir matricialmente con la siguiente notación: Si $\boldsymbol{u} := [\operatorname{Tr}(\alpha_i\beta)]_{i1}, \boldsymbol{v} := [\lambda_j]_{j1}$ y $M := [\operatorname{Tr}(\alpha_i\alpha_j)]_{ij}$, el sistema de ecuaciones se escribe de manera resumida como

$$\boldsymbol{u} = M \cdot \boldsymbol{v} \iff \boldsymbol{v} = M^{-1} \cdot \boldsymbol{v} = \frac{1}{d} \operatorname{adj}(M) \cdot \boldsymbol{u},$$

donde la última ecuación está en K. Aquí, recordamos que $\operatorname{adj}(M)$ y $\boldsymbol{u}$ tienen entradas en A (¿por qué?), de modo que $d\boldsymbol{v} \in A$, es decir, $d\lambda_j \in A$ para todo j. Finalmente es fácil concluir el enunciado. □

[3] Cf. [**1,** Teo. 4.42].

§4.2.1 $\mathbb{Z}[\sqrt{-1}]$**.** Por el teorema 4.14, los enteros de $\mathbb{Q}[\sqrt{-1}]$ son aquellos de la forma $a + b\sqrt{-1}$ con $a, b \in \mathbb{Z}$; éste anillo se denota $\mathbb{Z}[\mathrm{i}]$, donde[4] $\mathrm{i} = \sqrt{-1}$, y sus elementos se denominan ***enteros de Gauss***.

Proposición 4.19: $\mathbb{Z}[\mathrm{i}]$ es un dominio euclídeo y, por lo tanto, un DFU.

Demostración: Definamos la norma $\mathrm{Nm}(a + \mathrm{i}b) := \mathrm{Nm}_{\mathbb{Q}[\mathrm{i}]/\mathbb{Q}}(a + \mathrm{i}b) = a^2 + b^2$. Queremos ver que se satisface el algoritmo de la división, digase, que dados $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ existen $\gamma, \rho \in \mathbb{Z}[\mathrm{i}]$ tales que

$$\alpha = \gamma \cdot \beta + \rho, \qquad \mathrm{Nm}(\rho) < \mathrm{Nm}(\beta).$$

Vale decir, buscamos $\gamma \in \mathbb{Q}[\mathrm{i}]$ entero tal que $\mathrm{Nm}(\rho/\beta) = \mathrm{Nm}(\alpha/\beta - \gamma) < 1$.

Ésto se deduce de un argumento geométrico: todo punto α/β está contenido en un cuadrado de lado 1 cuyos extremos son enteros. Así pues, la distancia (que es $|z| = \sqrt{\mathrm{Nm}(z)}$) es a lo más $\sqrt{2}/2$ (ver fig. 4.1) de modo que existe algún γ entero tal que

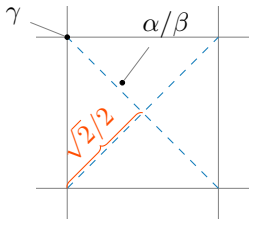


Figura 4.1

$$\mathrm{Nm}\left(\frac{\alpha}{\beta} - \gamma\right) \leq \left(\frac{\sqrt{2}}{2}\right)^2 < 1,$$

de lo que se concluye el enunciado. □

Como $\mathbb{Z}[\mathrm{i}]$ es un DFU, entonces tiene sentido hablar de primos de dicho anillo. Para distinguirlos, nos referiremos a los primos en $\mathbb{Z}$ como ***primos racionales*** y a los primos en $\mathbb{Z}[\mathrm{i}]$ como ***primos de Gauss***.

Proposición 4.20: Sus inversibles son $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\}$.

[4]Se denota $\mathrm{i} = \sqrt{-1}$ (en letras romanas o derechas) para no confundir con i (en cursivas) que usualmente reservamos para un subíndice.

Demostración: Es fácil notar que si $\alpha \in \mathbb{Z}[\mathrm{i}]$ es inversible, entonces $\mathrm{Nm}(\alpha)$ también, de modo que $\mathrm{Nm}(\alpha) = 1$ y $\mathrm{Nm}(a+\mathrm{i}b) = a^2+b^2$ es más grande que 1 en otros casos. □

Teorema 4.21: Todo primo $p > 2$ puede escribirse como suma de dos cuadrados syss $p \equiv 1 \pmod 4$. Todo primo $p > 2$ puede escribirse como suma de dos cuadrados syss $p \equiv 1 \pmod 4$

Demostración: $\Longrightarrow$. Trivial.

$\Longleftarrow$. Todo primo racional p no es inversible en $\mathbb{Z}[\mathrm{i}]$ por la proposición anterior, luego hay dos posibilidades, o bien es primo de Gauss o bien se descompone en factores primos en $\mathbb{Z}[\mathrm{i}]$. Veremos que p se puede escribir como a^2+b^2 si p no es primo en $\mathbb{Z}[\mathrm{i}]$: en efecto, si p no es primo entonces $p = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ no inversibles, luego $p^2 = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$ y como $\mathrm{Nm}(\alpha) \neq 1 \neq \mathrm{Nm}(\beta)$, entonces necesariamente $a^2+b^2 = \mathrm{Nm}(\alpha) = p$, donde $\alpha = a + \mathrm{i}b$.

Como $p \equiv 1 \pmod 4$, entonces -1 es un residuo cuadrático módulo p (teo. 2.37), es decir, $p \mid x^2+1$ para algún $x \in \mathbb{Z}$. Nótese que $x^2+1 = (x-\mathrm{i})(x+\mathrm{i})$ y $\frac{x\pm\mathrm{i}}{p} \notin \mathbb{Z}[\mathrm{i}]$ de modo que no puede ser un elemento primo de $\mathbb{Z}[\mathrm{i}]$; ésto concluye la demostración. □

Éste resultado lo podemos mejorar ligeramente, notando la identidad de cuadrados:

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (bc+ad)^2,$$

(que deriva de que $|\alpha\beta|^2 = |\alpha|^2\,|\beta|^2$ para $\alpha, \beta \in \mathbb{C}$). Así pues se tiene lo siguiente:

Teorema 4.22: Un número natural no nulo n es suma de dos cuadrados syss para todo primo $p \equiv 3 \pmod 4$ se cumple que $\nu_p(n)$ es par.

Teorema 4.23: Los primos de Gauss son, salvo asociados, los de la forma:

(a) $\pi = 1 + \mathrm{i}$.

(b) $\pi = a + \mathrm{i}b$, tal que $\mathrm{Nm}(\pi) = p \equiv 1 \pmod 4$.

(c) $\pi = p \equiv 3 \pmod 4$.

Donde p es un primo racional.

Demostración: Es fácil notar que si $\mathrm{Nm}(\alpha) = p$, donde p es un primo racional, entonces α es un primo de Gauss (puesto que la norma es multiplicativa y vimos que los inversibles tienen norma 1); ésto completa los casos (a) y (b). El teorema anterior nos permite concluir el caso (c).

Ahora hay que ver que no hay más primos: Sea $\pi \in \mathbb{Z}[\mathrm{i}]$ un primo arbitrario, entonces

$$\mathrm{Nm}(\pi) = \pi \cdot \overline{\pi} = p_1 \cdots p_n,$$

donde p_j son primos racionales. Como π es primo, entonces $\pi \mid p$ para algún $p = p_j$ y, por lo tanto, $\mathrm{Nm}(\pi) \mid \mathrm{Nm}(p) = p^2$. Ergo, $\mathrm{Nm}(\pi) = p$ o $\mathrm{Nm}(\pi) = p^2$.

Si $\mathrm{Nm}(\pi) = p$ entonces hay dos casos posibles: Si $p = 2$, entonces necesariamente π es una suma de ± 1 con $\pm \mathrm{i}$ y es fácil notar que todos son asociados de $1 + \mathrm{i}$. Si $p \equiv 1 \pmod 4$ entonces nos encontramos en el caso (b), y $p \not\equiv 3 \pmod 4$ por el teorema anterior. Si $\mathrm{Nm}(\pi) = p^2$, entonces p/π es un entero gaussiano de norma 1, es decir, un inversible; de modo que necesariamente llegamos al caso (c). □

En general trabajar con primos como tal es más difícil y se opta por cambiarles por ideales, pero en definitiva conlleva a la siguiente definición:

Definición 4.24: Sea k un cuerpo numérico y $\mathcal{O}_k$ su anillo de enteros. Un primo racional $p \in \mathbb{Z}$ se:

Conserva Si $p \cdot \mathcal{O}_k$ es un ideal primo de $\mathcal{O}_k$.

Escinde Si $p \cdot \mathcal{O}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, donde $\mathfrak{p}_i$ son ideales primos distintos de $\mathcal{O}_k$.

Ramifica Si $p \cdot \mathcal{O}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, donde $\mathfrak{p}_i$ son ideales primos distintos de $\mathcal{O}_k$ y $e_i > 1$ para algún i.

Así pues el teorema anterior nos dice que:

- El único primo que se ramifica en $\mathbb{Z}[\mathrm{i}]$ es el 2.
- p se escinde en $\mathbb{Z}[\mathrm{i}]$ si $p \equiv 1 \pmod 4$.
- p se conserva en $\mathbb{Z}[\mathrm{i}]$ si $p \equiv 3 \pmod 4$.

La factorización en $\mathbb{Z}[\mathrm{i}]$ no solo nos permite deducir *cuáles* números son sumas de dos cuadrados, sino de *cuántas* maneras:

Teorema 4.25: Sea n un natural que es suma de dos cuadrados y sean $e_1, \ldots, e_r$ los exponentes de sus divisores módulo $p \equiv 1 \pmod 4$. Denotemos

$N_0 := (e_1 + 1) \cdots (e_r + 1)$. Entonces n se expresa como $N_0/2$ sumas de dos cuadrados si n no es un cuadrado y se expresa como $(N_0 + 1)/2$ sumas de dos cuadrados en otro caso.

Demostración: Ésto equivale a preguntarse la cantidad de enteros de Gauss α con norma $\mathrm{Nm}(\alpha) = \alpha \cdot \overline{\alpha} = n$, salvo asociados. Es claro que α será un divisor de n, así que denotemos:

$$n = 2^{e_0} \cdot p_1^{e_1} \cdots p_r^{e_r} p_{r+1}^{e_{r+1}} \cdots p_m^{e_m},$$

donde $p_j \equiv 3 \pmod 4$ para $r+1 \leq j \leq m$, luego éstos e_j's son pares. Luego los divisores α con norma n son exactamente aquellos de la forma:

$$\alpha = \epsilon \lambda^{e_0} (\pi_1^{s_1} \bar{\pi}_1^{e_1 - s_1}) \cdots (\pi_r^{s_r} \bar{\pi}_r^{e_r - s_r}) p_{r+1}^{e_{r+1}/2} \cdots p_m^{e_m/2},$$

donde $\epsilon \in \mathbb{Z}[\mathrm{i}]^\times$, $\lambda := 1 + \mathrm{i}$, cada π_i es el único primo de Gauss (salvo asociados) que dividide a p_i con $1 \leq i \leq r$. Si fijamos $\epsilon = 1$, entonces obtendremos divisores no asociados entre sí, por lo que el único parámetro libre son los $0 \leq s_i \leq e_i$ con $1 \leq i \leq r$, lo que que cuenta un total de

$$N_0 := (e_1 + 1) \cdots (e_r + 1),$$

elementos con norma n. Éste número debemos dividirlo por 2 para eliminar $\bar{\alpha}$ de la lista que aparece repetido, exceptuando si $\alpha = \bar{\alpha}$.

No obstante, tendremos que si $\alpha = \bar{\alpha}$ obtendremos que α es en sí mismo racional y que $n = \mathrm{Nm}(\alpha) = \alpha^2 + 0^2$ por lo que n es un cuadrado. Además, acabamos de ver que ésto se da para una única combinación (puesto que un n sólo posee una raíz cuadrada salvo asociados), por ello el «+1». □

§4.2.2 Grupos de invertibles. Ahora que tenemos cierta experiencia con los cuerpos cuadráticos, ampliemos la perspectiva:

Definición 4.26: Un cuerpo cuadrático $\mathbb{Q}(\sqrt{d})$ (y su anillo de enteros), donde d está libre de cuadrados, se dice ***real*** (resp. ***imaginario*** si $d > 0$ (resp. $d < 0$).

En primer lugar, querremos estudiar el grupo de inversibles de los cuerpos cuadráticos, para lo cuál nos detendremos en otro ejemplo importante, los llamados ***enteros de Eisenstein***: Considere ζ una raíz cúbica primitiva de la unidad, vale decir, una raíz de

$$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \in \mathbb{Z}[x].$$

Uno puede calcular que las raíces complejas de ese polinomio son:

$$\frac{-1 \pm \sqrt{-3}}{2},$$

así que arbitrariamente elegimos $\zeta := \frac{-1+\sqrt{-3}}{2}$. Ésto es simplemente para justificar que $\mathbb{Z}[\zeta]$ es el anillo de enteros de $\mathbb{Q}(\sqrt{-3})$.

En el caso de $\sqrt{-1}$ vemos que el conjugado es $-\sqrt{-1}$, pero no sucede lo mismo con ζ: esudiando el polinomio $\Phi_3(x)$ es fácil notar que la otra raíz es $\zeta^2 = -1 - \zeta$, luego la conjugación aquí es:

$$\overline{a + b\zeta} = a + b\zeta^2 = (a - b) - b\zeta,$$

y la norma algebraica es:

$$\mathrm{Nm}(a + b\zeta) = (a + b\zeta)(a + b\zeta^2) = a^2 - ab + b^2.$$

Proposición 4.27: Sean $a+b\zeta+c\zeta^2 = \tilde{a}+\tilde{b}\zeta+\tilde{c}\zeta^2$ con $a, b, c, \tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}$. Entonces $a - \tilde{a} = b - \tilde{b} = c - \tilde{c}$.

Demostración: Sean $q(x) := a + bx + cx^2$ y $\tilde{q}(x) := \tilde{a} + \tilde{b}x + \tilde{c}x^2 \in \mathbb{Z}[x]$, luego notamos que $q(\zeta) - \tilde{q}(\zeta) = 0$, por lo que el polinomio minimal $f(x) := x^2 + x + 1$ ha de satisfacer: $q(x) - \tilde{q}(x) = f(x)g(x)$ para algún $g(x) \in \mathbb{Z}[x]$, pero comparando grados, vemos que g ha de ser constante. □

Teorema 4.28: $\mathbb{Z}[\zeta]$ es un dominio euclídeo con la norma algebraica.

Demostración: Nótese que la norma algebraica es positiva y vale cero solo en el cero, de modo que $\mathrm{Nm}(\alpha) \leq \mathrm{Nm}(\alpha\beta)$ para todo $\alpha, \beta \in \mathbb{Z}[\zeta]$ con $\beta \neq 0$. Sean $\alpha, \beta \in \mathbb{Z}[\zeta]$ con $\beta \neq 0$, se cumple que $\alpha/\beta = r + s\zeta$ con $r, s \in \mathbb{Q}$. Sean x, y los enteros más cercanos a r, s resp., de modo que $|r - x|, |s - y| \leq 1/2$ y luego definiendo $\gamma := x + y\zeta$ y $\rho := \alpha - \beta\gamma \in \mathbb{Z}[\zeta]$ vemos que

$$\begin{aligned} \alpha &= \beta\gamma + \rho, \\ \mathrm{Nm}(\rho/\beta) = \mathrm{Nm}(\alpha/\beta - \gamma) &= (r - x)^2 - (r - x)(s - y) + (s - y)^2 \leq 3/4 < 1 \end{aligned}$$

por lo que $\mathrm{Nm}(\rho) < \mathrm{Nm}(\beta)$. □

Proposición 4.29: $\mathbb{Z}[\zeta]^\times = \{\pm 1, \pm\zeta, \pm\zeta^2\}$.

Demostración: Como $\mathbb{Z}[\zeta]$ es cuadrático imaginario, entonces la norma es siempre positiva y los invertibles son los de norma 1, vale decir

$$\mathrm{Nm}(a+b\zeta) = a^2 - ab + b^2 = (a-b/2)^2 + 3b^2/4 = 1,$$

o equivalentemente, $(2a-b)^2 + 3b^2 = 4$ y notamos que $b \in \{0, \pm 1\}$ lo que nos da las seis soluciones del enunciado. □

Ahora sí, podemos comprobar que el grupo no es más complicado en otros casos:

Teorema 4.30: Sea $K := \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático imaginario y sea $\mathbb{Z}[\omega] = \mathcal{O}_K$.

(a) Si $d = -1$, entonces $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm \mathrm{i}\}$.

(b) Si $d = -3$, entonces $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$.

(c) En otro caso, $\mathbb{Z}[\omega]^\times = \{\pm 1\}$.

Demostración: En general, nótese que $\alpha \in \mathbb{Z}[\omega]$ es invertible syss $\mathrm{Nm}(\alpha) = \pm 1$, pero

$$\mathrm{Nm}(u + v\sqrt{d}) = u^2 - dv^2,$$

donde d es negativo, de modo que la norma algebraica siempre es positiva, así que buscamos que sea igual a 1. Ya hemos visto el caso (a) y el caso (b), los otros restantes se pueden confirmar notando que si $d \not\equiv 1 \pmod 4$ obtenemos la ecuación $a^2 - db^2 = 1$ con $-d > 1$, lo que fuerza a $b = 0$; y si $d \equiv 1 \pmod 4$ se obtiene la ecuación:

$$\left(\frac{a}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = 1 \iff a^2 - db^2 = 4,$$

con $-d > 3$ y mayor que cuatro también por la condición modular. □

El caso real es más complicado. Uno puede probar que el grupo de invertibles nunca es el trivial $\{\pm 1\}$, pero ésto tendrá que esperar unas secciones, no obstante, de mismo modo podemos probar algo igualmente conveniente.

Teorema 4.31: Si $\epsilon > 1$ es invertible en $\mathbb{Z}[\omega] = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ cuadrático real, entonces $\epsilon = a + b\omega$ con $a, b \geq 1$, exceptuando el caso $d = 5$ en donde $\epsilon = \omega$ también es invertible.

Demostración: Sea $\epsilon = a + b\omega$ como en el enunciado. Si es invertible, entonces $\mathrm{Nm}_K(\epsilon) = \epsilon \cdot \bar{\epsilon} = \pm 1$ y $\bar{\epsilon} = \pm 1/\epsilon$, donde $0 < 1/\epsilon < 1 < \epsilon$. Luego se cumple $\epsilon - \bar{\epsilon} > 0$, o equivalentemente $b(\omega - \bar{\omega}) > 0$ donde

$$\omega - \bar{\omega} = \begin{cases} 2\sqrt{d}, & d \not\equiv 1 \pmod 4 \\ \sqrt{d}, & d \equiv 1 \pmod 4 \end{cases}.$$

En cualquier caso, $\omega - \bar{\omega} > 0$ y $b > 0$. Si $d \neq 5$ entonces $\bar{\omega} < -1$: en efecto, si $d \not\equiv 1$ (4) entonces $\omega = -\sqrt{d} < -1$ y si no, entonces

$$\bar{\omega} = \frac{1 - \sqrt{d}}{2} < -1 \iff \sqrt{d} > 3 \iff d > 9.$$

Luego $|\bar{\omega}| > 1$ y

$$|a + b\bar{\omega}| = |\bar{\epsilon}| < 1,$$

lo que fuerza a que $a > 0$.

Para $d = 5$ vemos que

$$-1 < \bar{\epsilon} = a + b\bar{\omega} < 1 \implies a > -1 - b\bar{\omega} \geq -1 - \bar{\omega} = \frac{\sqrt{5} - 2}{2} \approx -0{,}38.$$

luego $a \geq 0$. Si $a = 0$, entonces $\epsilon = b\omega$, $\mathrm{Nm}(\epsilon) = -b^2$ y obtenemos que $b = \pm 1$. □

Teorema 4.32: Sea $K := \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático real con anillo de enteros $\mathbb{Z}[\omega]$. Si $\mathbb{Z}[\omega] \neq \{\pm 1\}$, entonces existe una unidad $\eta > 1$ tal que todos los invertibles son de la forma $\pm\eta^n$ con $n \in \mathbb{Z}$.

Demostración: Nótese que si el grupo de invertibles no es trivial, entonces existe una unidad $\epsilon > 1$ (¿por qué?). Por el teorema anterior, si $1 < a' + b'\omega < a + b\omega$ son dos unidades, entonces $0 \leq a < a$ o $0 < b' < b$, por lo que el conjunto

$$\{\delta \in \mathbb{Z}[\omega]^\times : 1 < \delta \leq \epsilon\}$$

es finito y posee un elemento mínimo η. Por desigualdad de Bernoulli se obtiene que:

$$\eta^m = (1 + (\eta - 1))^m \geq 1 + m(\eta - 1),$$

por lo que, si $\epsilon > 1$ es otra unidad, entonces existe un m natural tal que $\eta^m \leq \epsilon < \eta^{m+1}$ y luego $1 \leq \epsilon/\eta^m < \eta$ es una unidad, luego $1 = \epsilon/\eta^m$. Si ϵ fuese una unidad negativa, simplemente lo cambiamos por $-\epsilon$, y si $0 < \epsilon < 1$, entonces lo cambiamos por ϵ^{-1}. □

Definición 4.33: Sea $K := \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático real con anillo de enteros $\mathbb{Z}[\omega]$. Una unidad η tal que $\mathbb{Z}[\omega]^\times = \{\pm\eta^m : m \in \mathbb{Z}\}$ se dice una ***unidad fundamental***.

Es fácil notar que un anillo de enteros cuadráticos tiene a lo más cuatro unidades fundamentales, $\pm\eta$ y $\pm\eta^{-1}$, luego hablaremos de *la* unidad fundamental al $\eta > 1$ (si existe).

Ejercicio 4.34: Demostrar que la unidad fundamental de $\mathbb{Q}(\sqrt{5})$ es ω.

§4.2.3 Anillos de enteros cuadráticos que son euclídeos. De momento hemos probado que $\mathbb{Z}[\sqrt{-1}]$ y $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ son dominios euclídeos, y en ambos casos han sido mediante la norma algebraica. Responder directamente cuando un anillo de enteros es un dominio euclídeo es una pregunta difícil, pero al menos podemos descartar cuándo lo es, en el caso de enteros cuadráticos, mediante un argumento geométrico si consideramos que la norma es la algebraica.

Definición 4.35: Decimos que dado un cuerpo numérico K su anillo de enteros A es un ***dominio norma-euclídeo***[5] si la norma algebraica en valor absoluto $|\operatorname{Nm}_{K/\mathbb{Q}}| : A \to \mathbb{Z}$ es una norma euclídea.

Proposición 4.36: El anillo de enteros $\mathbb{Z}[\omega]$ del cuerpo cuadrático $K := \mathbb{Q}(\sqrt{d})$ es norma-euclídeo syss para todo $\delta \in K$, existe $\gamma \in \mathbb{Z}[\omega]$ tal que $|\operatorname{Nm}(\delta - \gamma)| < 1$.

Demostración: $\Longleftarrow$. Sean $\alpha, \beta \in \mathbb{Z}[\omega]$ con $\beta \neq 0$, luego elijamos γ como en el enunciado de modo que $|\operatorname{Nm}(\alpha/\beta - \gamma)| < 1$. Definiendo $\rho := \alpha - \beta\gamma$ vemos que

$$|\operatorname{Nm}(\rho)| = |\operatorname{Nm}(\beta)| \cdot \left|\operatorname{Nm}\left(\frac{\alpha}{\beta} - \gamma\right)\right| < |\operatorname{Nm}(\beta)|.$$

$\Longrightarrow$. Empleamos un método similar, pero para todo $\delta = \alpha/n$, donde α es entero y $n =: \beta$ es natural no nulo, obtenemos

$$\alpha = \gamma n + \rho, \qquad |\operatorname{Nm}(\rho)| < n^2,$$

de modo que $|\operatorname{Nm}(\delta - \gamma)| = |\operatorname{Nm}(\rho/n)| < 1$. □

[5] eng. *norm-Euclidean domain*.

Luego, para $\alpha = r + s\sqrt{d}$, con $r, s \in \mathbb{Q}$, buscamos $x, y \in \mathbb{Z}$ tales que

$$\operatorname{Nm}\left((r-x) + (s-y)\sqrt{d}\right) = |(r-x)^2 - d(s-y)^2| < 1, \qquad (4.2)$$

de existir, diremos que (x, y) están «cerca» de (r, s). Reemplazando $r = m + r'$ y $s = n + s'$ con $m, n \in \mathbb{Z}$ y $|r'|, |s'| \leq 1/2$ vemos que si encontramos (x, y) cercanos a (r', s'), entonces $(x + m, y + n)$ están cerca de (r, s). Además si $-1/2 \leq r < 0$, entonces si (x, y) está cerca de $(-r, s)$, entonces $(-x, y)$ está cerca de (r, s). De modo que podemos suponer que $r, s \in [0, 1/2]$. Si $d \equiv 1$ (mód 4) hay otra reducción posible: si se cumple que $1/4 < s \leq 1/2$ y (x, y) están cerca de (r, s), entonces $(1/2-x, 1/2-y)$ están cerca de $(1/2-r, 1/2-s)$, donde $0 \leq 1/2 - s < 1/2$ y donde $(1/2 - x, 1/2 - y)$ sí representa un entero algebraico.

En definitiva, verificar que el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es norma-euclídeo se reduce a ver que el rectángulo:

$$F(d) := \begin{cases} \{(r, s) \in \mathbb{Q}^2 : 0 \leq r \leq 1/2, 0 \leq s \leq 1/2\}, & d \not\equiv 1 \pmod 4 \\ \{(r, s) \in \mathbb{Q}^2 : 0 \leq r \leq 1/2, 0 \leq s \leq 1/4\}, & d \equiv 1 \pmod 4 \end{cases}$$

puede cubrirse con conjuntos de la forma

$$U(x, y) := \{(r, s) \in \mathbb{Q}^2 : |(r-x)^2 - d(s-y)^2| < 1\},$$

donde x, y son enteros (las coordenadas semienteras están cubiertas por la reducción explicada arriba).

Teorema 4.37: Los anillos de enteros cuadráticos imaginarios de $\mathbb{Q}(\sqrt{d})$ que son norma-euclídeos son exactamente los con

$$d \in \{-1, -2, -3, -7, -11\}.$$

La demostración, un tanto informal, se basa en notar que los conjuntos $U(x, y)$ son elipses centradas en (x, y) con semieje horizontal 1 y semieje vertical $1/\sqrt{-d}$. Luego, podemos simplemente graficar los rectángulos y verificar visualmente que están cubiertos por dichas elipses. Tecnicamente, la formalización sería un tratamiento de desigualdades que, en lo personal, considero innecesario.

En primer lugar veamos $d \not\equiv 1$ (mód 4) (ver fig. 4.2). Aquí podemos notar que para $d = -5$ falla, y para $d < -5$ las elipses se van haciendo más pequeñas, por lo que, éstos tampoco son dominios norma-euclídeos.

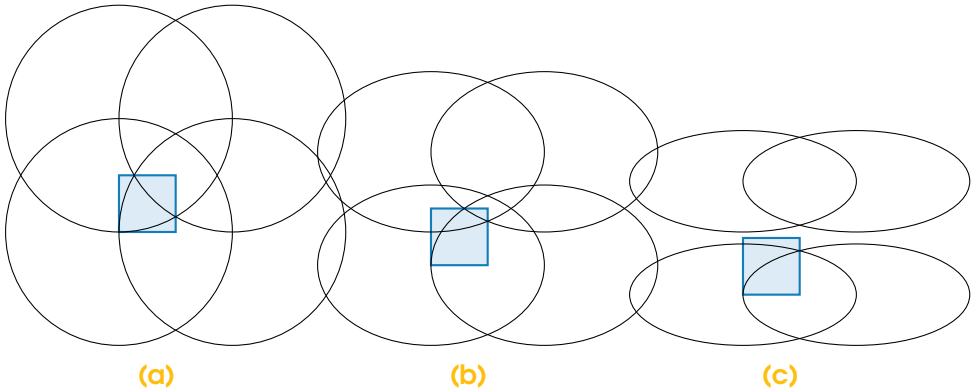


Figura 4.2. Dominios norma-euclídeos imaginarios con $d \not\equiv 1 \pmod 4$.

Ejemplo 4.38 ($\mathbb{Z}[\sqrt{-5}]$ no es un DFU)**:** Para probar ésto, veremos que no todos los elementos tienen factorización única por irreducibles, o equivalentemente, que los irreducibles no son primos. Para ello, nótese que

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}),$$

ahora bien, tomando normas algebraicas vemos que

$$\mathrm{Nm}(2) = 4, \qquad \mathrm{Nm}(3) = 9, \qquad \mathrm{Nm}(1 \pm \sqrt{-5}) = 6,$$

por lo que, de haber factorización prima, tendríamos que $6 = \pi_1\pi_2\pi_3\pi_4$ tales que los π_i son divisores de 2, de 3 y de $1 \pm \sqrt{-5}$. Debido a que conocemos las normas, ésto implicaría a que los π_i's tengan norma algebraica 2 y 3; pero es claro que 2 y 3 no son números de la forma $a^2 + 5b^2$. ⌟

Ésto también demuestra que $\mathbb{Z}[\sqrt{-5}]$ no es euclídeo, en particular.

Para el caso $d \equiv 1 \pmod 4$ (ver fig. 4.3) el procedimiento es exactamente el mismo, notando que falla en $d = -15$ y por ende, desde ese punto en adelante. Para dar una demostración formal, por el argumento anterior, simplemente sería necesario comprobar que el argumento geométrico funciona en $d = -2$ y $d = -11$, y falla en $d = -5, d = -15$.

Ejercicio 4.39: Demuestre que $\mathbb{Z}[\omega]$ con $\omega = \frac{1+\sqrt{-15}}{2}$ no es DFU.

Lema 4.40: $\mathbb{Z}[\sqrt{-6}]$ y $\mathbb{Z}[\sqrt{-10}]$ no son DFUs.

Teorema 4.41 (Motzkin): Los anillos de enteros cuadráticos imaginarios son dominios euclídeos syss son dominios norma-euclídeos.

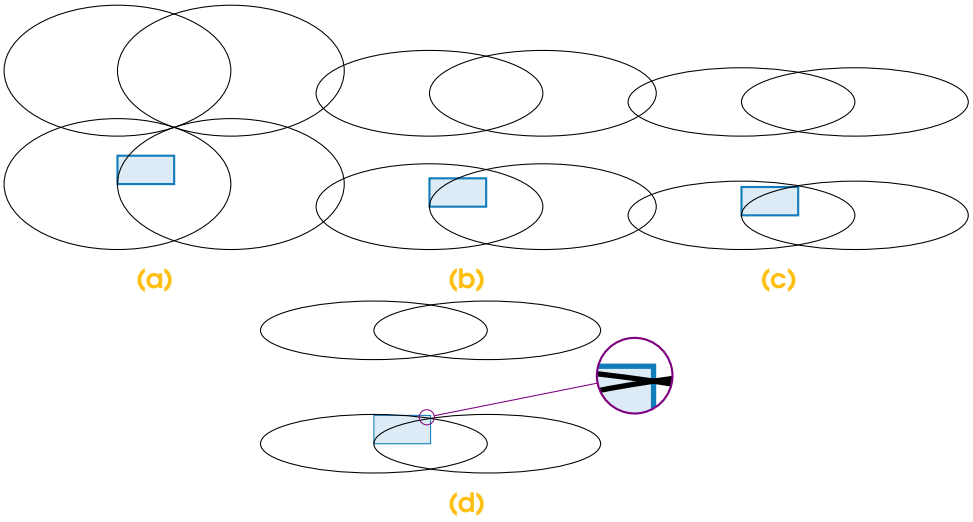


Figura 4.3. Dominios norma-euclídeos imaginarios con $d \equiv 1 \pmod 4$.

Demostración: Vamos a probar que el anillo de enteros A de $\mathbb{Q}(\sqrt{d})$ no es euclídeo si $d \leq -13$, puesto que por el lema, el resto de casos están cubiertos. Si A fuese euclídeo, entonces habría una norma euclídea ϕ sobre A y podemos elegir $\delta \in A$ no nulo ni inversible con norma minimal, de modo que $A/(\delta) = \{0, \pm 1\}$ (por algoritmo de la división y porque $A^\times = \{\pm 1\}$).

Así pues consideremos el valor de $1 + 1 \mod \delta$: No se da que $1 + 1 \equiv 1 \pmod \delta$ de lo contrario $1 \equiv 0 \pmod \delta$ y δ sería invertible. Si $1 + 1 \equiv 0 \pmod \delta$ entonces $\delta \mid 2$ y si $1 + 1 \equiv -1 \pmod \delta$ entonces $\delta \mid 3$.

Ahora bien, $\delta \notin \{\pm 2, \pm 3\}$ ya que ω no es congruente a 0 o ± 1 módulo un entero racional (¿por qué?), luego necesariamente $\mathrm{Nm}(\delta) \in \{2, 3\}$. Si $\delta = (a/2) + (b/2)\sqrt{d}$ donde a, b comparten paridad, entonces $\mathrm{Nm}(\delta) \leq 3$ lo que implica que

$$a^2 - db^2 \leq -12,$$

pero como $d < -13$, se cumple que $b = 0$ y luego δ es un entero racional, lo que es absurdo. □

Para el caso de enteros cuadráticos reales se tiene que los conjuntos ya no son elipses y, si bien la lógica aún aplica, los diagramas ya no son igualmente intuitivos, pero se puede probar que:

Teorema 4.42: Los anillos de enteros cuadráticos reales de $\mathbb{Q}(\sqrt{d})$ que

son norma-euclídeos son exactamente los con

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 38, 41, 57, 73\}.$$

No obstante, *no* daremos una prueba de ello y remitimos al lector al artículo **[81]** y para un recuento histórico a **[99].** Al contrario de lo que sucede con el caso imaginario, uno puede probar que $d = 14$ **[29]** y $d = 69$ **[20]** sí son dominios euclídeos.

Teorema 4.43 (ecuación de Ramanujan-Nagell): Las únicas soluciones enteras de $x^2 + 7 = 2^n$ son:

$$(x, n) \in \{(\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7), (\pm 181, 15)\}.$$

Demostración: Es claro que x es impar y podemos reducirnos al caso positivo. Si $n = 2m$, entonces podemos reescribir

$$7 = 2^{2m} - x^2 = (2^m + x)(2^m - x),$$

Comparando los tamaños concluimos que $2^m + x = 7$ y que $2^m - x = 1$, de modo que sumando ambos términos tenemos $2^{m+1} = 8$ y $m = 2$, lo que nos da la solución $(x, n) = (3, 4)$.

Si n es impar, entonces puede suceder que $n = 3$ lo que induce $(x, n) = (1, 3)$. Si $n > 3$, entonces trabajaremos en $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, el cual es euclídeo y luego DFU, y donde

$$2 = \left(\frac{1 + \sqrt{-7}}{2}\right)\left(\frac{1 - \sqrt{-7}}{2}\right) =: \omega \cdot \bar{\omega},$$

los cuales son primos. Como x es impar, entonces $x^2 + 7$ es múltiplo de 4, y definiendo $m := n - 2$ podemos considerar la factorización:

$$\frac{x + \sqrt{-7}}{2}\frac{x - \sqrt{-7}}{2} = \left(\frac{1 + \sqrt{-7}}{2}\right)^m \left(\frac{1 - \sqrt{-7}}{2}\right)^m,$$

nótese que los términos de la derecha sólo pueden tener divisores comúnes que sean factores de $\sqrt{-7}$, luego, y por factorización única sumando al hecho de que son conjugados, concluimos que

$$\frac{x + \sqrt{-7}}{2} = \pm\left(\frac{1 \pm \sqrt{-7}}{2}\right)^m,$$

donde en la derecha hay dos signos sin determinar. En cualquier caso, como son conjugados, se tiene que

$$\begin{aligned}\pm\sqrt{-7} &= \pm\left(\frac{x+\sqrt{-7}}{2} - \frac{x-\sqrt{-7}}{2}\right)\\ &= \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1+\sqrt{-7}}{2}\right)^m = \omega^m - \bar{\omega}^m.\end{aligned}$$

Veremos que ha de tener signo negativo: Nótese que $\omega + \bar{\omega} = 1$ y $\omega \cdot \bar{\omega} = 2$, luego

$$\omega^2 = (1-\bar{\omega})^2 = 1 - 2\bar{\omega} + \bar{\omega}^2 = 1 - \omega\cdot\bar{\omega}^2 + \bar{\omega}^2 \equiv 1 \pmod{\bar{\omega}^2},$$

luego $\omega^m = \omega\cdot(\omega^2)^{\frac{m-1}{2}} \equiv \omega \pmod{\bar{\omega}^2}$ (donde empleamos que m es impar), pero entonces:

$$\omega^m - \bar{\omega}^m \equiv \omega^m \equiv \omega \pmod{\bar{\omega}^2},$$

así pues, si $\omega^m - \bar{\omega}^m = \sqrt{-7} = \omega - \bar{\omega}$, concluiríamos que $\bar{\omega} \equiv 0 \pmod{\bar{\omega}^2}$ lo cual es absurdo.

Completar ecuaciones de Ramanujan-Nagell.

Luego se tiene que $-2^m\sqrt{-7} = (1+\sqrt{-7})^m - (1-\sqrt{-7})^m$. □

§4.2.4 $\mathbb{Z}[\sqrt{-2}]$. Si consideramos ahora, el cuerpo cuadrático $\mathbb{Q}(\sqrt{-2})$, entonces su anillo de enteros es $\mathbb{Z}[\sqrt{-2}]$. A sus elementos les llamamos ***enteros cuadráticos***, y por un razonamiento análogo al de la subsección anterior se concluye:

Teorema 4.44: $\mathbb{Z}[\sqrt{-2}]$ es un dominio euclídeo con la norma $\mathrm{Nm}_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}}$. En consecuencia, es un DIP y un DFU.

Proposición 4.45: $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$.

No sólo podemos extender a $\mathbb{Z}$, sino que, como hemos visto en **[1,** Teo. 4.5] podemos extender cualquier cuerpo y, en particular, podemos extender a $\mathbb{F}_p$. Así, veremos otra forma de comprender la reciprocidad cuadrática:

Teorema 4.46: Se cumple que

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

Demostración: La estrategia será la siguiente: la pregunta que queremos contestar es si $\sqrt{2} \in \mathbb{F}_p$, para lo cual extenderemos el cuerpo a otro K de manera que siempre $\sqrt{2} \in K$ y luego verificamos si $\sqrt{2}^p = \sqrt{2}$ para concluir si estaba o no en $\mathbb{F}_p$ originalmente.

Considere ζ una raíz primitiva ocatava de la unidad, vale decir, $\zeta^8 = 1$ con $\zeta^4 = -1$, y considere $K := \mathbb{F}_p[\zeta]$; ésto también fuerza a que $\zeta^i = \zeta^j$ si $i \equiv j \pmod 8$. En primer lugar, veremos que $\sqrt{2} \in K$, para lo cual:

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = \zeta^2 + \zeta^{4+2} + 2 = \zeta^2 - \zeta^2 + 2.$$

De modo que $\sqrt{2} = \zeta + \zeta^{-1} \in K$.

Luego calcularemos $\sqrt{2}^p$ tal como habíamos señalado, para ello empleamos el sueño del aprendiz (cf. [**1,** Teo. 2.39]):

$$\sqrt{2}^p = (\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p},$$

y tal como señalamos antes, las potencias de ζ dependen de su resto módulo 8, así que hay cuatro casos:

(a) Si $p \equiv 1 \pmod 8$, entonces $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$.

(b) Si $p \equiv -1 \pmod 8$, entonces $\zeta^p + \zeta^{-p} = \zeta^{-1} + \zeta$.

(c) Si $p \equiv 3 \pmod 8$, entonces $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3} = -\zeta^{-1} - \zeta$.

(d) Si $p \equiv -3 \pmod 8$, entonces $\zeta^p + \zeta^{-p} = \zeta^{-3} + \zeta^3 = -\zeta - \zeta^{-1}$.

Así que

$$\sqrt{2}^p = \begin{cases} \sqrt{2}, & p \equiv \pm 1 \pmod 8 \\ -\sqrt{2}, & p \equiv \pm 3 \pmod 8 \end{cases}$$

como se quería probar. □

Generalizando el método puede intentar lo siguiente:

Ejercicio 4.47: Deduzca que, para p primo:

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

Pista: Considere las raíces cuartas de la unidad. □

Ejercicio 4.48: Deduzca cuando 3 es un residuo cuadrático módulo p primo.

Pista: Considere una raíz sexta primitiva de la unidad ζ, la cual es raíz del polinomio:

$$x^6 - 1 = (x-1)(x^2+x+1)(x^3-1),$$

de ésto, deduzca que $\zeta^2 + \zeta^4 = -1$ y con ello note que $(\zeta + \zeta^2)^2 = -3$. Luego obtenga un criterio para cuando -3 es residuo cuadrático módulo p. □

§4.2.5 Ecuaciones de Mordell II.

Ejercicio 4.49: Las únicas soluciones enteras de la ecuación $y^2 = x^3 - 4$ son

$$(x, y) \in \{(2, \pm 2), (5, \pm 11)\}.$$

Solución: Reescribamos $x^3 = 4 + y^2 = (2 - \mathrm{i}y)(2 + \mathrm{i}y)$.

- Si y es impar: Notamos que un divisor común α de $2 - \mathrm{i}y$ y $2 + \mathrm{i}y$ es divisor común de su suma 4 y por lo tanto $\mathrm{Nm}(\alpha) \mid 16$ y $\mathrm{Nm}(\alpha) \mid x^3$. Si y es impar, entonces x también y luego $\alpha = 1$, por lo que son coprimos. Luego ambos factores son cubos en $\mathbb{Z}[\mathrm{i}]$ y aplicando conjugados comprobamos:

  $$2 + \mathrm{i}y = (a + \mathrm{i}b)^3, \qquad 2 - \mathrm{i}y = (a - \mathrm{i}b)^3,$$

  restando ambas expresiones, e igualando partes imaginarias, se obtiene que

  $$4 = 2b(b^2 - 3a^2) \iff 2 = b(b^2 - 3a^2).$$

  Los divisores (racionales) de 2 permiten deducir que $b \in \{\pm 1, \pm 2\}$. Fijando el valor de b vemos que los únicos posibles valores son $(b, a) = (-1, \pm 1)$ y $(a, b) = (2, \pm 1)$. Nótese que

  $$x^3 = \big((a - \mathrm{i}b)(a + \mathrm{i}b)\big)^3 = (a^2 + b^2)^3,$$

  de modo que ésto induce los valores $x \in \{2, 5\}$ y de la ecuación $y^2 + 4 = 8, 125$ deducimos que las soluciones son las descritas.

- Si y es par: Entonces $y = 2Y$, y claramente $x = 2X$ lo que reduce la ecuación a $2X^3 = (1 - \mathrm{i}Y)(1 + \mathrm{i}Y)$. Nótese que Y debe ser impar, y que todo factor común a $1 \pm \mathrm{i}Y$ es un divisor de 2, los cuales son (salvo asociados) $1, 1 + \mathrm{i}, 2$. Definamos $\lambda := 1 + \mathrm{i}$ y recordemos que $2 = -\mathrm{i}\lambda^2$. Claramente $2 \nmid 1 \pm \mathrm{i}Y$, pero $\lambda \mid 1 \pm \mathrm{i}Y$ debido a que Y es impar. Dividiendo por λ^2 se obtiene que:

  $$\frac{1 + \mathrm{i}Y}{\lambda} \frac{1 - \mathrm{i}Y}{\lambda} = -\mathrm{i}X^3 = (\mathrm{i}X)^3,$$

luego $\frac{1\pm \mathrm{i}Y}{\lambda_-}$ son cubos en $\mathbb{Z}[\mathrm{i}]$ y $1+\mathrm{i}Y = \lambda(a+\mathrm{i}b)^3$, y análogamente $1-\mathrm{i}Y = \overline{\lambda}(a-\mathrm{i}b)^3$. Sumando y cancelando por 2 se obtiene la ecuación

$$1 = (a+b)(a^2-4ab+b^2),$$

cuyas soluciones son $(a,b) \in \{(1,0),(0,1)\}$ que inducen $y = \pm 2$. □

Teorema 4.50: La única solución entera de $y^2+1 = x^p$ con $p \geq 2$ es $(1,0)$.

Demostración: Sea $p = qm$ con q primo y sea (x_0, y_0) solución no trivial de $x^{qm} = y^2+1$, entonces (x_0^m, y_0) es solución no trivial de $x^q = y^2+1$, así que podemos suponer que p es primo. El caso $p = 2$ es trivial, así que veremos $p \geq 3$.

Nótese que si x fuese par, entonces $y^2 \equiv -1 \pmod 8$ lo cual es imposible. Así que x es impar y por ende y es par. La ecuación se reescribe

$$x^p = (y+\mathrm{i})(y-\mathrm{i}).$$

Nótese que un factor común de ambos debe ser divisor de 2, pero como y es par y ± 1 impar se sigue que éste no es el caso. Los invertibles de Gauss son potencias p-ésimas, pues $(-\mathrm{i})^p = \mp \mathrm{i}$ si $p \equiv \pm 1 \pmod 4$, por lo que ambos factores son potencias p-ésimas conjugadas así que

$$y+\mathrm{i} = (m+\mathrm{i}n)^p = \sum_{j=0}^{p} \binom{p}{j} m^j (\mathrm{i}n)^{p-j},$$

igualando partes imaginarias se obtiene que

$$1 = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} m^{2j} n^{p-2j} (-1)^{\frac{p-1}{2}-j}.$$

Podemos notar que todos los términos poseen un n, de modo que $n \mid 1$ y $n = \pm 1$. Multiplicando por $(-1)^{\frac{p-1}{2}} n$ se obtiene que

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = (-1)^{\frac{p-1}{2}} n.$$

Volviendo a la ecuación original y recordando los conjugados se tiene que:

$$x^p = (y+\mathrm{i})(y-\mathrm{i}) = (m+\mathrm{i}n)^p (m-\mathrm{i}n)^p = (m^2+1)^p,$$

de modo que m es par, luego

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j \equiv 1 \pmod 4,$$

por lo que debe ser 1 y $n = (-1)^{\frac{p-1}{2}}$. Como

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = 1,$$

notamos que si $p = 3$ entonces ésta ecuación induce $m = 0$. Si $p \geq 5$, entonces podemos despejar:

$$\sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-m^2)^j = \binom{p}{2} m^2. \tag{4.3}$$

Ahora bien, nótese lo siguiente:

$$\begin{aligned} \binom{p}{2j} &= \frac{p!}{(p-2j)!(2j)!} = \frac{p(p-1)}{2j(2j-1)} \frac{(p-2)!}{(p-2j)!(2j-2)!} \\ &= \binom{p}{2} \cdot \frac{1}{j(2j-1)} \binom{p-2}{2j-2}. \end{aligned}$$

De ésto podemos notar que la valuación 2-ádica del lado izquierdo de (4.3) es:

$$\begin{aligned} \nu_2 \left(m^{2j} \binom{p}{2j} \right) &\geq 2j\nu_2(m) - \nu_2(j) + \nu_2 \left(\binom{p}{2} \right) \\ &\geq (2j - \nu_2(j))\nu_2(m) + \nu_2 \left(\binom{p}{2} \right) \\ &> j\nu_2(m) + \nu_2 \left(\binom{p}{2} \right), \end{aligned}$$

donde empleamos que $\nu_2(m) \geq 1$ (pues es par) y que $2j - \nu_2(j) > j$ cuando $j > 1$. Luego, el lado izquierdo posee mayor valuación 2-ádica que el derecho, lo cual es absurdo. □

Ejercicio 4.51: Las únicas soluciones de $y^2 = x^3 - 2$ son $(x, y) = (3, \pm 5)$.

Solución: Si x fuera par, entonces $y^2 \equiv -2 \pmod 8$, pero -2 no es un cuadrado módulo 8. Así que x es impar, e y también. Reescribiendo:

$$x^3 = (y - \sqrt{-2})(y + \sqrt{-2}),$$

donde los dos factores son coprimos en $\mathbb{Z}[\sqrt{-2}]$, puesto que de lo contrario dividiría a $2\sqrt{-2}$ cuyos únicos factores primos son $\sqrt{-2}$, pero y no es par. Luego cada factor debe ser un cubo:

$$y + \sqrt{-2} = (m + \sqrt{-2}n)^3,$$

y lo mismo en la otra con el conjugado y comparando las componentes lineales se obtiene

$$y = m^3 - 6mn^2 = m(m^2 - 6n^2), \quad 1 = 3m^2n - 2n^3 = n(3m^2 - 2n^2).$$

Por la segunda ecuación se obtiene que $n = \pm 1$. Si $n = -1$, entonces la segunda ecuación nos da que $3m^2 = 1$ lo cual es imposible. Así que $n = 1$ y $m = \pm 1$ lo que nos da las soluciones $y = \pm 5$, y $x = 3$. □

4.3 Dominios de Dedekind

Se recomienda ver la sección §12.1 de **[1]**.

Definición 4.52: Sea A un dominio íntegro y $K := \operatorname{Frac} A$. Se dice que un A-submódulo M de K es un ***ideal fraccionario*** si existe algún $a \in A_{\neq 0}$ tal que $aM \subseteq A$. A los ideales de A (en sentido usual) les diremos ***ideales enteros***. Si $M = bA$ para algún $b \in K$, entonces M se dice un ***ideal (fraccionario) principal***. Para un A-submódulo M se define:

$$(A : M) := \{x \in A : xM \subseteq A\}.$$

(Nótese que M es fraccionario syss $(A : M) \neq (0)$.)

Un A-submódulo M se dice ***inversible*** si existe otro A-submódulo N tal que $MN = A$.

Nótese que si M es inversible y N es una inversa, entonces:

$$N \subseteq (A : M) = (A : M)MN \subseteq AN = N,$$

de modo que $N = (A : M)$. Además si M es inversible, entonces es claro que es finitamente generado (¿por qué?).

Definición 4.53: Un dominio A se dice ***de Dedekind*** si es un dominio íntegro en donde todo ideal fraccionario no nulo es inversible.

Teorema 4.54: Un dominio íntegro A es de Dedekind syss es noetheriano, íntegramente cerrado y todo ideal primo no nulo es maximal (cfr. [**1,** teo. 12.25]).

Ahora veremos la propiedad fundamental de los dominios de Dedekind:

Proposición 4.55: En un dominio de Dedekind A, los ideales fraccionarios no nulos forman un grupo abeliano denotado $\mathbf{I}(A)$ (con la multiplicación entre ideales), y los ideales fraccionarios no nulos principales P_A un subgrupo.

Teorema 4.56: En un dominio de Dedekind, todo ideal fraccionario no nulo $I \in \mathbf{I}(A)$ se escribe forma única (salvo permutación) como

$$I = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_n^{\alpha_n},$$

donde los $\mathfrak{p}_i$'s son ideales primos distintos, cada $\alpha_i \in \mathbb{Z}_{\neq 0}$ (cfr. [**1,** teo. 12.31]).

Corolario 4.56.1: En un dominio de Dedekind A, el grupo $\mathbf{I}(A)$ es un grupo abeliano libre que tiene por base los ideales primos.

Definición 4.57: Dado un dominio de Dedekind A, se define su ***grupo de clases de ideales*** o ***grupo de Picard*** al cociente:

$$\operatorname{Pic}(A) := \mathbf{I}(A)/P_A.$$

A la cardinalidad del grupo de Picard se le llama el ***número de clases*** $h_A := |\operatorname{Pic}(A)|$.

Teorema 4.58: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$ y L/K una extensión finita de cuerpos. Sea B la clausura íntegra de A en L, entonces B es un dominio de Dedekind (cfr. [**1,** teo. 12.35]).

Corolario 4.58.1: Dado un cuerpo numérico k, se cumple que $\mathcal{O}_k$ es un dominio de Dedekind.

Proposición 4.59: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$ y L/K una extensión finita separable de cuerpos. Entonces $B := \mathcal{O}_{L/A}$ es un A-módulo finitamente generado (cfr. [**1,** prop. 12.36]).

Definición 4.60: Sea B/A una extensión de dominios de Dedekind. Dado $\mathfrak{p} \lhd A$ primo no nulo, se cumple que

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

donde cada $\mathfrak{P}_i \lhd B$ es un ideal primo distinto y cada $e_i \geq 1$. Si $\mathfrak{P}$ aparece en la factorización de $\mathfrak{p}B$, decimos que $\mathfrak{P}$ ***divide a*** $\mathfrak{p}$, denotado $\mathfrak{P} \mid \mathfrak{p}$. A cada $e_i =: e(\mathfrak{P}_i/\mathfrak{p})$ le llamamos el ***índice de ramificación*** de $\mathfrak{p}$ sobre $\mathfrak{P}_i$.

La notación e, f, g para los números es estándar en la teoría algebraica de números, trataremos de no confundir en ésta sección.

Lema 4.61: Sea B/A una extensión de dominios de Dedekind. Dados $\mathfrak{p} \lhd A, \mathfrak{P} \lhd B$ primos no nulos se cumple que

$$\mathfrak{P} \mid \mathfrak{p} \iff \mathfrak{p} = \mathfrak{P} \cap A.$$

Demostración: $\Longrightarrow$. Claramente $\mathfrak{p} \subseteq \mathfrak{P} \cap K$ y $\mathfrak{P} \cap K \lhd A$, pero como $\mathfrak{p}$ es primo no nulo, entonces es un ideal maximal y se alcanza igualdad.

$\Longleftarrow$. Si $\mathfrak{p} \subseteq \mathfrak{P}$, entonces $\mathfrak{p}B \subseteq \mathfrak{P}$ y luego claramente $\mathfrak{P}$ aparece en la factorización de $\mathfrak{p}B$. □

Lema 4.62: Sea B/A una extensión de dominios de Dedekind, con $K := \operatorname{Frac} A$ y $L := \operatorname{Frac} B$. Sea $\mathfrak{p} \lhd A$ primo no nulo y $\mathfrak{b} \lhd B$ tal que $\mathfrak{b} \cap A = \mathfrak{p}$. Entonces $B/\mathfrak{b}$ es un $A/\mathfrak{p}$-espacio vectorial y:

$$[B/\mathfrak{b} : A/\mathfrak{p}] \leq [L : K].$$

Demostración: Primero sea

$$\begin{aligned} \varphi\colon B/\mathfrak{b} &\longrightarrow B_{\mathfrak{p}}/\mathfrak{b}B_{\mathfrak{p}} \\ r \text{ mód } \mathfrak{b} &\longmapsto r \text{ mód } \mathfrak{b}B_{\mathfrak{p}}, \end{aligned}$$

probaremos que es un isomorfismo. Sea $r \equiv 0 \pmod{\mathfrak{b}B_{\mathfrak{p}}}$, entonces $r = b/s$ con $b \in \mathfrak{b}$ y $s \in A \setminus \mathfrak{p}$, y así $rs \equiv 0 \pmod{\mathfrak{b}}$. Ahora bien, s tiene inversa mód$\mathfrak{p}$ y luego mód$\mathfrak{b}$, por lo que, necesariamente $r \in \mathfrak{b}$, lo que prueba que φ es inyectiva.

Sea $b/s \in B_{\mathfrak{p}}$ con $b \in B, s \in A \setminus \mathfrak{p}$. Como $A/\mathfrak{p}$ es cuerpo, existe $t \in A$ tal que $st - 1 =: p \in \mathfrak{p}$. Luego

$$bt = \frac{bp}{s} + \frac{b}{s} \equiv \frac{b}{s} \pmod{\mathfrak{b}B_{\mathfrak{p}}},$$

lo que prueba que φ es suprayectiva y, por lo tanto, un isomorfismo.

Así pues, podemos probar el lema para $B_\mathfrak{p}/A_\mathfrak{p}$, y así, podemos suponer sin perdida de generalidad que A es un dominio de valuación discreta y $\mathfrak{p} = (\pi)$ es maximal. Denotaremos por $\overline{()}$ la proyección $B \to B/\mathfrak{b}$. Sean $\beta_1, \ldots, \beta_n \in B$ tales que son K-linealmente dependientes, es decir, sean $a_i \in K$ tales que $\sum_{i=1}^n a_i\beta_i = 0$ y tales que no todos los a_i's son nulos. Limpiando denominadores, podemos suponer que los $a_i \in A$'s y podemos dividir la mayor potencia común de π de modo que

$$\sum_{i=1}^{n} a_i\beta_i \equiv 0 \pmod{\mathfrak{b}},$$

y $\bar{a}_i \neq 0$ para algún i. Así pues, $\bar{\beta}_1, \ldots, \bar{\beta}_n$ son $A/\mathfrak{p}$-linealmente dependientes, lo que completa la demostración. □

Definición 4.63: Sea B/A una extensión de dominios de Dedekind y $\mathfrak{P} \lhd B$ un primo con $\mathfrak{p} := \mathfrak{P} \cap A$. Llamamos ***grado de inercia*** de $\mathfrak{P}$ sobre $\mathfrak{p}$ al número $[B/\mathfrak{P} : A/\mathfrak{p}]$, denotado $f(\mathfrak{P}/\mathfrak{p})$ o $f(\mathfrak{P}/A)$,

Proposición 4.64: Sean $C/B/A$ extensiones de dominios de Dedekind y sea $\mathfrak{P} \lhd C$ primo, entonces

$$f(\mathfrak{P}/B) \cdot f(\mathfrak{P} \cap B/A) = f(\mathfrak{P}/A).$$

Teorema 4.65: Sea B/A una extensión entera de dominios de Dedekind y sea $\mathfrak{p} \lhd A$ primo tal que

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

con los $\mathfrak{P}_i \lhd B$ primos distintos y cada $e_i > 0$. Sea $f_i := f(\mathfrak{P}_i/\mathfrak{p})$. Entonces:

1. $\sum_{i=1}^g e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}]$.
2. Si $K := \operatorname{Frac} A, L := \operatorname{Frac} B$ son tales que la extensión es finita, entonces $\sum_{i=1}^g e_i f_i \leq [L : K]$.
3. Si $B_\mathfrak{p}$ es un $A_\mathfrak{p}$-módulo finitamente generado, entonces

$$\sum_{i=1}^{g} e_i f_i = [L : K].$$

Demostración:

1. Por el teorema chino del resto, tenemos que

$$B/\mathfrak{p}B = B/\prod_{i=1}^{g}\mathfrak{P}_i^{e_i} \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}.$$

   Ahora bien, $B/\mathfrak{P}^{e+1}$ es un $B/\mathfrak{P}^e$-módulo de rango 1, puesto que lo contrario, habría un ideal $\mathfrak{b} \lhd B$ tal que $\mathfrak{P}^{e+1} \subset \mathfrak{b} \subset \mathfrak{P}^e$. Luego:

$$[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i \cdot [B/\mathfrak{P}_i : A/\mathfrak{p}] = e_i f_i.$$

2. Es consecuencia del lema 4.62.

3. Por el inciso 1, basta probar que $[L : K] = [B/\mathfrak{p}B : A/\mathfrak{p}]$. Si A fuese un DIP, entonces B es necesariamente libre y todo isomorfismo $\varphi\colon A^n \to B$ al tensorizar, nos da:

$$K^n \cong A^n \otimes_A K \xrightarrow{\varphi\otimes_A K} B \otimes_A K \cong L$$
$$(A/\mathfrak{p})^n \cong A^n \otimes_A (A/\mathfrak{p}) \xrightarrow{\varphi\otimes_A (A/\mathfrak{p})} B \otimes_A A/\mathfrak{p} \cong B/\mathfrak{p}B.$$

   El isomorfismo $\varphi\otimes_A K$ prueba que $n = m$, y el isomorfismo $\varphi\otimes_A (A/\mathfrak{p})$ prueba que $n = [B/\mathfrak{p}B : A/\mathfrak{p}]$.

   En el caso general, podemos localizar en $\mathfrak{p}$ de modo que $A_\mathfrak{p}$ es un dominio de valuación discreta, luego un DIP, y como $B_\mathfrak{p} = \mathcal{O}_{L/A_\mathfrak{p}}$ (cfr. [**1,** teo. 10.78]) y, por lo tanto,

$$\mathfrak{p}B_\mathfrak{p} = \prod_{i=1}^{g}(\mathfrak{P}_i B_\mathfrak{p})^{e_i},$$

   y finalmente, tensorizar por $A_\mathfrak{p}$ prueba que

$$[B_\mathfrak{p}/\mathfrak{P}_i B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = [B/\mathfrak{P}_i : A/\mathfrak{p}] = f_i. \qquad \square$$

Corolario 4.65.1: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$, L/K una extensión finita separable y $B := \mathcal{O}_{L/A}$. Para todo $\mathfrak{p} \lhd A$ primo no nulo se cumple que

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \cdot f(\mathfrak{P}/\mathfrak{p}) = [L : K].$$

Más aún, si L/K es de Galois, entonces los $\mathfrak{P}$'s son K-conjugados entre sí, $e(\mathfrak{P}/\mathfrak{p}) = e$ y $f(\mathfrak{P}/\mathfrak{p}) = f$ (valores constantes) y satisfacen $efg = [L : K]$, donde g es la cantidad de $\mathfrak{P}$'s.

Demostración: Para probar la igualdad, basta aplicar el teorema anterior inciso 3 empleando que B es un A-módulo finitamente generado.

Si la extensión L/K fuese de Galois, entonces claramente para todo $\sigma \in \mathrm{Gal}(L/K)$ se cumple que $\sigma[B] = B$ y si $\mathfrak{P} \mid \mathfrak{p}$, entonces también $\sigma\mathfrak{P} \mid \mathfrak{p}$ (¿por qué?). Más aún,

$$e(\sigma\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}), \qquad f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}),$$

así que probar que todos son conjugados basta.

Sean $\mathfrak{P}, \mathfrak{Q}$ primos de B que dividen a $\mathfrak{p}$ tales que $\sigma\mathfrak{P} \neq \mathfrak{Q}$ para todo $\sigma \in \mathrm{Gal}(L/K)$, entonces por el teorema chino del resto existe $\beta \in \mathfrak{Q}$ tal que $\beta \notin \sigma\mathfrak{P}$, o equivalentemente, $\sigma(\beta) \notin \mathfrak{P}$. Luego $b := \mathrm{Nm}_{L/K}(\beta) = \prod_\sigma \sigma(\beta) \in \mathfrak{Q} \cap A = \mathfrak{p} \subseteq \mathfrak{P}$, pero ninguno de los factores está en $\mathfrak{P}$ lo que es absurdo pues $\mathfrak{P}$ es primo. □

§4.3.1 ***Intermezzo:*** **finitud del grupo de clases.** Ésta sección reproduce la breve demostración algebraica de author **[107]** de la finitud del grupo de clases. Más adelante, veremos otra demostración, más clásica y más potente de este resultado, pero también con técnicas más avanzadas; para casi todos los propósitos de ésta primera parte, la mera finitud será útil.

Definición 4.66 (Stasinski): Sea A un anillo y sea $\mathfrak{a} \trianglelefteq A$ un ideal no nulo. Definimos su ***norma numérica*** como $\mathbf{N}(\mathfrak{a}) := |A/\mathfrak{a}|$ y extendemos $\mathbf{N}(0) := 0$. También para $a \in A$ denotamos $\mathbf{N}_A(a) := \mathbf{N}(aA)$.

Se dice que A es un ***DIP básico*** si:

DB1 A es un DIP y para todo $a \in A_{\neq 0}$ se cumple que $\mathbf{N}(a) < \infty$, vale decir, el anillo cociente $A/(a)$ es finito.

DB2 Para todo $m \in \mathbb{N}$ se satisface

$$|\{a \in A : \mathbf{N}(a) \leq m\}| > m.$$

DB3 Existe $C > 0$ tal que para todo $a, b \in A$ se satisface que

$$\mathbf{N}(a+b) \leq C \cdot \big(\mathbf{N}(a) + \mathbf{N}(b)\big).$$

Sea B/A una extensión de anillos. Se dice que B es un ***anillo aritmético básico (sobre A)*** si:

1. B es un dominio de Dedekind.

2. B es un A-módulo libre finitamente generado.

Ejemplo. Es fácil comprobar que $\mathbb{Z}$ y el anillo polinomial $\mathbb{F}_q[t]$ son DIPs básicos (donde q es la potencia de un primo).

Proposición 4.67: Sea A un DIP básico con $\operatorname{Frac} A =: K$ y sea B/A una extensión de dominios íntegros con $\operatorname{Frac} B =: L$.

1. Si B es un anillo aritmético sobre A, entonces la extensión de cuerpos L/K es finita y B es la clausura entera de A en L.

2. Si B es la clausura entera de A en L y la extensión L/K es separable finita, entonces B es un anillo aritmético básico sobre A.

Demostración: El inciso 2 ya lo hemos probado, así que solo falta el 1. Sea $S := A \setminus \{0\}$, entonces $S^{-1}B$ es finitamente generado sobre $S^{-1}A = K$ (como módulo), el cual es un cuerpo; así que $S^{-1}B$ es artiniano y además es un dominio íntegro, por tanto, también es un cuerpo y, así, $S^{-1}B = L$. En consecuencia, la extensión L/K es finita.

Como B es finitamente generado (como módulo) sobre A, entonces es una extensión entera de A; definiendo $C := \mathcal{O}_{L/A}$ tenemos que $B \subseteq C \subseteq L$. Como la extensión C/A es entera, se sigue que la extensión C/B también, pero como B es de Dedekind, es íntegramente cerrado, por lo que $C = B$ como se quería probar. □

Lema 4.68: Sea A un dominio de Dedekind con $K := \operatorname{Frac} A$, sea L/K una extensión finita separable de cuerpos y sea $B := \mathcal{O}_{L/A}$. Para todo $\beta \in B$ se cumple que $\mathbf{N}_B(\beta) = \mathbf{N}_A(\operatorname{Nm}_{L/K}(\beta))$, donde se subentiende que uno es finito cuando el otro lo es.

Lema 4.69.A: Sea A un anillo noetheriano. Para todo $n \in \mathbb{N}$ existen solo finitos ideales distintos $\mathfrak{a} \trianglelefteq A$ con $\mathbf{N}(\mathfrak{a}) = n$.

Demostración: Sea R un anillo finito y $(\mathfrak{a}_i)_{i\in I}$ ideales distintos tales que cada $A/\mathfrak{a}_i \cong R$. Sea $\mathfrak{b} := \bigcap_{i\in I} \mathfrak{a}_i$, entonces tenemos un homomorfismo inyectivo:

$$A/\mathfrak{b} \longrightarrow \prod_{i\in I} A/\mathfrak{a}_i \cong R^{|I|}.$$

Sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_n \in \operatorname{Spec} R$ los ideales maximales de R, sea $q_j := \mathbf{N}(\mathfrak{m}_j)$ y sea $s \geq 1$ el mínimo tal que $(\mathfrak{m}_1, \ldots, \mathfrak{m}_n)^s = 0$, en consecuente, todo $a \in R$

es raíz de

$$F(x) := \prod_{i=1}^{n} (x^{q_i} - x)^s \in \mathbb{Z}[x],$$

lo cual también aplica para todo elemento de $R^{|I|}$ y, también, para todo elemento de $B := A/\mathfrak{b}$.

Nótese que B también es noetheriano y que hemos probado que sus elementos son raíces de $F \in \mathbb{Z}[x]$ mónico. Dado un primo $\mathfrak{p} \in \operatorname{Spec} B$, vemos que los elementos del dominio íntegro $B/\mathfrak{p}$ también son raíces de un polinomio no nulo, por lo que $B/\mathfrak{p}$ es siempre finito y B ha de ser artiniano. Como B tiene longitud finita sobre $B/\mathfrak{p}$, se concluye que es también un anillo finito. Finalmente, los ideales de $B = A/\mathfrak{b}$ están en correspondencia con los ideales $\mathfrak{a} \subseteq \mathfrak{b}$ de A; por lo que son finitos. □

El resultado anterior es original de Samuel **[104].**

Lema 4.69.B: Sea B un anillo aritmético básico con $L := \operatorname{Frac} B$ sobre un DIP básico A con $K := \operatorname{Frac} A$, y sea $\beta_1, \ldots, \beta_n \in B$ una A-base. Existe un polinomio homogéneo $f(t_1, \ldots, t_n) \in A[\boldsymbol{t}]$ tal que para todo $(c_1, \ldots, c_n) \in A^n$ se cumple que

$$\operatorname{Nm}_{L/K}(c_1\beta_1 + \cdots + c_n\beta_n) = f(c_1, \ldots, c_n).$$

Más aún, existe $C > 0$ tal que

$$\mathbf{N}_B(c_1\beta_1 + \cdots + c_n\beta_n) \leq C \cdot \max_i\{\mathbf{N}_A(c_i)^n\}.$$

Demostración: Sean $a_{i,j,k} \in A$ tales que para cada $1 \leq i, j \leq n$:

$$\beta_i\beta_j = \sum_{k=1}^{n} a_{ijk}\beta_k.$$

Habiendo fijado $\gamma := c_1\beta_1 + \cdots + c_n\beta_n \in B$, denotamos por $\mu_\gamma \colon B \to B$ el A-endomorfismo dado por $x \mapsto \gamma \cdot x$. La i-ésima columna de la representación matricial de μ_γ respecto a la base de los β_i's está dada por

$$\gamma \cdot \beta_i = \sum_{j=1}^{n} c_j\beta_j\beta_i = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} c_j a_{ijk} \right) \beta_k.$$

Así vemos que la entrada (i, k) es la forma lineal $\sum_{j=1}^{n} a_{ijk}t_j$ y, por lo tanto, el determinante es un polinomio homogéneo de grado n con coeficientes en

A, el cual escribiremos en notación multiíndice como

$$f(\boldsymbol{t}) = \sum_{|\boldsymbol{j}|=n} b_{\boldsymbol{j}} \boldsymbol{t}^{\boldsymbol{j}} \in A[\boldsymbol{t}].$$

Finalmente, empleando el axioma DB3 vemos que existe $C_1 > 0$ tal que

$$\begin{aligned}\mathbf{N}_B(\gamma) &= \mathbf{N}_A\left(\mathrm{Nm}_{L/K}(\gamma)\right) = \mathbf{N}_A\left(f(c_1,\dots,c_n)\right)\\ &\le C_1\left(\sum_{|\boldsymbol{j}|=n} \mathbf{N}_A(b_{\boldsymbol{j}}) \prod_{i=1}^{n} \mathbf{N}_A(c_i)^{j_i}\right)\\ &\le C_1 C_2 \max_{\boldsymbol{j}}\{\mathbf{N}_A(b_{\boldsymbol{j}})\} \cdot \max_{i=1}^{n}\{\mathbf{N}_A(c_i)\}^n,\end{aligned}$$

donde $C_2 < (n+1)^n$ es la máxima cantidad de términos de un polinomio homogéneo de grado n en n variables. Así, la constante $C := C_1 C_2 \cdot \max_{\boldsymbol{j}}\{\mathbf{N}_A(b_{\boldsymbol{j}})\}$ sirve. □

Teorema 4.69: Sea B un anillo aritmético básico (e.g., $\mathcal{O}_K$ para un cuerpo numérico K) sobre un DIP básico A. Existe una constante $C > 0$ tal que para todo ideal no nulo $\mathfrak{b} \trianglelefteq B$, existe $\gamma \in \mathfrak{b}$ tal que

$$\mathbf{N}_B(\gamma) \le C \cdot \mathbf{N}(\mathfrak{b}).$$

En consecuencia, el grupo de clases de ideales $\mathrm{Cl}\, B$ es finito.

Demostración: Sea $\beta_1,\dots,\beta_n$ una A-base de B y sea $m \in \mathbb{Z}$ el único natural tal que $m^n \le \mathbf{N}(\mathfrak{b}) < (m+1)^n$. El axioma DB2 afirma que el conjunto

$$S := \{a \in A : \mathbf{N}(a) \le m\}$$

tiene $\ge m+1$ elementos, de modo que el conjunto

$$T := \{s_1\beta_1 + \cdots + s_n\beta_n : \forall i\ s_i \in S\} \subseteq B$$

tiene $\ge (m+1)^n > |B/\mathfrak{b}|$ elementos. Por principio del palomar existen $v := \sum_{i=1}^n v_i\beta_i, w := \sum_{i=1}^n w_i\beta_i \in T$ distintos tales que $v \equiv w \pmod{\mathfrak{b}}$. Por el axioma DB3 existe C_0 tal que

$$\mathbf{N}_A(v_i - w_i) \le C_0 \cdot \left(\mathbf{N}_A(v_i) + \mathbf{N}_A(w_i)\right) \le C_0 2m,$$

luego por el lema anterior,

$$\mathbf{N}_B(v-w) \le C_1 \cdot \max_i\{\mathbf{N}_A(v_i - w_i)\}^n \le C_1 \cdot (C_0 2m)^n,$$

así, definiendo $C_2 := C_1(2C_0)^n$ se obtiene que $\mathbf{N}_B(v-w) \leq C_2 m^n \leq C_2\,\mathbf{N}(\mathfrak{b})$.

Veamos el «en consecuencia»: sea $\kappa \in \operatorname{Cl} B$ una clase de ideales y sea $\mathfrak{b} \in \kappa^{-1}$ un ideal en su clase inversa. Ahora sabemos que existe $\gamma \in \mathfrak{b}$ tal que $\mathbf{N}_B(\gamma) \leq C \cdot \mathbf{N}(\mathfrak{b})$. También, ha de existir un ideal $\mathfrak{a} \trianglelefteq B$ tal que $(\gamma) = \mathfrak{a}\mathfrak{b}$, de modo que $\mathfrak{a} \in \kappa$ y, por multiplicatividad de $\mathbf{N}$ sabemos que

$$\mathbf{N}(\mathfrak{a}\mathfrak{b}) = \mathbf{N}_B(\gamma) \leq C\,\mathbf{N}(\mathfrak{b}) \iff \mathbf{N}(\mathfrak{a}) \leq C.$$

Y finalmente, por el lema 4.69.A, sabemos que solo hay finitos ideales de B de norma acotada. □

Esto nos da una cota efectiva para el número de clases si es que: tenemos un método efectivo para contar ideales de norma acotada, conocemos la constante C_0 en el axioma DB3 y conocemos una A-base de B.

§4.3.2 Primos que se ramifican.

Definición 4.70: Sea B/A una extensión de dominios de Dedekind. Un primo no nulo $\mathfrak{p} \lhd A$ tal que

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \tag{4.4}$$

se dice que:

Se conserva Si $\mathfrak{p}B = \mathfrak{P}_1$ es un ideal primo, o si $g = 1$ y $e_1 = 1$ en (4.4).

Se escinde Si $g > 1$ y cada $e_i = 1$ en (4.4).

Se ramifica Si algún $e_i > 1$ en (4.4), o si es $B/\mathfrak{P}_i$ es una extensión inseparable de $A/\mathfrak{p}$.

Ésta clasificación separa de manera disjunta al comportamiento de $\mathfrak{p}$ si $A/\mathfrak{p}$ es perfecto.

En el caso de cuerpos numéricos, $A/\mathfrak{p}$ siempre es la extensión finita de algún $\mathbb{F}_p$, luego es un cuerpo finito y perfecto.

Definición 4.71: Sea B/A una extensión entera de dominios íntegros tal que $L := \operatorname{Frac} B$ es una extensión finita de $K := \operatorname{Frac} A$. Sea $(\beta_1, \ldots, \beta_n)$ una K-base ordenada de L entonces el ***discriminante*** de B/A respecto a dicha base es

$$\mathfrak{d}(\beta_1, \ldots, \beta_n) := \det\left([\operatorname{Tr}_{L/K}(\beta_i\beta_j)]_{ij}\right).$$

El ***ideal discriminante*** de B/A es aquél generado por los discriminantes sobre todas las bases de L/K que están contenidas en B, y lo denotaremos por $\mathfrak{d}(B/A)$.

En particular, cuando $A = \mathbb{Z}$ podemos hablar del ***(número) discriminante*** de B como el $d > 0$ tal que $\Delta(B/\mathbb{Z}) = d\mathbb{Z}$.

Lema 4.72: Sea B/A una extensión entera de dominios íntegros tal que $L := \operatorname{Frac} B$ es una extensión finita de $K := \operatorname{Frac} A$, y sea S un sistema multiplicativo en A. Entonces

$$\mathfrak{d}(S^{-1}B/S^{-1}A) = S^{-1}\mathfrak{d}(B/A).$$

Demostración: Sea $\beta_1, \ldots, \beta_n$ una K-base de L contenida en B; entonces claramente está en $S^{-1}B$ lo que prueba que $\mathfrak{d}(S^{-1}B/S^{-1}A) \subseteq S^{-1}\mathfrak{d}(B/A)$.

Recíprocamente, si $\gamma_1, \ldots, \gamma_n$ es una K-base de L contenida en $S^{-1}B$, luego existe un $s \in S$ tal que $s\gamma_1, \ldots, s\gamma_n$ están en B y así

$$\mathfrak{d}(s\gamma_1, \ldots, s\gamma_n) = \det[\operatorname{Tr}_{L/K}(s\gamma_i \cdot s\gamma_j)]_{ij} = s^{2n}\mathfrak{d}(\gamma_1, \ldots, \gamma_n) \in \mathfrak{d}(B/A),$$

luego claramente $\mathfrak{d}(s\gamma_1, \ldots, s\gamma_n) \in S^{-1}\mathfrak{d}(B/A)$, lo que completa la demostración. □

Lema 4.73: Sea B/A una extensión entera de dominios íntegros tal que:

1. $L := \operatorname{Frac} B$ es una extensión finita de $K := \operatorname{Frac} A$.
2. B es un A-módulo libre con base $\{e_1, \ldots, e_n\}$.

Entonces $\mathfrak{d}(B/A) = \mathfrak{d}(e_1, \ldots, e_n) \cdot A$.

Teorema 4.74: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$, L/K una extensión finita separable y $B := \mathcal{O}_{L/A}$. Entonces, un primo $p \lhd A$ se ramifica en B syss $\mathfrak{d}(B/A) \subseteq \mathfrak{p}$. En particular, solo finitos primos de A se ramifican en B.

Demostración: Sea $\mathfrak{p} \lhd A$ un primo no nulo, por el lema 4.72, vemos que $\mathfrak{p} \supseteq \mathfrak{d}(B/A)$ syss $\mathfrak{p}A_\mathfrak{p} \supseteq \mathfrak{d}(B/A)_\mathfrak{p} = \mathfrak{d}(B_\mathfrak{p}/A_\mathfrak{p})$. Además, $\mathfrak{p}$ se ramifica en B syss $\mathfrak{p}A_\mathfrak{p}$ se ramifica en $B_\mathfrak{p}$. De ésto, se nota que basta probar el teorema para $B_\mathfrak{p}/A_\mathfrak{p}$ y, en particular, podemos suponer que A es un dominio de valuación discreta y un DIP.

Como A es un DIP y B es un A-módulo libre de torsión finitamente generado, entonces admite una base $\boldsymbol{U} := (u_1, \ldots, u_n)$, de modo que denotaremos

$\mathfrak{d}(\boldsymbol{U}) := \mathfrak{d}(u_1, \ldots, u_n)$ y, por el lema anterior, basta probar que $\mathfrak{d}(\boldsymbol{U}) \not\equiv 0 \pmod{\mathfrak{p}}$. Sea

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}. \tag{4.5}$$

$\Longleftarrow$. Por contrarrecíproca, sea $\mathfrak{p} \lhd A$ tal que no se ramifica. Luego, $\bar{B} \cong B/\mathfrak{P}_1 \times \cdots B/\mathfrak{P}_g$, donde cada $B/\mathfrak{P}_i$ es una extensión separable de $A/\mathfrak{p}$. Denotemos Tr_i la traza de $B/\mathfrak{P}_i$ sobre $A/\mathfrak{p}$. Elijamos la base $\boldsymbol{U}$ y unos enteros $0 =: n_0 < n_1 < \cdots < n_g := n$ tales que $u_{n_{i-1}+1}, \ldots, u_{n_i}$ es $A/\mathfrak{p}$-base de $B/\mathfrak{P}_i$. Denotaremos por Δ_i el discriminante $\mathfrak{d}(u_{n_{i-1}+1}, \ldots, u_{n_i})$ de $B/\mathfrak{P}_i$ sobre $A/\mathfrak{p}$. Finalmente, es fácil probar que

$$\mathfrak{d}(\boldsymbol{U}) \equiv \Delta_1 \cdots \Delta_g \pmod{\mathfrak{p}}.$$

Como cada extensión es separable, entonces cada $\Delta_i \not\equiv 0 \ (\mathfrak{p})$ y su producto es no nulo, lo que prueba que $\mathfrak{d}(\boldsymbol{U}) \not\equiv 0 \ (\mathfrak{p})$.

$\Longrightarrow$. Sea $\mathfrak{p}$ tal que se ramifica, entonces sin perdida de generalidad suponemos que $e_1 > 1$ o bien $B/\mathfrak{P}_1$ no es separable sobre $A/\mathfrak{p}$. Adoptaremos los convenios de la demostración anterior con $\Delta_1, \ldots, \Delta_g$.

(a) $\underline{e_1 > 1}$: Nuevamente, elijamos la base $u_1, \ldots, u_n$ como antes, pero ahora con la condición adicional de que $u_1 \in \mathfrak{P}_1 \smallsetminus \mathfrak{P}_1^{e_1}$. De este modo $u_1^{e_1} = 0$ en $B/\mathfrak{P}_1$, por lo que es nilpotente, y así cada $u_1 u_i$ también lo es; luego la aplicación lineal $r_{u_1 u_i}(a) := u_1 u_i a$ es nilpotente y su polinomio minimal es de la forma $x^m \in (A/\mathfrak{p})[x]$, por lo que su polinomio característico también y $\mathrm{Tr}_1(u_1 u_i) = 0$ (es el coeficiente libre del polinomio característico).

Así, la matriz $[\mathrm{Tr}_1(u_i u_j)]_{ij}$ tiene una fila nula, por lo que $\Delta_1 \equiv 0 \ (\mathfrak{p})$ y así $\Delta(\boldsymbol{U}) \equiv 0 \ (\mathfrak{p})$.

(b) $\underline{B/\mathfrak{P}_1 \text{ no es separable sobre } A/\mathfrak{p}}$: Entonces, trivialmente $\Delta_1 \equiv 0 \ (\mathfrak{p})$. □

Ejemplo 4.75: Sea $d \in \mathbb{Z}$ un número libre de cuadrados, $L := \mathbb{Q}(\sqrt{d})$ y $B := \mathcal{O}_{L/\mathbb{Z}}$. Sabemos que B tiene por $\mathbb{Z}$-base a $\{1, \omega\}$, donde $\omega = \sqrt{d}$ si $d \not\equiv 1 \pmod 4$ y $\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod 4$.

Luego, si $d \not\equiv 1 \ (4)$ calculamos:

$$\mathfrak{d}(\mathbb{Z}[\omega]/\mathbb{Z}) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

Si $d \equiv 1 \ (4)$, en cambio:

$$\mathfrak{d}(\mathbb{Z}[\omega]/\mathbb{Z}) = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}\left(\frac{1+d}{4} + \frac{\sqrt{d}}{2}\right) \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{vmatrix} = d.$$

Esto nos da un criterio de qué primos racionales se ramifican: todo divisor primo de d y 2 cuando $d \equiv 3 \pmod 4$. ⌟

Teorema 4.76 – *Teorema de Kummer*: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$, L/K una extensión finita y $B := \mathcal{O}_{L/A}$. Sea $\mathfrak{p} \lhd A$ un primo no nulo, y sea $\theta \in L$ un elemento tal que $B_\mathfrak{p} = A_\mathfrak{p}[\theta]$. Sea $\phi(x) \in K[x]$ el polinomio minimal de θ sobre K (luego $\phi(x) \in A_\mathfrak{p}[x]$) y supongamos que

$$\phi(x) \equiv \psi_1(x)^{e_1} \cdots \psi_g(x)^{e_g} \pmod{\mathfrak{p}},$$

donde $\psi_i(x) \in A_\mathfrak{p}[x]$ son mónicos y tales que los $\bar{\psi}_i(x) \in (A/\mathfrak{p})[x]$'s son irreducibles y distintos.

Entonces

$$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}, \qquad \mathfrak{P}_i := (\mathfrak{p}, \psi_i(\theta)),$$

donde cada $\mathfrak{P}_i$ es primo y donde para cada i:

$$\frac{B}{(\mathfrak{p}, \psi_i(\theta))} \cong \frac{(A/\mathfrak{p})[x]}{(\bar{\psi}_i(x))}, \qquad f((\mathfrak{p}, \psi_i(\theta))/A) = \deg(\psi_i).$$

Demostración: La factorización y ramificación de $\mathfrak{p}$ se determina de manera local, de modo que podemos sustituir B/A con $B_\mathfrak{p}/A_\mathfrak{p}$ en la demostración.

La hipótesis equivale a que

$$\mathrm{ev}_\theta \colon A[x]/(\phi(x)) \longrightarrow B,$$

es un isomorfismo, luego tensorizamos por $k := A/\mathfrak{p}$:

$$\mathrm{ev}_\theta \otimes_A k \colon k[x]/(\bar{\phi}(x)) \longrightarrow B/\mathfrak{p}B.$$

Los ideales maximales de $\frac{k[x]}{(\bar{\phi}(x))}$ son $(\bar{\psi}_1(x)), \ldots, (\bar{\psi}_g(x))$, así vemos que los $\mathfrak{P}_i$'s tales que $\mathfrak{P}_i \supseteq \mathfrak{p}B$ son precisamente los de la forma $(\mathfrak{p}, \psi_i(\theta))$. Finalmente el hecho de que $\mathfrak{p}B = \prod_{i=1}^{g} (\mathfrak{p}, \psi_i(\theta))^{e_i}$ viene del hecho de que $\prod_{i=1}^{g} (\bar{\psi}_i(x))^{e_i} = (0)$ en $k[x]/(\bar{\phi})$ para precisamente esos exponentes e_i's. □

Los teoremas anteriores, especialmente el último, están enunciados con un grado de abstracción que parece obscurecer la naturaleza aritmética, así que veamos un ejemplo esclarecedor de cómo se usan estos resultados:

Ejercicio 4.77: Los primos de la forma $p = x^2 + 2y^2$ son precisamente $p = 2$ o $p \mod 8 \in \{1, 3\}$.

Demostración: Defínanse $D := -2$ y $K := \mathbb{Q}(\sqrt{D})$. Como $D \not\equiv 1 \pmod 4$, vemos que $A := \mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$.

Vamos a calcular qué primos se conservan o se escinden en A: por el teorema de Kummer, calcular la descomposición de un primo p equivale a estudiar la ecuación $x^2 + 2 = 0$ en $\mathbb{F}_p$, o equivalentemente, a preguntarse por el valor de $(-2/p)$. Sabemos que $(-1/p) = 1$ cuando $p \mod 8 \in \{1, 5\}$ y que $(2/p) = 1$ cuando $p \mod 8 \in \{1, 7\}$; lo que nos da los valores en el enunciado.

Finalmente, nótese que $p = x^2 + 2y^2 = \mathrm{Nm}_{K/\mathbb{Q}}(x + y\sqrt{-2})$. Es decir, que la condición del enunciado equivale a que $p = \alpha \cdot \overline{\alpha}$ para algún $\alpha \in A$, el cual es necesariamente primo, lo que equivale a que $pA = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ porque A es un DIP y porque conocemos la estructura de las unidades (que son ± 1). □

Los pasos claves en la demostración anterior fueron una aplicación del teorema de Kummer para convertir el problema aritmético en un problema algebraico, pero el resto de detalles técnicos es que $2 \not\equiv -1 \pmod 4$ y que $\mathbb{Z}[\sqrt{-2}]$ es un DIP. Lamentablemente la última condición es bastante restrictiva para funcionar en mayor generalidad.[6]

Para el siguiente teorema, necesitaremos lo siguiente:

Ejercicio 4.78: En un dominio de Dedekind A, se cumple que $A = \bigcap_{\mathfrak{p} \neq (0)} A_{\mathfrak{p}}$, donde $\mathfrak{p}$ recorre los primos no nulos.

Que es deducible también de [**1,** teo. 12.23].

Teorema 4.79: Sea A un dominio de Dedekind, $K := \operatorname{Frac} A$, L/K una extensión separable de grado n y $B := \mathcal{O}_{L/A}$. Sea $\theta \in B$ tal que $K(\theta) = L$ y sea $\mathfrak{d}(\theta) := \mathfrak{d}(1, \theta, \ldots, \theta^{n-1})$. Entonces:

1. $\mathfrak{d}(\theta)B \subseteq A[\theta] \subseteq B$.

2. Si $\mathfrak{p} \lhd A$ es un primo no nulo tal que $\mathfrak{p} \not\supseteq \mathfrak{d}(\theta)A$, entonces $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\theta]$.

Demostración:

1. Sea $\mathfrak{p} \lhd A$ un primo no nulo. Probaremos que $\mathfrak{d}(\theta)B_{\mathfrak{p}} \subseteq A_{\mathfrak{p}}[\theta]$. Como $A_{\mathfrak{p}}$ es un DIP, entonces $B_{\mathfrak{p}}$ admite una $A_{\mathfrak{p}}$-base $u_1, \ldots, u_n$ y, así, existen

[6] De hecho, un teorema de Heegner nos dice que $\mathbb{Z}[\sqrt{-D}]$ con $D \not\equiv -1 \pmod 4$ es un DIP solo para $D \in \{1, 2\}$.

$a_{ij} \in A_\mathfrak{p}$ tales que

$$\theta^{i-1} = \sum_{j=1}^{n} a_{ij} u_j.$$

Así pues, $A := [a_{ij}]_{ij}$ es una matriz de cambio de base en K y, por lo tanto, $d := \det A \neq 0 \in A_\mathfrak{p}$.

Sea $B := A^{-1} \in \mathrm{Mat}_n(K)$, luego $d \cdot B = \mathrm{adj}\, A \in \mathrm{Mat}_n(A_\mathfrak{p})$. Sea $\beta \in B_\mathfrak{p}$ arbitrario, luego existen $r_i \in A_\mathfrak{p}$ tales que

$$\beta = \sum_{i=1}^{n} r_i u_i = \sum_{i=1}^{n} \sum_{j=1}^{n} r_i b_{ij} \theta^{j-1},$$

como $db_{ij} \in A_\mathfrak{p}$, entonces $d\beta \in A_\mathfrak{p}[\theta]$.

Trivialmente, $\mathfrak{d}(\theta) = d^2 \cdot \mathfrak{d}(u_1, \ldots, u_n)$, de modo que

$$\beta\, \mathfrak{d}(\theta) = (d\beta) \cdot (d\, \mathfrak{d}(u_1, \ldots, u_n)) \in A_\mathfrak{p}[\theta],$$

ergo $\mathfrak{d}(\theta) B_\mathfrak{p} \subseteq A_\mathfrak{p}[\theta]$. Del ejercicio anterior, se deduce:

$$A[\theta] \subseteq \bigcap_{\mathfrak{p} \lhd A} A_\mathfrak{p}[\theta],$$

donde $\mathfrak{p}$ recorre los primos de A. Como $\mathfrak{d}(\theta) B \subseteq \bigcap_\mathfrak{p} \mathfrak{d}(\theta) B_\mathfrak{p} \subseteq \bigcap_\mathfrak{p} A_\mathfrak{p}[\theta] = A[\theta]$.

2. Si $\mathfrak{d}(\theta) \notin \mathfrak{p}$, entonces $\mathfrak{d}(\theta)$ es invertible en $A_\mathfrak{p}$, de modo que $\mathfrak{d}(\theta) B_\mathfrak{p} = B_\mathfrak{p}$. □

Por el teorema anterior, vemos que será útil tener cálculos explícitos del determinante:

Teorema 4.80: Sea $L := K(\theta)$ una extensión separable de grado n, con $f(x) \in K[x]$ el polinomio minimal de θ. Entonces

$$\mathfrak{d}(\theta) := \mathfrak{d}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Nm}_{L/K}(f'(\theta)),$$

donde $f'(x)$ es el polinomio derivado de $f(x)$.

Demostración: Sea N la clausura normal de L/K, sean $\mathrm{Id} =: \sigma_1, \ldots, \sigma_n$ los monomorfismos desde $L \to N$ y sean $\theta_i := \sigma_i(\theta)$, es decir, todos los K-conjugados. Luego el polinomio minimal $f(x)$ es

$$f(x) = (x - \theta_1) \cdots (x - \theta_n).$$

Definamos

$$B := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{bmatrix},$$

luego es fácil comprobar que $[\mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1})]_{ij} = B \cdot B^t$. La matriz B es una matriz de Vandermonde, luego su determinante es (cfr. [**1,** prop. 3.58])

$$\det B = \prod_{i<j}(\theta_j - \theta_i), \qquad \mathfrak{d}(\theta) = \prod_{i<j}(\theta_j - \theta_i)^2.$$

Ahora bien, hay $\binom{n}{2} = \frac{n(n-1)}{2}$ pares de índices (i, j) con $1 \leq i < j \leq n$ y empleando que $(\theta_j - \theta_i)^2 = -(\theta_i - \theta_j)(\theta_j - \theta_i)$, obtenemos que

$$\mathfrak{d}(\theta) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (\theta_i - \theta_j).$$

Finalmente, un cálculo sencillo comprueba que para todo i:

$$f'(\theta_i) = \prod_{\substack{j=1 \\ j\neq i}}^{n} (\theta_i - \theta_j),$$

y para todo monomorfismo $\sigma_i \colon L \to N$ se comprueba que $f'(\theta_i) = \sigma_i\big(f'(\theta)\big)$, de modo que

$$\mathrm{Nm}_{L/K}\left(f'(\theta)\right) = \prod_{i=1}^{n} f'(\theta_i) = \prod_{i=1}^{n} \prod_{\substack{j=1 \\ j\neq i}}^{n} (\theta_i - \theta_j). \qquad \square$$

Proposición 4.81: Sea $K := \mathbb{Q}(\theta)$ una extensión de grado n de $\mathbb{Q}$, sea $A := \mathcal{O}_K$ y suponga que $\theta \in A$. Entonces:

1. $A = \mathbb{Z}[\theta]$ syss $\mathfrak{d}(\theta)\mathbb{Z} = \mathfrak{d}(A/\mathbb{Z})$.

2. Si $\mathfrak{d}(\theta)$ es un entero libre de cuadrados, entonces $A = \mathbb{Z}[\theta]$.

Pista: Emplee el hecho de que $\mathbb{Z}$ es un DIP y el lema 4.73. $\square$

Teorema 4.82: Sea A_K un dominio de Dedekind con $K := \operatorname{Frac} A_K$, sea E una extensión finita separable de K y sean L, F dos extensiones intermedias K-linealmente disjuntas ($L \cap F = K$). Si A_L, A_F, A_{LF} denotan la clausura íntegra de A en L, F, LF resp., entonces

$$\mathfrak{d}(A_L/A_K)A_{LF} \subseteq A_L[A_F],$$

donde $A_L[A_F]$ denota el mínimo subanillo de A_E que contiene a A_L y a A_F.

Demostración: Nótese que la inclusión del enunciado está en términos de A_K-módulos, así que basta probarla para todas las localizaciones de A_K. En particular, podemos suponer que A_K es un dominio de valuación discreta y un DIP. Sea $Y := \{y_1, \ldots, y_n\}$ una A_K-base de A_L, entonces como L, F son linealmente disjuntos se tiene que es una F-base de LF. Sea $\{z_1, \ldots, z_n\}$ la K-base dual de Y en L, es decir, tal que $\operatorname{Tr}_{L/K}(y_i z_j) = \delta_{ij}$. Luego, es fácil comprobar que

$$y_i = \sum_{j=1}^{n} \operatorname{Tr}_{L/K}(y_i y_j) z_j,$$

lo que prueba que las matrices

$$D := [\operatorname{Tr}_{L/K}(y_i y_j)]_{ij}, \qquad D' := [\operatorname{Tr}_{L/K}(z_i z_j)]_{ij}$$

son inversas la una de la otra. Nótese que $\mathfrak{d}(Y) := \det D$ es el generador del ideal $\mathfrak{d}(A_L/A_K)$, de modo que D' tiene entradas en $\frac{1}{\mathfrak{d}(Y)}A_K$, de modo que

$$z_i = \sum_{j=1}^{n} \operatorname{Tr}_{L/K}(z_i z_j) y_j \in \frac{1}{\mathfrak{d}(Y)} \sum_{j=1}^{n} A_K y_j = \frac{1}{\mathfrak{d}(Y)} A_L.$$

Sea $\alpha \in A_{LF}$, entonces es fácil ver que

$$\alpha = \sum_{i=1}^{n} \operatorname{Tr}_{LF/F}(\alpha y_i) z_i,$$

donde $\operatorname{Tr}_{LF/F}(\alpha y_i) \in A_F$, lo que prueba que

$$\alpha \in \sum_{i=1}^{n} A_F z_i \subseteq \frac{1}{\mathfrak{d}(Y)} A_F A_L,$$

y como α era un elemento arbitrario de A_{LF} se comprueba que

$$A_{LF} \subseteq \frac{1}{\mathfrak{d}(Y)} A_F A_L \iff \mathfrak{d}(A_L/A_K)A_{LF} \subseteq A_L[A_F]. \qquad \square$$

Corolario 4.82.1: Sea A_K un dominio de Dedekind con $K := \operatorname{Frac} A_K$, sea E una extensión finita separable de K, sean L, F dos extensiones intermedias K-linealmente disjuntas ($L \cap F = K$) y sean A_L, A_F, A_{LF} la clausura íntegra de A en L, F, LF resp. Si $\mathfrak{d}(A_L/A_K)$ y $\mathfrak{d}(A_F/A_K)$ son coprimos, entonces $A_{LF} = A_L[A_F]$. Más aún, el discriminante se calcula como

$$\mathfrak{d}(A_{LF}/A_K) = \mathfrak{d}(A_L/A_K)^{[L:K]}\mathfrak{d}(A_F/A_K)^{[F:K]}.$$

Demostración: Basta notar que si $\mathfrak{d}(A_L/A_K)+\mathfrak{d}(A_F/A_K) = A_K$, entonces la desigualdad del teorema anterior implica que

$$A_{LF} \subseteq \mathfrak{d}(A_L/A_K)A_{LF} + \mathfrak{d}(A_F/A_K)A_{LF} \subseteq A_L[A_F],$$

y la inclusión $A_L[A_F] \subseteq A_{LF}$ es trivial. □

4.4 Normas de ideales

Definición 4.83: Sea B/A una extensión entera de dominios de Dedekind con $L := \operatorname{Frac} B$ una extensión finita de $K := \operatorname{Frac} A$. Para todo ideal fraccionario I de B, definimos la norma del ideal

$$\mathfrak{N}_{B/A}(I) := \sum_{b \in I} \operatorname{Nm}_{L/K}(b)A.$$

Proposición 4.84: Sea B/A una extensión entera de dominios de Dedekind con $L := \operatorname{Frac} B$ una extensión finita de $K := \operatorname{Frac} A$. Entonces:

1. Para todo $\beta \in L$, se cumple que $\mathfrak{N}_{B/A}(\beta B) = \operatorname{Nm}_{L/K}(\beta)A$. Vale decir, el siguiente diagrama conmuta:

$$\begin{array}{ccc} L^\times & \xrightarrow{\beta \mapsto \beta \cdot B} & \mathbf{I}(B) \\ {\scriptstyle \operatorname{Nm}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathfrak{N}_{B/A}} \\ K^\times & \xrightarrow[\alpha \mapsto \alpha \cdot A]{} & \mathbf{I}(A) \end{array}$$

2. Si S es un sistema multiplicativo de A, e I es un ideal fraccionario de B, entonces $\mathfrak{N}_{S^{-1}B/S^{-1}A}(S^{-1}I) = S^{-1}\,\mathfrak{N}_{B/A}(I)$.

3. Para todo par de ideales fraccionarios I, J de B, se cumple que

$$\mathfrak{N}_{B/A}(I \cdot J) = \mathfrak{N}_{B/A}(I) \cdot \mathfrak{N}_{B/A}(J).$$

4. Si C/B es una extensión entera de dominios de Dedekind con $F := \operatorname{Frac} B$ una extensión finita de L, entonces $\mathfrak{N}_{C/A} = \mathfrak{N}_{C/B} \circ \mathfrak{N}_{B/A}$.

Por la propiedad 3, nótese que basta conocer el valor de $\mathfrak{N}_{B/A}$ sobre los primos de B.

Proposición 4.85: Sea B/A una extensión entera de dominios de Dedekind con $L := \operatorname{Frac} B$ una extensión separable de grado m de $K := \operatorname{Frac} A$. Entonces, para todo $\mathfrak{P} \lhd B$ primo tal que $\mathfrak{p} := \mathfrak{P} \cap A$ se cumple que $\mathfrak{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/A)}$.

Demostración:

(a) Si L/K es de Galois: Sea $G := \operatorname{Gal}(L/K)$, entonces para todo $\alpha \in \mathfrak{P}$ vemos que:

$$\operatorname{Nm}_{L/K}(\alpha) := \prod_{\sigma \in G} \sigma(\alpha) \subseteq \mathfrak{P} \cap K = \mathfrak{p},$$

de modo que $\mathfrak{N}_{B/A}(\mathfrak{P}) \subseteq \mathfrak{p}$.

Probaremos que ningún otro primo está en la factorización de $\mathfrak{N}_{B/A}(\mathfrak{P})$: Sea $\mathfrak{q} \neq \mathfrak{p}$ primo tal que $\mathfrak{N}(\mathfrak{P}) = \mathfrak{q}\mathfrak{a}$, donde $\mathfrak{a} \trianglelefteq A$. Como $\mathfrak{P} \nmid \mathfrak{q}$ entonces, con $C := A \smallsetminus \mathfrak{q}$, vemos que $C^{-1}\mathfrak{P} = C^{-1}B$, pero

$$C^{-1}\,\mathfrak{N}_{B/A}(\mathfrak{P}) = C^{-1}(\mathfrak{q}\mathfrak{a}) \subseteq \mathfrak{q}A_{\mathfrak{q}},$$
$$\mathfrak{N}_{C^{-1}B/C^{-1}A}(C^{-1}\mathfrak{P}) = \mathfrak{N}(C^{-1}B) = A_{\mathfrak{q}},$$

lo que contradice que $\mathfrak{N}_{C^{-1}B/C^{-1}A}(C^{-1}\mathfrak{P}) = C^{-1}\,\mathfrak{N}_{B/A}(\mathfrak{P})$.

Para determinar la potencia de $\mathfrak{p}$ en $\mathfrak{N}_{B/A}(\mathfrak{P})$, podemos localizar en $\mathfrak{p}$, de modo que A es un dominio de valuación discreta (y un DIP) y B es un dominio de Dedekind con finitos primos (aquellos que dividen a $\mathfrak{p}$) y, por lo tanto, es también un DIP (cfr. [**1,** teo. 12.33]).

Así pues, sea $\mathfrak{P} = \pi B$ y $\mathfrak{p} = \tau A$, y, por el corolario 4.65.1, tenemos

$$\tau B = \mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e,$$

donde los $\mathfrak{P}_i$'s son primos distintos, conjugados entre sí y $\mathfrak{P}_1 = \mathfrak{P}$. Sabemos también que $|G| = efg$ por el mismo corolario y así

$$\operatorname{Nm}_{L/K}(\pi)B = \prod_{\sigma \in G} \sigma(\pi)B = \prod_{\sigma \in G} \sigma(\mathfrak{P}) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef},$$

pues sabemos que como $\sigma \in G$, entonces cada $\mathfrak{P}_i$ aparece $efg/g = ef$ veces.

Así pues, $\mathfrak{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^n$ para algún n por determinar, y por lo anterior, $\mathfrak{N}_{B/A}(\pi B)B = \mathfrak{p}^n B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{en}$, por lo que $n = f = f(\mathfrak{P}/A)$ como se quería probar.

(b) Caso general: Sea N la clausura normal de L, de modo que N/K es de Galois; y sea $C := \mathcal{O}_{N/B}$, de modo que la extensión C/A es entera. Sea $\mathfrak{Q} \lhd C$ primo tal que $\mathfrak{Q} \mid \mathfrak{P}$, entonces el caso de Galois prueba que

$$\mathfrak{N}_{C/B}(\mathfrak{Q}) = \mathfrak{P}^{f(\mathfrak{Q}/B)}, \qquad \mathfrak{N}_{C/A}(\mathfrak{Q}) = \mathfrak{p}^{f(\mathfrak{Q}/A)}.$$

Así la propiedad multiplicativa entre ideales (proposición anterior, inciso 3), la transividad de la norma (ídem, inciso 4) y la transitividad de los grados de inercia (proposición 4.64) prueban que $\mathfrak{N}_{B/A}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/A)}$. □

Definición 4.86: Sea K un cuerpo numérico y $A := \mathcal{O}_K$, entonces dado un ideal $\mathfrak{a} \trianglelefteq A$ no nulo, se define su ***norma absoluta*** como

$$\mathbf{N}(\mathfrak{a}) := |A/\mathfrak{a}|.$$

Proposición 4.87: Sea K un cuerpo numérico y $A := \mathcal{O}_K$. Para todo ideal $\mathfrak{a} \trianglelefteq A$ no nulo, se cumple que $\mathfrak{N}_{A/\mathbb{Z}}(\mathfrak{a}) = (\mathbf{N}(\mathfrak{a}))$.

Demostración: Sea $\mathfrak{a} = \prod_{i=1}^m \mathfrak{p}_i^{r_i}$ y sea $p_i > 0$ el primo tal que $\mathfrak{p}_i \cap \mathbb{Z} = (p_i)$. Sea $f_i := f(\mathfrak{p}_i/\mathbb{Z})$. Por el teorema chino del resto

$$A/\mathfrak{a} \cong A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m},$$

Insertar referencia.

en la demostración del teorema ? hemos visto que $\mathfrak{p}^r/\mathfrak{p}^{r+1}$ es un $A/\mathfrak{p}$-espacio vectorial de dimensión 1, luego $|A/\mathfrak{p}^r| = |A/\mathfrak{p}|^r$. Por definición $\dim_{\mathbb{F}_{p_i}}(A/\mathfrak{p}_i) = f_i$, de modo que $|A/\mathfrak{p}_i| = p_i^{f_i}$. Así completamos la demostración. □

4.5* Un teorema de Rabinowitsch

En el libro ya hemos visto varias maneras en las que matemáticos encontraron fórmulas especiales para obtener varios primos (e.g., los números de Mersenne y de Fermat). Euler encontró que el polinomio $f(x) = x^2 + x + 41$

es tal que $f(n)$ es primo para todo $0 \leq n < 41$ (es claro que $41 \mid f(41)$), lo que motivará la siguiente búsqueda de relaciones entre polinomios y primos.

Proposición 4.88: Sea $f(x) \in \mathbb{Z}[x]$ un polinomio no constante. Entonces $f(n)$ es compuesto para infinitos n's.

Demostración: Como $f(x)$ es no constante, sólo puede tomar un mismo valor finitas veces, por tanto, existe algún primo p tal que $p \mid f(n_0)$. Nótese que $f(n_0 + ap) \equiv f(n_0) \equiv 0 \pmod{p}$ y como $f(x) = \pm p$ finitas veces, entonces $f(n_0+ap) \notin \{\pm p\}$ para infinitos a's y, por tanto, es compuesto. □

Los números primos nos pueden dar harta información sobre polinomios, por ejemplo:

Lema 4.89: Sea $f(x) \in \mathbb{Z}[x]$ un polinomio de grado $d > 0$. Si $|f(n)|$ es primo para $\geq 2d + 1$ enteros n. Entonces $f(x)$ es irreducible.

Demostración: Procedemos por contradicción. Si $f(x) = g(x)h(x)$, entonces $g(n), h(n) \in \{\pm 1, \pm p_n\}$ donde p_n's son primos. Luego cada n es raíz del polinomio

$$F(x) := (g(x) - 1)(h(x) - 1)(g(x) + 1)(h(x) + 1)$$

el cual tiene $\deg F \leq 2d$ y, como tiene más de $2d + 1$ raíces, necesariamente $F(x) = 0$. □

Teorema 4.90: Sea $p = a_0 + a_1 b + \cdots + a_d b^d$ un primo $p > b$ en base $b \geq 3$. Entonces $f(x) := a_0 + a_1 x + \cdots + a_d x^d \in \mathbb{Z}[x]$ es irreducible.

Demostración: Sea $f(x) = g(x)h(x)$. Como $f(b)$ es primo, entonces podemos suponer que $g(b) = \pm 1$. Existen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que

$$g(x) = c \prod_{j=1}^{n} (x - \alpha_j),$$

donde $c \in \mathbb{Z}$. Nótese que, como $|c| \geq 1$, tenemos que $\prod_{j=1}^{n} |b - \alpha_j| \leq g(b)$, por lo que existe alguna raíz α tal que $|b - \alpha| \leq 1$, es decir, $\operatorname{Re} \alpha \in [b-1, b+1], \operatorname{Re}(1/\alpha) > 0$ y $|\alpha| \geq b - 1$.

Como $f(\alpha) = 0$, se sigue que

$$0 = \operatorname{Re}\left(\frac{f(\alpha)}{\alpha^d}\right) = a_d + a_{d-1} \operatorname{Re}\left(\frac{1}{\alpha}\right) + \sum_{i=2}^{d} a_{d-i} \operatorname{Re}\left(\frac{1}{\alpha^i}\right).$$

Como $a_{d-1}\operatorname{Re}(1/\alpha) > 0$ entonces algún $\operatorname{Re}(1/\alpha^i) < 0$, pero $a_{d-i}\operatorname{Re}(1/\alpha^i) \geq -(b-1)/|\alpha|^i$. Luego

$$0 = \operatorname{Re}\left(\frac{f(\alpha)}{\alpha^d}\right) \geq 1 + 0 - (b-1)\sum_{i=2}^{d}\frac{1}{|\alpha|^i},$$

por lo que

$$1 < (b-1)\sum_{i=2}^{d}\frac{1}{|\alpha|^i} = \frac{b-1}{|\alpha|\,(|\alpha|-1)} \leq \frac{1}{b-2}$$

lo que es absurdo. □

Teorema 4.91 (Rabinowitsch): Sea $A \geq 2$, sea $D := 1 - 4A$ y sea $f(x) := x^2 + x + A \in \mathbb{Z}[x]$. Son equivalentes:

1. $f(n)$ es primo para todo $0 \leq n < A - 1$.
2. $f(n)$ es primo para todo $0 \leq n < \frac{1}{2}(\sqrt{|D|/3} - 1)$.
3. El anillo $\mathbb{Z}\left[\frac{-1+\sqrt{D}}{2}\right]$ es un DFU.

Demostración: 1 $\implies$ 2. Trivial.

2 $\implies$ 3. Por contrarrecíproca, supongamos que $\mathbb{Z}[\theta]$ no es un DFU, donde θ es raíz de

$$f(x) = x^2 + x + A = \left(x + \frac{1}{2}\right)^2 + \frac{4A-1}{4} = \left(x + \frac{1}{2}\right)^2 + \frac{|D|}{4},$$

(como en el enunciado.) Nótese que como $D \equiv 1 \pmod 4$, entonces $\mathbb{Z}[\theta] = \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, de modo que posee la norma y conjugación apropiados; además que como $|D| \geq 4 \cdot 2 - 1 = 7$ las unidades de $\mathbb{Z}[\theta]^\times = \{\pm 1\}$.

Como $\mathbb{Z}[\theta]$ es una $\mathbb{Z}$-álgebra de tipo finito, entonces es un anillo noetheriano y posee factorización en irreducibles; como no es un DFU por hipótesis, tenemos la existencia de algún $\alpha \in \mathbb{Z}[\theta]$ con

$$\alpha = \pi_1\pi_2\cdots\pi_r = \rho_1\rho_2\cdots\rho_s,$$

donde cada π_i, ρ_j es irreducible y las factorizaciones son distintas.[7] Elijamos α de norma minimal; en este caso, de hecho ninguno de los irreducibles a ambos lados aparece en el otro, y por tanto ninguno es primo. Supongamos,

[7] Vale decir, que no existe permutación de modo que $\pi_j = \pm\rho_j$.

sin perdida de generalidad, que $\mathrm{Nm}(\pi_1) \leq \mathrm{Nm}(\rho_1)$. Para $\beta, \gamma \in \mathbb{Z}[\theta]$ (sin fijar) tenemos

$$\alpha' := (\beta\rho_1 - \gamma\pi_1)\rho_2 \cdots \rho_s = \beta\alpha - \gamma\pi_1 \frac{\alpha}{\rho_1} = \pi_1(\beta\pi_2 \cdots \pi_r - \gamma\rho_2 \cdots \rho_s),$$

así que si elegimos β de modo que $\pi_1 \nmid \beta\rho_1$, entonces α' también tiene dos factorizaciones en irreducibles. Para llegar a una contradicción, basta probar que existen $\beta, \gamma \in \mathbb{Z}[\theta]$ tales que:

(P1) $\pi_1 \nmid \beta\rho_1$.

(P2) $\mathrm{Nm}(\beta\rho_1 - \gamma\pi_1) < \mathrm{Nm}(\rho_1)$ y como $\mathrm{Nm}(\delta) = |\delta|^2$ (la norma compleja), queremos que $\left|\beta - \frac{\pi_1}{\rho_1}\gamma\right| < 1$.

Si $\beta = \pm 1$ la condición (P1) se satisface trivialmente, por lo que moviendo $\gamma = \pm 1$ vemos que la fracción π_1/ρ_1 está en la región pintada de la fig. 4.4.

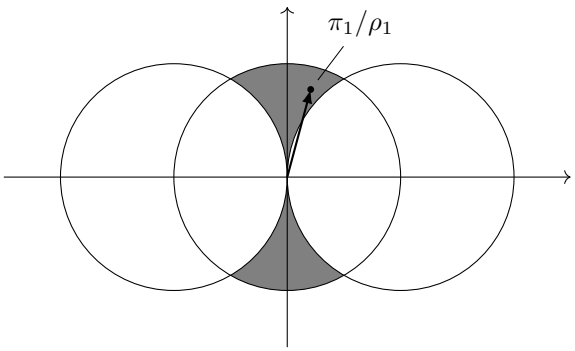


Figura 4.4

Ahora procedemos por un argumento geométrico. Construyamos e_1, e_2 los rayos desde el origen a 60° y 120° del eje x resp. Sea e el rayo desde el origen a π_1/ρ_1. Sea f la recta paralela al eje x a altura $\sqrt{|D|}/2$ (la cual contiene a los puntos de $\mathbb{Z}[\theta]$ de la forma $x + \theta$) y sea μ la intersección de e con f. El segmento ℓ de f delimitado por la intersección con e_1, e_2 tiene longitud

$$2 \cdot \frac{\sqrt{|D|}}{2} \tan(30°) = \sqrt{\frac{|D|}{3}} > 1,$$

por lo que ℓ contiene al menos un punto del reticulado $\mathbb{Z}[\theta]$. Sea β el punto de $\mathbb{Z}[\theta]$ en ℓ más cercano a μ (ver fig. 4.5).

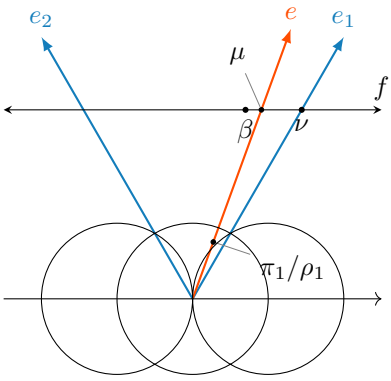


Figura 4.5

Como $\mu = x + \theta$ con x real, vemos que $|\mu - \beta| < 1$ y si $\beta + 1, \beta - 1 \in \ell$, entonces $|\mu - \beta| \leq 1/2$. Supongamos que $\beta + 1 \notin \ell$ y que $\mu > \beta$; sea ν la intersección entre e_1 y f, y nótese que el ángulo que se forma entre ellos tiene 60, de modo que la perpendicular a e_1 que pasa por β tiene una distancia $< \sqrt{3}/2$ y, por lo tanto, la distancia entre β y e es menor que $\sqrt{3}/2$. Luego, el círculo de radio 1 centrada en β corta un segmento de longitud > 1 de e y, por tanto, existe un entero γ tal que $\gamma\pi_1/\rho_1$ cae dentro de dicho círculo.

Así, se satisface la condición (P2) como se quería. Como $\beta = n + \theta$ con $|n| < \frac{1}{2}\sqrt{|D|/3}$, entonces

$$\mathrm{Nm}(\beta) = (n + \theta)(n + \overline{\theta}) = (n + \theta)(n - 1 - \theta) = n^2 + n + A = f(n)$$

es primo por hipótesis, luego β ha de ser primo, luego se satisface (P1) porque, de lo contrario, tendríamos que $\pi_1\delta = \rho_1\beta$ y, por tanto, $\beta \mid \pi_1\delta$. Pero $\beta \nmid \pi_1$ pues π_1 es irreducible, pero no primo; así que $\beta \mid \delta$. Cancelando múltiplos de β nos queda que $\rho_1 = \pi_1\phi$ lo que es absurdo pues ρ_1, π_1 son irreducibles no asociados. Así que P1 también se cumple, lo que completa nuestra contradicción.

3 $\implies$ 1. Para $0 \leq n < A - 1$ escribamos

$$f(n) = n^2 + n + A = (n - \theta)(n - \overline{\theta}) = (n - \theta)(n + 1 + \theta).$$

Sea $p \mid f(n)$, si p fuese irreducible en $\mathbb{Z}[\theta]$, entonces sería primo, y por tanto $p \mid n - \theta$ o $p \mid n + 1 + \theta$ lo cual es absurdo. Así pues si $p \mid f(n)$, entonces $p = \alpha\beta$ donde $\alpha, \beta \in \mathbb{Z}[\eta]$ no son unidades y, como $p^2 = \mathrm{Nm}(p) = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$ vemos que $\mathrm{Nm}(\alpha) = \mathrm{Nm}(\beta) = p$ y han de ser irreducibles. Ahora bien,

$$p = \mathrm{Nm}(\alpha) = \mathrm{Nm}(x + y\theta) = x^2 - xy + Ay^2 = \left(x - \frac{y}{2}\right)^2 + \left(A - \frac{1}{4}\right)y^2 \geq A - \frac{1}{4},$$

por lo que $p \geq A$ y también

$$f(n) = n^2 + n + A < (A-1)^2 + (A-1) + A = A^2,$$

pero si $pq \mid f(n)$ vemos que $pq \geq A^2$ lo que es absurdo; así que $f(n) = p$. □

Corolario 4.91.1: El anillo $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ es un DFU con

$$D \in \{-7,\ -11,\ -19,\ -43,\ -67,\ -163\}.$$

Esto demuestra la existencia de anillos de enteros de cuerpos cuadráticos imaginarios que son DFU's, pero no son euclídeos. Está comprobado, por ciertos teoremas más fuertes, que estos son todos los valores que el teorema de Rabinowitsch puede dar.

4.6 El último teorema de Fermat

El problema con el que creo que se debe comenzar la introducción a la teoría algebraica de números, es el conocido *Último Teorema de Fermat* para lo que conviene definir la siguiente fórmula:

$$\exists a, b, c \in \mathbb{Z}_{\neq 0} \quad a^n + b^n = c^n. \tag{Fmt(n)}$$

Así, el último teorema de Fermat se expresa diciendo que Fmt(n) es falso para $n \geq 3$. Éste teorema fue finalmente demostrado entre 1994 y 1995 por Andrew Wiles, pero, habiendo sido conjeturado por Fermat en 1637, la proposición estuvo en la incertidumbre durante 357 años, por lo que es natural que durante el siglo XX la literatura se refiriera a él como la *conjetura de Fermat*. En éste libro, seguimos la costumbre de llamarle «conjetura» para hacer hincapié en la idea de que vamos a ir tratando el problema con todo su halo de misterio sin ver una luz decisiva, como si estuvieramos resolviéndolo por vez primera.

Es consabido que Fmt(2) es cierto, y de hecho, se le llaman *ternas pitagóricas* a las ternas ordenadas (a, b, c) de enteros no nulos que cumplen que $a^2 + b^2 = c^2$; el nombre naturalmente procede del teorema de Pitágoras. Ejemplos de ternas pitágoricas se conocen desde los babilonios, y el más clásico es la terna $(3, 4, 5)$, pero tomar el caso por una mera trivialidad es un cinismo; en cierto modo, y dado que sabemos por entes externos que la conjetura es cierta, es nuestra única fuente de información ante la conjetura de Fermat, las únicas pistas del caso y por ello un mínimo de atención es menéster.

En primer lugar, veamos qué clases de observaciones se le pueden realizar para demostrar la conjetura:

- Podemos intentar una demostración por «decenso infinito» (contradicción de cierta minimalidad) para lo cual se exige minimalidad de c y se concluye que una terna (a, b, c) que satisfaga $a^n + b^n = c^n$ ha de ser coprima en conjunto. Pero más aún, la terna es coprima dos a dos, puesto que claramente si d es un factor común de a y b, entonces $c^n = d^n(\bar{a}^n + \bar{b}^n)$ y también lo es de c. Y análogamente si lo es de a y c, entonces $b^n = d^n(\bar{c}^n - \bar{a}^n)$.

- Siguiendo un argumento similar, podemos ver que mirando la ecuación módulo 2 se concluye que exactamente uno de los tres valores es par y el resto son impares.

- Si demostramos que $\mathrm{Fmt}(n)$ es falso, entonces lo es para todo múltiplo de n. En particular, basta demostrarlo para $n = 4$ y para todos los primos.

- Si n es impar, encontrar una solución al problema de Fermat equivale a encontrar soluciones de la forma

$$a^n + b^n + c^n = 0,$$

  lo cual es ventajoso por la simetría subyacente entre a, b, c.

Caso $n = 4$. Esta y las siguientes secciones siguen a Edwards **[80]** y Ribenboim **[103]**.

Aquí veremos dos demostraciones. La primera originaria de Fermat mismo:

Teorema 4.92: Sea (a, b, c) una terna pitagórica, entonces existen $d, u, v \in \mathbb{Z}$ con $(u; v) = 1$ tales que

$$a = d(u^2 - v^2), \quad b = 2duv, \quad c = d(u^2 + v^2). \tag{4.6}$$

Demostración: Definamos $d := \mathrm{mcd}(a, b, c)$ de modo que $d^2(x^2 + y^2) = d^2z^2$. Así x, y, z son coprimos en conjunto, pero también lo son dos a dos, puesto que si $p \mid (x; y)$ entonces $p \mid x^2 + y^2 = z^2$ y análogamente. En particular, necesariamente ha de haber al menos un par y un impar. Nótese

que los únicos cuadrados mód 4 son 0 y 1, así pues podemos ver que x, y no son ambos impares, ya que si no entonces

$$x^2 \equiv y^2 \equiv 1, \qquad z^2 \equiv 2 \pmod 4$$

lo cual es absurdo. Reordenando los nombres nos queda que x es impar, y es par y z es impar. Como $y^2 = (z-x)(z+x)$ y $(2x; 2z) = 2$, $2x = (z+x)-(z-x)$ y $2z = (z+x)+(z-x)$, entonces

$$\operatorname{mcd}\big((z+x),(z-x)\big) = 2;$$

de lo que se sigue que $4 \mid y$. Definiendo

$$y =: 2\tilde{b}, \quad x+z =: 2\tilde{a}, \quad z-x =: 2\tilde{c},$$

se tiene que $\tilde{b}^2 = \tilde{a}\cdot\tilde{c}$. Por las observaciones anteriores, $(\tilde{a};\tilde{c}) = 1$, luego se sigue de que $\tilde{a}, \tilde{c}$ deben ser cuadrados perfectos y $\tilde{a} = u^2, \tilde{c} = v^2$, de modo que $\tilde{b} = u\cdot v$. □

Teorema 4.93: La ecuación diofántica $x^4 - y^4 = z^2$ no posee soluciones no triviales. En consecuencia, Fmt(4) es falso.

Demostración: Sea (x, y, z) una solución de naturales no nulos, primitiva con $x > 0$ minimal. Es fácil notar que todos los números son coprimos dos a dos. Se satisface que $z^2 = (x^2-y^2)(x^2+y^2)$ con $\operatorname{mcd}(x^2-y^2, x^2+y^2) \in \{1, 2\}$, separamos por casos:

(a) $\underline{\operatorname{mcd}(x^2-y^2, x^2+y^2) = 1}$: Como los factores son coprimos, entonces ambos son cuadrados, digamos

$$x^2 - y^2 = s^2, \qquad x^2 + y^2 = t^2,$$

con $(s;t) = 1$. Como $s^2 + t^2 = 2x^2$, entonces s, t tienen la misma paridad, así que son ambos impares. Definamos, entonces:

$$a := \frac{s+t}{2}, \qquad b := \frac{s-t}{2},$$

con $(a;b) = 1$. Nótese que $ab = \frac{s^2-t^2}{4} = y^2/2$, o equivalentemente, $y^2 = 2ab$. Luego, como y es par, entonces o bien a, o bien b es par. Digamos que $a = \gamma^2$ y $b = 2m^2$. Ahora bien:

$$a^2 + b^2 = \frac{(s+t)^2 + (s-t^2)}{4} = \frac{s^2+t^2}{2} = x^2 =: c^2,$$

donde b es par y $(a;b;c) = 1$, por lo que, por el teorema anterior, existen $0 < v < u$:

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

con $(u;v) = 1$. Luego $m^2 = uv$ y como son coprimos, tenemos que $u = \alpha^2, v = \beta^2$. Así, $\alpha^4 - \beta^4 = u^2 - v^2 = a = \gamma^2$, donde $0 < \alpha < u < b < x$, lo que contradice la minimalidad de x.

(b) $\underline{\text{mcd}(x^2 - y^2, x^2 + y^2) = 2}$: Luego, x^2, y^2 son impares y z es par. Así que, la ecuación $(y^2)^2 + z^2 = (x^2)^2$ induce, por el teorema anterior, la existencia de $0 < v < u$:

$$y^2 = u^2 - v^2, \quad z = 2uv, \quad x^2 = u^2 + v^2,$$

con $(u;v) = 1$. De modo que $(xy)^2 = u^4 - v^4$ y $0 < u < x$, lo que contradice la minimalidad de x. □

Corolario 4.93.1: El área de un triángulo pitagórico no es un cuadrado perfecto.

Demostración: Dado un triángulo rectángulo de lados enteros (a, b, c) con $c^2 = a^2 + b^2$, entonces su área es $\frac{ab}{2} = s^2$. Luego

$$(a + b)^2 = c^2 + 4s^2, \qquad (a - b)^2 = c^2 - 4s^2,$$

de modo que $(a^2 - b^2)^2 = c^4 - (2s)^4$ admitiría una solución no trivial entera, por lo que s no puede ser entero. □

Euler también propuso su solución de que Fmt(4) es falso mediante otra ecuación diofántica:

Teorema 4.94: No existen $a, b, c \in \mathbb{Z}_{\neq 0}$ tales que $a^4 + b^4 = c^2$.

Demostración: Por contradicción, sea (a, b, c) una terna que cumple el enunciado, con c minimal. Si $p \mid (a;b)$, entonces $p^4 \mid c^2$ y $(a/p, b/p, c/p^2)$ es una terna que contradice la minimalidad de c; de modo que (a, b, c) son coprimos dos a dos.

Como $(a^2)^2 + (b^2)^2 = c^2$, se ha de cumplir que

$$a^2 = u^2 - v^2, \quad b^2 = 2uv, \quad c = u^2 + v^2.$$

Como $4 \mid b^2$, se ha de cumplir que o bien u o bien v es par. Si $u^2 \equiv 0$ y $v^2 \equiv 1 \pmod 4$, entonces $a^2 \equiv -1$ lo cual es absurdo. Así que u es impar y $v = 2v'$. Reordenando los términos se obtiene que $a^2 + v^2 = u^2$ por lo que, aplicando el teorema anterior,

$$a = d^2 - e^2, \quad v = 2de, \quad u = d^2 + e^2.$$

Sea $v' := de$, luego $b^2 = 4uv'$ con u, v' coprimos, de lo que se sigue que $u = z^2$, $v' = w^2$ y $de = w^2$. Como d, e son coprimos se sigue que $d = x^2$, $e = y^2$ y la última ecuación da

$$x^4 + y^4 = z^2,$$

donde $z^2 = u < c$, lo que contradice la minimalidad de c. □

Caso $n = 3$**.** Bajo nuestras observaciones estudiemos el problema $x^3 + y^3 + z^3 = 0$, ésto lo haremos principalmente en los enteros de Eisenstein $\mathbb{Z}[\zeta]$. Nótese que $\lambda := \zeta - 1$ tiene $\operatorname{Nm} \lambda = 3$, luego es primo y $3 = -\zeta^2\lambda^2$ así que se ramifica.

- Si sumamos las unidades $1, \zeta, \zeta^2$ se obtiene:

  $$1 + \zeta = -\zeta^2, \qquad 1 + \zeta^2 = -\zeta, \qquad \zeta + \zeta^2 = 1.$$

  Si las restamos se obtiene:

  $$\zeta - 1 = \lambda, \qquad \zeta^2 - 1 = -\zeta^2\lambda, \qquad \zeta^2 - \zeta = \zeta\lambda.$$

  Y si sumamos consigo mismo se obtiene

  $$1 + 1 = 2, \qquad \zeta + \zeta = 2\zeta, \qquad \zeta^2 + \zeta^2 = 2\zeta^2.$$

  Con ésta información vemos que si dos unidades ϵ_1, ϵ_2 satisfacen $\epsilon_1 \equiv \epsilon_2 \pmod 3$, entonces $\epsilon_1 = \epsilon_2$ puesto que $\epsilon_1 - \epsilon_2$ es o bien otra unidad, o bien un múltiplo de λ, o bien un múltiplo de 2.

- Por definición, $\zeta \equiv 1 \pmod \lambda$, de modo que $a + b\zeta \equiv a + b \ (\lambda)$, por lo que, si $\alpha := a + b\zeta$ vemos que $\lambda \mid \alpha$ syss $\lambda \mid a + b$ y luego $3 = \operatorname{Nm} \lambda \mid (a + b)^2$. Si $3 \mid a + b$, entonces como $\lambda \mid 3$ tenemos que $\lambda \mid a + b$ y $\lambda \mid \alpha$.

- Si $\lambda \nmid \alpha$, existe ϵ invertible tal que $\alpha \equiv \epsilon \ (3)$: Como $3 \nmid a + b$, entonces, con $e = \pm 1$ se cumple que:

  $$(a, b) \in \{(3h + e, 3k), (3h, 3k + e), (3h + e, 3k + e)\}$$

  para algunos $h, k \in \mathbb{Z}$.

- Si $\lambda \nmid \alpha$, entonces $\alpha^3 \equiv \pm 1 \pmod 9$: Si $\alpha = 3\beta + \epsilon$ con $\epsilon \in \mathbb{Z}[\zeta]^\times$, entonces $\alpha^3 = (3\beta+\epsilon)^3 \equiv \epsilon^3 = \pm 1 \pmod 9$.

- Considere $f(t) := t^3+1 \in \mathbb{Z}[t]$, entonces sus raíces en $\mathbb{Z}[\zeta]$ son $-1, -\zeta, -\zeta^2$, de modo que
$$t^3 + 1 = (t+1)\cdot(t+\zeta)\cdot(t+\zeta^2).$$
Si $\beta, \gamma \in \mathbb{Z}[\zeta]$ con $\gamma \neq 0$, entonces sustituyendo $t = \beta/\gamma$ y multiplicando por γ^3 se obtiene:
$$\beta^3 + \gamma^3 = (\beta+\gamma)\cdot(\beta+\gamma\zeta)\cdot(\beta+\gamma\zeta^2).$$
Multiplicando por $\zeta^3 = 1$ apropiadamente, reescribimos:
$$\beta^3 + \gamma^3 = (\beta+\gamma)\cdot(\beta\zeta^2+\gamma\zeta)\cdot(\beta\zeta+\gamma\zeta^2),$$
y además:
$$(\beta+\gamma) + (\beta\zeta^2+\gamma\zeta) + (\beta\zeta+\gamma\zeta^2) = 0.$$

Teorema 4.95: Fmt(3) es falso en $\mathbb{Z}[\zeta]$ (y luego también en $\mathbb{Z}$).

Demostración: Si existiese una solución no trivial, entonces podemos elegir una solución primitiva (α, β, γ). λ debe dividir a al menos uno de ellos, puesto que de lo contrario $\alpha^3 \equiv e_1, \beta^3 \equiv e_2, \gamma^3 \equiv e_3 \pmod 9$ con $e_i \in \{\pm 1\}$ y $e_1+e_2+e_3 \equiv 0 \pmod 9$ lo cual es absurdo. Por éste mismo razonamiento, λ sólo divide a uno de ellos.

Sea (α, β, γ) una solución primitiva, con $\lambda \mid \alpha$ y $\nu_\lambda(\alpha)$ minimal. Como $\lambda \mid \alpha$, entonces $\lambda^3 \mid \alpha^3$ y $\lambda^3 \mid \beta^3+\gamma^3$. Sabemos que $\beta^3 \equiv e, \gamma^3 \equiv f \pmod 9$ con $e, f \in \{\pm 1\}$. Como $\lambda^2 \mid 3$, entonces $\lambda^3 \mid 9$ y $e + f \equiv \beta^3 + \gamma^3 \equiv 0 \pmod{\lambda^3}$, en particular, $3 \mid e+f$ y $e = -f$. Ergo:
$$-\alpha^3 = \beta^3 + \gamma^3 \equiv e + f \equiv 0 \pmod 9.$$
Esto es $\lambda^4 \mid \alpha^3$ y $\lambda^2 \mid \alpha$. Ahora bien:
$$-\alpha^3 = \beta^3+\gamma^3 = (\beta+\gamma)(\beta\zeta^2+\gamma\zeta)(\beta\zeta+\gamma\zeta^2) =: \eta_1\eta_2\eta_3$$
con $\eta_1+\eta_2+\eta_3 = 0$. Como $\zeta \equiv 1 \pmod\lambda$, se tiene que $\eta_1 \equiv \eta_2 \equiv \eta_3 \pmod\lambda$, por definición, y como $\lambda^3 \mid \eta_1\eta_2\eta_3$ concluimos que λ divide a cada η_i.

Sea $\tilde{\eta}_i := \eta_i/\lambda$. Nótese que $\tilde{\eta}_1, \tilde{\eta}_2, \tilde{\eta}_3$ son coprimos dos a dos, pues si ρ fuese un primo común de $\tilde{\eta}_1, \tilde{\eta}_2$, entonces $\lambda\rho$ divide a η_1, η_2 y:
$$\lambda\rho \mid \eta_2 - \zeta^2\eta_1 = \beta(\zeta-\zeta^2) = -\zeta\beta\lambda, \quad \lambda\rho \mid \eta_2 - \zeta\eta_1 = \gamma(\zeta^2-\zeta) = \zeta\gamma\lambda.$$

Pero ζ es invertible y β, γ son coprimos.

Así, tenemos que $-\alpha^3 = \lambda^3\tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3$ con $\tilde{\eta}_1 + \tilde{\eta}_2 + \tilde{\eta}_3 = 0$. Sea $\tilde{\alpha} := \alpha/\lambda$ que aún satisface que $\lambda \mid \tilde{\alpha}$ y $-\tilde{\alpha}^3 = \tilde{\eta}_1\tilde{\eta}_2\tilde{\eta}_3$. Como los $\tilde{\eta}_i$'s son coprimos, entonces $\tilde{\eta}_i = \epsilon_i\theta_i^3$ donde ϵ_i es inversible. Así pues:

$$-\tilde{\alpha}^3 = \epsilon_1\epsilon_2\epsilon_3\,\theta_1^3\theta_2^3\theta_3^3, \qquad \epsilon_1\theta_1^3 + \epsilon_2\theta_2^3 + \epsilon_3\theta_3^3 = 0,$$

con los θ_i's coprimos dos a dos.

Además, $\tilde{\alpha} = \epsilon\theta_1\theta_2\theta_3$ con $\epsilon^3 = -\epsilon_1\epsilon_2\epsilon_3$. Pero todo inversible al cubo en $\mathbb{Z}[\zeta]$ da ± 1, ergo, $\epsilon_1\epsilon_2\epsilon_3 = \pm 1$. Como $\lambda \mid \tilde{\alpha}$, entonces λ divide a exactamente un θ_i, digamos $\lambda \mid \theta_1$. Luego $\theta_2^3 \equiv e, \theta_3^3 \equiv f \ (9)$ para $e, f \in \{\pm 1\}$. Nótese que $3 \mid \theta_1^3$ y:

$$0 \equiv -\epsilon_1\theta_1^3 = \epsilon_2\theta_2^3 + \epsilon_3\theta_3^3 = e\epsilon_2 + f\epsilon_3 \pmod 3.$$

Luego $\epsilon_2 = \pm\epsilon_3$ y $e = \pm\epsilon_1\epsilon_3^2$. Multiplicando por $\pm\epsilon_3^2$:

$$0 = e\theta_1^3 + \epsilon_3^3\theta_2^3 \pm \epsilon_3^3\theta_3^3 = (e\theta_1)^3 + (\epsilon_3\theta_2)^3 + (\pm\epsilon_3\theta_3)^3$$

con

$$\nu_\lambda\theta_1 = \frac{1}{3}\nu_\lambda(\tilde{\eta}_1) = \frac{1}{3}(\nu_\lambda\eta_1 - 1) < \frac{1}{3}\nu_\lambda(\alpha),$$

lo que contradice la minimalidad de $\nu_\lambda\alpha$. □

El teorema de Sophie Germain. Ya hemos probado que el Último Teorema de Fermat para el exponente $n = 4$, así que podemos enfocarnos en el caso de n primo impar. Digamos que (a, b, c) fueran una solución no trivial primitiva de $a^n + b^n + c^n = 0$, entonces caen en dos casos:

(I) $n \nmid abc$, i.e., ninguno de los números es divisible por n.

(II) Exactamente uno de los números es divisible por n, digamos a.

Éstos se conocen como ***caso I*** y ***II*** del Último Teorema de Fermat.

Teorema 4.96 (de Sophie Germain): Sea n un primo impar. Supongamos que existe un primo p con las siguientes propiedades:

1. Si $x^n + y^n + z^n \equiv 0 \pmod p$ entonces $xyz \equiv 0 \ (p)$
2. No existe x tal que $x^n \equiv n \ (p)$.

Entonces se satisface el caso I del Último Teorema de Fermat para n.

Demostración: Procedemos por contradicción, sea (a,b,c) una solución primitiva de $a^n+b^n+c^n=0$ con $abc\not\equiv 0\ (n)$. Reescribiendo tenemos

$$(-a)^n=b^n+c^n=\underbrace{(b+c)}_{\alpha}\underbrace{(b^{n-1}-b^{n-2}c+b^{n-3}c^2-\cdots+c^{n-1})}_{\beta}.$$

Los números α,β son coprimos: Sea q un factor primo común, ergo $c\equiv -b$ (q) y $\beta\equiv nb^{n-1}\equiv 0\ (q)$. Nótese que $q\neq n$, puesto que la primera condición forzaría que $0=a^n+b^n+c^n\equiv a^n\ (\text{mód } n)$, pero estamos en el caso I. Por ende, la segunda condición forzaría que $b\equiv 0\ (q)$ y luego $a\equiv c\equiv 0\ (q)$, pero la solución es primitiva.

Ahora bien, como α,β son coprimos, entonces son potencias n-ésimas y luego se ve que:

$$\begin{array}{lll} b+c=x^n, & b^{n-1}-b^{n-2}c+\cdots+c^{n-1}=u^n, & a=-xu,\\ a+c=y^n, & a^{n-1}-a^{n-2}c+\cdots+c^{n-1}=v^n, & b=-yv,\\ a+b=z^n, & a^{n-1}-a^{n-2}b+\cdots+b^{n-1}=w^n, & c=-zw. \end{array}$$

Nótese que $a^n+b^n+c^n\equiv 0\ (p)$, por lo que, por hipótesis, podemos suponer que $a\equiv 0\ (p)$. Luego $(-x)^n+y^n+z^n\equiv 2a\equiv 0\ (p)$ por lo que algún sumando es divisible por p. Si y o z lo fuesen, entonces c o b serían divisibles por p resp., lo que contradice la primitividad de la solución. Por lo tanto, $p\mid x$ y $b\equiv -c\ (p)$, por lo que, $u^n\equiv nb^{n-1}\equiv nw^n\ (p)$. Como $w\not\equiv 0\ (p)$, entonces $(u/w)^n\equiv n\ (p)$ lo que contradice la hipótesis (b). □

Corolario 4.96.1: Sea $p>2$ un primo tal que $2p+1$ es un primo (de Sophie Germain), entonces p satisface el caso I del Último Teorema de Fermat.

Demostración: Basta comprobar que $q:=2p+1$ con p satisfacen las hipótesis del teorema anterior.

Por el pequeño teorema de Fermat, si $q\nmid a$, entonces $a^{2p}\equiv 1\ (\text{mód } q)$, así que $a^p\equiv\pm 1\ (q)$ por lo que $p\not\equiv a^p\ (p)$. Así mismo, si $x^p+y^p+z^p\equiv 0$ (q), vemos que si ninguno fuera $\equiv 0\ (q)$, entonces la suma daría $\pm 1,\pm 3\ (q)$ (y $p\geq 3$ implica que $q\geq 7$), por lo que necesariamente alguno es divisible por q. □

Así, el teorema de Sophie Germain nos da un criterio relativamente sencillo para verificar el caso I del Último Teorema de Fermat; no obstante, el caso II es un tanto más complicado.

Caso $n = 5$**.** Para éste caso trabajaremos con el anillo de enteros A de $\mathbb{Q}(\sqrt{5})$ (i.e., $A = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$). Recuérdese que A es un dominio euclídeo, luego es un DIP y un DFU, lo que será importante.

Lema 4.97: Sean $a, b \in \mathbb{Z}$ coprimos con $5 \nmid a$ y $5 \mid b$.

(a) Si a, b tienen distinta paridad y $a^2 - 5b^2 = \gamma^5$ para algún $\gamma \in A$, entonces existen $c, d \in \mathbb{Z}$ tales que

$$\begin{aligned} a &= c(c^4 + 50c^2d^2 + 125d^4) \\ b &= 5d(c^4 + 10c^2d^2 + 5d^4) \end{aligned} \tag{4.7}$$

donde c, d son coprimos, de distinta paridad y $5 \nmid c$.

(b) Si a, b son impares y $\frac{1}{4}(a^2 - 5b^2) = \gamma^5$ para algún $\gamma \in A$, entonces existen $c, d \in \mathbb{Z}$ tales que

$$\begin{aligned} a &= c(c^4 + 50c^2d^2 + 125d^4)/16 \\ b &= 5d(c^4 + 10c^2d^2 + 5d^4)/16 \end{aligned} \tag{4.8}$$

donde c, d son coprimos, impares y $5 \nmid c$.

Demostración: Nótese que si c, d son tales que satisfacen (4.7) (resp. (4.8)) entonces necesariamente son coprimos y $5 \nmid c$. Más aún, tienen distinta paridad (resp. son impares) mirando las ecuaciones mód 2 (resp. mód 16, puesto que a^4 es 0 ó 1 si a es par o impar, mientras que los cuadrados mód 16 son $0, 4$ y $1, 9$).

(a) Sea $\alpha := a + b\sqrt{5}$. Como $\alpha = \beta^5$ con $\beta = \frac{1}{2}(h + k\sqrt{5})$, donde $h, k \in \mathbb{Z}$ tienen la misma paridad; entonces, expandiendo la potencia del binomio, tendremos que

$$2^5 b = 5k(h^4 + 10h^2k^2 + 5k^4).$$

Ahora bien, si ambos fuesen impares, entonces $h = \pm 1, \pm 3$ (mód 8), luego $h^2 = 1, 9$ (mód 16) y $h^4 = 1, 17$ (mód 32) y análogamente con k, k^2, k^4, por lo que

$$1 + 10k^2 + 5k^4 \equiv \begin{cases} 1 + 10 + 5 \equiv 16, \\ 1 + 90 + 85 \equiv 16, \end{cases}$$

$$17 + 26k^2 + 5k^4 \equiv \begin{cases} 17 + 26 + 5 \equiv 16, \\ 17 + 234 + 85 \equiv 16, \end{cases}$$

lo cual nunca es divisible por 32. Así que h, k son pares. Aquí podríamos elegir $c := h/2$ y $d := k/2$ para concluir, por lo que nos dedicaremos a probar que α es una potencia quinta.

Nótese que α y su conjugado $\overline{\alpha}$ son coprimos. Si $\delta \mid \alpha, \overline{\alpha}$, entonces $\delta \mid 2a$ y $\delta \mid 2b\sqrt{5}$, luego δ podría ser divisor de 2 (pero no, pues $2 \nmid \alpha$) o podría ser divisor de $\sqrt{5}$ (que es primo), pero en éste último caso $\sqrt{5} \mid 2a$ contradiciendo que $5 \nmid a$. Luego como $\mathrm{Nm}(\alpha) = \alpha \cdot \overline{\alpha} = \gamma^5$, entonces tanto α como su conjugado son potencias quintas en A salvo posiblemente una unidad. Así que $\alpha = \theta^5 \cdot \varepsilon$ con $\varepsilon \in A^\times$. Ahora bien, los invertibles son de la forma $\varepsilon = \pm\eta^e$ donde η es una unidad fundamental (teorema 4.32), y, por un ejercicio, sabemos que una unidad fundamental es $\eta = \omega = \frac{1+\sqrt{5}}{2}$ (y naturalmente su inversa también).

Llamemos $\theta = \frac{1}{2}(s + t\sqrt{5})$ y $\varepsilon = \frac{1}{2}(u + v\sqrt{5})$. Notemos primero que si $\theta^5 =: \frac{1}{2}(m + n\sqrt{5})$, entonces vemos que $s^5 \equiv 16m \equiv m \pmod 5$ y $0 \equiv t^5 \equiv n \ (5)$. Ahora bien como

$$\alpha = a + b\sqrt{5} = \frac{m + n\sqrt{5}}{2} \cdot \frac{u + v\sqrt{5}}{2},$$

entonces vemos que $4a = mu + 5nv$ y $4b = mv + nu$. Como $5 \nmid a$, entonces $5 \nmid m, u$, pero como $5 \mid b$, entonces $5 \mid v$. Si $v \neq 0$, entonces dicho exponente $e \neq 0$ y reemplazando η por su inversa, podemos suponer que $e > 0$. Luego tenemos que $\pm 2^{e-1}(u + v\sqrt{5}) = (1 \pm \sqrt{5})^e$ (aquí, ambos $\pm$ representan posiblemente distintos signos). Expandiendo el término de v, vemos que

$$\pm 2^{e-1} v = e + 5\binom{e}{3} + 5^2\binom{e}{5} + \cdots,$$

luego $\pm 2^{e-1} v \equiv e \ (5)$, por lo que $5 \mid e$.

(b) Es análogo. □

Teorema 4.98: Fmt(5) es falso.

Demostración: Sea (x, y, z) una solución no trivial primitiva de $x^5 + y^5 + z^5 = 0$.

(i) Si $5 \nmid xyz$: Basta notar que $2 \cdot 5 + 1 = 11$ es primo y aplicar el corolario al teorema de Sophie Germain.

(ii) Si $5 \mid x$: Como y, z son coprimos, entonces o bien tienen distinta paridad o son ambos impares.

(a) y, z impares: Como $x^5 = -y^5 - z^5$, entonces es par. Así, sea $x = 2^n 5^m \tilde{x}$, donde $n, m > 0$, $2 \nmid \tilde{x}$ y $5 \nmid \tilde{x}$. Reemplacemos x por $\tilde{x}$ y así vemos que:

$$2^{5n} 5^{5m} x^5 + y^5 + z^5 = 0,$$

donde x, y, z son coprimos dos a dos, impares y $5 \nmid xyz$.

Como y, z son impares, definamos $y + z =: 2p, y - z =: 2q$, los cuales son coprimos y tienen distinta paridad (¿por qué?), y así tenemos que

$$-2^{5n} 5^{5m} x^5 = (p+q)^5 + (p-q)^5 = 2p(p^4 + 10p^2q^2 + 5q^4).$$

Como $5 \mid p$ o $5 \mid p^4 + 10p^2q^2 + 5q^4$, vemos que necesariamente $5 \mid p$. Ergo definiendo $r := p/5$, tenemos que r, q son coprimos, $5 \nmid q$ y q, r son de distinta paridad. Ahora bien

$$-2^{5n} 5^{5m} x^5 = 2 \cdot 5^2 r(125r^4 + 50r^2q^2 + q^4) =: 2 \cdot 5^2 r \cdot t.$$

Nótese que $t \equiv q^4 \not\equiv 0 \pmod 5$ y $t \equiv r^4 + q^4 \not\equiv 0 \pmod 2$, así que todas las potencias de 2 y de 5 se las lleva r (en particular, $10 \mid r$), y es fácil notar que t, r son coprimos, de lo cual, se concluye que t debe ser una potencia quinta. Una factorización $t = (q^2 + 25r^2)^2 - 5(10r^2)^2$ conlleva a definir $a := q^2 + 25r^2$ y $b := 10r^2$, con lo que $t = a^2 - 5b^2$. Aquí, $a, b > 0$, son coprimos; a es impar y $10 \mid b$ (tienen distinta paridad), así, por el lema, existen $c, d \in \mathbb{Z}$ tales que:

$$\begin{aligned} a &= c(c^4 + 50c^2d^2 + 125d^4), \\ b &= 5d(c^4 + 10c^2d^2 + 5d^4), \end{aligned}$$

con c, d coprimos, de distinta paridad, $5 \nmid c$ y $d > 0$. Como $b = 10r^2$ y $5 \mid r$, tenemos que $5^3 \mid b$. Multiplicando por $2 \cdot 5^3$, se tiene que

$$2 \cdot 5^3 b = (2 \cdot 5^2 r)^2 = 2 \cdot 5^4 d(c^4 + 10c^2d^2 + 5d^4),$$

como $2 \cdot 5^2 r$ es una potencia quinta, entonces éste número también lo es.

Nótese que como a es impar, c también; $5 \nmid c$ y $(c; d) = 1$, luego $\mathrm{mcd}(2 \cdot 5^4 d, c^4 + 10c^2d^2 + 5d^4) = 1$, y ambos números son potencias quintas. Pero $c^4 + 10c^2d^2 + 5d^4 = (c^2 + 5d^2)^2 - 5(2d^2)^2$, donde

$c^2+5d^2, 2d^2$ son coprimos, tienen distinta paridad y $5 \mid 2d^2$. Luego, por el lema, existen $c', d' \in \mathbb{Z}$ tales que:

$$c^2 + 5d^2 = c'(c'^4 + 50c'^2d'^2 + 125d'^4),$$
$$2d^2 = 5d'(c'^4 + 10c'^2d'^2 + 5d'^4),$$

con $d' > 0$. Multiplicando la última ecuación por $2 \cdot 5^8$ obtenemos que

$$(2 \cdot 5^4 d)^2 = 2 \cdot 5^9 d'(c'^4 + 10c'^2d'^2 + 5d'^4),$$

donde $2 \cdot 5^4 d$ es una potencia quinta, los factores son coprimos, así que $c'^4 + 10c'^2d'^2 + 5d'^4$ es una potencia quinta y aplicaríamos un proceso análogo. Nótese que $25d'^5 \leq 5d'(c'^4 + 10c'^2d'^2 + 5d'^4) = 2d^2$, de modo que $0 < d' \leq \sqrt[5]{2d^2/25} < d$; así que nuestro proceso eventualmente terminaría en un $0 < d'' < 1$ lo cual es absurdo.

(b) $\underline{y, z \text{ tienen distinta paridad:}}$ Redefinamos x de modo que $(5^m x)^5 + y^5 + z^5 = 0$ con $5 \nmid x$. Definamos $y + z =: p, y - z =: q$ los cuales son coprimos, impares y satisfacen que $2y = p + q$ y $2z = p - q$, luego

$$-2^5 5^{5m} x^5 = (2y)^5 + (2z)^5 = (p+q)^5 + (p-q)^5 = 2p(p^4 + 10p^2q^2 + 5q^4),$$

similarmente $5 \mid p$ y $r := p/5$. Así, q, r son coprimos, impares, $5 \nmid q$ y $5 \mid r$, de modo que

$$-2^5 5^{5m} x^5 = 2 \cdot 5^2 r(125r^4 + 50r^2q^2 + q^4) =: 2 \cdot 5^2 r \cdot t,$$

donde $t = 125r^4 + 50r^2q^2 + q^4 = a^2 - 5b^2$ con $a := q^2 + 25r^2$ y $b := 10r^2$. Se cumple que $a, b > 0$, ambos son pares, $a \equiv b \equiv 2$ (mód 4); r, t son coprimos, $5 \nmid t$ y $5 \mid r$. Definamos $a' := a/2, b' := b/2, t' := t/4$, entonces $t' = a'^2 - 5b'^2$ con $t' \equiv 0$ (4). Luego $-5^{5m} x^5 = 5^2 r t'/4$ con $\operatorname{mcd}(5^2 r, t'/4) = 1$, de modo que ambos son potencias quintas y por el lema:

$$a' = c(c^4 + 50c^2d^2 + 125d^4)/16,$$
$$b' = 5d(c^4 + 10c^2d^2 + 5d^4)/16,$$

donde c, d son coprimos impares positivos. Multiplicando la última igualdad por 5^3 vemos que

$$(5^2 r)^2 = 5^3 b' = \frac{5^4 d}{4}\left(\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4\right),$$

donde $((c^2+5d^2)/2)^2 - 5d^4 \equiv 0\ (4)$ y los factores son coprimos. Como $5^2 r$ es una potencia quinta, entonces $5^4 d$ y $\frac{1}{4}(((c^2+5d^2)/2)^2 - 5d^4)$ también. Por el lema, existen $c', d' \in \mathbb{Z}$ tales que

$$\begin{aligned}(c^2+5d^2)/2 &= c'(c'^4 + 50c'^2d'^2 + 125d'^4)/16,\\ d^2 &= 5d'(c'^4 + 10c'^2d'^2 + 5d'^4)/16,\end{aligned}$$

al igual que antes, podemos proseguir el proceso por decenso infinito notando que $0 < d' \leq \sqrt[5]{16d^2/25} < d$. □

Teorema 4.99 (Chevalley): Sea k un cuerpo finito, $f(x_1,\ldots,x_n)$ un polinomio homogéneo de grado d con coeficientes en k. Si $d < n$, existe $(a_1,\ldots,a_n) \in k^n_{\neq 0}$ tal que $F(a_1,\ldots,a_n) = 0$.

Demostración: Sea $q := |k|$ y $p := \operatorname{car} k$, de modo que $q = p^s$. Sea $V \subseteq k^n$ el conjunto de los ceros de $F(\boldsymbol{x})$. Luego $G(\boldsymbol{x}) := F(\boldsymbol{x})^{q-1}$ vale cero en V, pero vale 1 fuera de V por el teorema 2.18. Por lo tanto,

$$|k^n \smallsetminus V| = \sum_{\boldsymbol{x}\in k^n} G(\boldsymbol{x}) =: S.$$

Nótese que no es necesario calcular el valor de S, sino que basta probar que $p \mid S$ para concluir. Además, podemos notar que el problema se reduce a calcular el valor de S sobre los monomios de $G(\boldsymbol{x})$, para lo cual emplearemos la notación de los multi-índices:

$$\begin{aligned}\sum_{\boldsymbol{x}\in k^n} G(\boldsymbol{x}) &= \sum_{\boldsymbol{x}\in k^n} \sum_{|\alpha|=d^{q-1}} c_\alpha \boldsymbol{x}^\alpha.\\ \sum_{\boldsymbol{x}\in k^n} \boldsymbol{x}^\alpha &= \sum_{\boldsymbol{x}\in k^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \sum_{x_1\in k}\cdots\sum_{x_n\in k} x_1^{\alpha_1}\cdots x_n^{\alpha_n}\\ &= \sum_{x_2\in k}\cdots\sum_{x_n\in k} x_2^{\alpha_1}\cdots x_n^{\alpha_n}\cdot\left(\sum_{x_1\in k} x_1^{\alpha_1}\right)\\ &= \left(\sum_{x_1\in k} x_1^{\alpha_1}\right)\cdot\left(\sum_{x_2\in k} x_2^{\alpha_2}\right)\cdots\left(\sum_{x_n\in k} x_n^{\alpha_n}\right).\end{aligned}$$

Así pues, el problema se reduce a calcular $S_\beta := \sum_{z\in k} z^\beta$:

(a) Si $\beta = 0$: $\sum_{z\in k} z^\beta = \sum_{z\in k} 1 = q \equiv 0\ (\text{mód } p)$.

(b) Si $\beta > 0$: Como $0^\beta = 0$; así que se reduce a $\sum_{z\in k^\times} z^\beta$. Como $k^\times$ es un grupo cíclico (teo. 2.26) sea ω un generador, luego

$$S_\beta = \sum_{j=0}^{q-2} (\omega^j)^\beta = \sum_{j=0}^{q-2} (\omega^\beta)^j,$$

la cual es una suma geométrica que se analiza por casos:

i) Si $\omega^\beta \neq 1$: Luego $q-1 \nmid \beta$ y

$$\sum_{j=0}^{q-2} (\omega^\beta)^j = \frac{(\omega^\beta)^{q-1} - 1}{\omega^\beta - 1} = 0,$$

pues $\omega^{q-1} = 1$.

ii) Si $\omega^\beta = 1$: Luego $q-1 \mid \beta$ y $S_\beta = q-1$.

Así pues, $\sum_{\boldsymbol{x}\in k^n} \boldsymbol{x}^\alpha$ es no nulo syss todos los α_i's son no nulos y múltiplos de $(q-1)$, lo que daría $|\alpha| = \alpha_1 + \cdots + \alpha_n \geq (q-1)n$, pero G tiene grado $(q-1)d$ y $(q-1)d < (q-1)n$ por hipótesis como se quería probar. □

4.7* ¿Qué es la teoría algebraica de números?

En ésta sección, más divulgativa que rigurosa, pretendemos dar un recuento histórico que motive al lector a entender el qué y el por qué de la teoría.

La teoría algebraica de números comenzó principalmente con las afirmaciones sin demostrar de Fermat. Euler les dio principal atención y se esmeró en demostrar algunas de sus conjeturas, lo cual, creo personalmente, fue lo que motivó a varios otros matemáticos a hacer lo mismo. Del legado de Fermat es la afirmación más difícil, y quizá también la más enigmática y fascinante, su Último Teorema. De entre todas las estrategias intentadas se destacan dos: la primera es la adaptación natural de varias demostraciones hecha por Gauss a un lenguaje más algebraico, probando las afirmaciones en extensiones de $\mathbb{Z}$ como lo son los enteros gaussianos $\mathbb{Z}[\sqrt{-1}]$; y la segunda es el éxito de Kummer en probar el Último Teorema de Fermat para primos regulares.

Ésto hizo notar que las estrategias más efectivas parecían trabajar con extensiones de $\mathbb{Z}$, lo que conllevó a la definición de cuerpo numérico, elemento entero y de anillos de enteros algebraicos. Si bien, éstos demuestran ser

conceptos que surgen naturalmente del estudio aritmético de $\mathbb{Q}$ y $\mathbb{Z}$ poseen el gravísimo defecto de que no todos gozan de un teorema fundamental de la aritmética o, más formalmente, no todos son DFUs.

Aún así, la batalla no está tan perdida y deseamos entender tres problemas fundamentales para estudiar apropiadamente los anillos de enteros algebraicos A:

1. Si A no es un DFU, ¿hay algún sustituto de la factorización única? ¿Existe una característica común que señale que la factorización tampoco es en extremo caótica?

2. Si A no es un DFU, ¿cómo medir qué tan mala es la factorización?

3. ¿Cómo describir el grupo de unidades de A?

A la primera pregunta tornamos al álgebra conmutativa y vemos que un invariante que describe complejidad de ideales primos es el de la dimensión de Krull. La ventaja es que A siempre tiene dimensión de Krull 1, lo que algebraicamente se describe como un *dominio de Dedekind*; en éste texto no veremos un tratado general de la dimensión de Krull, pero sí discutiremos las implicancias aritméticas de ser un dominio de Dedekind.

A la segunda pregunta, se logra demostrar que hay un número, llamado el *número de clases*, íntimamente relacionado con el hecho de ser dominio de Dedekind, que mide –dentro del contexto de dominios de Dedekind– qué tan mala es la factorización.

Así, históricamente la primera pregunta queda zanjada por Dedekind, pero las otras dos quedan parcialmente abiertas y buena parte de la teoría se dedica a encontrar métodos para calcular (o comprender) los números de clase y los grupos de unidades.

Notas históricas

Pierre de Fermat (1601-1665) pese a ser uno de los grandes nombres en la teoría de números (e inclusive, ser considerado el padre de la teoría moderna) tiene dos particularidades que hoy resultarían inconcebibles: la primera es que era un jurista francés, no un matemático propiamente como tal; la segunda es que nunca escribió ninguna obra publicada.[8] Las investigaciones de Fermat se conocen principalmente por dos medios: la correspondencia que

[8]Con una única excepción: En 1660 autorizó la publicación de un apéndice a un libro de un colega suyo, no obstante, su publicación fue anónima.

Fermat mantenía con otros matemáticos de la época, y las anotaciones que hacía Fermat en su copia de la *Aritmética* de Diofanto.

Entre los trabajos de Fermat contamos la conjetura de que todo primo $p \equiv 1\ (4)$ es de la forma $p = x^2 + y^2$ en una carta a Mersenne (1640). Leonhard Euler descubrió los trabajos de Fermat gracias a su correspondencia con Goldbach. En 1747, Euler probó éste teorema (cfr. teo. 4.21) en un artículo publicado en 1758 **[26].** En una carta con Goldbach, Euler admite que su objetivo original era probar que todo número es suma de cuatro cuadrados, pero ésto sería probado más adelante por Lagrange en su lugar.

La famosa conjetura que se le atribuye a Fermat, también conocido como el Último Teorema de Fermat, estaba situada al lado de la parametrización de todas las ternas pitagóricas (vid. teo. 4.92) en donde escribe:

> Ningún cubo puede partirse en dos cubos, ni tampoco ningún bicuadrático puede partirse en bicuadráticos, ni tampoco ninguna potencia después de la segunda puede partirse en dos del mismo tipo. He encontrado una demostración verdaderamente destacable que éste margen es demasiado estrecho para contener.[9]

Se cree (cfr. [**7,** Vol. 2, pág. 731]) que Fermat escribió su teorema alrededor de 1637.

El nombre «Último Teorema de Fermat» se debe a que todas las afirmaciones sin demostrar de Fermat fueron confirmadas tras inmenso esfuerzo de sus contemporáneos, pero ésta era la última en resistirse. Hoy en día, tras haberse encontrado una prueba de éste teorema se tiene certeza casi absoluta de que una *demostración verdaderamente destacable* tan concisa como Fermat la describe es inexistente, y varios señalan que Fermat se refiere a un caso particular. El Último Teorema de Fermat hoy ostenta el record mundial del «teorema más difícil»: aquel con el mayor número de intentos fallidos, ésto principalmente debido a que varias organizaciones ofrecían buena recaudación por la hazaña.

Los casos del Último Teorema de Fermat han pasado por personajes destacables. El caso $n = 4$ fue demostrado originalmente por Fermat, quien propuso el problema como desafío[10] a Saint-Croix (septiembre de 1636), a Frenicle (mayo de 1640), a Pascal (25 de septiembre de 1654) y a Wallis

[9] *Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum, olloque potestatem in duos ejusdem nominis fas est dividere. Cujus rei ermat's demonstrationem mirabilem sane detexi. Hanc margin is exiguitas non caperet.*

[10] En realidad propuso un corolario que dimos: encontrar un triángulo pitagórico cuya área sea un cuadrado perfecto.

(7 de abril de 1658); en las mismas cartas también propuso el caso general. Wallis intentó una demostración replicando métodos de Diofanto, a Pascal le dijo que el problema era imposible y a Carcavi (agosto de 1659) le describió detalles de su prueba por descenso infinito. de Bessy **[21]** (1676) publicó póstumo la primera prueba, con clara influencia de la correspondencia con Fermat. Leibniz dió otra demostración de manera independiente en un manuscrito en 1678. Euler **[25]** probó que $x^4 + y^4 = z^2$ no tiene soluciones no triviales en 1738 (publ. 1747).

El caso $n = 3$ fue falsamente demostrado por el árabe Alkhodjandi antes de 972 d.C., y fue propuesto como problema por el árabe Beha-Eddin. Además de ser comunicado como problema por Fermat a otros matemáticos, Frans van Sehooten (17 de febrero de 1657) le comunicó el problema a Fermat, quien le respondió que era imposible (sin prueba de ello). El historiador J. Kersey afirmó que J. Wallis fue el primero en demostrar éste caso, pero sin referencia. Actualmente, la mayoría señala que Euler fue el primero en demostrarlo en su libro de álgebra **[27]** (1767, publ. 1770) dando una «demostración incompleta» (para más detalles, vid. **[80,** págs. 39-54]). La primera demostración completa fue dada por Kausler **[35]** en 1795 (publ. 1802). La demostración que nosotros presentamos, empleando la aritmética de los enteros de Eisenstein, es original de Gauss **[28]** 1863, publicada póstuma.

El caso $n = 5$ también fue demostrado por Dirichlet **[24]** (1889) quien presentó su demostración en julio de 1825 ante la Academia de Paris a la edad de veinte años, en la que Legendre formaba parte. La demostración de Dirichlet, aquí adaptada en lenguaje moderno, tenía un par de detalles a pulir, los cuales fueron arreglados por el mismo Legendre para la tercera edición de su libro en teoría de números **[39]** (1830). Otra demostración también pertenece al trabajo póstumo de Gauss **[28].**

Uno de los primeros intentos generales de abarcar el Último Teorema de Fermat, fue el teorema de Sophie Germain. **Sophie Germain** fue una matemática, quien dio a conocer su obra principalmente mediante su correspondencia con otros matemáticos; entre ellos, comunica su teorema a Gauss y a Legendre. Mediante éste teorema, Germain logra demostrar el caso I del Último Teorema de Fermat para todos los primos $p \leq 100$.

Después de los trabajos de Gauss, Legendre, Sophie Germain y Kummer, el Último Teorema de Fermat continuó siendo un problema intrigante para toda clase de matemáticos, entre ellos a Paul Friedrich Wolfskehl, el hijo de un rico banquero judío, quién dejó 100000 marcos para quién lograse resolver el Último Teorema de Fermat (mediante una demostración o un contraejemplo). Dos años después de su muerte en 1908, la Sociedad Real de Ciencia en Göttingen el premio fue hecho público y el primer año recibieron

un total de 621 falsas soluciones; hasta 2007 la Sociedad afirma recibir más de 5000 respuestas, entre ellas incluyendo una falsa demostración de 64 páginas de Ferdinand von Lindemann, el matemático que demostró la trascendencia de π.

Una anécdota divertida es que, en los primeros días de aviación, Hilbert fue invitado a dar un seminario en una universidad, a lo que tuvo que viajar en avión. Hilbert declaró que el título de su seminario era «Una demostración del Último Teorema de Fermat» y demás está decir que el seminario tuvo una gran audiencia que esperaba ansioso. Cuando Hilbert llegó, expuso sobre un tema absolutamente distinto y no fue sino hasta el final de su seminario que alguien le preguntó por qué había dado aquél título engañoso. «Oh», respondió Hilbert, «eso era por si el avión se estrellaba.»

El estudio de los anillos de enteros cuadráticos tiene una larga trayectoria histórica: la clasificación de qué anillos de enteros cuadráticos imaginarios son norma-euclídeos fue hecha por DICKSON [**23,** págs. 150-151] (1927) y el teorema de Motzkin fue probado en [**44**] (1949). El caso de los anillos de enteros cuadráticos reales es más complicado, Dickson originalmente dio una prueba (fallida) de que $\mathcal{O}_K$, donde $K = \mathbb{Q}(\sqrt{d})$ con $d \in \{2, 3, 5, 13\}$ eran todos los casos norma-euclídeos, luego PERRON [**54**] (1933) añadió $d \in \{6, 7, 7, 11, 17, 21, 29\}$ a la lista y finalmente la lista fue completada por OPPENHEIM [**48**], REMAK [**57**] (1934) y RÉDEI [**55**] (1941) incluyendo $d \in \{19, 33, 37, 41, 55, 73\}$. Rédei también creía que $d = 97$ funcionaba, pero ésto fue contrariado por BARNES y SWINNERTON-DYER [**13**] (1952). La demostración de que ésta lista está completa fue finalizada independientemente por INKERI [**34**] (1947) (quien comete el mismo error de Rédei) y por CHATLAND y DAVENPORT [**19**] (1950) mediante una larga serie de trabajos previos (para más detalles, vid. [**99,** págs. 174-175]).

Referencias

107. AUTHOR. title. *Amer. Math. Monthly* **128,** 239-249. arXiv: 1909.07121 (2021).

80. EDWARDS, H. M. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory Graduate Texts in Mathematics* **50** (Springer-Verlag, 1977).

81. EGGLETON, R. B., LACAMPAGNE, C. B. y SELFRIDGE, J. L. Euclidean Quadratic Fields. *Amer. Math. Mon.* doi:10.2307/2324118 (1992).

87. Janusz, G. J. *Algebraic Number Fields* 2.ª ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).

99. Narkiewicz, W. Class number and factorization in quadratic number fields. *Colloquium Math.* doi:10.4064/CM-17-2-167-190 (1967).

102. Pollack, P. *Not Always Buried Deep* (American Mathematical Society, 2009).

103. Ribenboim, P. *Fermat's Last Theorem for Amateurs* (Springer-Verlag New York, 1999).

104. Samuel, P. About Euclidean rings. *J. Algebra* **19,** 282-301. doi:10.1016/0021-8693(71)90110-4 (1971).

Otros recursos.

1. Cuevas, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).

2. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

3. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).

4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

5. Wilson, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. Brieskorn, E. y Knorrer, H. *Plane Algebraic Curves* trad. por Stillwell, J. (Birkhäuser Verlag, 1981).

7. Dickson, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

8. Newton, I. *The Correspondence of Isaac Newton* (ed. Turnbull, H. W.) (Cambridge University Press, 1960).

9. Roquette, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

10. Williams, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. Bennett, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. Alford, W. R., Granville, A. y Pomerance, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).

12. APÉRY, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. BARNES, E. S. y SWINNERTON-DYER, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. BEUKERS, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).
15. BOMBIERI, E. y VAALER, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).
16. CASSELS, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).
17. CATALAN, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).
18. CHAO, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).
19. CHATLAND, H. y DAVENPORT, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).
20. CLARK, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).
21. De BESSY, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
22. DEDEKIND, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).
23. DICKSON, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).
24. DIRICHLET, G. L. en *G. Lejeune Dirichlet's Werke* (ed. KRONECKER, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.
25. EULER, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).
26. EULER, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).
27. EULER, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).
28. GAUSS, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.

29. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

30. Hensel, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).

31. Hensel, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. Hyyrö, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. Inkeri, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. Inkeri, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. Kausler, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. Keller, W. y Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. Kürschák, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. Lang, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. Legendre, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. Lehmer, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. Mahler, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. Mignotte, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. Minkowski, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. Motzkin, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. Nagell, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. Northcott, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. Ochem, P. y Rao, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. OSTROWSKI, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. OSTROWSKI, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. OSTROWSKI, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. OSTROWSKI, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. OSTROWSKI, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. PERRON, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. RÉDEI, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. RELLA, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. REMAK, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. ROTH, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. RYCHLÍK, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. RYCHLÍK, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. SIEGEL, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. TATE, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. CASSELS, J. W. S. y FRÖHLICH, A.) (Academic Press, 1967), 305-347.

63. VERGER-GAUGRY, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

5

Teoría de valuación

5.1 Valores absolutos y cuerpos métricos

Definición 5.1: Sea k un cuerpo, una función $|\,|\colon k \to \mathbb{R}$ se dice una aplicación ***valor absoluto*** si:

VA1. $|x| > 0$ para todo $x \neq 0$ y $|0| = 0$.

VA2. $|xy| = |x|\,|y|$.

VA3. $|x + y| \leq |x| + |y|$ (desigualdad triangular).

Si además, satisface que $|x + y| \leq \text{máx}\{|x|, |y|\}$ (desigualdad ultramétrica), entonces $|\,|$ se dice un ***valor absoluto no arquimediano*** y de lo contrario se dice ***arquimediano***.

Todo valor absoluto induce una métrica $d(x, y) := |x - y|$ sobre k, y por ende, una topología. Por ello, se dice que el par $(k, |\,|)$ es un ***cuerpo métrico*** si $|\,|$ es un valor absoluto sobre k; de no haber ambigüedad sobre los signos obviaremos el valor absoluto. Se dice que k es un ***cuerpo métrico arquimediano*** si $|\,|$ es arquimediano y que k es un ***cuerpo ultramétrico*** de lo contrario. Se dice que dos valores absolutos son ***equivalentes*** si inducen la misma topología sobre k.

Ejemplo.

- Sea k un cuerpo arbitrario. Entonces $|\,|\colon k \to \mathbb{R}$ dado por

$$|x| = \chi_{k^\times}(x) = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$$

  es un valor absoluto no aquimediano, llamado el valor absoluto ***trivial***. Nótese que el valor absoluto induce la topología discreta. *Ojo*, la expresión «cuerpo métrico discreto» la emplearemos con otros fines.

- Los valores absoluto estándar sobre $\mathbb{R}$ y $\mathbb{C}$ son efectivamente funciones «valor absoluto» e inducen las topologías usuales resp.; les denotaremos $|\,|_\infty$ para diferenciarles de otros valores absoluto.

Corolario 5.1.1: Sea k un cuerpo métrico. Entonces:

1. $|1| = 1$.
2. $|a^n| = |a|^n$ para todo $n \in \mathbb{Z}$.
3. $|-1| = 1$, por ende, $|-a| = |a|$.
4. Para todo $n \in \mathbb{N}$ se cumple que $|n| \leq n$.
5. Si k es finito, entonces $|\,|$ es trivial.

Será necesario comprobar lo siguiente:

Teorema 5.2: Sea k un cuerpo métrico. Las funciones:

$$+\colon k \times k \to k, \quad \cdot\colon k \times k \to k, \quad ()^{-1}\colon k^\times \to k^\times$$

son continuas. Equivalentemente, k es un cuerpo topológico. Además, como es un espacio métrico, la función $|\,|\colon k \to \mathbb{R}$ es continua.

Demostración: En el enunciado y la demostración $k \times k$ denota el producto como espacios topológicos. Es sabida que dicha topología es la misma que aquella inducida por la métrica L^2 (y cualquier métrica L^p con $p \in [1, \infty]$). En particular fijaremos la métrica L^∞, en donde:

$$d\big((a_1, b_1), (a_2, b_2)\big) = \text{máx}\{|a_1 - a_2|, |b_1 - b_2|\} < \delta$$

Sean $a, b \in k$, demostrar que $+$ es continua equivale a ver que para todo $\epsilon > 0$ existe $\delta > 0$ tal que

$$d\big((a_1, b_1), (a_2, b_2)\big) < \delta \implies |(a_1 + b_1) - (a_2 + b_2)| < \epsilon.$$

Así pues, basta elegir $\delta = \epsilon/2$.

Para el producto, sea $(a_1, b_1) \in k$ un punto arbitrario y sea $M := \text{máx}\{|a_1|, |b_1|, 1\} > 0$. Luego elegimos $\delta := \text{mín}\{\frac{\epsilon}{2M+1}, 1\}$, y vemos que

$$\begin{aligned} |a_1b_1 - a_2b_2| &= |a_1b_1 - a_2b_1 + a_2b_1 - a_2b_2| \leq |a_1 - a_2|\,|b_1| + |a_2|\,|b_1 - b_2| \\ &< \delta(|b_1| + |a_2|) \leq \delta(|b_1| + |a_2| + \delta) \\ &< \frac{\epsilon}{2M+1}(M + M + 1) = \epsilon. \end{aligned}$$

Finalmente, para la inversa, sea $a \in k^\times$, luego $|a| > 0$. Elegimos $\delta := \text{mín}\{\frac{|a|^2}{2}\epsilon, \frac{|a|}{2}\} > 0$ y notamos que si $|a-b| < \delta$, entonces $|b| > |a| - \delta \geq |a|/2$ y

$$\left|\frac{1}{a} - \frac{1}{b}\right| = \frac{|a-b|}{|a|\,|b|} < \frac{\delta}{|a|\,|a|/2} \leq \epsilon. \qquad \square$$

Proposición 5.3: Sean $|\,|_1$, $|\,|_2$ dos valores absolutos no triviales sobre k. Entonces las siguientes afirmaciones son equivalentes:

1. $|\,|_1$ y $|\,|_2$ son valores absolutos equivalentes.
2. $|x|_1 < 1$ implica $|x|_2 < 1$ para todo $x \in k$.
3. Existe un $\lambda > 0$ real tal que $|x|_1 = |x|_2^\lambda$ para todo $x \in k$.

Demostración: 1 $\implies$ 2. Si $|x|_1 < 1$, entonces $\lim_n |x|_1^n = 0$, por lo que $\lim_n x = 0$. Como las topologías son la misma, la convergencia se da para ambos valores absolutos, luego $\lim_n |x|_2^n = 0$, por lo que $|x|_2 < 1$.

2 $\implies$ 3. Nótese que si $|x|_1 < 1$ implica $|x|_2 < 1$, luego si $|x|_1 > 1$ elijamos x^{-1} luego $|x^{-1}|_1 < 1$ implica $|x^{-1}|_2 < 1$. Como $|\,|_1$ y $|\,|_2$ son no triviales, elijamos x_0 tal que $a := |x_0|_1 > 1$ y $b := |x_0|_2 > 1$. Sea

$$\lambda := \frac{\ln b}{\ln a} > 0,$$

y claramente se satisface que $|x_0|_1 = |x_0|_2^\lambda$. Sea $x \in k^\times$, entonces sea $\alpha > 0$ tal que $|x|_1 = |x_0|_1^\alpha$. Luego sean m, n enteros tales que $m/n > \alpha$, luego

$$|x|_1 < |x_0|_1^{m/n} \iff |x^n/x_0^m|_1 < 1 \iff |x^n/x_0^m|_2 < 1 \iff |x|_2 < |x_0|_2^{m/n}$$

como ello aplica para todo racional, entonces $|x|_2 \leq |x_0|_2^\alpha$. De manera análoga se comprueba que $|x|_2 \geq |x_0|_2^\alpha$. Finalmente se estable que $|x|_1 = |x_0|_1^\alpha = |x_0|_2^{\lambda\alpha} = |x|_2^\lambda$.

3 $\implies$ 1. Trivial. $\square$

Proposición 5.4: Un cuerpo métrico k es ultramétrico syss para todo $n \in \mathbb{Z}$ se cumple que $|n| \leq 1$.

Demostración: $\Longrightarrow$. Basta notar que

$$|n| = |\underbrace{1+1+\cdots+1}_{n}| \leq \text{máx}\{|1|, \ldots, |1|\} = 1$$

para $n \geq 0$, y emplear que $|-n| = |n|$ para $n < 0$.

$\Longleftarrow$. Sean $a, b \in k$ arbitrarios, entonces

$$\begin{aligned} |(a+b)^n| &= \left| a^n + \binom{n}{1} a^{n-1}b + \cdots + \binom{n}{n-1} ab^{n-1} + b^n \right| \\ &\leq |a|^n + |a|^{n-1}|b| + \cdots + |b|^n \leq (n+1)\,\text{máx}\{|a|^n, |b|^n\}. \end{aligned}$$

Luego aplicando raíces (reales) a los valores absolutos se obtiene que $|a+b| \leq \sqrt[n]{n+1}\,\text{máx}\{|a|, |b|\}$ para todo $n \in \mathbb{N}_{\neq 0}$, pero $\lim_n \sqrt[n]{n+1} = 1$, lo que comprueba que $|a+b| \leq \text{máx}\{|a|, |b|\}$. □

Corolario 5.4.1: Todo cuerpo métrico de característica no nula es ultramétrico.

Corolario 5.4.2: El único valor absoluto (salvo equivalencia) sobre $\mathbb{F}_p$ es el trivial.

Demostración: Sea $a \in \mathbb{F}_p^\times$, entonces como $\mathbb{F}_p$ es ultramétrico, $|a| \leq 1$, pero $a^{-1} \equiv n \pmod p$ para algún $n \in \mathbb{N}$, así que $|a^{-1}| \leq 1$ y luego $|a| = 1$. □

Corolario 5.4.3: Si un valor absoluto $|\,|$ sobre k es no arquimediano sobre algún subcuerpo (e.g., es trivial), entonces es no arquimediano en todo k.

Ejemplo 5.5: Sea $p \in \mathbb{Z}$ primo. Se define $\nu_p(a)$, la ***valuación p-ádica*** de $a \in \mathbb{Z}$, como el máximo $n \in \mathbb{N}$ tal que $p^n \mid a$; se extiende a que $\nu_p(0) := \infty$. Ésto lo podemos extender a $\mathbb{Q}$ definiendo que $\nu_p(a/b) := \nu_p(a) - \nu_p(b)$ (¿por qué está bien definido?). Finalmente, eligiendo un real $\lambda \in (0,1)$ podemos definir:

$$\left|\frac{a}{b}\right|_p := \lambda^{\nu_p(a/b)},$$

y verificamos que efectivamente sea un valor absoluto no arquimediano.

La condición VA1 es clara. Además, para enteros se verifica que $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ de lo que se concluye VA2. Nótese lo siguiente, $n = \nu_p(a/b)$ syss $\frac{a}{b} = p^n \frac{u}{v}$ donde $p \nmid uv$, de éste modo si $n := \nu_p(a/b) \leq \nu_p(c/d) =: m$

$$\frac{a}{b} + \frac{c}{d} = p^n \frac{u}{v} + p^m \frac{w}{z} = p^n \frac{uz + p^{m-n}wv}{vz},$$

donde claramente $p \nmid uz + p^{m-n}wv$ y $p \nmid vz$. Con ésto se comprueba que $\nu_p(a/b + u/v) = \min\{\nu_p(a/b), \nu_p(c/d)\}$, ésto se traduce en la desigualdad ultramétrica.

La observación de cierre es que la elección de λ para el valor absoluto no afecta en nada, en el sentido de que otorga valores absolutos equivalentes. Por ello, el estándar es escoger $\lambda = 1/p$ de modo que $|a/b|_p = p^{-\nu_p(a/b)}$. ⌟

Más generalmente, si A es un DFU y $K := \operatorname{Frac} A$, el ejemplo anterior nos permite construir valores absoluto mediante los elementos irreducibles de A.

Definición 5.6: Un dominio íntegro A se dice un ***anillo de valuación*** si para todo $a \in \operatorname{Frac}(A)^\times$ se cumple que $a \in A$ o $a^{-1} \in A$.

Ejemplo.

- Todo cuerpo es un anillo de valuación.
- $\mathbb{Z}$ no es de valuación, puesto que $2/3 \in \mathbb{Q}$ satisface que $2/3 \notin \mathbb{Z}$ y $3/2 \notin \mathbb{Z}$.
- Considere la localización $\mathbb{Z}_{(p)}$, proponemos que es un anillo de valuación. En efecto, $\operatorname{Frac}(\mathbb{Z}_{(p)}) = \mathbb{Q}$ y para toda fracción reducida $a/b \in \mathbb{Q}$ se cumple que o bien $p \nmid b$, en cuyo caso $a/b \in \mathbb{Z}_{(p)}$, o bien $p \mid b$ y $p \nmid a$, en cuyo caso $b/a \in \mathbb{Z}_{(p)}$.

El nombre «anillo de valuación» sugiere que todo anillo de valuación desciende una valor absoluto en K, pero ésto podría no ser cierto. Para ello, vemos que la complicación está en que las funciones hasta $\mathbb{R}$ son demasiado *concretas* y también demasiado *rígidas*, mientras que buscamos una definición más *abstracta* que sí nos permita establecer una analogía con los valores absolutos. Ésta definición, es la de *valuación*, propuesta por W. Krull que estudiamos en el capítulo 12 de **[1].**

El último ejemplo es parte de algo más general:

Proposición 5.7: Sea (k, v) un cuerpo ultramétrico. Definamos:

$$\mathfrak{o} := \{a \in k : |a| \leq 1\}, \qquad \mathfrak{m} := \{a \in k : |a| < 1\},$$

entonces $(\mathfrak{o}, \mathfrak{m})$ es un anillo local de valuación, y su cuerpo de residuos $\Bbbk(v) := \mathfrak{o}/\mathfrak{m}$ se le dice el ***cuerpo de restos (de clases)*** de (k, v).

Demostración: El que $\mathfrak{o}$ sea un dominio íntegro deriva de que $1 \in \mathfrak{o}$, no posee divisores de cero por estar contenido en k, es cerrado bajo multiplicación por VA2 y es cerrado bajo adición por la desigualdad ultramétrica.

El hecho de que $\mathfrak{m}$ sea su ideal maximal se deriva de que, las razones anteriores demuestran que $\mathfrak{m}$ es ideal de $\mathfrak{o}$ y si $a \in \mathfrak{m}$, entonces $a^{-1} \in k$ tiene valor absoluto $|a|^{-1} > 1$, luego $a^{-1} \notin \mathfrak{o}$. □

Con ésto podemos dar un primer teorema de clasificación:

Teorema 5.8 – *Primer teorema de Ostrowski*: Todo valor absoluto no trivial sobre $\mathbb{Q}$ es (salvo equivalencia):

1. $|\,|_\infty$ si $|\,|$ es arquimediano.
2. Un valor p-ádico $|\,|_p$ si es no arquimediano.

Demostración:

1. Sea $n > 1$ entero. Entonces nótese que todo m posee una única expansión en base n:

$$m = m_t n^t + \cdots + m_1 n + m_0, \qquad 0 \leq m_i \leq n-1, m_t \neq 0$$

donde $n^t \leq m < n^{t+1}$. Luego por desigualdad triangular, empleando que $|m_i| \leq n-1$, se concluye que $|m| \leq (t+1)(n-1)r^t$. Como $m^j < n^{j(t+1)}$, luego

$$|m|^j = |m^j| \leq j(t+1)(n-1)r^{jt} \implies r > \frac{\sqrt[t]{m}}{\sqrt[jt]{j(t+1)(n-1)}},$$

aplicando límites se concluye que $r \geq \sqrt[t]{|m|}$; como algún m tiene valor absoluto $|m| > 1$ (por ser arquimediano), entonces $r > 1$ y como $t = \lfloor \log_n(m) \rfloor = \log_n(m)$ se concluye que

$$|m| \leq r^t \leq r^{\log_n(m)}.$$

Cambiando m entero a x racional, vemos que la misma cota aplica, luego si $|x|_\infty < 1$, entonces $\log_n(x) < 0$ y $|x| < 1$ lo que prueba que los valores absolutos son equivalentes.

2. Supongamos que $||$ es un valor absoluto no trivial sobre $\mathbb{Q}$. Por la proposición anterior, sea $(\mathfrak{o}, \mathfrak{m})$ el anillo de valuación asociado a $||$. Nótese que, como $|n| \leq 1$ para todo $n \in \mathbb{Z}$, concluimos que $\mathbb{Z} \subseteq \mathfrak{o}$. Luego $\mathbb{Z} \cap \mathfrak{m}$ es un ideal primo de $\mathbb{Z}$, digamos (p); luego $A \supseteq \mathbb{Z}_{(p)}$. Como $||$ es no trivial, entonces $\mathfrak{o} \neq \mathbb{Q}$ y $\mathbb{Z}_{(p)} \neq \mathbb{Q}$ por lo que $p \neq 0$. Si $a \in \mathbb{Z}$ es tal que $p \nmid a$, entonces $a \notin \mathfrak{m}$ y necesariamente $|a| = 1$. Luego si $p \nmid ab$, entonces $|p^n \frac{a}{b}| = |p|^n$ y de ahí se concluye que $||$ es equivalente a $|\,|_p$. □

Y hay también otro caso:

Teorema 5.9: Sea t trascendente sobre $\mathbb{F}_p$. Entonces todos los valores absoluto no triviales sobre $\mathbb{F}_p(t)$ son (salvo equivalencia):

1. $|\,|_q$ para algún polinomio $q(t)$ irreducible.
2. $||_\infty$ dado por $|f(t)/g(t)|_\infty = c^{\deg g - \deg f}$, donde $c \in (0,1)$ es arbitrario.

Demostración: Fijemos un valor absoluto $||$ sobre $\mathbb{F}_p(t) =: K$; nótese que si lo restringimos a $\mathbb{F}_p$ necesariamente dará el valor absoluto trivial.

Supongamos que $|t| \leq 1$, entonces por desigualdad ultramétrica $|f(t)| \leq 1$ para todo $f(x) \in \mathbb{F}_p[x]$ y elijamos $q(t)$ como un polinomio de grado minimal tal que $|p(t)| < 1$. Es fácil probar que $q(t)$ es irreducible (¿por qué?). Sea $g(t)$ otro polinqmio tal que $|g(t)| < 1$, entonces, por algoritmo de la división

$$g(t) = q(t) \cdot h(t) + r(t),$$

donde $\deg r < \deg q$ o $r = 0$. Despejando, tenemos que $r(t) = g(t) - q(t)h(t)$ es también tal que $|r(t)| < 1$, de modo que, por definición de $q(t)$, se ha de cumplir que $r(t) = 0$.

Sea $\phi(t) \in K$, luego $\phi(t) = q(t)^\alpha \cdot \psi(t)$, donde ni el numerador ni el denominador de $\psi(t)$ son divisibles por $q(t)$, de modo que $|\psi(t)| = 1$ y $|\phi(t)| = |q(t)|^\alpha$, y elegir $c := |q(t)| \in (0,1)$.

Por otro lado, supongamos que $|t| > 1$, entonces definamos $y := 1/t$. Nótese que $\mathbb{F}_p(t) = \mathbb{F}_p(y)$ y que $|y| =: c < 1$, de modo que, éste ya es el polinomio de grado minimal tal que $|f(y)| < 1$. Sea $\phi(t) = g(t)/h(t)$ donde $g(t), h(t)$ son polinomios de grados m, n resp., entonces

$$\phi(t) = y^{n-m} \frac{g_1(y)}{h_1(y)},$$

donde $g_1(y), h_1(y)$ son polinomios (respecto a y) que no son divisibles por y, de modo que $|\phi(t)| = c^{n-m}$. □

Al igual que con los valores absoluto p-ádicos, existen infinitas elecciones, por ello hablaremos de las normalizaciones así:

$$\|q(t)\|_q := \left|\frac{\mathbb{F}_p[t]}{(q(t))}\right|^{-1} = p^{-\deg q}, \qquad \|f(t)\|_\infty = p^{\deg f},$$

(en la primera igualdad, el $||$ denota cardinalidad). A veces al teorema anterior se le llama *teorema de Ostrowski para $k(t)$.*

Si k es un cuerpo métrico, entonces podemos importar las siguientes definiciones de la topología/análisis:

Definición 5.10: Sea k un cuerpo métrico. Sea $(a_n)_{n\in\mathbb{N}} \subseteq k$ una sucesión. Se dice que $(a_n)_n$ converge a un límite $L \in k$, denotado $\lim_n a_n = L$, si para todo

$$\forall \epsilon > 0 \exists N \in \mathbb{N} \forall n > N \quad |a_n - L| < \epsilon.$$

Se dice que $(a_n)_n$ es una ***sucesión fundamental*** si es una sucesión de Cauchy, i.e., si para todo $\epsilon > 0$ existe $N \in \mathbb{N}$ tal que

$$\forall n, m > N \quad |a_n - a_m| < \epsilon.$$

Un cuerpo con valor absoluto se dice ***completo*** si toda sucesión fundamental es convergente.

Se dice que un cuerpo K con un valor absoluto $\|\ \|$ es una ***compleción*** de k si:

1. K es completo.
2. K/k es una extensión de cuerpos y $\|x\| = |x|$ para todo $x \in k$.
3. k es (topológicamente) denso en K, i.e., para todo $x \in K$ y todo $\epsilon > 0$ existe $y \in k$ tal que $\|x - y\| < \epsilon$.

Luego veremos otra definición categorial de *compleción* que nos servirá para fines del álgebra conmutativa, pero ésta definición es suficiente por el momento.

Teorema 5.11: Todo cuerpo métrico k posee una compleción. Más aún, sus compleciones son isométricamente isomorfas.[1]

[1] Es decir, existe un isomorfismo de cuerpos que además preserva distancias o, en este caso, que respeta el valor absoluto; en particular, es también un homeomorfismo.

Demostración: Como k es un espacio métrico, entonces posee una compleción K (como espacio) y podemos definir $\|\alpha\| := d(\alpha, 0)$ para $\alpha \in K$, donde d es la métrica en K que extiende a la métrica de k.

Los elementos de K son límites de sucesiones fundamentales en k, así pues definimos $\alpha := \lim_n a_n$ y $\beta := \lim_n b_n$. Luego $\alpha + \beta := \lim_n(a_n + b_n)$, $\alpha \cdot \beta := \lim_n(a_n \cdot b_n)$ y si $\alpha \neq 0$ y $(a_n)_n$ no se anula, entonces se comprueba que $\alpha^{-1} = \lim_n a_n^{-1}$ (esta última es una igualdad, no una definición). Todo ésto se puede comprobar a partir de que la suma, el producto y la inversa es continua en un cuerpo topológico y, en particular, lo es en un cuerpo métrico.

Finalmente, si $(K_1, |\,|_1)$ y $(K_2, |\,|_2)$ son compleciones de k, con los encajes de cuerpos topológicos $f\colon k \to K_1$ y $g\colon k \to K_2$ (que son encajes topológicos y monomorfismos de cuerpos), entonces todos los elementos de K_1 son de la forma $\lim_n f(a_n)$ para alguna sucesión fundamental $(a_n)_n \in k$. Luego definimos:

$$\begin{aligned} \varphi\colon K_1 &\longrightarrow K_2 \\ \lim_n f(a_n) &\longmapsto \lim_n g(a_n), \end{aligned}$$

el cual está bien definido y es un homeomorfismo.[2] Para ver que además es un homomorfismo de cuerpos, basta recordar que f y g lo son, y que la suma, producto e inverso son continuas. □

Corolario 5.11.1: Sea $\varphi\colon k \to L$ un encaje de cuerpos topológicos, donde k es métrico y L es métrico completo. Entonces, $\overline{\varphi[k]}$ (la clausura topológica) es una compleción de k.

Corolario 5.11.2: $\mathbb{R}$ sólo posee un valor absoluto arquimediano salvo equivalencia, $|\,|_\infty$.

Demostración: Basta notar que $\mathbb{R}$ es la compleción de $(\mathbb{Q}, |\,|_\infty)$ y de que todo valor absoluto en $\mathbb{R}$ se restringe a $\mathbb{Q}$. □

Lema 5.12: Sean $|\,|_1, \ldots, |\,|_n$ valores absoluto sobre k tales que ningún par es equivalente. Existe $a \in k$ tal que

$$|a|_1 > 1, \quad \forall i \neq 1 \quad |a|_i < 1.$$

[2]De hecho, ésta misma función es la que se emplea para probar que la compleción de un espacio métrico es única salvo homeomorfismo.

Demostración: Lo probaremos por inducción sobre n. El caso base $n = 2$ esta dado puesto que, por la proposición 5.3, podemos encontrar $b, c \in k$ tales que

$$|b|_1 < 1,\ |b|_2 \geq 1, \quad |c|_1 \geq 1,\ |c|_2 < 1.$$

Luego elegimos $a = bc^{-1}$ y notamos que $|a|_1 < 1$ y $|a|_2 > 1$ como se quería.

Para el caso $n + 1$, por hipótesis inductiva y por lo anterior podemos encontrar $b, c \in k$ tales que

$$|b|_1 > 1, \quad |b|_2 < 1, \cdots, |b|_n < 1$$
$$|c|_1 > 1, \qquad |c|_{n+1} < 1.$$

(a) Si $|b|_{n+1} \leq 1$: Entonces elegimos $a := b^r c$ donde $r \in \mathbb{N}$ no está fijo. Nótese que $|a|_1 > 1$ y $|a|_i = |b|_i^r |c|$ para $1 < i \leq n$, luego como $|b|_i^r \to 0$ podemos elegir r suficientemente grande de modo que $|a|_i < 1$ para $1 < i \leq n$ y es claro que $|a|_{n+1} < 1$.

(b) Si $|b|_{n+1} > 1$: Entonces elegimos

$$a := \frac{b^r}{1 + b^r} c,$$

con $r \in \mathbb{N}$ sin fijar. Como $|b|_i^r \to 0$, entonces se comprueba que $|a|_i < 1$ para todo $1 < i \leq n$ si r es suficientemente grande. Para $j = 1$ o $j = n + 1$, nótese que $|b|_j > 1$ luego nótese que

$$|b|_j^r - 1 \leq |1 + b^r|_j \leq 1 + |b|_j^r$$

por desigualdad triangular, luego

$$1 = \lim_r \frac{|b|_j^r}{|b|_j^r - 1} \geq \lim_r \frac{|b|_j^r}{|1 + b^r|_j} \geq \lim_r \frac{|b|_j^r}{|b|_j^r + 1} = 1,$$

con lo cual, por teorema del sandwich, el límite de al medio converge a 1, luego para un r suficientemente grande se cumple que $|a|_j$ está «cerca» de $|c|_j$ y luego $|a|_1 > 1$ y $|a|_n < 1$ como se quería probar. □

Teorema 5.13 (de aproximación): Sean $|\,|_1, \ldots, |\,|_n$ valores absoluto sobre k tales que ningún par es equivalente. Sean $a_1, \ldots, a_n \in k$ y sea $\epsilon > 0$, entonces existe $a \in k$ tal que

$$\forall 1 \leq i \leq n \quad |a - a_i|_i < \epsilon.$$

Demostración: Empleando el lema, podemos obtener $b_i \in k$ tal que $|b_i|_i > 1$ y $|b_i|_j < 1$ para $j \neq i$. Luego nótese que

$$\lim_r \left| \frac{b_i^r}{1+b_i^r} \right|_i = 1, \qquad \lim_r \left| \frac{b_i^r}{1+b_i^r} \right|_j = 0,\ j \neq i.$$

Luego $a_i b_i^r/(1+b_i^r)$ tendrá valor absoluto en $|\ |_i$ cercano a $|a_i|_i$ y valor absoluto en $|\ |_j$ cercano a 0. Definimos

$$a := \sum_{i=1}^{n} \frac{a_i b_i^r}{1+b_i^r},$$

el cual, con r suficientemente grande, satisface las hipótesis requeridas. □

Nótese que hay un paralelo entre el teorema chino del resto y el teorema de aproximación: En efecto, podemos considerar a los valores absolutos como los p-ádicos y los a_i's como residuos mód p_i, luego el $a \in \mathbb{Q}$ dado satisface que $|a - a_i|_i < p^{-n_i}$, o equivalentemente, satisface que $\nu_{p_i}(a - a_i) \geq n_i$

Corolario 5.13.1: Sean $|\ |_1, \ldots, |\ |_n$ valores absoluto no triviales sobre k tales que ningún par es equivalente, y sean $\eta_j \in \mathbb{R}$. Una relación del estilo

$$\prod_{j=1}^{n} |a|_j^{\eta_j} = 1,$$

para todo $a \in k^\times$ se da syss cada $\eta_j = 0$.

Demostración: Sin perdida de generalidad supongamos que $\eta_1 \neq 0$. Sea a_1 tal que $|a_1|_1^{\eta_1}$ es suficientemente grande, luego podemos elegir $a_j = 1$ para $j \neq 1$ y, por el teorema de aproximación con un ϵ suficientemente pequeño podemos obtener un $\beta \in k$ tal que $|\beta|_1^{\eta_1}$ es suficientemente grande y $|\beta|_j^{\eta_j} \approx 1$ para $j \neq 1$, de modo que la relación falle. □

Ahora, a por una sorpresa:

Proposición 5.14 (fórmula del producto): Para todo $x \in \mathbb{Q}^\times$ se satisface que

$$|x|_\infty \cdot |x|_2 \cdot |x|_3 \cdots = |x|_\infty \cdot \prod_p |x|_p = 1,$$

donde p recorre todos los primos de $\mathbb{Z}$. (Nótese que el producto converge pues $|x|_p = 1$ para todos salvo finitos p's.)

Demostrar ésta proposición no es más que un ejercicio, pero lo interesante es que por el teorema de Ostrowski estamos tomando un producto sobre todos los valores absoluto de $\mathbb{Q}$ salvo equivalencia, y que por el corolario anterior, ésto sería imposible de sólo consistir de finitos factores.

En particular, (y ésto nunca lo he visto mencionado en otra parte) tenemos otra demostración de la infinitud de los primos.

También hicimos el caso de $\mathbb{F}_p(t)$ porque obtenemos el mismo resultado:

Proposición 5.15 (fórmula del producto): Para todo $f(t) \in \mathbb{F}_p(t)^\times$ se satisface que

$$\|f\|_\infty \cdot \prod_{q(t)} \|f\|_q = 1,$$

donde $q(t)$ recorre todos los irreducibles de $\mathbb{F}_p[t]$ salvo asociados.

§5.1.1 Segundo teorema de Ostrowski. El primer teorema de Ostrowski nos clasifica los valores absolutos sobre $\mathbb{Q}$, pero hay una segunda versión, también atribuida a Ostrowski, que nos clasifica los valores absolutos arquimedianos, simplificando enormemente su estudio. En cierta manera, éste teorema nos dará otro indicio de unicidad para $\mathbb{R}$.

Lema 5.16: El único valor absoluto arquimediano $|\,|$ sobre $\mathbb{C}$ es (salvo equivalencia) $|\,|_\infty$.

Demostración: Sea $\zeta = a + b\mathrm{i}$ con $a, b \in \mathbb{R}$. Como $\mathrm{i}^4 = 1$, entonces $|\mathrm{i}| = 1$. Además, sabemos que $|\,|$ en $\mathbb{R}$ es equivalente a $|\,|_\infty$, luego $|a| = |a|_\infty^\lambda$ para algún $\lambda > 0$ real. Luego:

$$|\zeta| = |a + b\mathrm{i}| \leq |a| + |b| = |a|_\infty^\lambda + |b|_\infty^\lambda \leq 2|\zeta|_\infty^\lambda.$$

Luego elijamos α, β y por el teorema de aproximación existe γ tal que $|\alpha - \gamma|, |\beta - \gamma|_\infty < \epsilon$, pero nótese que

$$|\alpha - \gamma|_\infty \geq \left(\frac{|\alpha - \gamma|}{2}\right)^{1/\lambda} \geq \left(\frac{|\alpha - \beta| - \epsilon}{2}\right)^{1/\lambda},$$

lo cual, eligiendo $|\alpha - \beta|$ y ϵ apropiadamente, conlleva a una contradicción. □

Lema 5.17: Sea k un cuerpo métrico completo. Supongamos que $t^2 + 1$ es irreducible en $k[t]$, entonces existe $\Delta > 0$ real tal que

$$\forall a, b \in k \quad |a^2 + b^2| \geq \Delta \,\mathrm{máx}\{|a|^2, |b|^2\}.$$

Demostración: Definamos

$$\Delta := \frac{|4|}{1+|4|}.$$

Probaremos la contrarrecíproca: supongamos que existe $c_1 \in k$ tal que

$$\delta_1 := |c_1^2 + 1| < \Delta < 1,$$

entonces construiremos una sucesión fundamental que converja a una solución del polinomio. Para ello definamos $c_2 := c_1 + h_1$, luego

$$c_2^2 + 1 = c_1^2 + 1 + 2c_1h_1 + h_1^2,$$

por lo que elegimos

$$h_1 := -\frac{(c_1^2+1)}{2c_1},$$

con lo que se comprueba que

$$\delta_2 := |c_2^2 + 1| = |h_1|^2 = \frac{|c_1^2+1|^2}{|4|\,|c_1|^2} \leq \delta_1\theta,$$

donde

$$\theta := \frac{\delta_1}{|4|(1-\delta_1)} < 1,$$

donde empleamos que $|c_1| \geq 1 - \delta_1 > 0$ por desigualdad triangular; nótese que $\delta_2 < \delta_1$. Definiendo por recursión c_n y h_n del mismo modo, vemos que, por inducción sobre n se cumple

$$\delta_{n+1} = |c_{n+1}^2 + 1| = |h_n|^2 \leq \delta_n\theta \leq \delta_1\theta^n.$$

Finalmente, basta notar que $(c_n)_n$ es una sucesión fundamental:

$$|c_{n+1} - c_n|^2 = |h_n|^2 \leq \delta_1\theta^n.$$

Y así, $c^* := \lim_n c_n$ existe y satisface que $|c^{*2} + 1| = \lim_n |c_n^2 + 1| = 0$. □

Lema 5.18: Sea k un cuerpo y $|\,|\colon k \to [0,\infty)$ una función tal que:

1. $|a| = 0$ syss $a = 0$.
2. $|ab| = |a|\,|b|$.
3. Si $|a| \leq 1$, entonces existe $C > 0$ tal que $|1 + a| \leq C$.

Entonces existe un $\lambda > 0$ tal que $|\,|^\lambda$ es un valor absoluto.

Demostración: Es claro que $|\,|^\lambda$ satisface VA1 y VA2, sólo falta probar la desigualdad triangular. Sin perdida de generalidad, podemos suponer que $C > 1$ y así, elegimos λ de modo que $C = 2$.

Ahora, hay que probar la desigualdad triangular. En primer lugar, se comprueba que $|a + b| \leq 2\,\text{máx}\{|a|, |b|\}$. De modo que, por inducción, se comprueba que

$$\left|\sum_{i=1}^{2^r} a_i\right| \leq 2^r \max_i\{|a_i|\},$$

así que eligiendo r de modo que $n \leq 2^r < 2n$ vemos que

$$\left|\sum_{i=1}^{n} a_i\right| \leq 2^r \max_i\{|a_i|\} \leq 2n \max_i\{|a_i|\}.$$

Empleando la desigualdad anterior con cada $a_i = 1$, tenemos $|n| \leq 2n$.

Finalmente, sean $a, b \in k$ arbitrarios y sea $n > 0$ natural, por el teorema del binomio:

$$\begin{aligned} |a+b|^n = \left|\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right| &\leq 2(n+1) \max_i \left\{\left|\tbinom{n}{i}\right| |a|^i\, |b|^{n-i}\right\} \\ &< 4(n+1) \max_i \left\{\tbinom{n}{i} |a|^i\, |b|^{n-i}\right\} \leq 4(n+1)(|a| + |b|)^n, \end{aligned}$$

tomando raíces n-ésimas a ambos lados y considerando el límite cuando $n \to \infty$ se comprueba la desigualdad triangular. □

Lema 5.19: Sea k un cuerpo métrico completo. Supongamos que $t^2 + 1$ es irreducible en $k[t]$, entonces $|\,|$ posee una extensión a un valor absoluto en $k(\sqrt{-1})$.

Demostración: Sea $\mathrm{i} := \sqrt{-1}$ y definamos en $k(\mathrm{i})$:

$$\|a + \mathrm{i}b\| := \sqrt{|a^2 + b^2|}.$$

Es fácil notar que $\|\ \|$ extiende a k. Y es fácil también comprobar que satisface VA1 y VA2. Vamos a comprobar la desigualdad triangular: sean $\alpha, \beta \in k(\mathrm{i})$, la desigualdad es trivial si alguno fuese nulo, así que en caso contrario, elijamos $0 \neq \|\alpha\| \geq \|\beta\|$, entonces vemos que

$$\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\| \iff \left\|1 + \frac{\beta}{\alpha}\right\| \leq 1 + \left\|\frac{\beta}{\alpha}\right\|,$$

donde $\gamma := \beta/\alpha$ satisface que $\|\gamma\| \leq 1$. Así, supongamos que $\|a + \mathrm{i}b\|^2 \leq 1$, entonces, por el lema anterior, se cumple que $|a|, |b| \leq \Delta^{-1/2}$. Luego vemos que

$$\begin{aligned}\|1 + (a + \mathrm{i}b)\|^2 = |(1 + a)^2 + b^2| &\leq 1 + |2|\,|a| + |a|^2 + |b|^2 \\ &\leq 1 + |2|\Delta^{-1/2} + 2\Delta^{-1} =: C^2.\end{aligned}$$

Con lo que se cumple lo pedido. □

Teorema 5.20 – *Segundo teorema de Ostrowski*: Sea k un cuerpo métrico arquimediano. Entonces existe un monomorfismo de cuerpos $\sigma\colon k \to \mathbb{C}$ y una constante real $\lambda > 0$ tales que

$$|x| = |\sigma(x)|_\infty^\lambda.$$

Más aún, si k es completo, entonces k es isométricamente isomorfo a $\mathbb{R}$ o a $\mathbb{C}$.

Demostración: En particular, probaremos lo siguiente:

> Si k es un cuerpo métrico arquimediano completo e $\mathrm{i} = \sqrt{-1} \in k$, entonces k es isométricamente isomorfo a $\mathbb{C}$.

Como k es arquimediano, entonces $\operatorname{car} k = 0$ y contiene a $\mathbb{Q}$. Como es completo, entonces contiene a $\mathbb{R}$ y como contiene a i, entonces contiene a $\mathbb{C}$. Es claro que la restricción de $|\,|$ en $\mathbb{C}$ es equivalente al valor absoluto usual $|\,|_\infty$.

Sea $\alpha \in k$ arbitrario. Luego $z \mapsto |\alpha - z|$ es una función continua de dominio $\mathbb{C}$ y codominio $\mathbb{R}$ que, veremos, alcanza un mínimo. Nótese que $|\alpha - z| \geq |z|_\infty^\lambda - |\alpha|$, de modo que para un radio $R > 0$ suficientemente grande se cumple que si $|z| > R$ entonces $|\alpha - z| \geq |\alpha|$, luego, por compacidad de la bola de radio R, el mínimo se alcanza en su interior, digamos en el complejo $b \in \mathbb{C}$ y definimos $\beta := \alpha - b$. Si $\alpha \notin \mathbb{C}$, entonces $\beta \neq 0$ y $|\beta| > 0$. Nótese que

$$0 < |\beta| = \inf_{z \in \mathbb{C}} |\alpha - z|.$$

Sea $c \in \mathbb{C}$ tal que $0 < |c| < |\beta|$. Por la propiedad superior se cumple que $|\beta - c| \geq |\beta|$. Notemos que

$$\frac{\beta^n - c^n}{\beta - c} = \prod_{\substack{\zeta^n = 1 \\ \zeta \neq 1}} (\beta - \zeta c),$$

como $\mathbb{C}$ contiene a todas las raíces de la unidad, entonces $\zeta c \in \mathbb{C}$ y $|\beta - \zeta c| \geq |\beta|$. Aplicando $|\,|$ a ambos lados se obtiene que:

$$\frac{|\beta - c|}{|\beta|} \leq \frac{|\beta^n - c^n|}{|\beta|^n} = |1 - (c/\beta)^n| = 1 + |c/\beta|^n,$$

el cual converge a 1 para n suficientemente grande. Luego $|\beta - c| \leq |\beta|$ y por antisimetría de $\leq$ se concluye igualdad, es decir, en el complejo $b - c$ también se alcanza el mínimo.

Sustituyendo β por $\beta - c$ y repitiendo el proceso notamos que el mínimo siempre se alcanza en $b - nc$ para todo $n \in \mathbb{N}$, pero

$$|n|\,|c| \leq |\beta| + |\beta - nc| = 2|\beta|.$$

Luego, como $|n| > 1$ para algún n y claramente también para sus potencias, se concluye que $|c| = 0$ lo cual es absurdo por elección de $|c|$. En conclusión, necesariamente $\alpha \in \mathbb{C}$. □

§5.1.2 Valuaciones y dominios de valuación discreta. Como señalamos anteriormente, no estudiaremos en detalle las valuaciones en éste libro, pero aún así veremos instancias de ellas:

Definición 5.21: Una ($\mathbb{R}$-)***valuación*** sobre un anillo A es una función $v\colon A \to \mathbb{R} \cup \{\infty\}$ tal que:

V1. $v(a) = \infty$ syss $a = 0$.

V2. $v(ab) = v(a) + v(b)$ para todo $a, b \in A$.

V3. $v(a + b) = \min\{v(a), v(b)\}$ para todo $a, b \in A$.

Hay una gran familia de ejemplos de valuaciones que será de nuestro interés, para lo cual requerimos el siguiente resultado de álgebra conmutativa (cfr. **[1],** cor. 11.30):

Teorema 5.22 (de las intersecciones de Krull): Sea A un dominio íntegro noetheriano y sea $\mathfrak{a} \lhd A$. Entonces:

$$\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n = 0.$$

Proposición 5.23: Sea A un dominio íntegro noetheriano y sea $\mathfrak{p} \lhd A$ un ideal primo. Definamos $\nu_{\mathfrak{p}}(a) := n$ como el natural tal que $a \in \mathfrak{p}^n$ pero $a \notin \mathfrak{p}^{n+1}$. Entonces $\nu_{\mathfrak{p}} \colon A \to \mathbb{Z} \cup \{\infty\}$ es una $\mathbb{R}$-valuación, llamada la ***valuación $\mathfrak{p}$-ádica***.

Así, las valuaciones p-ádicas que habíamos introducido en el texto son un caso particular de la construcción anterior.

Teorema 5.24: Sea k un cuerpo.

1. Si $|\,|$ es un valor absoluto no arquimediano sobre k, entonces para todo $r \in (0,1)$ real se cumple que $v(a) := \log_r |a|$ es una $\mathbb{R}$-valuación.
2. Recíprocamente, si v es una $\mathbb{R}$-valuación sobre k, entonces para todo $r \in (0,1)$ real se cumple que $|a| := r^{\phi(v(a))}$ es un valor absoluto no arquimediano.

En ambos casos, el anillo de valuación del valor absoluto $|\,|$ y de la valuación v coinciden.

Definición 5.25: Sea k un cuerpo métrico. Decimos que un valor absoluto es ***discreto***, cuando el grupo multiplicativo $\{|a| : a \in k^\times\} \subseteq \mathbb{R}^\times$ es discreto como subespacio (con la topología usual).

Como el grupo multiplicativo de un cuerpo métrico es claramente un grupo topológico, entonces basta notar que el neutro 1 está aislado, vale decir, que existe un $\delta > 0$ tal que

$$1 - \delta < |a| < 1 + \delta \implies |a| = 1.$$

Proposición 5.26: El valor absoluto de un cuerpo es discreto syss en su anillo de valuación $(\mathfrak{o}, \mathfrak{m})$ se cumple que $\mathfrak{m}$ es principal.

Demostración: $\Longleftarrow$. Si $\mathfrak{m} = (\pi)$ es principal, entonces

$$|a| < 1 \implies a \in \mathfrak{m} \implies \exists b \in \mathfrak{o} : a = \pi b \implies |a| \leq |\pi|.$$

Por otro lado, si $|a| > 1$, entonces $|a^{-1}| < 1$ y $|a| \geq |\pi|^{-1}$. Concluimos pues $|\pi| < 1$ (por estar en $\mathfrak{m}$).

$\Longrightarrow$. Si $|\,|$ es discreto, entonces el conjunto

$$\{|a| : |a| < 1\}$$

alcanza su máximo, digamos en $\pi \in \mathfrak{m}$. Luego si $|a| < 1$, entonces $|\pi^{-1}a| \leq 1$ así que $b = \pi^{-1}a \in \mathfrak{o}$ y luego $a = b\pi$ con lo que comprobamos que $\mathfrak{m} = (\pi)$. □

Definición 5.27: Se dice que un anillo A es un ***dominio de valuación discreta*** si existe un valor absoluto discreto $||$ sobre $\operatorname{Frac} A$ tal que A es el anillo de valuación de $||$.

El nombre proviene de que un anillo es de valuación discreta si existe una valuación v con valores en $\mathbb{Z}$ que es positiva y tal que los elementos del maximal son aquellos de valuación no nula.

Corolario 5.27.1: Sea A un dominio de valuación discreta v. Entonces:

1. Todos los ideales impropios de A son de la forma:
$$\mathfrak{a}_n = \{x \in A : v(x) \geq n\}.$$
2. A es noetheriano.
3. A es local y su único ideal maximal es $\mathfrak{a}_1$.

Demostración: Es claro que de la primera se sigue el resto. Supongamos que $v(x) = v(y)$, entonces supongamos que $xy^{-1} \in A$ (por ser anillo de valuación), luego $v(xy^{-1}) = 0$, por lo que es inversible y luego $(x) = (y)$. Si $\mathfrak{b} \lhd A$ es un ideal impropio, entonces $v[\mathfrak{b}] \subseteq \mathbb{N}$, por lo que posee un mínimo n y un $x \in \mathfrak{b}$ con $v(x) = n$, luego es fácil concluir que $\mathfrak{b} = (x) = \mathfrak{a}_n$. □

Definición 5.28: Si $(A, \mathfrak{m})$ es un dominio de valuación discreta y $\mathfrak{m} = (\pi)$, entonces decimos que π es un ***uniformizador*** de A.

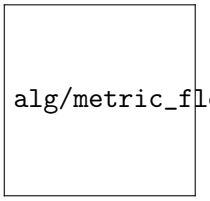


Figura 5.1. Cuerpo métrico discreto.

5.2 Análisis ultramétrico

La siguiente proposición es fundamental y la emplearemos a lo largo de casi toda la teoría:

Proposición 5.29: Sea k un cuerpo ultramétrico. Si $a, b \in k$ son tales que $|a| < |b|$, entonces $|a + b| = |b|$.

Demostración: Claramente $|a + b| \leq |b|$ y nótese que

$$|b| = |(a + b) + (-a)| \leq \text{máx}\{|a|, |a + b|\}. \qquad \square$$

Definición 5.30: Sea k un cuerpo métrico y sea $(a_n)_{n\in\mathbb{N}} \subseteq k$ una sucesión. Decimos que la suma formal $\sum_{n\in\mathbb{N}} a_n$ converge a un valor S, si la sucesión de las sumas parciales:

$$S_n := \sum_{i=0}^{n} a_n$$

converge a S; en cuyo caso anotaremos que $S = \sum_{n=0}^{\infty} a_n$.

Proposición 5.31: Sea k un cuerpo ultramétrico completo. La serie $\sum_{n\in\mathbb{N}} a_n$ converge syss $\lim_n a_n = 0$.

Demostración: $\Longrightarrow$. Basta notar que

$$\lim_n a_n = \lim_n (s_n - s_{n-1}) = (\lim_n S_n) - (\lim_n S_{n-1}) = S - S = 0.$$

$\Longleftarrow$. Basta notar que, por desigualdad ultramétrica, se cumple que para $m > n$

$$|S_m - S_n| = |a_{n+1} + a_{n+2} + \cdots + a_m| \leq \text{máx}\{|a_j| : n < j \leq m\},$$

el cual, eligiendo n suficientemente grande, podemos acotar por un $\epsilon > 0$ arbitrario, y así, la sucesión $(S_n)_n$ es fundamental y converge. $\square$

Ésto genera un símil con las series de $\mathbb{C}$, pero demuestra por qué la propiedad de ser *no arquimediano* es mucho más potente (¡y útil!) en éstos casos. Otro ejemplo es que casi siempre podemos intercambiar sumas:

Proposición 5.32: Sea k un cuerpo ultramétrico completo, $(a_{ij})_{i,j} \in k$ una sucesión (doble). Si para todo $\epsilon > 0$ existe un N tal que $|a_{ij}| < \epsilon$ si $\max\{i,j\} \geq N$, entonces las series inducidas

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_{ij}, \qquad \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} a_{ij},$$

convergen y coinciden.

Demostración: Sea $\epsilon > 0$ arbitrario y N como en la hipótesis. Luego, nótese que $|a_{ij}| < \epsilon$ para todo $i \geq N$, de modo que la serie $\left|\sum_{j=0}^{\infty} a_{ij}\right| < \epsilon$ converge para todo $i \geq N$ y en el resto de índices también, luego es claro que la serie doble también.

Finalmente, nótese que

$$\left|\sum_{i=0}^{N}\sum_{j=0}^{N} a_{ij} - \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_{ij}\right| < \epsilon,$$

y como el término de la izquierda es una suma finita, así que podemos reordenarla y así es fácil concluir que ambas sumas coinciden. □

Definición 5.33: Sea k un cuerpo métrico, dada una serie formal

$$f(x) := f_0 + f_1 x + f_2 x^2 + \cdots \in k[[x]],$$

se define su ***radio de convergencia*** como:

$$R := \frac{1}{\limsup_n |f_n|^{1/n}} \in [0, \infty]$$

(con el convenio usual de que si $\limsup_n |f_n|^{1/n} = 0$, entonces $R = \infty$). Definimos su ***dominio de convergencia*** como el conjunto $\mathcal{D} \subseteq k$ en donde la serie determinada por $f(x)$ converge.

Proposición 5.34: Sea k un cuerpo ultramétrico completo, y sea $f(x) \in k[[x]]$ una serie formal con radio de convergencia R y dominio de convergencia $\mathcal{D}$. Entonces:

(a) Si $R = 0$, entonces $\mathcal{D} = \{0\}$.

(b) Si $R = \infty$, entonces $\mathcal{D} = k$.

(c) Si $0 < R < \infty$ y $|f_n|R^n \to 0$, entonces

$$\mathcal{D} = \overline{B}_R(0) = \{a \in k : |a| \leq R\}.$$

(d) Si $0 < R < \infty$ y $|f_n|R^n \not\to 0$, entonces

$$\mathcal{D} = B_R(0) = \{a \in k : |a| < R\}.$$

Lema 5.35: Sea k un cuerpo ultramétrico completo. Sea $f(x) \in k[[x]]$ una serie formal con dominio de convergencia $\mathcal{D}$ y sea $c \in \mathcal{D}$. Para $m \in \mathbb{N}$ definamos

$$g_m := \sum_{n \geq m} \binom{n}{m} f_n c^{n-m}, \tag{5.1}$$

entonces la serie formal $g(x) := g_0 + g_1 x + g_2 x^2 + \cdots \in k[[x]]$ tiene el mismo dominio de convergencia $\mathcal{D}$ y para todo $b \in \mathcal{D}$ se cumple que $f(b+c) = g(b)$.

Demostración: Nótese que $|g_m| \leq \sup_{n \geq m}\{|f_n c^{n-m}|\}$ y, por hipótesis, $f_n c^{n-m} \to 0$ para m fijo; de modo que aplicando la proposición anterior es fácil verificar que los dominios de convergencia coinciden. Para $b \in \mathcal{D}$, vemos que

$$f(b+c) = \sum_{n=0}^{\infty} f_n (b+c)^n = \sum_{n=0}^{\infty} \sum_{m=0}^{n} \binom{n}{m} f_n c^{n-m} b^m,$$

y aplicando intercambio de series dobles se concluye el enunciado. □

Corolario 5.35.1: Sea k un cuerpo ultramétrico completo, y sea $f(x) \in k[[x]]$ una serie formal con dominio de convergencia $\mathcal{D}$. Entonces $f\colon \mathcal{D} \to k$ (como función) es continua.

Demostración: Es fácil comprobar que toda serie formal (como función) es continua en el 0, y el lema anterior permite ver que en otro punto de $\mathcal{D}$ es también una serie formal centrada en 0 y, por ende, continua. □

Definición 5.36: Sea k un cuerpo ultramétrico. Un subconjunto $S \subseteq k$ se dice un ***conjunto de representantes de restos*** si para toda clase de equivalencia C de su cuerpo de restos de clases $\mathfrak{o}/\mathfrak{m}$ se cumple que existe exactamente un elemento de C en S.

Proposición 5.37: Sea k un cuerpo ultramétrico discreto. Sea $(\mathfrak{o}, \mathfrak{m})$ su anillo de valuación y sea $(\pi) = \mathfrak{m}$. Si S es un conjunto de representantes

de restos y $(\pi_j)_{j\in\mathbb{N}}$ es una sucesión tal que cada $|\pi_j| = |\pi|^j$, entonces todo elemento $a \in \mathfrak{o}$ se escribe de forma única como

$$a = \sum_{n=0}^{\infty} a_n \pi_n, \qquad a_i \in S.$$

Demostración: Como acotación, nótese que si k es completo entonces las series de esa forma siempre convergen por la proposición 5.31, de modo que hay una correspondencia biunívoca.

Sea $a \in \mathfrak{o}$, entonces considere la clase de equivalencia $[a] \in \mathfrak{o}/(\pi)$, nótese que, por definición de S, existe un único $a_0 \in S$ tal que $a_0 \equiv a/\pi_0 \pmod{\pi}$, vale decir, tal que $a - a_0\pi_0 = b_0\pi_1$ para un único $b_0 \in \mathfrak{o}$. Análogamente existe un único $a_1 \in S$ tal que $a_1 \equiv b_0 \pmod{\pi}$, vale decir, tal que $(b_0 - a_1)\pi_1 = b_1\pi_2$ para un único $b_1 \in \mathfrak{o}$; luego notamos que $a = a_0\pi_0 + a_1\pi_1 + b_1\pi_2$. Así procedemos definiendo por recursión $(a_n)_n \subseteq S$ y $(b_n)_n \in \mathfrak{o}$. Luego, comprobamos que

$$\left| a - \sum_{n=0}^{N} a_n \pi_n \right| = |b_N \pi_N| \leq |\pi|^N,$$

donde como $|\pi| < 1$, vemos que para $N \to \infty$ el valor absoluto converge a 0, o equivalentemente, $a = \sum_{n=0}^{\infty} a_n \pi_n$.

Para comprobar unicidad empleamos un método similar. Si $\sum_{n=0}^{\infty} c_n \pi^n = \sum_{n=0}^{\infty} a_n \pi^n$, entonces vemos que $c_0 \equiv a_0 \pmod{\pi}$ con lo que $c_0 = a_0$ por definición de conjunto de representantes de restos, y así vamos inductivamente comprobando. □

Tradicionalmente se emplea la sucesión $\pi_j := \pi^j$, pero ésta ligera generalización será útil más adelante. Nótese que en un cuerpo ultramétrico discreto k tenemos que $k = \operatorname{Frac}\mathfrak{o} = \mathfrak{o}[\pi^{-1}]$, de modo que todo $a \in k$ es tal que $\pi^j a \in \mathfrak{o}$ para algún $j \geq 0$, luego todo $a \in k$ admite una expansión

$$a = \sum_{n=-j}^{\infty} a_j \pi^j = a_{-j}\pi^{-j} + \cdots + a_{-1}\pi^{-1} + a_0 + a_1\pi + \cdots$$

Series de éste estilo se dicen *series de Laurent*, surgen naturalmente en el análisis complejo y fueron parte de la motivación para estudiar $\mathbb{Q}_p$.

Teorema 5.38: Sea k un cuerpo ultramétrico discreto, completo y que su cuerpo de restos de clases es finito. Entonces $\mathfrak{o}$ es (topológicamente) compacto.

Demostración: Para espacios métricos, ser compacto equivale a ser secuencialmente compacto (cf. [**2,** Teo. 3.55]). Así pues, debemos comprobar que dada una sucesión $(a_j)_{j\in\mathbb{N}} \subseteq \mathfrak{o}$, entonces posee una subsucesión convergente. Sea S un conjunto de representantes de restos, el cual es finito por hipótesis; por la proposición anterior se cumple que

$$a_j = \sum_{n=0}^{\infty} a_{jn}\pi^n, \qquad a_{j,n} \in S.$$

Nótese que para cada n hay una sucesión $(a_{j,n})_j$ de puntos en S, luego necesariamente hay un valor que se repite infinitamente, para $j = 0$ escogemos una subsucesión $\sigma(j, 0)$ tal que $a_{\sigma(j,0),0}$ es constante. Similarmente, para $j = 1$ podemos extraer una subsucesión $\sigma(j, 1)$ de $\sigma(j, 0)$ tal que $a_{\sigma(j,0),0}$ y $a_{\sigma(j,1),1}$ son ambas constantes. Y esto lo podemos hacer para todo j, y finalmente definimos $\eta(j) := \sigma(j, j)$, la cual fija a la coordenada n-ésima para todo $j \geq n$, luego notamos que claramente converge. □

Corolario 5.38.1: Sea k un cuerpo ultramétrico. Son equivalentes:

1. k es localmente compacto.

2. k es completo, discreto y su cuerpo de restos de clases es finito.

Note que si uno quiere extender el corolario a cuerpos métricos arquimedianos, entoces ser localmente compacto equivale a ser completo por el teorema de Ostrowski.

Teorema 5.39: Todo cuerpo ultramétrico es hereditariamente disconexo.

Demostración: Sea $(k, |\,|)$ un cuerpo ultramétrico. Si $|\,|$ es trivial, entonces k es un espacio discreto así que se satisface. Si $|\,|$ no es trivial, basta probar que posee una base de la topología formada por conjuntos abiertos y cerrados; en particular, probaremos que las bolas abiertas son siempre cerradas.

Sea $\epsilon > 0$ y $a \in k$. Sea $b \in B_\epsilon(a)^c$, entonces $B_\epsilon(b) \cap B_\epsilon(a) = \varnothing$ pues si $c \in B_\epsilon(b)$ entonces

$$|c - b| < \epsilon \leq |b - a| \implies |c - a| = |b - a| \geq \epsilon.$$

Así pues, $B_\epsilon(b) \subseteq B_\epsilon(a)^c$, por lo que $B_\epsilon(a)^c$ es abierto y $B_\epsilon(a)$ es cerrado. □

§5.2.1 El teorema de Strassmann y aplicaciones.

Teorema 5.40 – *Teorema de Strassmann*: Sea k un cuerpo ultramétrico completo, y sea $f(x) \in k[[x]]$ una serie formal no nula. Supongamos que $f_n \to 0$ (o equivalentemente, tal que f converge en $\mathfrak{o}$), entonces $f(a) = 0$ para finitos $a \in \mathfrak{o}$'s. Más aún, hay a lo más N raíces $a \in \mathfrak{o}$, donde N es el natural tal que $|f_N| > |f_n|$ para todo $n > N$.

Demostración: Lo haremos por inducción sobre N.

Si $N = 0$, entonces no puede darse que $f(a) = 0$ para algún $a \in \mathfrak{o}$, pues

$$f_0 = -\sum_{n=1}^{\infty} f_n a^n,$$

pero

$$\left|\sum_{n=1}^{\infty} f_n a^n\right| \leq \max_{n\geq 1} |f_n a^n| \leq \max_{n\geq 1} |f_n| < |f_0|.$$

Si $N > 0$, entonces sea $a \in \mathfrak{o}$ tal que $f(a) = 0$ y sea $b \in \mathfrak{o}$, entonces

$$f(b) = f(b) - f(a) = \sum_{n=1}^{\infty} f_n(b^n - a^n) = (b-a)\sum_{n=1}^{\infty}\sum_{j<n} f_n b^j a^{n-j-1},$$

luego, intercambiando sumatorias y definiendo:

$$g(x) := \sum_{j=0}^{\infty} g_j x^j, \qquad g_j := \sum_{r=0}^{\infty} f_{j+1+r} a^r;$$

se tiene que $f(b) = (b-a)g(b)$. En particular se puede verificar que:

- $|g_{N-1}| = |f_N|$.
- $|g_j| \leq |f_N|$ para todo j y $|g_j| < |f_N|$ para $j > N-1$.

Luego, por hipótesis inductiva, g posee a lo más $N-1$ ceros en $\mathfrak{o}$ y así, f posee a lo más N ceros en $\mathfrak{o}$. □

Corolario 5.40.1: Sea k un cuerpo ultramétrico completo. Dos series formales $f(x), g(x) \in k[[x]]$ que convergen en $\mathfrak{o}$ son iguales syss $f(a) = g(a)$ para infinitos $a \in \mathfrak{o}$.

Corolario 5.40.2: Sea k un cuerpo ultramétrico completo de $\operatorname{car} k = 0$. Sea $f(x) \in k[[x]]$ una serie formal que converge en $\mathfrak{o}$ tal que $f(x+d) = f(x)$ para algún $d \in \mathfrak{o}_{\neq 0}$, entonces f es constante.

Demostración: Basta notar que $f(x) - f(0)$ tiene infinitos ceros en $x = nd \in \mathfrak{o}$ para todo $n \in \mathbb{Z}$. □

Un ejemplo del cómo emplear el teorema de Strassmann radica en las sucesiones por recursión lineal.

Un ejemplo es la siguiente aplicación detallada en Alter y Kubota **[64]:**

Ejercicio 5.41: Este problema tiene por objetivo resolver $x^2+11z^2 = 3^n$.

1. Considere la sucesión

$$a_0 := 0, \qquad a_1 := 1, \qquad a_{n+2} := a_{n+1} - 3a_n,$$

demuestre que

$$a_n = \frac{1}{\sqrt{-11}}(r^n - r'^n).$$

2. Demuestre que $a_{n+m} = a_{n+1}a_m - 3a_n a_{m-1}$.
3. Demuestre que $(a_n; a_m) = \pm a_{(n;m)}$.
4. Concluya que la ecuación diofántica $a_n = t$ con $t \in \mathbb{Z}$ tiene a lo más una solución para un t fijo, salvo si $t = 1$, en cuyo caso, admite tres soluciones ($n \in \{1, 2, 5\}$).
5. Emplee lo anterior para concluir que $x^2 + 11z^2 = 3^n$ tiene a lo más una solución con $x \geq 0$.

§5.2.2 Lema de Hensel y anillos henselianos. El llamado lema de Hensel es una de las herramientas más importantes en teoría de cuerpos de clases y ha probado ser de extrema utilidad. En primer lugar introducimos un glosario de las distintas versiones en las que se puede encontrar el lema de Hensel:

Teorema 5.42: Sea $(A, \mathfrak{m}, k)$ un anillo local y fijemos $|\,| := |\,|_{\mathfrak{m}}$ el valor absoluto $\mathfrak{m}$-ádico. Son equivalentes:

1. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $f(a_0) \equiv 0 \pmod{\mathfrak{m}}$, entonces existe $a \equiv a_0 \pmod{\mathfrak{m}}$ tal que $f(a) = 0$.

2. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $|f(a_0)| < 1$ y $|f'(a_0)| = 1$, entonces existe $a \equiv a_0 \pmod{\mathfrak{m}}$ tal que $f(a) = 0$.

3. Sea $f(x) \in A[x]$ mónico. Si existe a_0 tal que $|f(b)| < |f'(b)|^2$, entonces existe un único $a \in A$ tal que $f(a) = 0$ y $|a - b| < |f'(b)|$.

4. Sea $f(x) \in A[x]$ mónico. Si $f \equiv g_0 h_0 \pmod{\mathfrak{m}}$ con g_0 mónico y $g_0, h_0 \in k[x]$ coprimos (en $k[x]$), entonces existen $g, h \in A[x]$ tales que $f = gh$, $g \equiv g_0$ y $h \equiv h_0 \pmod{\mathfrak{m}}$.

Definición 5.43: Un anillo local $(A, \mathfrak{m}, k)$ que satisface lo anterior, se dice un ***anillo henseliano***. Un cuerpo métrico $(K, |\,|)$ se dice ***henseliano*** si o bien es arquimediano y completo, o bien es ultramétrico y su anillo de valuación es henseliano.

Teorema 5.44 – *Lema de Hensel*: Todo cuerpo métrico completo k es henseliano.

Demostración: Sean $f_j(x) \in \mathfrak{o}[x]$ polinomios tales que

$$f(x + y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots \in \mathfrak{o}[x, y],$$

donde los f_i's vendrán dados por expandir un binomio de Newton en cada monomio original. Se puede comprobar que $f_1(x) = f'(x)$. Luego, por el enunciado, existe $b_0 \in \mathfrak{o}$ tal que

$$f(a_0) + b_0 f_1(a_0) = 0,$$

luego, definamos $a_1 := a_0 + b_0$ y notemos que por desigualdad ultramétrica

$$|f(a_1)| = |f(a_0 + b_0)| \leq \max_{j \geq 2} |f_j(a_0) b_0^j|,$$

como $f_j(a_0) \in \mathfrak{o}$ entonces $|f_j(a_0)| \leq 1$, luego

$$|f(a_1)| \leq |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} < |f(a_0)|,$$

además de que $|b_0| < |f'(a_0)|$. Del mismo modo se nota que

$$|f'(a_1) - f'(a_0)| \leq |b_0| < |f'(a_0)|.$$

Luego se cumple que $|f'(a_1)| = |f'(a_0)|$. Ahora podemos volver a elegir un b_1 con las mismas propiedades, en particular, notando que $|f(a_1)| < |f(a_0)| \leq |f'(a_0)|^2 = |f'(a_1)|^2$, y así recursivamente comprobamos que

$$|f(a_{n+1})| \leq |b_n|^2 = \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2},$$

como $|f'(a_0)|^2$ es solo una constante, entonces vemos que $|f(a_n)| \to 0$ y luego, por la igualdad superior, $b_n \to 0$, de modo que $(a_n)_n$ es una sucesión fundamental que converge a una raíz de f (¿por qué está en $\mathfrak{o}$?). □

Veamos algunas aplicaciones del lema de Hensel:

Teorema 5.45: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 2$: Sea $b \in \mathbb{Z}_p$ tal que $|b| = 1$ (i.e., $p \nmid b$). Supongamos que b es un residuo cuadrático módulo p, entonces b es un cuadrado en $\mathbb{Z}_p$.
- Si $p = 2$: Sea $b \in \mathbb{Z}_2$ tal que $b \equiv 1 \pmod 8$, entonces existe algún $a \in \mathbb{Z}_p$ tal que $b = a^2$.

Demostración: En ambos casos se emplea el lema con $f(x) := x^2 - b$. Nótese que $f'(x) = 2x$. El ser residuo cuadrático equivale a que existe a_0 con $a_0^2 \equiv b \pmod p$, de modo que $|f(a_0)| < 1 = |2a_0|^2 = |f'(a_0)|^2$ (pues $|2| = 1$). Para el segundo caso evaluamos en $a_0 = 1$ y se tiene que $|f(1)| \leq 2^{-3} < 2^{-2} = |2|^2$. □

Nótese que la condición de que $b \equiv 1 \pmod 8$ nos dice que b es un residuo cuadrático módulo 2^n para todo $n > 0$.

Corolario 5.45.1: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 2$: El grupo $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, y representantes de las clases laterales son $1, p, c, cp$ con c un residuo no cuadrático módulo p. En consecuencia, $\mathbb{Q}_p$ tiene exactamente 3 extensiones cuadráticas.
- Si $p = 2$: El grupo $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$, y representantes de las clases laterales son los generados por $-1, 5, 2$. En consecuencia, $\mathbb{Q}_2$ tiene exactamente 7 extensiones cuadráticas.

Demostración: Sea x un número no nulo libre de cuadrados en $\mathbb{Z}_p$ con $p \neq 2$. Aplicamos reducción módulo p: si $x \not\equiv 0 \pmod p$, entonces x es una

unidad y existe $y \in \mathbb{Z}_p$ tal que $xy = c$, luego $y = c/x$ es un residuo cuadrático no nulo módulo p (pues es división de dos residuos no cuadradáticos) y por lo tanto $[c] = [x] \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. Si $x \equiv 0 \pmod{p}$, entonces como $p^2 \nmid x$ se tiene que $x/p \not\equiv 0 \pmod{p}$ luego, o bien x/p es un cuadrado o no, i.e., o bien $[x] = [p]$ o bien $[x] = [cp] \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

Para $p = 2$ siga un procedimiento similar. Otra manera de verlo es que $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ es un grupo abeliano de ocho elementos y tal que $[x^2] = 1$ para todo elemento del grupo. □

Proposición 5.46: Sea $p \in \mathbb{Z}$ primo:

- Si $p \neq 3$: Sea $b \in \mathbb{Z}_p$ con $|b| = 1$. Supongamos que b un residuo cúbico módulo p, entonces b es un cubo en $\mathbb{Z}_p$.
- Si $p = 3$: Sea $b \in \mathbb{Z}_3$ con $|b| = 1$. Se cumple que $b \equiv \pm 1 \pmod{9}$ syss b es un cubo en $\mathbb{Z}_3$.

Demostración: En éste caso empleamos el lema de Hensel con $f(x) := x^3 - b$. Veamos el caso de $p = 3$. La condición de que $b \equiv \pm 1$ (9) se traduce en que existe $e \in \{0, \pm 1\}$ tal que $b \equiv \pm(1 + 3e)^3 \pmod{27}$. Luego con $a_0 := \pm(1+3e)^3$ vemos que $|f(a_0)| \leq 3^{-3}$ y que $|f'(a_0)| = |3|\,|a_0^2| = 3^{-1}$. □

Aquí vemos un ejemplo del «comportamiento local» de los p-ádicos. Para hablar de ecuaciones diofantinas conviene admitir la siguiente terminología:

Definición 5.47: Se dice que $\mathbb{Q}$ es un ***cuerpo global*** y que sus compleciones $\mathbb{R}, \mathbb{Q}_p$ son ***cuerpos locales***.

Como los cuerpos locales contienen al cuerpo global, vemos la siguiente observación a modo de eslógan:

> *La existencia de soluciones globales implica la existencia de soluciones locales.*

Una pregunta interesante sería tener una especie de recíproco, vale decir, ¿existen soluciones globales si existen soluciones locales en todas partes? La respuesta en general es que no:

Ejercicio 5.48: La ecuación diofántica:

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

tiene soluciones locales en todas partes, pero no soluciones globales.

Demostración: Es claro que la ecuación no posee soluciones globales. Por otro lado, sabemos que 2 es un cuadrado en $\mathbb{Q}_{17}$ y que 17 es un cuadrado en $\mathbb{Q}_2$ pues $17 \equiv 1 \pmod 8$. Finalmente, nótese que en $\mathbb{Z}_p$ con $p \notin \{2, 17\}$ siempre se cumple que $2, 17, 34$ son inversibles (tienen $|\,| = 1$) y siempre alguno es un cuadrado módulo p (basta expresarlos como potencias de una raíz primitiva). □

5.3 Extensiones del valor absoluto

En ésta sección veremos como dada una extensión de cuerpos L/k con k (ultra)métrico, podemos asignarle un valor absoluto a L que extienda al de k. Para ello, contemplaremos dos posibilidades.

§5.3.1 Extensiones trascendentes.

Teorema 5.49: Sea $(k, |\,|)$ un cuerpo ultramétrico y sea $c > 0$ arbitrario. Para $f(x) = f_0 + f_1 x + \cdots + f_n x^n \in k[x]$ defínase

$$\|f\| = \|f\|_c := \max_j\{|f_j| c^j\}.$$

Para $h(x) = f(x)/g(x) \in k(x)$ extendamos $\|h\| := \|f\|/\|g\|$. Entonces $\|\,\|$ es un valor absoluto sobre $k(x)$ que extiende a $|\,|$.

Demostración: Primero veamos algunos axiomas para polinomios $f(x) \in k[x]$. Evidentemente $\|f\| = 0$ syss $f = 0$, y la desigualdad ultramétrica se comprueba, pues si $f(x) := \sum_{j\geq 0} f_j x^j, g(x) := \sum_{j\geq 0} g_j x^j$, entonces

$$\|f + g\| = \max_j\{|f_j + g_j| c^j\} \leq \max_j\{\max\{|f_j|, |g_j|\} c^j\} = \max\{\|f\|, \|g\|\}.$$

Claramente, $\|fg\| \leq \|f\|\,\|g\|$, veamos que se alcanza igualdad: Sean $I, J \geq 0$ los naturales tales que

$$\begin{aligned} \|f_I x^I\| &= \|f\|, & \forall i \leq I \quad \|f_i x^i\| &< \|f\|, \\ \|g_J x^J\| &= \|g\|, & \forall j \leq J \quad \|g_j x^j\| &< \|g\|, \end{aligned}$$

El coeficiente de x^{I+J} en $f \cdot g$ es $\sum_{i+j=I+J} f_i g_j$. Separamos por casos:

(a) Si $i < I$: Entonces $\|f_i x^i\| < \|f\|$, o equivalentemente, $|f_i| < c^{-i}\|f\|$ y $\|g_j x^j\| \leq \|g\| \iff |g_j| \leq c^{-j}\|g\|$. Luego:

$$|f_i g_j| < c^{-i-j}\|f\|\,\|g\| \iff \|f_i g_j x^{I+J}\| < \|f\|\,\|g\|. \tag{5.2}$$

(b) Si $j < J$: Se concluye (5.2) análogamente.

(c) Si $(i,j) = (I,J)$: Entonces $|f_I| = c^{-I}\|f\|$ y $|g_J| = c^{-J}\|g\|$, por lo que

$$|f_I g_J| = c^{-I-J}\|f\|\,\|g\| \iff \|f_I g_J x^{I+J}\| = \|f\|\,\|g\|.$$

En conclusión:

$$\left\| \sum_{i+j=I+J} f_i g_j x^{I+J} \right\| = \|f\|\,\|g\|,$$

de modo que $\|f \cdot g\| \geq \|f\|\,\|g\|$, y luego $\|fg\| = \|f\|\,\|g\|$ (VA2).

Por VA2 se puede comprobar que la extensión a $k(x)$ está bien definida y es fácil ver que es un valor absoluto que extiende a $|\,|$. □

Corolario 5.49.1: Sea $(k, |\,|)$ un cuerpo ultramétrico. Sea $\boldsymbol{x} := (x_1, \ldots, x_n)$ una tupla de indeterminadas, y sea $\boldsymbol{c} := (c_1, \ldots, c_n)$ una tupla de reales > 0. Para $f(\boldsymbol{x}) = \sum_\alpha f_\alpha \boldsymbol{x}^\alpha \in k[\boldsymbol{x}]$, en notación multiíndice, defínase

$$\|f\|_{\boldsymbol{c}} := \max_\alpha \{|f_\alpha| \boldsymbol{c}^\alpha\}.$$

Y para $h := f/g \in k(\boldsymbol{x})$ extendamos $\|h\|_{\boldsymbol{c}} := \|f\|/\|g\|$. Entonces $\|\,\|_{\boldsymbol{c}}$ es un valor absoluto sobre $k(\boldsymbol{x})$ que extiende a $|\,|$.

Proposición 5.50: Sea k un cuerpo ultramétrico, $c > 0$ arbitrario y sea $\|\,\| := \|\,\|_c$. Sean $R(x) \in k[x]$, y $G(x) = \sum_{j=0}^m G_j x^j \in k[x]$ no nulo tal que $\|G\| = \|G_m x^m\|$. Sean $L(x), M(x) \in k[x]$ tales que

$$R(x) = L(x)G(x) + M(x), \qquad M = 0 \vee \deg M < m.$$

Entonces $\|L\|\,\|G\| \leq \|R\|$ y $\|M\| \leq \|R\|$.

Demostración: Sea $R(x) = R_0 + R_1 x + \cdots + R_n x^n$ con $R_n \neq 0$ y sea $L(x) = L_0 + \cdots + L_{n-m} x^{n-m}$. Los coeficientes de $L(x)$ son tales que satisfacen el sistema de ecuaciones lineales

$$G_m L_{n-m-j} + G_{m-1} L_{n-m-j+1} + \cdots + G_{m-j} L_{n-m} = R_{n-j},$$

donde $j \leq \min\{m, n-m\}$. Empleando el hecho de que $\|G\| = \|G_m x^m\|$ se prueba, por inducción, que

$$\|L_{n-m-j} x^{n-m-j}\|\,\|G\| \leq \|R\|,$$

de lo que se comprueba que $\|L\|\,\|G\| \leq \|R\|$. Finalmente, $M = R - LG$ implica que $\|M\| \leq \|R\|$ (por desigualdad ultramétrica). □

Teorema 5.51 (lema de Gauss): Sea k un cuerpo ultramétrico y sea $\boldsymbol{x} := (x_1, \ldots, x_n)$ una tupla de indeterminadas. Si $f(\boldsymbol{x}) \in \mathfrak{o}[\boldsymbol{x}]$ es un producto de polinomios no constantes en $k[\boldsymbol{x}]$, entonces también es un producto de polinomios no constantes en $\mathfrak{o}[\boldsymbol{x}]$.

Demostración: Considere la extensión $\| \, \| := \| \, \|_{(1,\ldots,1)}$ en $k(\boldsymbol{x})$. Nótese que el grupo de valores de $\| \, \|$ coincide con el de $| \, |$ y también:

$$\mathfrak{o}[\boldsymbol{x}] = \{f \in k[\boldsymbol{x}] : \|f\| \leq 1\}.$$

Si $f = gh$ para algunos $g, h \in k[\boldsymbol{x}]$ no constantes, entonces existe $a \in k$ tal que $|a| = \|g\|$, luego sustituyendo g por $a^{-1}g$ podemos suponer que $\|g\| = 1$ y así:

$$1 \geq \|f\| = \|g\| \, \|h\| = \|h\|,$$

luego, $g, h \in \mathfrak{o}[\boldsymbol{x}]$ como se quería probar. □

Corolario 5.51.1: Sea k un cuerpo ultramétrico. Si $f \in \mathfrak{o}[\boldsymbol{x}]$ es irreducible en $\mathfrak{o}[\boldsymbol{x}]$, entonces también lo es en $k[\boldsymbol{x}]$.

Éste teorema lo probamos en más generalidad con el nombre de *criterio de irreducibilidad de Gauss* en [**1,** Teo. 2.86]. Gauss originalmente formuló su criterio en el siguiente contexto:

Proposición 5.52 (lema de Gauss): Sea $f(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$. Si f es un producto de polinomios no constantes en $\mathbb{Q}[\boldsymbol{x}]$, entonces lo es en $\mathbb{Z}[\boldsymbol{x}]$.

Demostración: Sea $f = gh$ para algunos $g, h \in \mathbb{Q}[\boldsymbol{x}]$ no constantes. Luego, $g, h \in \mathbb{Z}_p[\boldsymbol{x}]$ para todo primo $p \notin S$, donde S es un conjunto finito (¿cuál conjunto?). Nótese que $\bigcap_p \mathbb{Z}_p = \mathbb{Z}$, por lo que si $S = \varnothing$, entonces está probado.

Si $S \neq \varnothing$, entonces para todo $p \in S$ la demostración del lema de Gauss nos da que existe $m(p) \in \mathbb{Z}$ tal que $p^{m(p)}g \in \mathbb{Z}_p[\boldsymbol{x}]$ y $p^{-m(p)}h \in \mathbb{Z}_p[\boldsymbol{x}]$. Así, definiendo

$$r := \prod_{p \in S} p^{m(p)},$$

se obtiene que $rg, r^{-1}h \in \mathbb{Z}_p[\boldsymbol{x}]$ para todo p primo; por lo que $rg, r^{-1}h \in \mathbb{Z}[\boldsymbol{x}]$. □

Definición 5.53: Sea $(\mathfrak{o}, \mathfrak{m})$ un anillo de valuación. Un polinomio $f(x) := a_0 + a_1 x + \cdots + a_n x^n \in \mathfrak{o}[x]$ se dice ***de Eisenstein*** si

$$a_n \in \mathfrak{o}^\times = \mathfrak{o} \smallsetminus \mathfrak{m}, \qquad \forall j < n \quad a_j \in \mathfrak{m}, \qquad a_0 \notin \mathfrak{m}^2.$$

Teorema 5.54 (criterio de irreducibilidad de Eisenstein): Sea k un cuerpo ultramétrico discreto de anillo de valuación $\mathfrak{o}$. Todo polinomio de Eisenstein en $\mathfrak{o}[x]$ es irreducible en $k[x]$.

Polígonos de Newton. Sea k un cuerpo ultramétrico y sea $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$ con $a_0 \neq 0 \neq a_n$. Para obtener su polinomio de Newton, graficaremos los puntos:

$$P(j) := (j, -\log |a_j|) \in \mathbb{R}^2.$$

y consideraremos su clausura convexa $\Pi(f)$ a la que llamamos el ***polígono de Newton***. Dicho polígono está compuesto por varios segmentos $\lambda_1, \ldots, \lambda_s$ de pendientes crecientes, donde λ_i une los puntos $P(m_{i-1}), P(m_i)$ y su pendiente es:

$$\gamma_i := \frac{-\log |a_{m_i}| + \log |a_{m_{i-1}}|}{m_i - m_{i-1}}.$$

donde $0 = m_0 < m_1 < \cdots < m_s = n$ y $\gamma_1 < \cdots < \gamma_s$. En éste sentido, diremos que f es de ***tipo***:

$$(m_1, \gamma_1; m_2 - m_1, \gamma_2; \ldots; m_s - m_{s-1}, \gamma_s) \tag{5.3}$$

Un polinomio del tipo (n, γ) se dice un ***polinomio Newton-puro***.[3]

num-th/newton_polygon.pdf

Figura 5.2. Polígono de Newton de $f(x) = 4x^5 - \frac{1}{4}x^4 + 7x^3 + 5x^2 - 6x - 2$.

[3]La terminología *polinomio de tipo ...* o *Newton-puro* son originales de Cassels [**71,** pág. 100], quien señala que son expresiones no estándar.

Lema 5.55: Sea k un cuerpo ultramétrico. Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n \in k[x]$ con $a_0 \neq 0 \neq a_n$ un polinomio de tipo (5.3). Definiendo $c = \exp(\gamma_s)$ y $\| \, \| := \| \, \|_c$. Entonces $\|f\| = \|a_jx^j\|$ para $j \in \{m_{s-1}, m_s\}$ y

$$\left\| f - \sum_{m_{s-1} \leq j \leq m_s} a_jx^j \right\| < \|f\|.$$

Demostración: Basta notar que si $\ell < j \leq n$, entonces la condición de que $\|a_jx^j\| \geq \|a_\ell x^\ell\|$ equivale a que

$$\frac{-\log|a_j| + \log|a_\ell|}{j - \ell} \leq \gamma_s,$$

donde el lado izquierdo representa la pendiente del segmento que une los puntos $P(\ell)$ y $P(j)$ del polígono de Newton de f. Finalmente aplicamos la elección de γ_s para concluir. □

Ejercicio para el lector: ¿por qué requerimos que k sea ultramétrico?

Lema 5.56: Sea k un cuerpo ultramétrico. Sean $f, g \in k[x]$ dos polinomios Newton-puros de pendiente común γ, entonces $f \cdot g$ es Newton-puro de pendiente γ.

Demostración: Fijemos $c := e^\gamma$ y $\| \, \| := \| \, \|_c$. Si $f(x) = a_0 + \cdots + a_nx^n$ y $g(x) = b_0 + \cdots + b_mx^m$ con $a_n \neq 0 \neq b_m$, entonces por el lema anterior, vemos que

$$\|f\| = |a_0| = \|a_nx^n\|, \qquad \|g\| = |b_0| = \|b_mx^m\|,$$

luego $\|fg\| = |a_0b_0| = \|a_nb_mx^{n+m}\|$ y concluimos por el lema anterior que fg es Newton-puro, y es fácil verificar que la pendiente es también la misma. □

Lema 5.57: Sea k un cuerpo ultramétrico. Sea $f \in k[x]$ un polinomio de tipo (5.3) y $g \in k(x)$ un polinomio Newton-puro de tipo (N, γ). Si $\gamma_s < \gamma$, entonces $f \cdot g$ es de tipo

$$(m_1, \gamma_1; m_2 - m_1, \gamma_2; \ldots; m_s - m_{s-1}, \gamma_s; N, \gamma).$$

Demostración: Sea $c := e^{\gamma_s}$ y $d := e^\gamma$, aquí trabajaremos con ambos valores absolutos por separado. Como $\gamma > \gamma_s$ vemos que $\|g(x) - b_0\|_c <$

$\|g(x)\|_c$. Luego, por el lema 5.55,

$$\left\| f \cdot g - b_0 \sum_{m_{s-1} \le j \le m_s} a_j x^j \right\|_c < \|f \cdot g\|_c.$$

Similarmente, $\|f(x) - a_n x^n\|_d < \|f(x)\|_d$, luego

$$\|f \cdot g - a_n x^n g(x)\|_d < \|f \cdot g\|_d.$$

Verificar conclusión.

Se puede verificar que las condiciones del lema 5.55 implican que fg es del tipo descrito. □

Lema 5.58: Sea k un cuerpo ultramétrico henseliano (e.g., completo) y $\|\,\| = \|\,\|_c$. Sea $f(x) = \sum_{j=0}^{n} a_j x^j \in k[x]$ con $a_n \neq 0$. Si existe m con $0 < m < n$ tal que

$$\|f\| = \|a_n x^n\|, \qquad \forall j > m \quad \|a_j x^j\| < \|f\|.$$

Entonces $f = gh$ donde $g, h \in k[x]$ tienen grados $m, n - m$ resp.

Completar demostración, vid. **[71,** págs. 103-104].

Demostración: ... □

Corolario 5.58.1: Sea k un cuerpo ultramétrico henseliano. Si $f(x) \in k[x]$ es irreducible, entonces es Newton-puro.

Demostración: Basta notar que si f no es Newton-puro, entonces podemos encontrar un m como en el lema anterior y así ver que es reducible. □

Teorema 5.59 (del polígono de Newton): Sea k un cuerpo ultramétrico henseliano. Sea $f(x) \in k[x]$ un polinomio de tipo (5.3), entonces se puede escribir como

$$f(x) = g_1(x) \cdots g_s(x),$$

donde cada $g_j \in k[x]$ es Newton-puro de tipo $(m_j - m_{j-1}, \gamma_j)$.

Demostración: Nótese que $f = \prod_{j=1}^{n} h_j$, donde cada h_j es irreducible y, por lo tanto, Newton-puro. Podemos definir los g_ℓ's como los productos de h_j's que tienen la misma pendiente δ_ℓ, de modo que g_ℓ es de tipo (q_ℓ, δ_ℓ); lo que dará que f se escribe como producto de polinomios Newton-puros de

distintas pendientes. Empleando repetidas veces el lema 5.57 se obtiene que el producto de g_ℓ, quizá tras reordenar, es

$$(q_1, \delta_1; q_2, \delta_2; \ldots; q_r, \delta_r),$$

y por ello, vemos que $r = s$, $q_j = m_j - m_{j-1}$ y $\delta_j = \gamma_j$. □

§5.3.2 Extensiones algebraicas.

Definición 5.60: Sea k un cuerpo métrico y sea V un k-espacio vectorial. Una función $\| \|\colon V \to [0, \infty)$ se dice una ***norma*** si para todo $\boldsymbol{u}, \boldsymbol{v} \in V$ y todo $c \in k$ se cumple que:

1. $\|\boldsymbol{v}\| = 0$ syss $\boldsymbol{v} = \vec{0}$.
2. $\|\boldsymbol{u} + \boldsymbol{v}\| \leq \|\boldsymbol{u}\| + \|\boldsymbol{v}\|$.
3. $\|c\boldsymbol{v}\| = |c|\,\|\boldsymbol{v}\|$.

Un par $(V, \| \|)$ se dice un ***k-espacio normado***, obviaremos los índices de no haber ambigüedad sobre los signos. Nótese que $d(\boldsymbol{u}, \boldsymbol{v}) := \|\boldsymbol{u} - \boldsymbol{v}\|$ determina una métrica sobre V, luego una topología. Dos normas $\| \|_1, \| \|_2$ sobre V se dicen ***equivalentes*** si inducen la misma topología sobre V.

Comenzamos con unos resultados clásico de análisis:

Lema 5.61: Sea k un cuerpo métrico no trivial y V un k-espacio vectorial. Dos normas $\| \|_1, \| \|_2$ sobre V son equivalentes syss existen constantes $c_1, c_2 > 0$ tales que para todo $\boldsymbol{a} \in V$ se cumpla

$$c_1\|\boldsymbol{a}\|_1 \leq \|\boldsymbol{a}\|_2 \leq c_2\|\boldsymbol{a}\|_1.$$

Demostración: Supondremos que $V \neq 0$.

$\Longleftarrow$. Sea U un abierto relativo a $\| \|_2$, probaremos que es abierto relativo a $\| \|_1$ y por simetría veremos que los abiertos coinciden. Sea $\boldsymbol{u} \in U$, luego existe un $\epsilon > 0$ tal que

$$\{\boldsymbol{v} : \|\boldsymbol{v} - \boldsymbol{u}\|_2 < \epsilon\} \subseteq U,$$

Luego, claramente

$$\boldsymbol{u} \in \left\{\boldsymbol{v} : \|\boldsymbol{v} - \boldsymbol{u}\|_1 < \frac{\epsilon}{c_1}\right\} \subseteq U,$$

por lo que U es abierto respecto a $\|\ \|_1$.

$\Longrightarrow$. Como las normas son equivalentes, entonces existe $r > 0$ tal que

$$\{\boldsymbol{v} \in V : \|\boldsymbol{v}\|_1 < r\} \subseteq \{\boldsymbol{v} \in V : \|\boldsymbol{v}\|_2 < 1\},$$

como k no es trivial, existe $\alpha \in k$ tal que $|\alpha| > 1$ de modo que $\lim_n |\alpha|^{-n} = 0$ y $\lim_n |\alpha|^n = \infty$. Luego, para todo $\boldsymbol{v} \in V$ existe un $n \in \mathbb{Z}$ tal que

$$|\alpha|^n \leq \frac{1}{r}\|\boldsymbol{v}\|_1 < |\alpha|^{n+1} \implies \left\| \frac{1}{\alpha^{n+1}}\boldsymbol{v} \right\|_1 < r,$$

de modo que $\|\boldsymbol{v}/\alpha^{n+1}\|_2 < 1$, ergo

$$\|\boldsymbol{v}\|_2 < |\alpha|^{n+1} = |\alpha|\,|\alpha|^n \leq \frac{|\alpha|}{r}\|\boldsymbol{v}\|_1,$$

de modo que $c_1 := |\alpha|/r$ funciona. Análogamente se construye c_2. □

Lema 5.62: Sea k un cuerpo métrico y V un k-espacio vectorial con base $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$. Entonces, la función

$$\|a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n\|_\infty := \max_i\{|a_i|\},$$

es una norma y $(V, \|\ \|_\infty)$ es completo si k lo es.

Teorema 5.63: Sea k un cuerpo métrico no trivial completo y sea V un k-espacio vectorial de dimensión finita. Todas las normas sobre V son equivalentes y bajo todas V resulta ser (un espacio métrico) completo.

Demostración: Fijemos una base $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$, y sea $\|\ \|_\infty$ la norma descrita en el lema anterior. Sea $\|\ \|$ otra norma de V, y definamos $c_2 := n\,\max_i\{\|\boldsymbol{e}_i\|\}$; por desigualdad triangular se comprueba que

$$\|a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n\| \leq |a_1|\,\|\boldsymbol{e}_1\| + \cdots + |a_n|\,\|\boldsymbol{e}_n\| \leq c_2\|a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n\|_\infty.$$

Probaremos el teorema por inducción sobre n, el caso $n = 1$ es claro.

Para el caso inductivo, supondremos que no existe $c_1 > 0$ tal que $c_1\|\boldsymbol{v}\|_\infty \leq \|\boldsymbol{v}\|$ para todo $\boldsymbol{v} \in V$, de modo que escogiendo $c_1 = 1/m$ existe $\boldsymbol{v}_m \in V$ tal que $\|\boldsymbol{v}_m\| < \frac{1}{m}\|\boldsymbol{v}_m\|_\infty$. Ahora bien, tenemos infinitos $\boldsymbol{v}_m$'s y como solo consta de finitas coordenadas hay, por palomar, al menos una que es la que tiene máximo valor absoluto infinitas veces, digamos que $\boldsymbol{e}_n$. Además podemos normalizar la sucesión de modo que obtenemos una sucesión $\{\boldsymbol{v}_{\sigma m}\}_m$ tal que:

- $\|\boldsymbol{v}_{\sigma m}\|_\infty = 1$.
- $\boldsymbol{v}_{\sigma m} = a_1\boldsymbol{e}_1 + \cdots + a_n\boldsymbol{e}_n$ donde $a_n = 1$.
- $\|\boldsymbol{v}_{\sigma m}\| < 1/\sigma(m)$.

Así $\lim_m \|\boldsymbol{v}_{\sigma m}\| = 0$. Definamos $W := \mathrm{Span}_k\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}\}$ el cual tiene dimensión menor y sean $\boldsymbol{w}_m := \boldsymbol{v}_{\sigma m} - \boldsymbol{e}_n \in W$. Luego $\lim_m \|\boldsymbol{w} + \boldsymbol{e}_n\| = 0$ y

$$\|\boldsymbol{w}_m - \boldsymbol{w}_M\| = \|(\boldsymbol{w}_m + \boldsymbol{e}_n) - (\boldsymbol{w}_M + \boldsymbol{e}_n)\| \leq \|\boldsymbol{w}_m + \boldsymbol{e}_n\| + \|\boldsymbol{w}_M + \boldsymbol{e}_n\| \to 0,$$

de modo que $(\boldsymbol{w}_m)_{m\in\mathbb{N}}$ es una sucesión de Cauchy respecto a la norma $\|\,\|$ contenida en W.

En W, por hipótesis inductiva, todas las normas coinciden y son completas, de modo que $\boldsymbol{w}_m$ converge a un valor $\boldsymbol{w} \in W$ y así:

$$\|\boldsymbol{w} + \boldsymbol{e}_n\| = \|(\boldsymbol{w} - \boldsymbol{w}_m) + (\boldsymbol{w}_m + \boldsymbol{e}_n)\| \leq \|\boldsymbol{w} - \boldsymbol{w}_m\| + \|\boldsymbol{w}_m + \boldsymbol{e}_n\| \to 0,$$

por lo que $\boldsymbol{w} = -\boldsymbol{e}_n$, pero $-\boldsymbol{e}_n \notin W$ lo que es absurdo. □

Corolario 5.63.1: Sea $(k, |\,|)$ un cuerpo métrico completo y sea L/k una extensión finita de cuerpos. Existe a lo más un valor absoluto $\|\,\|$ sobre L (salvo equivalencia) que extiende a $|\,|$. Más aún, L también es un completo respecto a ésta métrica.

Demostración: Basta notar que un valor absoluto sobre L es una norma de L como k-espacio vectorial. □

Teorema 5.64: Sea $(k, |\,|)$ un cuerpo métrico completo no trivial y sea L/k una extensión finita de cuerpos. Existe exactamente un valor absolutos $\|\,\|$ sobre L (salvo equivalencia) que extiende a $|\,|$. En consecuencia, existe exactamente un valor absoluto sobre k^{alg} que extiende a $|\,|$.

Demostración: Si $k = \mathbb{R}$ o $\mathbb{C}$, entonces es claro así que nos enfocaremos en el caso ultramétrico.

Considere la norma $\mathrm{Nm}_{L/k}\colon L \to k$, y defínase $\|\alpha\| := |\mathrm{Nm}_{L/k}(\alpha)|^{1/n}$ donde $n := [L : k]$. Si $a \in k$, entonces $\mathrm{Nm}_{L/k}(a) = a^n$, así que vemos que $\|\,\|$ extiende a $|\,|$. Si $\alpha \in L$ es no nulo, entonces $\mathrm{Nm}_{L/k}(\alpha) = \prod_\sigma \sigma(\alpha)$, donde σ recorre todos los k-monomorfismos de L en su clasura normal, luego $\mathrm{Nm}_{L/k}(\alpha) \neq 0$ y, por ello, $\|\alpha\| \neq 0$ (VA1). Como $\mathrm{Nm}_{L/k}$ es multiplicativa, entonces $\|\,\|$ también (VA2).

Falta ver la desigualdad ultramétrica: Sea $\|\alpha\| \leq 1$, sea $f(t) = a_0 + \cdots + a_{n-1}t^{n-1} + t^n \in k[t]$ el polinomio minimal de α y sea $F(t) := \psi_{\alpha,L/k}(t) = c_0 + \cdots + c_{m-1}t^{m-1} + t^m \in k[t]$ el polinomio característico de α. Sabemos que $\mathrm{Nm}_{L/k}(\alpha) = \pm c_0$ (cfr. [**1,** def. 4.63] y [**1,** prop. 3.67]) y también sabemos que el polinomio característico es alguna potencia natural de $f(t)$, de modo que $c_0 = a_0^r$ para algún $r \geq 1$. Si:

$$|a_0|^{r/n} = |c_0|^{1/n} = |\,\mathrm{Nm}_{K/k}(\alpha)|^{1/n} = \|\alpha\| \leq 1,$$

entonces $|a_0| \leq 1$. Como $f(t)$ es irreducible, entonces es Newton-puro (corolario 5.58.1) y como $\|f(t)\|_c = |a_0|$ (lema 5.55), entonces vemos que $\|f(t)\| \leq 1$, por lo que $f(t) \in \mathfrak{o}[t]$ y luego $F(t) \in \mathfrak{o}[t]$. Ahora bien, nótese que

$$\|1 + \alpha\| = |\,\mathrm{Nm}_{L/k}(1 + \alpha)|^{1/n} = |(-1)^n F(-1)|^{1/n} \leq \|F(t)\|_1 \leq 1.$$

Aquí empleamos el hecho de que $\mathrm{Nm}_{L/k}(x - \alpha) = F(x)$ para todo $x \in k$, ¿por qué ésto es cierto?

Finalmente, la última desigualdad comprueba la desigualdad ultramétrica y, por tanto, completa la demostración. □

Por la unicidad, denotaremos a éste valor absoluto $|\,|$. Nótese que $|\alpha| := |\,\mathrm{Nm}_{L/K}(\alpha)|^{1/n}$ siempre determina un valor absoluto sobre L, independiente de si K es completo o no; no obstante la completitud de K se exige si se desea unicidad.

Ejemplo 5.65: Una extensión finita L/K de cuerpos con K métrico, donde L admite más de una extensión del valor absoluto Considere $(\mathbb{Q}, |\,|_\infty)$ el cual no es completo y considere la extensión finita $L := \mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Considere al elemento α que es raíz de $(x-1)^2 - 2$. Éste elemento, tradicionalmente lo elegimos como $\sqrt{2} + 1 > 0$, donde $|\sqrt{2} + 1| \approx 2{,}41$; pero también podríamos elegirlo como $-\sqrt{2} + 1 < 0$, donde $|-\sqrt{2} + 1| \approx 0{,}41$.

Otra manera de entender éste ejemplo es que $2 \in \mathbb{R}$ posee dos raíces, una positiva y otra negativa, y ambas son *algebraicamente indistinguibles*; el ordenamiento de $\mathbb{R}$ induce un valor absoluto sobre $L \subseteq \mathbb{R}$, así pues ambas elecciones (de que $\sqrt{2}$ sea positivo o no) inducen dos valores absolutos no equivalentes. ⌟

De la construcción se sigue:

Corolario 5.65.1: Sea k un cuerpo ultramétrico completo. Todo k-conjugado de un elemento k-algebraico comparte su valor absoluto.

Corolario 5.65.2 (lema de Krasner): Sea k un cuerpo ultramétrico completo. Sea $\alpha \in k^{\text{alg}}$ y sea β un k-conjugado distinto de α. Entonces, para todo $a \in k$ se cumple que $|a - \alpha| \geq |\alpha - \beta|$.

Demostración: De lo contrario, existiría algún $a \in k$ tal que

$$|a - \alpha| < |\alpha - \beta| = |a - \beta|,$$

pero $a - \alpha, a - \beta$ son k-conjugados por lo que la desigualdad es absurda. □

Nótese que la prueba de la unicidad es universal al caso arquimediano y ultramétrico, pero la prueba de existencia es exclusiva del caso ultramétrico, aunque mediante la clasificación de cuerpos métricos arquimedianos por el teorema de Ostrowski también podemos contemplar ese caso.

§5.3.3 Compleción de un cuerpo algebraicamente cerrado. Recuento sobre lo que hemos hecho: dado un cuerpo métrico, podemos completarlo, y dado un cuerpo métrico completo podemos tomar su clausura algebraica que también será métrica. Ahora, bien podría darse (y se dá) que dicha clausura algebraica no sea completa, lo que veremos en ésta sección.

Teorema 5.66: Sea k un cuerpo ultramétrico completo y sea $\alpha \in k^{\text{sep}}$. Defínase

$$r := \min_{\beta \neq \alpha} |\beta - \alpha|,$$

donde β recorre los k-conjugados de α. Sea $\gamma \in B_r(\alpha) \subseteq k^{\text{alg}}$, entonces $k(\alpha) \subseteq k(\gamma)$.

Demostración: Sean $f(x) \in k[x]$ y $\phi(x) \in k(\gamma)[x]$ el polinomio minimal de α sobre k y sobre $k(\gamma)$ resp. Luego $\phi(x) \mid f(x)$. Sea $\sigma \in \text{Gal}(k(\alpha, \gamma)/k(\gamma))$, de modo que $\sigma(\gamma - \alpha) = \gamma - \sigma(\alpha)$. Como los conjugados comparten norma por el corolario 5.65.1, vemos que

$$|\gamma - \sigma(\alpha)| = |\gamma - \alpha| < r,$$

luego, por desigualdad ultramétrica, $|\alpha - \sigma(\alpha)| \leq |\gamma - \alpha| < r$, de modo que por definición de r se sigue que $\sigma(\alpha) = \alpha$. Así pues, como α es separable, vemos que $k(\alpha, \gamma) = k(\gamma)$ como se quería probar. □

En el siguiente teorema, la expresión «suficientemente cerca» significa que existe algún $\epsilon > 0$ tal que si $\|f(x) - g(x)\| < \epsilon$, entonces se cumple lo enunciado.

Teorema 5.67: Sea k un cuerpo ultramétrico completo. Sean $f(x), g(x) \in k[x]$ mónicos de grado común n y fijemos la norma $\| \, \| := \| \, \|_1$ sobre $k[x]$. Para f, g suficientemente cerca se cumplen las siguientes:

1. Si $f(x)$ es irreducible en k y separable en k^{alg}, entonces $g(x)$ también y genera el mismo cuerpo de escisión.[4]
2. Si una raíz $\alpha \in k^{\mathrm{alg}}$ en $f(x)$ tiene multiplicidad m, entonces la cantidad de raíces β_i de $g(x)$ tales que $k(\beta_i) \subseteq k(\alpha)$ es (contando multiplicidad) m.
3. Si $f(x)$ es irreducible en k, entonces $g(x)$ también.

Demostración: Digamos que $\|f(x)-g(x)\| < \epsilon$ para un ϵ que determinaremos en cada inciso, y denotemos $\alpha_1, \ldots, \alpha_n$ y $\beta_1, \ldots, \beta_n$ las raíces (contando multiplicidad) de $f(x), g(x)$ en k^{alg} resp.

1. Supongamos que $\|f(x)\| \leq C$ (sin fijar) y sea $|\gamma| > C$, si $f(x) = \sum_{j=0}^{n} c_j x^j$ entonces $|\gamma|^n > |c_j \gamma^j|$ para $j < n$, de modo que γ no puede ser raíz de $f(x)$. Es decir, cada $|\alpha_j| \leq C$.

   Si elegimos $C := \max\{\|f\|, \|g\|, 1\}$, vemos que cada $|\beta_j| \leq C$ y, por ende, para cualquier β_j vemos también que

   $$|f(\beta_j)| = |f(\beta_j) - g(\beta_j)| \leq \epsilon C^n.$$

   Y por desigualdad ultramétrica vemos que

   $$|\beta_j - \alpha_1| \cdots |\beta_j - \alpha_n| \leq \epsilon C^n,$$

   luego, al menos un α_i, digamos α_1, satisface que

   $$|\beta_j - \alpha_1| \leq C \sqrt[n]{\epsilon}.$$

   Ahora fijemos

   $$\epsilon := \left(\min_{i \neq j} \{|\alpha_i - \alpha_j|\} \right)^n > 0,$$

   de modo que, como f es irreducible, vemos que los α_j's son k-conjugados, luego por el teorema anterior comprobamos que $k(\beta_j) \supseteq k(\alpha_1)$.

   Como f, g son del mismo grado, entonces concluimos que g es irreducible (pues genera una extensión de cuerpos de su mismo grado) y es separable (pues los cuerpos coinciden).

[4] El cuerpo de escisión de un polinomio $h(x) \in k[x]$ es la mínima extensión L/k en la cual h se escinde, es decir, contiene a todas sus raíces (cfr. [**1,** def. 4.19]).

2. De lo contrario, para cualquier $n > 0$ podríamos encontrar otro polinomio g_n tal que $\|f - g_n\| < 1/n$ y donde g_n posee raíces $\beta_{n,j}$ de multiplicidad μ_j tal que $\lim_n \beta_{n,j} = \alpha_j$. Así, por completitud de k, vemos que $\lim_n g_n = f$ y así tenemos que

$$(x-\alpha_1)^{\eta_1} \cdots (x-\alpha_n)^{\eta_n} = f(x) = \lim_n g_n(x) = (x-\alpha_1)^{\mu_1} \cdots (x-\alpha_n)^{\mu_n},$$

donde $\eta_j \neq \mu_j$ para algún j lo que contradice la factorización única de $k^{\text{alg}}[x]$.

3. Al igual que en el inciso anterior construimos una sucesión de Cauchy que converja a f donde cada término se factoriza en dos polinomios cuyas raíces convergen a algunas raíces de f y llegamos a una contradicción pues sus límites prueban que f es reducible. □

Teorema 5.68: Sea K un cuerpo ultramétrico algebraicamente cerrado, entonces $\hat{K}$ también es algebraicamente cerrado.

Demostración: La demostración prosigue dos pasos:

(i) $\hat{K}$ es perfecto: Es claro si $\operatorname{car} K = 0$ (cfr. [**1,** teo. 4.34]), así que supondremos que $p := \operatorname{car} K > 0$. Basta probar que el endomorfismo de Frobenius es suprayectivo (también, cfr. [**1,** teo. 4.34]): sea $\alpha \in \hat{K}$, luego $\alpha = \lim_n \beta_n$ para $(\beta_n)_n \subseteq K$; como K es algebraicamente cerrado, entonces vemos que $\lim_n \beta_n^{1/p} = \alpha^{1/p} \in \hat{K}$.

(ii) Como $\hat{K}$ es perfecto, entonces basta probar que todo polinomio irreducible, mónico, separable $f(x) \in \hat{K}[x]$ es lineal. Como $K[x]$ es denso en $\hat{K}[x]$, podemos encontrar $g(x) \in K[x]$ suficientemente cerca de $f(x)$ de modo que g sea separable, irreducible y genere el mismo cuerpo de escisión. Como K es algebraicamente cerrado, entonces g es lineal y así f también debe serlo. □

Notas históricas

La genesis de la teoría de valuaciones está en el llamado *análisis p-ádico*, lo cual fue una invención de **Kurt Hensel** en [**30**] (1897). Hensel [**31**] (1904) demostró que $\mathbb{Q}_p$, definido formalmente como series formales sobre $x = p$, es un cuerpo.

La definición de *cuerpo con valor absoluto* (o *cuerpo métrico*, como lo empleamos aquí) fue formulada por vez primera por el hungaro **Josef Kürschák**, presentado en el Congreso Internacional de Matemáticos de Cambridge y publicado en **[37]** (1913). El resultado de Kürschák era que todo cuerpo métrico se extiende (con su valor absoluto) a un cuerpo métrico completo y algebraicamente cerrado. El método de Kürschák es equivalente al nuestro:

i) Todo cuerpo métrico admite una compleción a un cuerpo métrico (cfr. teorema 5.11).

ii) Un cuerpo métrico completo admite una extensión a un cuerpo métrico algebraicamente cerrado (cfr. teorema 5.64).

iii) La compleción de un cuerpo métrico algebraicamente cerrado es también algebraicamente cerrada (cfr. teorema 5.68).

El paso i) lo sigue de los argumentos clásicos de análisis, en particular citando a Cantor; el paso ii) emplea la construcción de la clausura algebraica de Steinitz y el paso iii) sigue la demostración del teorema fundamental del álgebra dada por Weierstrass. Además, Kürschák afirma (sin demostración) que los cuerpos ultramétricos satisfacen el lema de Hensel.

Los dos teoremas de Ostrowski fueron descubiertos por el ruso **Alexander Ostrowski** en **[51]** (abril 1916, publ. 1918); los nombres *primero* y *segundo* son añadido propio. Si cambiamos cuerpo métrico arquimediano por $\mathbb{R}$-álgebra normada[5] completa entonces la lista se amplía a $\mathbb{R}, \mathbb{C}$ y $\mathbb{H}$, donde los últimos son los cuaterniones y forman una $\mathbb{R}$-álgebra de división no conmutativa.

En otro artículo **[49]** (1913) y en una simplificación tardía **[50]** (1917), Ostrowski reanuda un estudio sobre los trabajos de Kürschák que incluye una demostración de que una extensión finita de un cuerpo métrico completo es también completa (cfr. teorema 5.64) siguiendo la estrategia de espacios normados y, mediante su demostración, probando que hay una *única* extensión del valor absoluto a la clausura algebraica (algo que Kürschák no probó). En el mismo trabajo vemos que Ostrowski emplea el llamado *lema de Krasner* (cfr. corolario 5.65.2). Finalmente, respondió a la duda de Kürschák respecto a cuando es la clausura algebraica de un cuerpo métrico completa.

Los resultados desarrollados por Hensel, Kürschák y Ostrowski fueron recopilados y reordenados en simplicidad por el checo Karel Rychlík, primero publicados en checo en **[59]** (1919) con poca repercusión, y más tarde en

[5]Una k-álgebra normada es una k-álgebra $(A, \| \|)$ que es un k-espacio normado y en donde $\|\alpha\beta\| = \|\alpha\| \, \|\beta\|$ para todo $\alpha, \beta \in A$.

alemán en [**60**] (1924); de ahí que algunas versiones del lema de Hensel sean llamadas «lema de Rychlík». Como las demostraciones de éste lema siguen el llamado *método de Newton* para encontrar ceros de funciones continuas, también hay versiones del lema de Hensel llamados «lema de Newton».

El teorema de aproximación fue demostrado en toda su generalidad por Artin y Whaples [**67**] (1945). El teorema, restringido a valores absolutos no arquimedianos, también fue empleado en un manuscrito de Ostrowski [**53**] escrito cerca de 1916, pero publicado en 1935.

Los polígonos de Newton fueron introducidos por Newton en su correspondencia con Oldenburg (13 de junio de 1676, vid. [**8,** págs. 20-47], y 24 de octubre de 1676, vid. [**8,** págs. 162-164]); una buena exposición moderna se encuentra en la sección §8.3 de Brieskorn y Knorrer [**6,** págs. 370-454]. La aplicación del polígono de Newton a la teoría de valuación, particularmente el teorema 5.59, es originaria por Ostrowski [**52**] (1933), aunque fue inicialmente estudiado por Rella [**56**] (1927).

Referencias

64. Alter, R. y Kubota, K. K. The Diophantine Equation $x^2 + 11 = 3^n$ and a Related Sequence. *J. Number Theory* **7,** 5-10. doi:10.1016/0022-314X(75)90003-7 (1975).

67. Artin, E. y Whaples, G. Axiomatic Characterization of Fields by the Product Formula for Valuations. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1945-08383-9 (1945).

71. Cassels, J. W. S. *Local Fields* (Cambridge University Press, 1986).

Otros recursos.

1. Cuevas, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).
2. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).
3. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).
5. Wilson, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. BRIESKORN, E. y KNORRER, H. *Plane Algebraic Curves* trad. por STILLWELL, J. (Birkhäuser Verlag, 1981).
7. DICKSON, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).
8. NEWTON, I. *The Correspondence of Isaac Newton* (ed. TURNBULL, H. W.) (Cambridge University Press, 1960).
9. ROQUETTE, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).
10. WILLIAMS, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. BENNETT, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. ALFORD, W. R., GRANVILLE, A. y POMERANCE, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).
12. APÉRY, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. BARNES, E. S. y SWINNERTON-DYER, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. BEUKERS, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).
15. BOMBIERI, E. y VAALER, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).
16. CASSELS, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).
17. CATALAN, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).
18. CHAO, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).
19. CHATLAND, H. y DAVENPORT, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).
20. CLARK, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).

21. De Bessy, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
22. Dedekind, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).
23. Dickson, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).
24. Dirichlet, G. L. en *G. Lejeune Dirichlet's Werke* (ed. Kronecker, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.
25. Euler, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).
26. Euler, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).
27. Euler, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).
28. Gauss, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.
29. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).
30. Hensel, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).
31. Hensel, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).
32. Hyyrö, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).
33. Inkeri, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).
34. Inkeri, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).
35. Kausler, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).
36. Keller, W. y Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).
37. Kürschák, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. LANG, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. LEGENDRE, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. LEHMER, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. MAHLER, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. MIGNOTTE, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. MINKOWSKI, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. MOTZKIN, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. NAGELL, T. Sur l'impossibilité de l'équation indéterminée $z^p+1=y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. NORTHCOTT, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. OCHEM, P. y RAO, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. OSTROWSKI, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. OSTROWSKI, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. OSTROWSKI, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y)=\varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. OSTROWSKI, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. OSTROWSKI, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. PERRON, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. RÉDEI, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. RELLA, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. Remak, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. Roth, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. Rychlík, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. Rychlík, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. Siegel, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. Tate, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 305-347.

63. Verger-Gaugry, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

6

Ramificación

6.1 Nociones básicas

§6.1.1 Cuerpos locales.

Definición 6.1: Se dice que un cuerpo métrico $(K, |\,|)$ es un ***cuerpo local*** si es localmente compacto, o equivalentemente, si:

(a) Es arquimediano y completo, en cuyo caso es o bien $(\mathbb{R}, |\,|_\infty)$ o $(\mathbb{C}, |\,|_\infty)$.

(b) Es ultramétrico discreto, completo y su cuerpo de restos es finito.

Lema 6.2: Sea K un cuerpo local no arquimediano con anillo de valuación $(\mathfrak{o}, \mathfrak{m})$ y donde $N := |\mathfrak{o}/\mathfrak{m}|$. Entonces existen N distintas raíces $\zeta_1, \ldots, \zeta_N$ de $x^N = x$ en $\mathfrak{o}$ las cuales constituyen un conjunto de representantes de restos.

Demostración: Nótese que como $k := \mathfrak{o}/\mathfrak{m}$ es un cuerpo de cardinalidad finita N, necesariamente $k = \mathbb{F}_N$ y sus elementos son todas las raíces de $f(x) := x^N - x \in \mathfrak{o}[x]$ (vid. **[1,** teo. 4.35]). Luego, por el lema de Hensel, para toda raíz $\alpha \in k$ de $f(x)$, existe una única raíz $\zeta \in \mathfrak{o}$ tal que $\zeta \equiv \alpha$ (mód $\mathfrak{m}$). Así construimos todas las raíces del enunciado y vemos que forman un conjunto de representantes de restos. □

Lema 6.3: Sea K un cuerpo local no arquimediano con anillo de valuación $(\mathfrak{o}, \mathfrak{m}, \mathbb{F}_N)$ y sean $\Lambda := \{\zeta_1, \ldots, \zeta_N\}$ las raíces de $x^N - x$ en $\mathfrak{o}$. Si $k \subseteq K$ es un subcuerpo tal que:

(a) $k \supseteq \Lambda$.

(b) k es un subconjunto cerrado.

(c) $\mathfrak{m}_0 := \mathfrak{m} \cap k \neq \{0\}$.

Sea π un uniformizador de $\mathfrak{o}$, entonces $K = k(\pi)$ donde π es k-algebraico y su polinomio minimal es de Eisenstein sobre $\mathfrak{o}_0 := \mathfrak{o} \cap k$.

Demostración: Con la restricción del valor absoluto de K sobre k, vemos que k es un cuerpo local. Sea $(\mathfrak{o}_0, \mathfrak{m}_0)$ su anillo de valuación y sea τ un uniformizador de k. Necesariamente $|\tau| = |\pi|^e$ para algún $e \geq 1$. Para todo $j \in \mathbb{Z}$ sea $q := \lfloor j/e \rfloor$ y $r := j - qe \geq 0$, entonces definamos $\pi_j := \tau^q \pi^r$ y notemos que $|\pi_j| = |\pi|^j$. Luego, por la proposición 5.37, todo $a \in \mathfrak{o}$ se representa de forma única como

$$a = \sum_{n=0}^{\infty} a_n \pi_n = \alpha_0 + \alpha_1 \pi + \cdots + \alpha_{e-1} \pi^{e-1}, \tag{6.1}$$

donde cada $a_n \in \Lambda$, y donde hemos agrupado a la derecha

$$\alpha_r := a_r + a_{e+r}\tau + a_{2e+r}\tau^2 + \cdots = \sum_{q=0}^{\infty} a_{qe+r} \tau^q \in \mathfrak{o}_0.$$

Si permitimos que $\beta_r \in k$, entonces $|\beta_r| = |\tau|^q = |\pi|^{eq}$ para algún q y los términos $|\beta_r \pi^r| = |\pi|^{eq+r}$ tienen distinta magnitud para $0 \leq r \leq e-1$, luego $\sum_{r=0}^{e-1} \alpha_r \pi^r = 0$ syss cada $\alpha_r = 0$. Luego $\{1, \pi, \ldots, \pi^{e-1}\}$ es una base de K como k-espacio vectorial y $K = k(\pi)$ es una extensión algebraica.

Finalmente, empleando $a = \pi^e \in \mathfrak{o}$ en (6.1) tenemos que

$$\pi^e + \beta_{e-1}\pi^{e-1} + \cdots + \beta_0 = 0,$$

donde cada $\beta_r \in \mathfrak{o}_0$ es único. Ergo, $f(x) := \beta_0 + \beta_1 x + \cdots + x^e \in \mathfrak{o}_0[x]$ es el polinomio minimal de π sobre k (¿por qué?), Luego $\mathrm{Nm}_{K/k}(\pi) = \pm\beta_0$ y, como todos los k-conjugados de π comparten valor absoluto (corolario 5.65.1), entonces:

$$|\beta_0| = |\mathrm{Nm}_{K/k}(\pi)| = |\pi|^e = |\tau| \neq |\tau|^2.$$

Más aún, si algún $\beta_r \notin (\tau)$, entonces $|\beta_r| = 1$ y veríamos que $|\pi^e + \beta_{e-1}\pi^{e-1} + \cdots + \beta_0| = |\pi^r| \neq 0$ lo que sería absurdo; luego $f(x)$ es de Eisenstein. $\square$

Como ejercicio para el lector, ¿dónde se emplearon las hipótesis (a)-(c) en el lema anterior?

Teorema 6.4: Los cuerpos locales no arquimedianos son precisamente las extensiones finitas de $\mathbb{Q}_p$ (característica 0) y $\mathbb{F}_p((t))$ (característica $p > 0$).

Demostración: Sea K un cuerpo local con anillo de valuación $(\mathfrak{o}, \mathfrak{m}, \mathbb{F}_N)$. Si K tiene característica $p > 0$, entonces $\mathbb{F}_N$ también y así $N = p^n$ para algún $n \geq 1$. Sean $\Lambda := \{\zeta_1, \ldots, \zeta_N\}$ las raíces de $x^N - x$ en K y sea π un uniformizador de $\mathfrak{o}$; entonces por el lema anterior se obtiene que $K = \Lambda((\pi)) = \mathbb{F}_{p^n}((\pi))$, el cual es una extensión finita de $\mathbb{F}_p((\pi))$.

Si K tiene característica 0, entonces contiene a $\mathbb{Q}$ y su valor absoluto $|\,|$ se restringe a $\mathbb{Q}$ a algún $|\,|_p$, y como K es completo, entonces $\mathbb{Q}_p \subseteq K$. Sea Λ como antes y fijemos $k := \mathbb{Q}_p(\Lambda)$. Es fácil comprobar que k satisface las hipótesis (a)-(c) del lema anterior y luego vemos que $K = k(\pi) = \mathbb{Q}_p(\Lambda, \pi)$, el cual es una extensión finita de $\mathbb{Q}_p$. □

§6.1.2 Grado de inercia. En ésta sección trabajaremos con extensiones algebraicas de cuerpos ultramétricos, de modo que en general, dado un cuerpo ultramétrico K denotaremos su anillo de valuación $(\mathfrak{o}_K, \mathfrak{m}_K, \Bbbk_K)$.

En primer lugar, un comentario útil: la mayoría de resultados de hecho solo dependen del lema de Hensel. Un contraejemplo parcial: el teorema 5.63 no es del todo generalizable, pero en realidad nos interesa el teorema por lo siguiente:

Teorema 6.5: Un cuerpo métrico $(K, |\,|_K)$ es henseliano syss toda extensión algebraica L posee un único valor absoluto $|\,|_L$ que extiende a $|\,|_K$.

Demostración: $\Longrightarrow$. Si $|\,|_K$ es arquimediano, entonces $K \in \{\mathbb{R}, \mathbb{C}\}$ y es claro. Si K es ultramétrico y L/K es una extensión finita de grado n entonces, igual que antes, la fórmula $|\beta| := \sqrt[n]{|\mathrm{Nm}_{L/K}(\beta)|}$ define un valor absoluto sobre L.

Sean $|\,|, \|\,\|$ dos valores absolutos sobre L que extiendan a K, donde $|\,|$ es el descrito anteriormente y cuyos anillos de valuación son $(\mathfrak{O}_1, \mathfrak{P}_1)$ y $(\mathfrak{O}_2, \mathfrak{P}_2)$ resp. Supongamos que existe $\beta \in \mathfrak{O}_1 \setminus \mathfrak{O}_2$ y sea

$$f(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in K[x]$$

su polinomio minimal. Entonces cada $c_i \in \mathfrak{o}_K$ y, como $\beta \notin \mathfrak{O}_2$, entonces $\beta^{-1} \in \mathfrak{P}_2$ (por ser anillo de valuación). Luego $1 = -c_1\beta^{-1} - \cdots - c_d(\beta^{-1})^d \in$

$\mathfrak{P}_2$ lo que es absurdo. Así vemos que $\mathfrak{O}_1 \subseteq \mathfrak{O}_2$. Si $|\,|, \|\,\|$ no fuesen equivalentes, entonces, por el teorema de aproximación, existiría $\beta \in L$ tal que $|\beta| \leq 1$ y $\|\beta\| > 1$, lo cual es absurdo.

$\Longleftarrow$. ... □

Teorema 6.6: Sea (K, v) un cuerpo ultramétrico henseliano y L/K una extensión finita de cuerpos con $w \mid v$. Entonces $\Bbbk(w) \supseteq \Bbbk(v)$ también es una extensión finita de cuerpos donde

$$[\Bbbk(w) : \Bbbk(v)] \leq [L : K].$$

DEMOSTRACIÓN: Como el anillo de valuación $\mathfrak{o}_v$ y su ideal maximal están caracterizados como una bola abierta (resp., cerrada) de radio 1 en torno al 0, entonces es claro que $\mathfrak{o}_v \subseteq \mathfrak{o}_w$. Luego induce un homomorfismo $\mathfrak{o}_v \to \Bbbk(w)$ y nótese que un elemento $a \in \mathfrak{o}_v$ está en $\mathfrak{m}_w$ syss $a \in \mathfrak{m}_v$.

Sea $n := [L : K]$ y sean $\alpha_1, \ldots, \alpha_{n+1} \in \mathfrak{o}_w \subseteq L$. Luego existen $b_1, \ldots, b_{n+1} \in K$, no todos nulos, tales que

$$\sum_{j=1}^{n+1} \alpha_j b_j = 0,$$

digamos que $\max_j |b_j| = r > 0$, el que se alcanza en $|b_\ell| = r$, luego multiplicando por b_ℓ^{-1} tenemos que $\max_j |b_j| = 1$ de modo que al pasar al cociente muestra que $[\alpha_1], \ldots, [\alpha_{n+1}] \in \Bbbk(w)$ son $\Bbbk(v)$-linealmente dependientes. □

Definición 6.7: Sea (K, v) un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos de grado n con $w \mid v$. Llamamos el ***grado de inercia***, denotado $f(L/K) := [\Bbbk(w) : \Bbbk(v)]$.

Si la extensión en cuerpos de restos $\Bbbk(w)/\Bbbk(v)$ es separable y $f = n$ (resp. $f = 1$), entonces decimos que la extensión L/K es ***no ramificada*** (resp. ***totalmente ramificada***) .

Lema 6.8: Sea K un cuerpo ultramétrico henseliano y sean $F/L/K$ extensiones finitas de cuerpos. Entonces $f(F/K) = f(F/L)\, f(L/K)$.

Teorema 6.9: Sea (K, v) un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos con $w \mid v$. Sea $\alpha \in \Bbbk(w)$ separable sobre $\Bbbk(v)$, entonces existe $\beta \in L$ tal que $\beta \equiv \alpha \pmod{\mathfrak{m}_L}$ y $K(\beta)/K$ es no ramificado, es decir

$$[K(\beta) : K] = [\Bbbk(v)(\alpha) : \Bbbk(v)].$$

Más aún, si γ también satisface lo anterior, entonces $K(\gamma) = K(\beta)$.

Demostración: Denotemos $k := \Bbbk(v)$. Sea $\phi(t) \in k[t]$ el polinomio minimal de α, el cual satisface que $\phi'(\alpha) \neq 0$ puesto que α es separable; sea $\Phi(t) \in \mathfrak{o}_v[t]$ un polinomio tal que $\Phi(t) \equiv \phi(t) \pmod{\mathfrak{m}_v}$.

Sea $\delta \in \mathfrak{o}_w$ tal que $\delta \equiv \alpha \pmod{\mathfrak{m}_v}$, entonces $\Phi(\delta) \equiv \phi(\delta) \equiv 0 \pmod{\mathfrak{m}_v}$, de modo que

$$|\Phi(\delta)| < 1, \qquad |\Phi'(\delta)| = 1.$$

Luego, por el lema de Hensel sobre $K(\delta)$ vemos que existe un único $\beta \in K(\delta)$ tal que

$$\Phi(\beta) = 0, \qquad |\beta - \delta| < 1,$$

de modo que $\beta \equiv \delta \equiv \alpha \ (\mathfrak{m}_v)$ y el polinomio minimal de β es $\Phi(t)$ que tiene mismo grado que $\phi(t)$.

Nótese que si $K(\delta)/K$ ya fuese no ramificado, entonces, como $K(\beta) \subseteq K(\delta)$ por igualdad de grados, ambas extensiones coincidirían. □

Corolario 6.9.1: Sea (K, v) un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos con $w \mid v$ tal que la extensión $\Bbbk(w)/\Bbbk(v)$ sea separable. Entonces:

1. Existe una biyección entre subextensiones de cuerpos $\Bbbk(v) \subseteq \mu \subseteq \Bbbk(w)$ y subextensiones $K \subseteq M \subseteq L$ que son no ramificadas sobre K.

2. En consecuencia, existe una subextensión no ramificada $K \subseteq F \subseteq L$ tal que si $K \subseteq M \subseteq L$ es no ramificada, entonces $M \subseteq F$. Además, L/F es totalmente ramificada.

Demostración: Basta aplicar el teorema anterior junto al teorema del elemento primitivo que dice que las extensiones separables son simples (cfr. [**1**]). Para el segundo inciso basta considerar la extensión M dada por $\mu := \Bbbk(w)$. □

Proposición 6.10: Sea (K, v) un cuerpo ultramétrico henseliano y sean L/K, F/K un par de extensiones algebraicas (contenidas en K^{alg}). Si L/K es no ramificada, entonces LF/F y toda subextensión $K \subseteq M \subseteq L$ también es no ramificada. En consecuencia, si L/K y F/K son no ramificadas, entonces LF/K también.

Demostración: Supongamos que L/K es finita con $w \mid v$. Como $\Bbbk(w)/\Bbbk(v)$ es separable, entonces está generado por un elemento $\alpha \in \Bbbk(w)$. Sea $\beta \in {}_w$

tal que $\beta \equiv \alpha \pmod{\mathfrak{m}_w}$ y sea $f(x) \in \mathfrak{o}_w[x]$ su polinomio minimal respecto a K. Sea $g(x) := f(x) \mod \mathfrak{m}_w \in \Bbbk(w)[x]$ el cual anula a α, de modo que

$$[\Bbbk(w) : \Bbbk(v)] \leq \deg g = \deg f = [K(\beta) : K] \leq [L : K] = [\Bbbk(w) : \Bbbk(v)],$$

por lo que g es de hecho el polinomio minimal de α y $L = K(\alpha)$.

Así pues, $LF = F(\alpha)$; denotemos por $V \mid v$ el lugar en F/K y por $W \mid V$ el lugar en LF/F. Sea $h(x) \in \mathfrak{o}_V[x]$ el polinomio minimal de β, y sea $\overline{h}(x) := h(x) \mod \mathfrak{m}_V$. Por el lema de Hensel, $\overline{h}$ es irreducible, de modo que es el polinomio minimal de α respecto a $\Bbbk(V)$. Finalmente

$$[\Bbbk(W) : \Bbbk(V)] \leq [LF : F] = \deg h = \deg \overline{h} = [\Bbbk(V)(\alpha) : \Bbbk(V)] \leq [\Bbbk(W) : \Bbbk(V)],$$

lo que implica que la extensión LF/F es no ramificada.

Si $L/M/K$ es una subextensión, entonces la extensión $LM = L$ es no ramificada sobre M y concluimos por la transitividad del grado de inercia. □

Corolario 6.10.1: Sea (K, v) un cuerpo ultramétrico henseliano con cuerpo de restos $\Bbbk(v)$ perfecto, y sea $w \mid v$ en K^{alg}. Entonces, $\Bbbk(w) = \Bbbk(v)^{\mathrm{alg}}$ y existe una extensión algebraica K^{nr}/K tal que si L/K es no ramificada, entonces $L \subseteq K^{\mathrm{nr}}$.

En consecuencia, si tenemos una extensión L/K, podemos obtener la máxima subextensión no ramificada como $L \cap K^{\mathrm{nr}}$.

§6.1.3 Índice de ramificación.

Definición 6.11: Sea $(K, |\,|)$ un cuerpo métrico. Entonces $K^\times$ es un grupo abeliano y $|\,|\colon K^\times \to \mathbb{R}^\times$ es un homomorfismo de grupos abelianos. Llamamos a

$$G_K := \{|a| : a \in K^\times\} \subseteq \mathbb{R}^\times$$

el ***grupo de valores*** de K.

Si K es ultramétrico henseliano y L/K es una extensión finita, entonces claramente $G_L \geq G_K$. Habíamos también dicho que K se dice *discreto* si G_K es un subconjunto discreto de[1] $\mathbb{R}^\times$.

[1] Nótese que a menos que sea trivial, siempre existe algún $a \in K$ tal que $0 < |a| < 1$. Luego observese que $|a|^n \to 0$, de modo que el 0 siempre ha de ser un punto de acumulación de G_K, por eso indicamos que es discreto en $\mathbb{R}_{\neq 0}$.

Lema 6.12: Sea K un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos. Si K es discreto, entonces L también.

Demostración: Recuerdese que el valor absoluto estándar sobre L viene dado por

$$|\alpha| := |\operatorname{Nm}_{L/K}(\alpha)|^{1/n},$$

donde $\operatorname{Nm}_{L/K}(\alpha) \in K$, de modo que a lo más $G_L \subseteq G_K^{1/n}$. □

Definición 6.13: Sea K un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos. Llamamos el ***índice de ramificación*** a

$$e(L/K) := [G_L : G_K].$$

De la demostración anterior concluimos que $e(L/K) \mid [L : K]$.

Lema 6.14: Sea K un cuerpo ultramétrico henseliano discreto, y sean $F/L/K$ extensiones finitas de cuerpos. Entonces $e(F/K) = e(F/L)\, e(L/K)$.

Teorema 6.15: Sea (K, v) un cuerpo ultramétrico y sea L/K una extensión de cuerpos con $w \mid v$ tales que:

(a) K es henseliano.

(b) w es discreto tanto en L como en K.

(c) La extensión de cuerpos $\Bbbk(w)/\Bbbk(v)$ tiene grado f finito.

Entonces la extensión L/K tiene grado finito y de hecho

$$[L : K] = f(L/K)\, e(L/K).$$

Demostración: Sean π, τ uniformizadores de K, L resp. Por definición de e, ha de cumplirse que $|\tau|^e = |\pi|$. Sea $\{[\beta_1], \ldots, [\beta_f]\}$ una base de $\Bbbk(w)/\Bbbk(v)$, y sea

$$B := \{\beta_i \tau^j : 1 \leq i \leq f, 0 \leq j < e\}.$$

Se cumple que B es un conjunto de ef elementos que probaremos es una base de L como K-espacio vectorial.

(I) B es un conjunto linealmente independiente: Por contradicción, sean $a_{ij} \in K$ no todos nulos tales que

$$\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\beta_i\tau^j = 0,$$

supongamos, sin perdida de generalidad, que $\max_{i,j} |a_{ij}| = 1$. Elijamos los índices I, J de modo que

$$\forall 1 \leq i \leq f,\ j < J \quad |a_{ij}| < 1, \qquad |a_{IJ}| = 1.$$

Luego, como los β_i's son base de $\Bbbk_L$, vemos que $\sum_{i=1}^{f} a_{iJ}\beta_i \not\equiv 0$ (mód $\mathfrak{m}$) y, así, se tiene que

$$\left|\sum_{i=1}^{f} a_{iJ}\beta_i\right| = 1,$$

luego vemos que

$$\left|\sum_{i=1}^{f} a_{ij}\beta_i\tau^j\right| \begin{cases} \leq |\pi| = |\tau|^e, & j < J, \\ = |\tau|^J, & j = J, \\ \leq |\tau|^{J+1}, & j > J. \end{cases}$$

Lo que, por la proposición 5.29 nos daría que la sumatoria tiene valor absoluto $= |\tau|^J$ lo cual es absurdo.

(II) B es un sistema generador: Como los β_i's son base de $\Bbbk_L$, entonces para todo $\alpha \in \mathfrak{o} := \mathfrak{o}_L$ se ha de cumplir que existen $a_{i0} \in \mathfrak{o}_K \subseteq K$ tales que

$$\alpha - \sum_{i=1}^{f} a_{i0}\beta_i = \tau\alpha_1 \in \tau\mathfrak{o},$$

para un único $\alpha_1 \in \mathfrak{o}$. Llamemos $u_{ij} := \beta_i\tau^j$, de modo que $B = \{u_{ij}\}_{ij}$. Iterando inductivamente el procedimiento obtendremos $a_{ij} \in \mathfrak{o}_K \subseteq K$ tales que

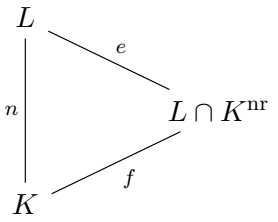
$$\alpha - \sum_{j=0}^{e-1}\sum_{i=1}^{f} a_{ij}\beta_i\tau^j = \alpha - \sum_{i,j} a_{ij}u_{ij} = \tau^e\alpha_e = \pi\alpha_e \in \pi\mathfrak{o},$$

Llamemos $C_0 := \sum_{i,j} a_{ij} u_{ij}$ el cual es una combinación lineal generada por B sobre K, e iterando inductivamente vemos que

$$\alpha - C_0 - C_1\pi - \cdots - C_m\pi^m \in \pi^{m+1}\mathfrak{o},$$

de modo que, como K es completo, la serie $\sum_{m=0}^{\infty} C_m\pi^m$ converge y a α, justo como se quería probar. □

El siguiente diagrama resume la situación anterior:



Teorema 6.16: Sea K un cuerpo ultramétrico henseliano discreto, y sea L/K una extensión finita de cuerpos. Entonces

$$e(L/K)\, f(L/K) = [L : K].$$

Corolario 6.16.1: Sea (K, v) un cuerpo ultramétrico henseliano y sea L/K una extensión finita de cuerpos de grado n con $w \mid v$ cuya extensión de cuerpos de restos $\Bbbk(w)/\Bbbk(v)$ sea separable. Entonces $e = 1$ (resp. $e = n$) syss la extensión L/K es no ramificada (resp. totalmente ramificada).

Definición 6.17: Sea (K, v) un cuerpo ultramétrico henseliano. Una extensión algebraica L/K con $w \mid v$ se dice ***mansamente ramificada***[2] si la extensión de cuerpos de restos $\Bbbk(w)/\Bbbk(v)$ es separable y si $\operatorname{car}\Bbbk(v) \nmid [L : L \cap K^{\mathrm{nr}}]$; de lo contrario, se dice que la extensión es ***salvajemente ramificada***.

Para el caso de extensiones de grado infinito, el índice $[L : L \cap K^{\mathrm{nr}}]$ es un número supernatural o número de Steinitz; estas nociones vienen descritas en la teoría de grupos profinitos que es una herramienta aquí para la teoría de Galois infinita.

[2]De. *zahm verzweigt*, eng. *tamely ramified*. La palabra *manso* tiene el sentido aquí de «dócil, tranquilo, domesticado».

Proposición 6.18: Sea (K, v) un cuerpo ultramétrico henseliano. Una extensión finita L/K es mansamente ramificada syss definiendo $M := L \cap K^{\mathrm{nr}}$ se cumple que

$$L = M(\sqrt[m_1]{\alpha_1}, \ldots, \sqrt[m_r]{\alpha_r}),$$

donde cada m_i no es múltiplo de $\operatorname{car} \Bbbk(v)$. En cuyo caso, $[L : K] = e(L/K)\, f(L/K)$.

Corolario 6.18.1: Sea K un cuerpo ultramétrico henseliano y sean $L/K, F/K$ un par de extensiones algebraicas. Si L/K es mansamente ramificada, entonces LF/F y toda subextensión $L/M/K$ también es mansamente ramificada. Si L/K y F/K son mansamente ramificadas, entonces LF/K también.

Definición 6.19: Sea K un cuerpo ultramétrico henseliano, entonces se denota su extensión mansamente ramificada maximal como

$$K_{\mathrm{tr}} := \bigcup \{K \subseteq L \subseteq K^{\mathrm{alg}} : L/K \text{ es mansamente ramificada}\}.$$

Nótese que en la mayoría de teoremas hemos exigido que el cuerpo base K sea completo, pero ésto es una mera justificación para no hacer elecciones sobre el valor absoluto de L/K.

Teorema 6.20: Sea K un cuerpo ultramétrico, entonces $G_{\hat{K}} = G_K$.

Demostración: Sea $\alpha \in \hat{K}$ no nulo, entonces $\alpha = \lim_n a_n$ para alguna sucesión $a_n \in K$. Nótese que como $|a_n| = |\alpha + (a_n - \alpha)|$, entonces para n suficientemente grande tenemos que $|a_n - \alpha| < |\alpha|$, de modo que $|a_n| = |\alpha|$ para dichos n's. □

Otra forma de enunciar el teorema es que la compleción $\hat{K}/K$ es una extensión totalmente ramificada.

6.2 Lugares y cuerpos globales

Definición 6.21: Sea K un cuerpo fijo. Las clases de valores absolutos no triviales equivalentes sobre K se llaman ***lugares***.[3] En particular, los valores absolutos arquimedianos sobre K se dicen ***lugares al infinito***. Dado un lugar v, denotaremos por K_v la compleción de $(K, |\,|_v)$.

[3] Algunos autores (e.g., Milne [**96**]) emplean la palabra *primo*. Además, algunos denotan por $\mathfrak{p}$ a los lugares; en su lugar, reservaré dicha notación exclusivamente para los lugares que vengan de ideales primos.

Sea v un lugar sobre K tal que K_v es un cuerpo local. Entonces:

(a) Si $K_v = \mathbb{R}$, decimos que v es un ***lugar real***. Sea $\sigma\colon K \to \mathbb{R}$ el monomorfismo correspondiente a v, llamamos su *normalización* como:

$$\forall \alpha \in K \quad \|\alpha\|_v := |\sigma\alpha|_\infty.$$

(b) Si $K_v = \mathbb{C}$, decimos que v es un ***lugar imaginario***. Sea $\sigma\colon K \to \mathbb{C}$ el monomorfismo correspondiente a v, llamamos su *normalización* como:

$$\forall \alpha \in K \quad \|\alpha\|_v := |\sigma\alpha|_\infty^2.$$

(c) Si v no es arquimediano, entonces (K, v) tiene un cuerpo de restos $\Bbbk(v)$ asociado, el cual es finito y consta de q elementos. La *normalización* de v es tal que si π es un uniformizador entonces

$$\|\pi\|_v = q^{-1}.$$

Los valores absolutos p-ádicos los exigíamos normalizados, por ejemplo.

El primer teorema de Ostrowski es ahora un enunciado de clasificación de lugares sobre $\mathbb{Q}$, mientras que el segundo teorema de Ostrowski es un enunciado sobre lugares al infinito:

Corolario 6.21.1: Sea K un cuerpo de $\operatorname{car} K = 0$. La poscomposición con la conjugación compleja $\tau \in \operatorname{Gal}(\mathbb{C}/\mathbb{R})$ induce una acción sobre los encajes complejos $\operatorname{Hom}(K, \mathbb{C})$ y los lugares al infinito de K están en biyección con los elementos del cociente $\operatorname{Hom}(K, \mathbb{C})/\operatorname{Gal}(\mathbb{C}/\mathbb{R})$.

En consecuencia, si K es un cuerpo numérico con r lugares reales y s lugares imaginarios, entonces su grado es $r + 2s$.

Pista: Esto es porque $\mathbb{R}$, siendo un cuerpo métrico completo, solo posee una extensión de su valor absoluto a $\mathbb{C}$, por lo que componer con la conjugación no cambia el lugar arquimediano. □

Para un cuerpo cualquiera, clasificar los lugares puede ser toda una proeza. Conviene restringirse a lo siguiente:

Definición 6.22: Un ***cuerpo p-ádico*** K es un cuerpo local no arquimediano de característica 0, o equivalentemente, una extensión finita de $\mathbb{Q}_p$.

Sobre un cuerpo p-ádico K consideramos los dos siguientes valores absolutos (que determinan el mismo lugar):

1. Denotamos por $|\,|$ el valor absoluto sobre K que coincide con $|\,|_p$ en $\mathbb{Q}_p$ (concretamente, $|\alpha| = |\mathrm{Nm}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}$, donde $n := [K : \mathbb{Q}_p]$).

2. Denotamos por $\|\,\|_K$ al valor absoluto (llamado *normalizado*) tal que dado un uniformizador π de K se cumpla que $\|\pi\|_K = q^{-1}$, donde q es la cardinalidad del cuerpo de restos de K.

Lema 6.23: Sea $K/\mathbb{Q}_p$ una extensión de grado n. Entonces para todo $\alpha \in K$ se cumple:

$$\|\alpha\|_K = |\alpha|^n.$$

Demostración: Basta probarlo para un elemento $\alpha \in K$ que no sea unitario (¿por qué?). Fijemos $f := f(K/\mathbb{Q}_p)$ y $e := e(K/\mathbb{Q}_p)$, y sea π un uniformizador de K. Por definición $[\mathbb{F}_q : \mathbb{F}_p] = f$, de modo que $q = p^f$, y además

$$\|p\|_K = \|\pi\|_K^e = q^{-e} = p^{-ef} = p^{-n}. \qquad \square$$

Corolario 6.23.1: Sean L/K una extensión finita de cuerpos p-ádicos, entonces

1. Para todo $\alpha \in K$ se cumple que $\|\alpha\|_K = |\mathrm{Nm}_{K/\mathbb{Q}_p}(\alpha)|_p$.

2. Para todo $\alpha \in K$ se cumple que $\|\alpha\|_L = \|\alpha\|_K^{[L:K]}$.

Definición 6.24: Sea L/K una extensión de cuerpos. Si w es un lugar sobre L de modo que $|\,|_w$ sobre K corresponde a un lugar v, entonces decimos que w ***divide a*** v, denotado $w \mid v$.

Así pues, el corolario 5.4.3 nos dice que un lugar v es arquimediano syss $v \mid \infty$ (ésto justifica el nombre «lugar al infinito»).

Ahora, queremos poder dar una teoría de ramificación para cuerpos métricos incompletos.

Lema 6.25: Sea $(K, |\,|)$ un cuerpo métrico, $\hat{K}$ su compleción y sea $L = K(\alpha)$ una extensión finita separable. Sea $f(x) \in K[x]$ el polinomio minimal de α sobre K y sea

$$f(x) = g_1(x) \cdots g_m(x) \in \hat{K}[x],$$

una descomposición, donde cada $g_j(x) \in \hat{K}[x]$ es mónico, irreducible y posee alguna raíz β_j.

En primer lugar, los g_j's son todos distintos. En segundo lugar, sea $|\,|_j$ la restricción del valor absoluto canónico sobre $L_j := \hat{K}(\beta_j)$ a $K(\alpha)$; entonces los $|\,|_j$'s representan todos los lugares que dividen a $|\,|$.

Demostración: Sea $\|\,\|_v$ un valor absoluto sobre L que extienda a $|\,|$, y denotemos L_v su compleción. Claramente, $\hat{K}(\alpha) \subseteq L_v$ y como $\hat{K}(\alpha)$ es completo, entonces $\hat{K}(\alpha) = L_v$. Sea $\phi(x) \in \hat{K}[x]$ el polinomio minimal de α sobre $\hat{K}$, entonces como $f(\alpha) = 0$ se cumple que $\phi(x) \mid f(x)$, de modo que ϕ es alguno de los g_j's.

Recíprocamente, notamos que los L_j's coinciden (como cuerpos) todos con $\hat{K}(\alpha) = L_v$, de modo que podemos identificar a $K(\alpha)$ con todos los subcuerpos de L_j, por lo que se comprueba que los lugares descritos en el enunciado corresponden a todas las extensiones de $|\,|$. El que los g_j's sean distintos se deduce de que $f(x)$ es separable. □

Nótese que en la prueba hemos constatado nuevamente un hecho fundamental: al añadir un valor absoluto (vale decir, una topología) estamos considerando estructuras más sofisticadas que sólo la parte de cuerpo. En efecto, todos los L_j's son cuerpos isomorfos, pero las métricas son distintas.

Para ello comencemos con lo siguiente: sea L/K una extensión finita de cuerpos, sea w un lugar sobre L y v el único lugar sobre K tal que $w \mid v$; entonces claramente $L_w \supseteq K_v$, donde ésta extensión sí está contemplada por nuestra teoría de ramificación. Fijemos $\{\beta_1, \ldots, \beta_n\}$ es una K-base de L. Sea $\alpha \in L_w$, entonces $\alpha = \lim_m a_m$ para algunos $a_m \in L$; luego cada $a_m = \sum_{j=1}^n c_{mj}\beta_j$ y, por tanto,

$$\alpha = \lim_m a_m = \lim_m \sum_{j=1}^n c_{mj}\beta_j = \sum_{j=1}^n \left(\lim_m c_{mj}\right)\beta_j,$$

de modo que $\beta_1, \ldots, \beta_n$ generan a L_w/K_v. Por lo que, $[L_w : K_v] \leq [L : K]$.

Teorema 6.26: Sea L/K una extensión separable de grado n. Fijado un lugar v sobre K, existen finitos lugares w's sobre L tales que $w \mid v$. Entonces:

$$K_v \otimes_K L \cong \prod_{w|v} L_w,$$

(como K-álgebras) y, en particular,

$$\sum_{w|v} [L_w : K_v] = [L : K].$$

Demostración: Sea $L = K(\alpha)$, donde α tiene polinomio minimal $f(x)$ como en el lema anterior. Luego $f(x) = g_1(x) \cdots g_m(x) \in K_v[x]$, donde los g_j's son mónicos e irreducibles en $K_v[x]$, luego son coprimos dos a dos, y por el teorema chino del resto (cfr. [**1,** teo. 2.59]) vemos que

$$K_v \otimes_K L \cong \frac{K_v[x]}{(f)} \cong \prod_{j=1}^{m} \frac{K_v[x]}{(g_j)} \cong \prod_{w|v} L_w. \qquad \square$$

Definición 6.27: Sea L/K una extensión finita de cuerpos. El valor $[L_w : K_v]$ con $w \mid v$ se dice el ***grado local*** de la extensión en w.

Sea K un cuerpo y sea v un lugar no trivial sobre K. Decimos que v es un ***lugar bien comportado***[4] Si para toda extensión finita L se cumple que

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

Como señala Lang [**91,** pág. 14], este concepto será útil en ciertos contextos de característica prima cuando el cuerpo base K no es perfecto.

Corolario 6.27.1: Sea L/K una extensión finita de cuerpos, y sea v un lugar bien comportado sobre K. Para todo $\alpha \in L$ se cumple que:

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha), \qquad \mathrm{Nm}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(\alpha).$$

Corolario 6.27.2: Sea L/K una extensión finita de cuerpos, y sea v un lugar bien comportado sobre K. Para todo $\alpha \in L$ se cumple que:

$$\prod_{w|v} |\alpha|_w^{[L_w:K_v]} = |\mathrm{Nm}_{L/K}(\alpha)|_v,$$

donde $|\,|_v$ es cualquier valor absoluto que represente a v, y $|\,|_w$ es la única representación que coincide con $|\,|_v$ en K.

Corolario 6.27.3: Sean L/K una extensiones finitas de cuerpos numéricos, y sea v un lugar sobre K. Entonces para todo $\alpha \in L$ se cumple que

$$\prod_{w|v} \|\alpha\|_w = \|\,\mathrm{Nm}_{L/K}(\alpha)\|_v.$$

[4] eng. *well-behaved*.

Corolario 6.27.4: Sea K un cuerpo numérico, sea $\mathfrak{p} \lhd \mathcal{O}_K$ un primo tal que $\mathfrak{p} \mid p$ y sea $|\,|_{\mathfrak{p}}$ el valor absoluto $\mathfrak{p}$-ádico que extiende al p-ádico. Entonces para todo $\alpha \in K$ se cumple que

$$\|\alpha\|_{\mathfrak{p}} = (\mathbf{N}\,\mathfrak{p})^{-\nu_{\mathfrak{p}}(\alpha)}.$$

Lema 6.28: Sea K un cuerpo numérico y sea $\alpha \in K^\times$, entonces $|\alpha|_v = 1$ para todos salvo finitos lugares v sobre K.

Demostración: Fijemos a α, primero probaremos que $|\alpha|_v \leq 1$ para todos salvo finitos lugares. Como α es ($\mathbb{Q}$-)algebraico, entonces posee algún polinomio minimal

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{Q}[x].$$

Hay finitos lugares al infinito sobre K y es fácil concluir que $f(x) \in \mathbb{Z}_p[x]$ para todos salvo finitos primos p. De modo que $|\alpha|_v \leq 1$ para todo $v \mid p$. Aplicando el mismo razonamiento a $1/\alpha$, vemos que $|\alpha|_v \geq 1$ para todos salvo finitos lugares v, de lo que se concluye el enunciado. □

Teorema 6.29 – *Fórmula del producto*: Sea K un cuerpo numérico y sea $\alpha \in K^\times$. Entonces

$$\prod_v \|\alpha\|_v = 1,$$

donde v recorre todos los lugares sobre K. De hecho, en detalle:

$$\prod_{v|\infty} \|\alpha\|_v = |\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)|_\infty, \qquad \prod_{v\nmid\infty} \|\alpha\|_v = |\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)|_\infty^{-1}.$$

§6.2.1 Cuerpos globales. Aquí otorgamos una clasificación de los llamados *cuerpos globales* mediante una axiomatización de Artin y Whaples **[67]**. En general, la mayoría de libros evitan estos resultados, por lo que, si el lector lo desea puede considerar que un *cuerpo global* es por definición una extensión finita de $\mathbb{Q}$ o de $\mathbb{F}_p(t)$, donde t es un elemento trascendente.

Definición 6.30: Un par (K, M) se dice un ***cuerpo global***[a] si K es un cuerpo y M es un conjunto no vacío de lugares sobre K tal que:

CG1. Existen representantes $|\,|_v$ para cada $v \in M$ tal que para todo $a \in K^\times$ se cumple que $|a|_v = 1$ para todos salvo finitos $v \in M$ y

además:

$$\prod_{v\in M} |a|_v = 1.$$

CG2. Existe al menos un lugar $v \in M$ tal que K_v es un cuerpo local.

[a] Weil [**109**] emplea el término $\mathbb{A}$-*cuerpo*.

Al final de la clasificación especificaremos y erradicaremos el conjunto M, pero previo a ello será útil. De momento, los cuerpos numéricos con M siendo el conjunto de todos los lugares son un ejemplo de cuerpo global.

El corolario 5.13.1 nos señala que cualquier cuerpo global (K, M) es tal que M debe ser infinito. Si v es un lugar al infinito, entonces $|2|_v > 1$, por lo que M siempre consta de a lo más finitos lugares arquimedianos.

Proposición 6.31: Sea (K, M) un cuerpo global donde M solo contiene lugares no arquimedianos. Entonces

$$K_0 := \{a \in K : \forall v \in M \quad |a|_v \leq 1\}$$

es un subcuerpo de K. De hecho, $K_0 = \{0\} \cup \{a \in K : \forall v \in M \quad |a|_v = 1\}$.

Demostración: Basta notar que si $a \neq 0$ está en K_0, entonces por CG1 se cumple necesariamente que $|a|_v = 1$ para todo $v \in M$. Luego, trivialmente $a^{-1} \in K_0$ y por desigualdad ultramétrica, si $b \in K_0$ entonces $a+b \in K_0$. □

Lema 6.32: Sea (K, M) un cuerpo que satisface CG1 y sea $R \subseteq K$ un subcuerpo que posee algun $a \in R^\times$ tal que $|a|_v \neq 1$ para algún $v \in M$. Sea N el conjunto de lugares w sobre R tales que $v \mid w$ para algún $v \in M$; entonces (R, N) es también satisface CG1.

Demostración: La condición que de R no posea constantes es solo para notar que si sólo posee constantes, entonces N es vacío. Fijemos $w \in N$ y sea $a \in R$ tal que $|a|_w > 1$, entonces, por CG1 sobre K, existen a lo más finitos v's tales que $|a|_v > 1$, y luego se cumple que existen a lo más finitos $v \in M$ tales que $v \mid w$. Definamos el representante:

$$|b|_w := \prod_{\substack{v|w \\ v\in M}} |b|_v.$$

Así, es fácil notar que si $b \in R^\times$, entonces $\prod_{w\in N} |b|_w = \prod_{v\in M} |b|_v = 1$. □

Lema 6.33: Sea (K, M) un cuerpo global y sea L/K una extensión finita de cuerpos. Sea N el conjunto de lugares w sobre L tales que $w \mid v$ para algún $v \in M$; entonces (L, N) también es un cuerpo global.

Demostración: Basta aplicar el mismo razonamiento que empleamos para concluir que un cuerpo numérico es global: es fácil comprobar que L posee a lo más finitos lugares al infinito. Dado $\alpha \in L$, sea $f(x) \in K[x]$ su polinomio minimal y dado un lugar finito $v \in M$ denotemos $\mathfrak{o}_v = \{a \in K : |a|_v \leq 1\}$. Es fácil comprobar que $f(x) \in \mathfrak{o}_v[x]$ para todos salvo finitos lugares no arquimedianos $v \in M$, de modo que si $w \mid v$, entonces $|\alpha|_w = 1$ para todos salvo finitos lugares $w \in N$.

Para comprobar la fórmula del producto hay que distinguir el caso separable del puramente inseparable. Sea N la clausura normal de L/K y sea $\alpha \in L^\times$. Sea $\beta := \prod_\sigma \sigma(\alpha)$, donde σ recorre todos los elementos de $\mathrm{Gal}(N/K)$; luego β es un elemento puramente inseparable y, por tanto, existe $m \geq 1$ entero tal que $\beta^m = c \in K$. Para todo $w \in N$ tal que $w \mid v$ se cumple que

$$|c|_v = \prod_\sigma |\sigma(\alpha)|_w^m.$$

Reemplazando $|\,|_w$ por $|\,|_w^m$ con un m suficientemente grande (e.g., basta $m = [N : K]$) vemos que α^m es separable, luego para todo $\sigma \in \mathrm{Gal}(N/K)$ existe w' tal que $|\sigma(\alpha)|_w = |\alpha|_{w'}$, de modo que

$$\prod_{w \in N} |\alpha|_w = \prod_{v \in M} \prod_{w \mid v} |\alpha|_w = 1.$$

El axioma CG2 se comprueba trivialmente notando que toda extensión finita de un cuerpo local es local. □

Lema 6.34: Son cuerpos globales:

(a) (K, M), donde K es un cuerpo numérico y M son todos los lugares en K normalizados.

(b) $(K_1(t), M)$, donde K_1 es un cuerpo finito, t es K_1-trascendente y M son todos los lugares sobre $K_1(t)$ que son triviales en K_1.

Definición 6.35: Sea (K, M) un cuerpo global, y sea $S \subseteq K$ un subconjunto.

(a) Si M contiene algún lugar al infinito, llamamos ***orden*** de S a su cardinalidad.

(b) Si M sólo contiene lugares finitos, entonces sea K_0 el subcuerpo de constantes. Definamos:

$$q := \begin{cases} |K_0|, & |K_0| < \infty, \\ 2, & |K_0| = \infty. \end{cases}$$

Entonces el orden de S refiere a q^s, donde s es la cantidad de elementos K_0-linealmente independientes de S.

Si (K, M) es un cuerpo global y $v \in M$ es tal que K_v es local, entonces definimos $\rho(v) > 0$ real tal que $|a|_v = \|a\|_v^{\rho(v)}$, donde $\| \|_v$ es el valor absoluto normalizado según la sección anterior.

Lema 6.36: Sea (K, M) un cuerpo global y sea $v \in M$ tal que K_v es local. Sea $S \subseteq K$ un conjunto de elementos de orden $N > 1$, y sea x real tal que $|a|_v \leq x$ para todo $a \in S$. Entonces existe $\theta \in K$ que satisface lo siguiente:

- Si M contiene un lugar al infinito, entonces θ es resta de elementos en S; y si no, entonces $\theta \in \mathrm{Span}_{K_0}(S)$.
- $\theta \neq 0$.
- $|\theta|_v \leq C_v x / N^{\rho(v)}$, donde C_v es una constante que depende únicamente de v.

Demostración: Lo separamos por casos:

(a) $\underline{K_v = \mathbb{R}}$: Consideramos a $K \subseteq \mathbb{R}$, y a $\| \|_v$ siendo una restricción del valor absoluto usual $| |_\infty$. Por definición, se tiene que $S \subseteq [-x^{1/\rho(v)}, x^{1/\rho(v)}]$ y divida al último intervalo en $M - 1$ partes iguales; por el principio del palomar hay dos elementos distintos de S en el mismo subintervalo y defina θ como su diferencia (da igual el signo), de tal forma que

$$\|\theta\|_v \leq \frac{2x^{1/\rho(v)}}{N-1} \leq \frac{4x^{1/\rho(v)}}{N} \implies |\theta|_v \leq \frac{4^{\rho(v)} x}{N^{\rho(v)}}.$$

(b) $\underline{K_v = \mathbb{C}}$: Consideramos a $K \subseteq \mathbb{C}$, y a $\| \|_v^{1/2}$ siendo el valor absoluto usual $| |_\infty$. Así S es un subconjunto de la bola de radio $x^{1/2\rho(v)}$ centrada en el origen, y en particular, del cuadrado

$$\{x + \mathrm{i}y \in \mathbb{C} : |x| \leq x^{1/2\rho(v)}, |y| \leq x^{1/2\rho(v)}\},$$

éste lo subdividimos en n^2 cuadrados de igual tamaño, donde $n^2 < N \leq (n+1)^2$. Nuevamente por palomar, dos elementos distintos yacen en el mismo subcuadrado y definimos su diferencia como θ, el cual satisface:

$$\|\theta\|_v^{1/2} \leq \frac{2^{3/2}x^{1/2\rho(v)}}{n} \leq \frac{2^{5/2}x^{1/2\rho(v)}}{\sqrt{N}} \implies |\theta|_v \leq \frac{2^{5\rho(v)}x}{N^{\rho(v)}}.$$

(c) v es discreto: Por ser discreto, elijamos $\beta \in S$ tal que $|\beta|_v = \max_{a\in S}\{|a|_v\}$, luego para todo $\alpha \in S$ se cumple que $|\alpha/\beta|_v \leq 1$ y $S \subseteq \mathfrak{o}_v$.

Sea $(\mathfrak{o}_v, \mathfrak{p}_v, k_v)$ el anillo de valuación de $(K, |\,|_v)$ y fijemos $q := |k_v|$. Sea $r \geq 0$ el natural tal que $q^r < N \leq q^{r+1}$, luego es claro que hay q^r clases distintas $\mathrm{mód}\,\mathfrak{p}_v^r$. Por palomar, hay dos elementos de $\frac{1}{\beta}S$ en la misma clase de equivalencia $\mathrm{mód}\,\mathfrak{p}_v^r$, luego denotamos θ/β a su diferencia. Para probar la cuestión de la combinación lineal, considere K_0 el cuerpo de constantes, que es un subcuerpo de k_v, sea $f = [k_v : K_1]$ de modo que en $\mathfrak{o}_v$ hay a lo más rf elementos K_0-linealmente independientes con clases distintas $\mathrm{mód}\,\mathfrak{p}_v^r$, luego hay una combinación lineal (pues $N > q^r \geq rf$) que es $\equiv 0 \pmod{\mathfrak{p}_v^r}$. Así pues

$$\left\|\frac{\theta}{\beta}\right\|_v \leq \frac{1}{q^r} = \frac{q}{q^{r+1}} \leq \frac{q}{N}.$$

Despejando β obtendremos $|\theta|_v \leq q^{\rho(v)}x/|\beta|_v$. □

Definición 6.37: Sea (K, M) un cuerpo global. Un ***adèle***[5] sobre K es una tupla $\boldsymbol{a}\colon M \to \prod_{v\in M} K_v$ tal que

1. Para todo $v \in M$ se cumple que $a_v \in K_v$.
2. $|a_v|_v \leq 1$ para todos salvo finitos $v \in M$. Definimos $|a|_v := |a_v|_v$ por brevedad.

Si $\alpha \in K$, denotamos también por α al idèle $\boldsymbol{a}$ tal que $a_v = \alpha$. Definimos su ***volumen***:

$$V(\boldsymbol{a}) := \prod_{v\in M} |a|_v.$$

Sea $\boldsymbol{x}\colon M \to [0, \infty)$, definimos el ***paralelótopo*** de dimensiones $\boldsymbol{x}$ como:

$$P(\boldsymbol{x}) := \{\boldsymbol{a} : |a|_v \leq x_v\}.$$

[5]Del fr., abrev. de *additive idéal élément* ('elemento ideal aditivo').

Lema 6.38: Sea (K, M) un cuerpo global. Sea N el orden del paralelótopo $P(\boldsymbol{x})$ y sea $w \in M$ tal que K_w es local, entonces existe una constante D_w tal que $N = 1$ (y $P(\boldsymbol{x}) = \{0\}$) o

$$N \leq D_w \left(\prod_{v \in M} x_v \right)^{1/\rho(w)}.$$

Demostración: Supongamos que $N > 1$, por el lema anterior existe $\theta \neq 0$ tal que

$$|\theta|_w \leq \frac{C_w x_w}{N^{\rho(w)}},$$

y para los otros lugares $v \in M_{\neq w}$ podemos dar una cota inmediata

$$|\theta|_v \leq \begin{cases} x_v, & v \text{ finito}, \\ 4^{\rho(v)} x_v, & v \text{ arquimediano}. \end{cases}$$

como un cuerpo global solo posee finitos lugares arquimedianos, podemos agruparlo todo en una constante E_w de modo que, por la fórmula del producto:

$$1 \leq \prod_{v \in M} |\theta|_v \leq \frac{E_w \prod_{v \in M} x_v}{N^{\rho(w)}}.$$ □

6.3 Grupos de ramificación

Una aclaración importante es que desde ésta sección en adelante, L/K puede ser *cualquier* extensión de cuerpos, de modo que $\mathrm{Gal}(L/K)$ puede ser infinito y, en cuyo caso, estar dotado de estructura de grupo topológico *profinito* (i.e., es Hausdorff, compacto y hereditariamente disconexo). El lector incómodo con éstas definiciones puede o bien suponer que todo es finito (y obviar los adjetivos como «continuo») o bien está invitado a leer de grupos profinitos en Wilson **[5],** Ch. 1-3.

Sea L/K una extensión de cuerpos de Galois y sea v un lugar sobre K. Dada una extensión $w \mid v$ en L y dado un K-automorfismo $\sigma \in \mathrm{Gal}(L/K)$, entonces el lugar $|a|_{\sigma w} := |\sigma a|_w$ extiende también a v; es decir, $\mathrm{Gal}(L/K)$ actúa sobre los lugares que extienden a v.

Proposición 6.39: Sea (K, v) un cuerpo métrico y sea L/K una extensión de cuerpos de Galois. El grupo de Galois $\mathrm{Gal}(L/K)$ actúa transitivamente sobre las extensiones $w \mid v$ en L.[6]

Demostración: Supongamos que la extensión L/K es finita. Entonces el conjunto $P := \{w \mid v \text{ en } L\}$ es finito. Si $w, w' \in P$ no fueran conjugados entre sí, entonces sus órbitas son disjuntas resp., y finitas. Por el teorema de aproximación débil existe $\alpha \in L$ tal que

$$\forall \sigma \in \mathrm{Gal}(L/K) \qquad |\sigma(\alpha)|_w < 1,\ |\sigma(\alpha)|_{w'} > 1.$$

Luego obtenemos que

$$|\,\mathrm{Nm}_{L/K}(\alpha)|_w = \prod_{\sigma \in \mathrm{Gal}(L/K)} |\sigma(\alpha)|_w < 1, \qquad |\,\mathrm{Nm}_{L/K}(\alpha)|_{w'} > 1.$$

Pero esto es absurdo, puesto que $\mathrm{Nm}_{L/K}(\alpha) \in K$ donde ambos lugares coinciden.

Si L/K no es finita, entonces considere $\mathcal{F}$ el conjunto de las subextensiones $K \subseteq F \subseteq L$ con F/K finita de Galois. Fijemos dos lugares w, w' en L que extienden a K, entonces para todo $F \in \mathcal{F}$ sea

$$X_F := \{\sigma \in \mathrm{Gal}(L/K) : (\sigma \circ w)|_F = w'|_F\} \leq \mathrm{Gal}(L/K),$$

el cual es un subgrupo cerrado, puesto que todo $\sigma \notin X_F$ está contenido en el entorno $\sigma \in \sigma\,\mathrm{Gal}(L/F) \subseteq \mathrm{Gal}(L/K) \setminus X_F$. Finalmente, la intersección $\mathcal{F} \in \mathcal{F}X_F$ es no vacía ya que $\mathrm{Gal}(L/K)$ es un grupo compacto y la familia posee la p.i.f.[7] □

Definición 6.40: Sea (K, v) un cuerpo métrico, sea L/K una extensión de cuerpos y $w \mid v$. El ***grupo de descomposición*** de L/K respecto a w se define como

$$G_w = G_w(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : \forall \alpha \in L \quad |\sigma\alpha|_w = |\alpha|_w\}.$$

Si además v es ultramétrico, entonces se definen el ***grupo de inercia*** y ***de ramificación*** resp. como

$$I_w = I_w(L/K) := \{\sigma \in G_w : \forall \alpha \in \mathfrak{o}_w \quad \sigma\alpha \equiv \alpha \pmod{\mathfrak{m}_w}\}$$
$$R_w = R_w(L/K) := \left\{\sigma \in G_w : \forall \alpha \in L^\times \quad \frac{\sigma\alpha}{\alpha} \equiv 1 \pmod{\mathfrak{m}_w}\right\}.$$

Nótese que si v es henseliano, entonces $G_w(L/K) = \mathrm{Gal}(L/K)$ por el corolario 5.65.1. Claramente $G_w \supseteq I_w \supseteq R_w$.

[6] Vale decir, dadas dos extensiones $w \mid v$ y $w' \mid v$ existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $w = \sigma w'$.

[7] Propiedad de intersecciones finitas, es decir, que ningún conjunto finito de X_F's tiene intersección total vacía.

Corolario 6.40.1: Sea K un cuerpo ultramétrico con dominio de valuación discreta $(\mathfrak{o}, \mathfrak{p})$ y sea L/K una extensión finita de cuerpos con $\mathfrak{P} \mid \mathfrak{p}$. Entonces

$$G_{\mathfrak{P}}(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : \sigma[\mathfrak{P}] = \mathfrak{P}\}.$$

Demostración: Como la extensión es finita, entonces el anillo de valuación $(\mathfrak{O}, \mathfrak{P})$ de L también es de valuación discreta, y por tanto $\mathfrak{P} = \pi\mathfrak{O}$ para un uniformizador $\pi \in \mathfrak{O}$. Recuérdese ahora lo siguiente: el anillo $\mathfrak{O}$ es la clausura entera de $\mathfrak{o}$ en L, por lo que para todo K-automorfismo $\sigma \in \mathrm{Gal}(L/K)$ y todo elemento entero $\beta \in \mathfrak{O}$ se cumple que $\sigma(\beta) \in \mathfrak{O}$. Sea $u \in \mathfrak{O}^\times$ una unidad, es decir, un elemento entero no nulo de L tal que $u^{-1} \in \mathfrak{O}$; nótese que ambas propiedades son invariantes bajo σ, de modo que $\sigma(u) \in \mathfrak{O}^\times$.

Finalmente, todo elemento de L se escribe de forma única como $\alpha := u\pi^n$, donde $u \in \mathfrak{O}^\times$ y $n \in \mathbb{Z}$; así que para verificar que $|\sigma(\alpha)|_{\mathfrak{P}} = |\alpha|_{\mathfrak{P}}$, solo basta verificar que $|\sigma(\pi)|_{\mathfrak{P}} = |\pi|_{\mathfrak{P}}$. □

Si $w \mid v$ es una extensión de lugares en L/K, entonces $G_w(L/K)$ es el estabilizador de w. En el caso finito, cuando $\Bbbk(w)/\Bbbk(v)$ es separable, un argumento de conteo nos dice que $G_w(L/K)$ tiene ef elementos.

Lema 6.41: Sea L/K una extensión de cuerpos arbitraria, sea w un lugar sobre L y $v := w|_L$ un lugar sobre K. Entonces G_w (e I_w, R_w si w es no arquimediano) son subgrupos cerrados de $\mathrm{Gal}(L/K)$. En consecuente, también poseen una estructura (canónica) de grupo profinito.

Considere un retículo de extensiones de cuerpos, donde L/K y L'/K' son de Galois:

$$\begin{array}{ccc} & & L' \\ & \overset{\tau}{\nearrow} & \big| \\ L & & \\ \big| & & \\ \big| & \overset{\tau|_K}{\nearrow} & K' \\ K & & \end{array} \tag{6.2}$$

Este induce el siguiente homomorfismo (continuo) en grupos de Galois:

$$\mathrm{Gal}(\tau)\colon\ \mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K), \qquad \sigma \mapsto (\tau \circ \sigma)|_{\tau L} \circ \tau^{-1}.$$

Nótese que como L/K es normal, entonces $\tau L/\tau K$ también, por lo que τL es estable bajo σ y poscomponer con τ^{-1} tiene sentido.

Proposición 6.42: Sean L/K y L'/K' un par de extensiones de Galois con un homomorfismo $\tau\colon L \to L'$. Sean w' un lugar sobre L' y sea $w := w'|_L$. Se cumplen:

1. $\mathrm{Gal}(\tau)$ se restringe a un homomorfismo continuo $G_{w'}(L'/K') \to G_w(L/K)$. Si además w' es no arquimediano, entonces también se restringe a homomorfismos:

$$I_{w'}(L'/K') \to I_w(L/K), \qquad R_{w'}(L'/K') \to R_w(L/K).$$

2. Si $L = L'$ (y $M := K' \supseteq K$), entonces se satisface

$$\begin{aligned} G_w(L/M) &= G_w(L/K) \cap \mathrm{Gal}(L/M), \\ I_w(L/M) &= I_w(L/K) \cap \mathrm{Gal}(L/M), \\ R_w(L/M) &= R_w(L/K) \cap \mathrm{Gal}(L/M). \end{aligned}$$

3. Si $L' := L_w$, $K' := K_v$ (con $v := w|_L$) y τ es la inclusión canónica, entonces se tienen los siguientes isomorfismos:

$$G_w(L/K) \cong G_w(L_w/K_v), \qquad I_w(L/K) \cong I_w(L_w/K_v),$$
$$R_w(L/K) \cong R_w(L_w/K_v).$$

Demostración:

1. Dado $\sigma \in G_{w'}$ y $\alpha \in L$, es claro que $|\sigma\tau\alpha|_{w'} = |\tau\alpha|_{w'}$. Luego aplicamos τ^{-1} a ambos lados y así ganamos.

   Dado $\sigma' \in I_{w'}$ y definiendo $\sigma := \mathrm{Gal}(\tau)(\sigma')$ vemos que para $\alpha \in \mathfrak{o}_w$:

$$|\sigma\alpha - \alpha|_w = |\tau^{-1}(\sigma\tau\alpha - \tau\alpha)|_w = |\sigma(\tau\alpha) - \tau\alpha|_{w'} < 1,$$

   pues $\tau\alpha \in \mathfrak{o}_{w'}$. El razonamiento es análogo con $R_{w'}$.

2. Es claro que el homomorfismo inducido es inyectivo y que sea sobreyectivo también es claro.

3. El grupo $G_w(L_w/K_v)$ consiste precisamente de los automorfismo continuos de L_w respecto a w que fijan a K_v. Como $L \subseteq L_w$ es denso, este induce un único K-automorfismo continuo de L respecto a w. Así que, queremos ver que los elementos de $G_w(L/K)$ sean exactamente los K-automorfismos de L continuos respecto a w. Claramente todo

elemento de $G_w(L/K)$ es continuo y, recíprocamente, si $\sigma \in \mathrm{Gal}(L/K)$ es continuo, entonces dado $\alpha \in L$ tal que $|\alpha|_w < 1$, como

$$\sigma(\lim_n \alpha^n) = 0 = \lim_n \sigma(\alpha^n) = \lim_n \sigma(\alpha)^n$$

vemos que $|\sigma\alpha|_w < 1$, lo que demuestra que pertenece a $G_w(L/K)$. □

Parte del propósito de los métodos de la teoría de cuerpos de clase es la clasificación de extensiones de cuerpos. Conviene comenzar a deducir una teoría de Galois relativa a la ramificación.

Definición 6.43: Sea L/K una extensión de cuerpos de Galois con una extensión de lugares $w \mid v$. Definamos el ***cuerpo de descomposición*** como la subextensión fija por el grupo de descomposición:

$$Z_w(L/K) := \mathrm{Fix}(G_w(L/K)) = \{\alpha \in L : \forall \sigma \in G_w(L/K) \quad \sigma(\alpha) = \alpha\}.$$

Corolario 6.43.1: Sea L/K una extensión de cuerpos de Galois con una extensión de lugares $w \mid v$. Sea $Z := Z_w(L/K)$ el cuerpo de descomposición, entonces:

1. La restricción $w|_Z$ de w en Z admite una única extensión en L.
2. Si v es ultramétrico, entonces $w|_Z$ tiene el mismo cuerpo de restos y grupo de valores que v.
3. Se satisface que $Z = L \cap K_v$ (donde la intersección sucede en L_w).

Proposición 6.44: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. Entonces la extensión $\Bbbk(w)/\Bbbk(v)$ es normal y tenemos la siguiente sucesión exacta (en Grp):

$$1 \longrightarrow I_w(L/K) \longrightarrow G_w(L/K) \xrightarrow{\rho} \mathrm{Gal}(\Bbbk(w)/\Bbbk(v)) \longrightarrow 1.$$

Demostración: Es claro que si L/K es normal, entonces $\Bbbk(w)/\Bbbk(v)$ también es normal; así demostraremos que el homomorfismo ρ es sobreyectivo.

Supongamos que L/K sea finita, de modo que la extensión $\Bbbk(w) \supseteq k := \Bbbk(v)$ también es finita. Si ahora consideramos la clausura separable de $\Bbbk(v)$ en $\Bbbk(w)$, entonces por el teorema del elemento primitivo existe $\overline{\theta} \in \Bbbk(w)$ tal que

$$\lambda := \Bbbk(w) \cap \Bbbk(v)^{\mathrm{sep}} = \Bbbk(v)(\overline{\theta}).$$

Nótese que $\mathrm{Gal}(\Bbbk(w)/\Bbbk(v)) \cong \mathrm{Gal}(\lambda/k)$ donde el isomorfismo es la restricción. Sea $\overline{f}(x) \in k[x]$ el polinomio minimal de $\overline{\theta}$; cada $\sigma \in \mathrm{Gal}(\lambda/k)$ viene completamente determinado por $\sigma\overline{\theta}$, el cual es una raíz de $\overline{f}(x)$. Sea $f(x) \in \mathfrak{o}_v[x]$ un polinomio mónico tal que $f(x) \cong \overline{f}(x) \mod \mathfrak{m}_v$, entonces por el lema de Hensel existe una raíz $\beta \in L \cap K_v = Z_w$ de $f(x)$ con $|\beta|_w \leq 1$ tal que $\beta \equiv \sigma\overline{\theta}$ $(\mathfrak{m}_w)$. Eligiendo apropiadamente $\theta \in \mathfrak{o}_v$ tal que $\theta \equiv \overline{\theta}$ $(\mathfrak{m}_v)$ podemos asegurarnos de que β y θ sean K-conjugados, de modo que existe un monomorfismo $\tau\colon K(\theta) \to L$ que los intercambia y, por tanto, se extiende a un elemento de $\mathrm{Gal}(L/Z_w) = G_w(L/K)$.

Para el caso infinito aplicamos un argumento topológico. Sea σ un $\Bbbk(v)$-automorfismo de $\Bbbk(w)$ y sea $\Bbbk(v) \subseteq \Phi \subseteq \Bbbk(w)$ una subextensión finita, entonces eligiendo una $\Bbbk(v)$-base de Φ podemos elevarla para construir una subextensión finita $K \subseteq F \subseteq L$. Ahora, el conjunto de elementos de $\tau \in G_w(L/K)$ tales que $\rho(\tau|_F) = \sigma|_\Phi$ es cerrado (¿por qué?), así que constituyen una familia de cerrados con la p.i.f. dentro de un espacio compacto, luego tienen intersección total no vacía. □

Definición 6.45: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. Se define el ***cuerpo de inercia*** como

$$T_w(L/K) := \mathrm{Fix}\left(I_w(L/K)\right) = \{\alpha \in L : \forall \sigma \in I_w(L/K) \quad \sigma(\alpha) = \alpha\}.$$

Como $I_w(L/K) \subseteq G_w(L/K)$, esto significa que $T_w(L/K) \supseteq Z_w(L/K)$ y, por teoría de Galois:

Corolario 6.45.1: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. Entonces:

1. Existe un isomorfismo canónico $\mathrm{Gal}(T_w/Z_w) \cong I_w(L/K)$.
2. El cuerpo T_w es la subextensión maximal no ramificada (¡respecto a w!) de L/Z_w.

Querremos definir a continuación el cuerpo de ramificación, para ello primero determinaremos un homomorfismo importante:

Definición 6.46: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K, y denotemos por $\Gamma_K = \{|\alpha|_v : \alpha \in K^\times\} \subseteq \mathbb{R}^\times$ el grupo de valores de K (y análogamente con Γ_L). Definimos el homomorfismo

$$\chi_-\colon I_w(L/K) \longrightarrow \mathrm{Hom}(\Gamma_L/\Gamma_K, \Bbbk(w)^\times)$$

como prosigue: dado $\alpha \in \Gamma_L$, es claro que existe $\alpha' \in \mathfrak{o}_L$ tal que $\alpha \equiv \alpha'$ (mód Γ_K); dado $\sigma \in I_w$ definimos

$$\chi_\sigma \colon \Gamma_L/\Gamma_K \longrightarrow \Bbbk(w)^\times, \qquad \alpha \longmapsto \frac{\sigma\alpha'}{\alpha} \mod \mathfrak{m}_\mathfrak{w}.$$

Corolario 6.46.1: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. El grupo de ramificación $R_w(L/K)$ es el núcleo de $\chi\colon I_w \to \mathrm{Hom}(\Gamma_L/\Gamma_K, \Bbbk(w)^\times)$ descrito arriba.

Proposición 6.47: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. El grupo de ramificación R_w es el (único) p-subgrupo de Sylow de I_w, donde $p = \operatorname{car} \Bbbk(v)$.

Demostración: Pasando a la completación, podemos suponer que K es henseliano y haremos el caso finito (pues el infito se sigue, mediante técnicas de grupos profinitos).

Si R_w no fuese un p-grupo, entonces existiría un $\sigma \in R_w$ de orden primo $\ell \neq p$. Sea $M := \mathrm{Fix}(\sigma)$ con lugar $v' \mid v$; veremos que $\Bbbk(v') = \Bbbk(w)$. La contención $R_w \subseteq I_w$ se traduce en que $M \supseteq T_w$ de lo que se sigue que $\Bbbk(v') \supseteq \Bbbk(w) \cap \Bbbk(v)^{\mathrm{sep}}$, por lo que la extensión $\Bbbk(w) \supseteq \Bbbk(v')$ es puramente inseparable y, por tanto, con grado una potencia de p. Ahora, también

$$[\Bbbk(w) : \Bbbk(v')] \mid [L : M] = [L : \mathrm{Fix}(\langle\sigma\rangle)] = |\langle\sigma\rangle| = \ell,$$

de modo que necesariamente $[\Bbbk(w) : \Bbbk(v')] = 1$. Por tanto, la extensión L/M es mansamente ramificada y, por la proposición 6.18, es de la forma $L = M(\sqrt[\ell]{\alpha})$ para algún $\alpha \in M$. Así pues, si $\sigma(\alpha) = \zeta\alpha$, donde $\zeta \in M$ es una raíz ℓ-ésima primitiva de la unidad. Por otro lado, $\zeta = \sigma(\alpha)/\alpha \equiv 1$ (mód $\mathfrak{m}_w$), por lo que

$$\ell \equiv 1 + \zeta + \zeta^2 + \cdots + \zeta^{\ell-1} = 0 \mod \mathfrak{m}_w),$$

lo que es absurdo, pues $\operatorname{car} \Bbbk(w) = p \nmid \ell$.

Así que R_w es un p-grupo. Como $\operatorname{car} \Bbbk(w) = p$, vemos que los elementos de orden finito de $\Bbbk(w)^\times$ tienen orden coprimo a p, luego también los elementos del grupo $\mathrm{Hom}(\Gamma_L/\Gamma_K, \Bbbk(w)^\times)$, y lo mismo aplica para $I_w/R_w \subseteq \mathrm{Hom}(\Gamma_L/\Gamma_K, \Bbbk(w)^\times)$. Esto prueba que R_w es el p-subgrupo de Sylow de I_w. □

Definición 6.48: Sea $w \mid v$ una extensión de lugares ultramétricos sobre

una extensión de Galois L/K. Se define el ***cuerpo de ramificación*** como

$$V_w(L/K) := \mathrm{Fix}\left(R_w(L/K)\right) = \{\alpha \in L : \forall \sigma \in R_w(L/K) \quad \sigma(\alpha) = \alpha\}.$$

Corolario 6.48.1: Sea $w \mid v$ una extensión de lugares ultramétricos sobre una extensión de Galois L/K. Entonces:

1. Existe un isomorfismo canónico $\mathrm{Gal}(V_w/Z_w) \cong R_w(L/K)$.
2. El cuerpo V_w es la subextensión maximal mansamente ramificada de L/Z_w.
3. La sucesión

$$1 \longrightarrow R_w(L/K) \longrightarrow I_w(L/K) \xrightarrow{\chi_-} \mathrm{Hom}(\Gamma_L/\Gamma_K, \Bbbk(w)^\times) \longrightarrow 1$$

es exacta.

Demostración: Para la demostración, supondremos que $K = Z_w$ es henseliano.

1. Trivial de la definición.
2. Como V_w es el subcuerpo que fija al p-subgrupo de Sylow R_w de I_w, entonces V_w es la unión finita de las subextensiones L/T_w de Galois finitas de grado coprimo a p. Así pues, V_w contiene a la subextensión mansamente ramificada maximal de T (y, luego, también de Z_w). Como el grado de cada subextensión finita M/V de V_w/V es coprimo a p, entonces la extensión en cuerpos de restos de M/V es separable (¿por qué?), luego la extensión V_w/V es mansamente ramificada; ergo $V_w = V$.
3. Lo único por verificar es que χ_- es sobreyectivo. □

§6.3.1 Grupos de ramificación superior. La teoría de Galois de valuaciones puede profundizarse exponencialmente bajo las siguientes hipótesis:

Situación 6.49: Sea (K, v) un cuerpo ultramétrico henseliano con anillo de valuación discreta $(\mathfrak{o}, \mathfrak{p}, \Bbbk(v))$. Denotaremos por $\pi \in \mathfrak{p}$ un uniformizador y por $v_K \colon K^\times \to \mathbb{Z}$ al (único) homomorfismo de valuación normalizado, es decir, tal que $v_K(\pi) = 1$.

Sea L/K una extensión normal de grado d con $w \mid v$; denotaremos su anillo de valuación discreta por $(\mathfrak{O}, \mathfrak{P}, \Bbbk(w))$, por $\Pi \in \mathfrak{P}$ un uniformizador, por $v_L \colon L^\times \to \mathbb{Z}$ al homomorfismo de valuación, por

$f := [\Bbbk(w) : \Bbbk(v)]$ y por $e := v_L(\pi)$ (equivalentemente, $\Pi^e = u\pi$ para algún $u \in \mathfrak{o}^\times$).

Definición 6.50: En la situación 6.49, para $s \geq -1$ real definimos el ***s*-ésimo grupo de ramificación*** como:

$$G_s(L/K) := \{\sigma \in \mathrm{Gal}(L/K) : \forall \alpha \in \mathfrak{O} \quad v_L(\sigma\alpha - \alpha) \geq s+1\}.$$

De no haber ambigüedad sobre la extensión, denotaremos $G_s := G_s(L/K)$.

Observación 6.50.1: En la situación 6.49 se tiene que $G_{-1}(L/K) = G_w(L/K) = \mathrm{Gal}(L/K)$ es el grupo de descomposición, que $G_0(L/K) = I_w(L/K)$ es el grupo de inercia y que $G_1(L/K) = R_w(L/K)$ es el grupo de ramificación.

Corolario 6.50.2: En la situación 6.49, los grupos de ramificación forman una cadena descendiente de subgrupos normales

$$G_{-1} \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s = \{\mathrm{Id}\}, \qquad s \gg 0.$$

Para todo $s \geq 0$ entero, el homomorfismo

$$G_s/G_{s+1} \to U_L^{(s)}/U_L^{(s+1)}, \qquad \sigma \mapsto \frac{\sigma\Pi}{\Pi}$$

es inyectivo e independiente de la elección de $\Pi \in \mathfrak{P}$.

En consecuente, los cocientes G_s/G_{s+1} son abelianos y, para $s \geq 1$, son p-grupos.

Demostración: El que los subgrupos sean normales y que eventualmente $G_s = \{\mathrm{Id}\}$ para $s \gg 0$ es un ejercicio para el lector. La inyectividad del homomorfismo es por definición. □

Lema 6.51: En la situación 6.49 supongamos que la extensión $\Bbbk(w) \supseteq \Bbbk(v)$ es separable (e.g., cuando K es un cuerpo local). Entonces existe $\theta \in \mathfrak{O}$ tal que $\mathfrak{O} = \mathfrak{o}[\theta]$.

Definición 6.52: En la situación 6.49 cuando $\Bbbk(w)/\Bbbk(v)$ es separable, sea

$$i_{L/K}(\sigma) := v_L(\sigma\beta - \beta),$$

donde $\mathfrak{O} = \mathfrak{o}[\beta]$ y sea

$$\eta_{L/K}(s) := \int_0^s \frac{1}{[G_0 : G_x]}\,\mathrm{d}x,$$

donde $[G_0 : G_x] := [G_x : G_0]^{-1}$ para $-1 \leq x < 0$.

Proposición 6.53: En la situación 6.49, supongamos que $\Bbbk(w)/\Bbbk(v)$ es separable. Dada $K \subseteq M \subseteq L$ una subextensión intermedia, entonces para $\tau \in \mathrm{Gal}(M/K)$:

$$i_{M/K}(\tau) = \frac{1}{e(L/M)} \sum_{\sigma|_M = \tau} i_{L/K}(\sigma).$$

Proposición 6.54: En la situación 6.49, supongamos que $\Bbbk(w)/\Bbbk(v)$ es separable. Para $s \geq -1$ real se cumple que

$$\eta_{L/K}(s) = \frac{1}{|G_0(L/K)|} \sum_{\sigma \in G_{-1}} \mín\{i_{L/K}(\sigma), s+1\} - 1.$$

Teorema 6.55 (Herbrand): En la situación 6.49, supongamos que $\Bbbk(w)/\Bbbk(v)$ es separable. Sea $K \subseteq M \subseteq L$ una subextensión de Galois y sea $H := \mathrm{Gal}(L/M)$, entonces

$$G_s(L/K)H/H = G_t(M/K), \qquad t := \eta_{L/M}(s).$$

6.4 Discriminante y diferente

Comenzaremos con una discusión general del discriminante (aquí K ni siquiera debe tener un valor absoluto asociado).

Definición 6.56: Sea L/K una extensión finita de cuerpos, de modo que sea $B := (\alpha_1, \ldots, \alpha_n)$ una base (ordenada) de L como K-espacio vectorial. El ***discriminante*** de L/K relativa a B es

$$\Delta_B(L/K) := \det\big([\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)]_{ij}\big).$$

Proposición 6.57: Sea L/K una extensión finita de cuerpos. Sean $A := (\alpha_1, \ldots, \alpha_n), B := (\beta_1, \ldots, \beta_n)$ dos K-bases de L con cambio de coordenadas:

$$\alpha_i = \sum_{j=1}^n c_{ij}\beta_j, \qquad C := [c_{ij}]_{ij} \in \mathrm{Mat}_n(K), \qquad A = C \cdot B.$$

Entonces $\Delta_A(L/K) = \det(C)^2 \cdot \Delta_B(L/K)$. En consecuencia, si el discriminante es nulo en alguna base, lo es en todas.

Demostración: Sean $X := [\mathrm{Tr}(\alpha_i\alpha_j)]_{ij}, Y := [\mathrm{Tr}(\beta_i\beta_j)]_{ij}$. Nótese que

$$\begin{aligned} X_{ij} = \mathrm{Tr}(\alpha_i\alpha_j) &= \sum_{p=1}^{n} \mathrm{Tr}(c_{ip}\beta_p\alpha_j) = \sum_{p=1}^{n} c_{ip}\,\mathrm{Tr}(\beta_p\alpha_j) \\ &= \sum_{p=1}^{n}\sum_{q=1}^{n} c_{ip}\,\mathrm{Tr}(\beta_p c_{jq}\beta_q) = \sum_{p=1}^{n}\sum_{q=1}^{n} c_{ip}\,\mathrm{Tr}(\beta_p\beta_q)c^t_{qj} = (C\cdot Y\cdot C^t)_{ij}, \end{aligned}$$

de modo que se comprueba el enunciado. □

Un teorema que probamos en el libro de álgebra es el siguiente:

Teorema 6.58: Sea L/K una extensión finita de cuerpos. El discriminante de L/K es no nulo en alguna (y luego en toda) base syss L/K es separable (cfr. [**1,** teo. 13.18]).

Definición 6.59: Sea L/K una extensión finita separable de cuerpos. Definimos

$$\Delta(L/K) := [\Delta_B(L/K)] \in K^\times/K^{\times 2},$$

donde B es cualquier base de L como K-espacio vectorial.

Por la proposición anterior, el discriminante queda bien definido salvo cuadrados.

Ahora volvemos a nuestro contexto:

Lema 6.60: Sea K un cuerpo ultramétrico y sea $\mathfrak{o}$ su anillo de valuación. Todo $\mathfrak{o}$-modulo finitamente generado libre de torsión es libre.

Demostración: Sea M un $\mathfrak{o}$-modulo finitamente generado libre de torsión, y sea $B := \{u_1, \ldots, u_n\}$ una base minimal.[8] Si B no fuese una base, entonces existen $a_1, \ldots, a_n \in \mathfrak{o}$ no todos nulos tales que

$$\sum_{j=1}^{n} a_j u_j = 0.$$

[8]Se dice que B es una ***base minimal*** si es un sistema de generadores minimal, es decir, si le quitamos algún elemento deja de generar el módulo (cfr. [**1,** def. 6.45]).

Sin perdida de generalidad, sea $|a_n| = \max_j |a_j|$, de modo que cada $a_j = a_n b_j$ para algunos $b_j \in \mathfrak{o}$, de modo que

$$a_n(b_1u_1 + \cdots + b_{n-1}u_{n-1} + u_n) = 0.$$

Como M está libre de torsión, entonces $b_1u_1 + \cdots + u_n = 0$ y así $u_n = -\sum_{j=1}^{n-1} b_j u_j$, lo que contradice que B sea base minimal. Así que B tiene que ser base. □

Nótese que si K es discreto, entonces su anillo de valuación es un DIP de modo que ésto es trivial; lo impresionante son los otros casos.

Ahora fijaremos un contexto:

Situación 6.61: Sea (K, v) un cuerpo ultramétrico henseliano con anillo de valuación discreta y sea L/K una extensión finita separable de cuerpos con extensión de lugares $w \mid v$. Denotaremos por π un uniformizador de K.

Lema 6.62.A: En situación 6.61, sean B_1, B_2 un par de $\mathfrak{o}_v$-bases ordenadas de $\mathfrak{o}_w$, entonces

$$\Delta_{B_1}(L/K) \equiv \Delta_{B_2}(L/K) \pmod{\mathfrak{o}_v^{\times 2}}.$$

Demostración: La existencia de bases viene dada por el lema anterior. Como $\mathfrak{o}_v$ es íntegramente cerrado, entonces para todo $\alpha \in \mathfrak{o}_w$ se cumple que $\mathrm{Tr}(\alpha) \in \mathfrak{o}_v$, de modo que $\Delta_{B_1}(L/K) \in \mathfrak{o}_v$. Por un proceso análogo al de la proposición 6.57 es claro que el discriminante queda determinado salvo cuadrados de unidades de $\mathfrak{o}_v$. □

Definición 6.62: En situación 6.61, se define $|\Delta(L/K)| := |\Delta_B(L/K)|$, donde B es cualquier $\mathfrak{o}_v$-base ordenada de $\mathfrak{o}_w$.

El lema permite ver que $|\Delta(L/K)|$ es independiente de la base escogida y de que $|\Delta(L/K)| \leq 1$.

Lema 6.63: En situación 6.61 supongamos que L/K es una extensión no ramificada. Para todo $\alpha \in \mathfrak{o}_w$ se cumple que su polinomio característico $\psi_{L/K,\alpha}(x) \in \mathfrak{o}_v[x]$ satisface:

$$\psi_{L/K,\alpha}(x) \equiv \psi_{\bar{L}/\bar{K},\bar{\alpha}}(x) \pmod{\mathfrak{m}_K}.$$

Demostración: Fijemos $\beta_1, \ldots, \beta_n$ una K-base de L, y fijemos $\alpha \in \mathfrak{o}_L$ arbitrario. Para todo i ha de cumplirse que

$$\alpha\beta_i = \sum_{j=1}^{n} c_{ij}\beta_j, \qquad c_{ij} \in \mathfrak{o}_K.$$

Luego $C := [c_{ij}]_{ij}$ es una matriz de modo que $\psi_{L/K,\alpha}(x) = \det(xI - C) \in \mathfrak{o}[x]$ por definición de polinomio característico. Ahora bien, nótese que $\bar{\beta}_1, \ldots, \bar{\beta}_n$ es una $\bar{K}$-base de $\bar{L}$ y claramente se satisface que

$$\bar{\alpha}\bar{\beta}_i = \sum_{j=1}^{n} \bar{c}_{ij}\bar{\beta}_j, \qquad \bar{c}_{ij} \in \bar{K},$$

de lo que es fácil concluir el enunciado. □

Nuevamente es un buen ejercicio localizar el uso de todas las hipótesis.

Teorema 6.64: En la situación 6.61 supongamos que $\Bbbk(w)/\Bbbk(v)$ es separable. El discriminante $|\Delta(L/K)| = 1$ syss L/K es una extensión no ramificada.

Demostración: $\Longrightarrow$. Por contrarrecíproca, sea L/K una extensión ramificada y sea τ un uniformizador de L. Luego, por la demostración del teorema 6.15, sabemos que si $[\beta_1], \ldots, [\beta_n]$ es base de $\Bbbk(w)/\Bbbk(v)$, entonces

$$B := \{\beta_i\tau^j : 1 \leq i \leq f, 0 \leq j < e\},$$

es base de L/K, donde $e > 1$ puesto que es ramificada. Llamemos $X := [\mathrm{Tr}_{L/K}(\beta_{n_i}\beta_{n_j}\tau^{m_i+m_j})]_{ij}$ de modo que $\Delta_B(L/K) = \det X$. Ahora bien, la norma se preserva bajo K-conjugados y como los β_i's son base, todos han de tener $|\beta_i| = 1$, luego $|\beta_i\tau^j| = |\tau|^j < 1$ si $0 < j < e$, luego al sumar los K-conjugados tendremos que $|\mathrm{Tr}(\beta_i\tau^j)| \leq |\tau|^j$; así que X posee toda una columna de norma < 1 y así $|\Delta(L/K)| < 1$.

$\Longleftarrow$. Si L/K es no ramificada, entonces por el lema anterior para todo $\alpha \in \mathfrak{o}_w$ se cumple que

$$\overline{\mathrm{Tr}_{L/K}(\alpha)} = \mathrm{Tr}_{\bar{L}/\bar{K}}(\bar{\alpha}),$$

luego, fijada una base ordenada B de L/K se cumple que

$$\overline{\Delta_B(L/K)} = \Delta_{\bar{B}}(\bar{L}/\bar{K}),$$

y como $\bar{L}/\bar{K}$ es separable, entonces el discriminante es no nulo (en $\bar{K}$), luego se comprueba que $|\Delta(L/K)| = 1$. □

De hecho, de la demostración podemos sacar una mejor cota:

Corolario 6.64.1: En la situación 6.61 supongamos que $\Bbbk(w)/\Bbbk(v)$ es separable. Entonces:

$$|\Delta(L/K)| \leq |\pi|^{(e-1)f}.$$

Teorema 6.65: En la situación 6.61, sea $n := [L : K]$ el grado de la extensión. Entonces L/K es totalmente ramificada syss $L = K(\alpha)$ donde α es raíz de un polinomio de Eisenstein.

Demostración: $\Longleftarrow$. Sea π un uniformizador de K y sea α raíz del polinomio

$$c_n x^n + \cdots + c_1 x + c_0 = 0,$$
$$|c_n| = 1, \qquad \forall j < n \quad |c_j| \leq |\pi|, \qquad |c_0| = |\pi|.$$

Luego, es fácil concluir que necesariamente $|\alpha|^n = |\pi|$ (¿por qué?), de modo que $e(L/K) \geq n$.

$\Longrightarrow$. Sea τ un uniformizador de L, de modo que $|\tau|^n = |\pi|$ por definición de ser totalmente ramificada. Aplicando normas es fácil concluir que $1, \tau, \ldots, \tau^{n-1}$ son K-linealmente independientes y, por tanto, conforman una base de L. Luego podemos obtener una relación del estilo

$$\tau^n + c_{n-1}\tau^{n-1} + \cdots + c_1\tau + c_0 = 0.$$

Aplicando normas es fácil concluir que cada $c_j \in \mathfrak{o}_K$ y, de hecho, que cada $|c_j| < 1$ y además que $|c_0| = |\tau|^n = |\pi|$. De modo que $L = K(\tau)$ donde τ es raíz de un polinomio de Eisenstein. □

§6.4.1 Tránsito local-global. Ahora vamos a *globalizar* la noción de discriminante, para lo cual comenzaremos por dar ciertas definiciones en el contexto de dominios de Dedekind:

Situación 6.66: Sea A un dominio de Dedekind con $K := \operatorname{Frac} A$, sea $F/L/K$ una extensión finita y separable de cuerpos, y sean $B := \mathcal{O}_{L/A}$ y $C := \mathcal{O}_{F/A}$ las clausuras enteras de A en L y F resp.

Dados $\mathfrak{P} \mid \mathfrak{p}$ una extensión de ideales primos entre $B \supseteq A$, denotaremos por $\widehat{A} := \widehat{A_{\mathfrak{p}}}$ y $\widehat{B} := \widehat{B_{\mathfrak{P}}}$ las completaciones $\mathfrak{p}$- y $\mathfrak{P}$-ádicas resp.

Definición 6.67 (Dedekind): En la situación 6.66, dado un ideal fraccionario $\mathfrak{b}$ de B definimos su B-módulo dual:

$$\mathfrak{b}^* := \{\gamma \in L : \forall b \in \mathfrak{b} \quad \mathrm{Tr}_{L/K}(b\gamma) \in A\}.$$

El ***codiferente*** de B/A es

$$\mathfrak{C}_{B/A} := B^* = \{\gamma \in L : \forall b \in B \quad \mathrm{Tr}_{L/K}(b\gamma) \in A\},$$

este es un ideal fraccionario que contiene a B (¿por qué?), de modo que su inversa

$$\mathfrak{D}_{B/A} := (B^*)^{-1} = \{\gamma \in L : \gamma B^* \subseteq B\}$$

es un ideal entero de B, llamado el ***diferente***.

Observación 6.67.1: La hipótesis de que la extensión de cuerpos L/K sea separable en la situación 6.66 tiene dos propósitos: uno más banal de que B sea un A-módulo finitamente generado, y el otro más crucial de que la forma bilineal de la traza $(a, b) \mapsto \mathrm{Tr}_{L/K}(ab)$ sea un emparejamiento perfecto (y, en particular, no sea degenerada; i.e., no existan $a \in L^\times$ tales que $\mathrm{Tr}_{L/K}(ab) = 0$ para todo $b \in L$).

Proposición 6.68: En la situación 6.66, se cumple:

1. $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B} \cdot \mathfrak{D}_{B/A}$.
2. Sea $S \subseteq A \smallsetminus \{0\}$ un sistema multiplicativo, entonces
$$\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$
3. Sea $\mathfrak{P} \mid \mathfrak{p}$ entre primos de $B \supseteq A$, entonces $\mathfrak{D}_{B/A} \cdot \widehat{B} = \mathfrak{D}_{\hat{B}/\hat{A}}$.

Demostración:

1. Basta probar que $\mathfrak{C}_{C/A} = \mathfrak{C}_{C/B} \cdot \mathfrak{C}_{B/A}$ (como ideales fraccionarios). La inclusión «$\supseteq$» se sigue de que
$$\begin{aligned}\mathrm{Tr}_{F/K}(\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}C) &= \mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{F/L}(\mathfrak{C}_{C/B}\mathfrak{C}_{B/A}C)\right)\\ &= \mathrm{Tr}_{L/K}(\mathfrak{C}_{B/A}\,\mathrm{Tr}_{F/L}(\mathfrak{C}_{C/B}C)) \subseteq A.\end{aligned}$$
Para probar la inclusión «$\subseteq$», nótese que
$$\mathrm{Tr}_{F/K}(\mathfrak{C}_{C/A}C) = \mathrm{Tr}_{L/K}(B\,\mathrm{Tr}_{F/L}(\mathfrak{C}_{C/A}C)) \subseteq A,$$

de modo que $\mathrm{Tr}_{F/L}(\mathfrak{C}_{C/A}C) \subseteq \mathfrak{C}_{B/A}$, luego

$$\mathrm{Tr}_{F/L}(\mathfrak{C}_{B/A}^{-1}\mathfrak{C}_{C/A}C) = \mathfrak{C}_{B/A}^{-1}\,\mathrm{Tr}_{F/L}(\mathfrak{C}_{C/A}C) \subseteq B.$$

Así que $\mathfrak{C}_{B/A}^{-1}\mathfrak{C}_{C/A} \subseteq \mathfrak{C}_{C/B}$ o, equivalentemente, $\mathfrak{C}_{C/A} \subseteq \mathfrak{C}_{C/B}\mathfrak{C}_{B/A}$.

2. Trivial.

3. Cambiando A por $A_{\mathfrak{p}}$, podemos suponer que A es un anillo de valuación discreta. Asociado a $\mathfrak{p}$ tendremos un lugar v sobre K con una elección de valor absoluto $|\,|$; veremos que $\mathfrak{C}_{B/A}$ es denso en $\mathfrak{C}_{\widehat{B}/\widehat{A}}$.

   Sea $x \in \mathfrak{C}_{B/A}$ e $y \in \widehat{B_{\mathfrak{P}}} =: \mathfrak{o}_{\mathfrak{P}}$. Por el teorema de aproximación débil, existe $\eta \in L$ tal que $|\eta - y|_{\mathfrak{P}} < 1$ y $|\eta|_{\mathfrak{Q}} < 1$ para todo $\mathfrak{Q} \mid \mathfrak{p}$ con $\mathfrak{Q} \neq \mathfrak{P}$. Como $B \subseteq \mathfrak{o}_{\mathfrak{Q}}$ es denso, para $\eta \in \mathfrak{Q}$ existe una sucesión $\{\beta_n\}_{n\in\mathbb{N}} \subseteq B$ tal que $\eta = \lim_n \beta_n$ (en la topología $\mathfrak{Q}$-ádica), de modo que

$$\mathrm{Tr}_{L_{\mathfrak{Q}}/K_{\mathfrak{p}}}(x\eta) = \lim_n \mathrm{Tr}_{L_{\mathfrak{Q}}/K_{\mathfrak{p}}}(x\beta_n) \in \mathfrak{o}_{\mathfrak{Q}} \cap K = A$$

   por lo que

$$\mathrm{Tr}_{L/K}(x\eta) = \sum_{\mathfrak{Q}\mid\mathfrak{p}} \mathrm{Tr}_{L_{\mathfrak{Q}}/K_{\mathfrak{p}}}(x\eta) \in A.$$

   Esto prueba que $\mathfrak{C}_{B/A} \subseteq \mathfrak{C}_{\widehat{B_{\mathfrak{Q}}}/\widehat{A_{\mathfrak{p}}}}$ para todo $\mathfrak{Q} \mid \mathfrak{p}$.

   Por otro lado, sea $x \in \mathfrak{C}_{\widehat{B_{\mathfrak{P}}}/\widehat{A}}$ y sea $\xi \in L$ tal que $|\xi - x|_{\mathfrak{P}} < 1$ y $|\xi|_{\mathfrak{Q}} < 1$ para todo $\mathfrak{Q} \mid \mathfrak{p}$ con $\mathfrak{Q} \neq \mathfrak{P}$. Para todo $y \in B$ se tiene la siguiente implicancia

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy) \in A \implies \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\xi y) \in A,$$

   que se sigue del lema de Krasner (todos los $K_{\mathfrak{p}}$-conjugados de ξy tienen el mismo valor absoluto $\mathfrak{P}$-ádico); por otro lado, $\mathrm{Tr}_{L_{\mathfrak{Q}}/K_{\mathfrak{p}}}(\xi y) \in A$ trivialmente de que $\xi, y \in \mathfrak{o}_{\mathfrak{Q}}$. Así, $\xi \in \mathfrak{C}_{B/A}$, por lo que $\mathfrak{C}_{B/A} \subseteq \mathfrak{C}_{\widehat{B_{\mathfrak{P}}}/\widehat{A}}$ es denso. □

Corolario 6.68.1: En la situación 6.66 se satisface que

$$\mathfrak{D}_{B/A} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}},$$

donde $\mathfrak{D}_{\mathfrak{P}} := \mathfrak{D}_{\widehat{B_{\mathfrak{P}}}/\widehat{A_{\mathfrak{p}}}} \cap B$, con $\mathfrak{p} := \mathfrak{P} \cap A$.

Demostración: Basta notar que

$$\mathfrak{D}_{B/A} = \bigcap_{\mathfrak{P}} (\mathfrak{D}_{B/A} B_{\mathfrak{P}}) = \bigcap_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}},$$

y cambiar «$\bigcap$» por «$\prod$», ya que $\mathfrak{D}_{\mathfrak{P}}$ solo puede tener por factores primos al $\mathfrak{P}$; de modo que los términos son coprimos dos a dos. □

Definición 6.69: Sea L/K una extensión algebraica simple (i.e., generada por un solo elemento). Para $\beta \in L$ de polinomio minimal $f(x) \in K[x]$ respecto a K, se define su ***diferente*** como

$$\delta_{L/K}(\beta) := \begin{cases} f'(\beta), & L = K(\beta), \\ 0, & L \neq K(\beta). \end{cases}$$

Lema 6.70: En la situación 6.66, sea $\alpha \in B$ tal que $L = K(\alpha)$. Entonces el A-módulo dual $A[\alpha]^* = f'(\alpha)^{-1} B$.

En consecuencia, si la extensión $B = A[\alpha]$ es monogénica, entonces $\mathfrak{D}_{B/A} = \delta_{L/K}(\alpha) B$.

Demostración: Sea $f(x) := a_0 + a_1 x + \cdots + a_d x^d \in A[x]$ el polinomio minimal de α y sea

$$\frac{f(x)}{x - \alpha} = b_0 + b_1 x + \cdots + b_{d-1} x^{d-1} \in B[x].$$

Nótese que se tiene la siguiente igualdad

$$\forall 0 \leq r < d, \qquad \sum_{j=1}^{d} \frac{f(x)}{x - \alpha_j} \frac{\alpha_j^r}{f'(\alpha_j)} = x^r,$$

puesto que la diferencia es un polinomio de grado $\leq d - 1$ que se anula en $\alpha_1, \ldots, \alpha_d$ (¿por qué?); ergo es el polinomio nulo. Así que, evaluando, vemos que

$$\mathrm{Tr}_{L/K} \left(\frac{f(x)}{x - \alpha} \frac{\alpha^r}{f'(\alpha)} \right) = x^r,$$

de modo que, evaluando en $x = \alpha$, se tiene que

$$\mathrm{Tr}_{L/K} \left(\alpha^i \frac{b_j}{f'(\alpha)} \right) = \delta_{ij},$$

donde δ_{ij} denota la delta de Kronecker. Con ésto, hemos probado que la base dual de $(1, \alpha, \ldots, \alpha^{d-1})$ respecto a la forma bilineal $\mathrm{Tr}_{L/K}$ es

$$\left(\frac{b_0}{f'(\alpha)}, \quad \ldots, \quad \frac{b_{d-1}}{f'(\alpha)}\right).$$

Así que el dual de $B = A + \alpha A + \cdots + \alpha^{d-1}A$ es $\mathfrak{C}_{B/A} = \sum_{j=0}^{d-1} \frac{b_j}{f'(\alpha)} A$. Aplicando el algoritmo de Horner-Ruffini nos da las relaciones recursivas

$$b_{d-1} = 1, \qquad \forall 2 \le n < d, \quad b_{n-2} - \alpha b_{n-1} = a_{n-1},$$

que se expanden en

$$b_{n-r} = \alpha^{r-1} + a_{n-1}\alpha^{r-2} + \cdots + a_{n-r+1},$$

de modo que el A-módulo dual de $Ab_0 + \cdots + Ab_{d-1} = A[\alpha]$ es $A[\alpha]^* = f'(\alpha)^{-1}B$. □

El lema anterior se extiende a lo siguiente:

Teorema 6.71: En la situación 6.66, el diferente $\mathfrak{D}_{B/A}$ está generado por los diferentes $\delta_{L/K}(\beta)$ donde α recorre los elementos de B.

Demostración: Sea $\alpha \in B$ tal que $L = K(\alpha)$ con polinomio minimal $f(x) \in A[x]$, entonces podemos considerar el orden $A[\alpha] \subseteq B$ y el conductor $\mathfrak{f}_\alpha := \{\beta \in L : \beta B \subseteq A[\alpha]\} \trianglelefteq B$. Definiendo $c := f'(\alpha)$ tenemos la siguiente cadena de equivalencias:

$$\begin{aligned} \beta \in \mathfrak{f}_\alpha &\iff \beta B \subseteq A[\alpha] &&\iff c^{-1}\beta B \subseteq c^{-1}A[\alpha] = A[\alpha]^* \\ &\iff \mathrm{Tr}_{L/K}(c^{-1}\beta B) \subseteq A &&\iff \beta \in c\mathfrak{D}_{B/A}^{-1}, \end{aligned}$$

lo que prueba que $\delta_{L/K}(\alpha)B = \mathfrak{f}_\alpha \mathfrak{D}_{B/A}$ y, en particular, $\delta_{L/K}(\alpha) \in \mathfrak{D}_{B/A}$.

El primo $\mathfrak{P}$ induce un lugar en L, que a su vez induce un encaje $L \hookrightarrow K_\mathfrak{p}^{\mathrm{sep}}$. Existe $\beta \in \widehat{B}$ tal que $\widehat{A}[\beta] = \widehat{B}$, de lo que se sigue que

$$\nu_\mathfrak{P}(\mathfrak{D}_{B/A}) = \nu_\mathfrak{P}(\mathfrak{D}_{\widehat{B}/\widehat{A}}) = \nu_\mathfrak{P}(\delta_{L_\mathfrak{P}/K_\mathfrak{p}}(\beta)).$$

Denotemos por $\sigma_2, \ldots, \sigma_r \colon L \to K_\mathfrak{p}^{\mathrm{sep}}$ a los encajes asociados a los primos $\mathfrak{Q} \mid \mathfrak{p}$ con $\mathfrak{Q} \neq \mathfrak{P}$. Sea $a \in \widehat{A}$ tal que

$$\forall \tau \in \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{sep}}/K_\mathfrak{p}), \qquad |\tau(\beta) - a| = 1 \tag{6.3}$$

Ahora bien, si $\alpha \in \widehat{B}$ está suficientemente cerca de β, vemos que $\widehat{B} = \widehat{A}[\alpha]$. Así, por el teorema de aproximación, elegimos $\alpha \in B$ (por densidad) tal que $|\alpha - \beta|$ y $|\sigma_i(\alpha) - a|$ sean suficientemente pequeños y, en particular, $L = K(\alpha)$. Como

$$\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha) = \prod_{\tau \neq \mathrm{Id}} (\alpha - \tau\alpha),$$

donde τ recorre los monomorfismos $L_{\mathfrak{P}} \hookrightarrow K_{\mathfrak{p}}^{\mathrm{sep}}$, luego

$$\delta_{L/K}(\alpha) = \prod_{\sigma \neq \mathrm{Id}} (\alpha - \sigma\alpha) = \prod_{\tau \neq 1} (\alpha - \tau\alpha) \prod_{j=2}^{r} \prod_{\ell} (\alpha - \tau_{\ell j}\sigma_j\alpha),$$

donde σ recorre los monomorfismos $L \hookrightarrow K^{\mathrm{sep}}$ y los $\tau_{\ell j}$'s son elementos de $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{sep}}/K_{\mathfrak{p}})$.

Por la construcción de a (**??**), como $|\sigma_j\alpha - a| \to 0$ y cada $\tau_{\ell j}^{-1}(\alpha)$ está suficientemente cerca de $\tau_{\ell j}^{-1}(\beta)$, vemos que

$$|\alpha - \tau_{\ell j}\sigma_j\alpha| = |\tau_{\ell j}^{-1}\alpha - \sigma_j\alpha| = |\tau_{\ell j}^{-1}\alpha - a + a - \sigma_j\alpha| = 1,$$

por lo que

$$\nu_{\mathfrak{P}}(\mathfrak{D}_{B/A}) = \nu_{\mathfrak{P}}(\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta)) = \delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha) = \nu_{\mathfrak{P}}(\delta_{L/K}(\alpha)). \qquad \square$$

Teorema 6.72: En la situación 6.66, la extensión de primos $\mathfrak{P} \mid \mathfrak{p}$ es ramificada syss $\mathfrak{P} \mid \mathfrak{D}_{B/A}$. Además, definiendo $s := \nu_{\mathfrak{P}}(\mathfrak{D}_{B/A})$ y $e := e(\mathfrak{P}/\mathfrak{p})$, se satisface lo siguiente:

(a) Si $\mathfrak{P}/\mathfrak{p}$ es mansamente ramificado, entonces $s = e - 1$.

(b) Si $\mathfrak{P}/\mathfrak{p}$ es salvajemente ramificado, entonces $e \leq s \leq e - 1 + \nu_{\mathfrak{P}}(e)$.

Definición 6.73: En la situación 6.66, llamamos el ***(ideal) discriminante*** de $B \supseteq A$, al ideal $\mathfrak{d}_{B/A}$ de A generado por todos los elementos discriminantes $\Delta_B(L/K)$, donde B recorre bases de L/K con elementos en B.

Teorema 6.74: En la situación 6.66, se satisface que

$$\mathfrak{d}_{B/A} = \mathfrak{N}_{L/K}(\mathfrak{D}_{B/A}).$$

Y como consecuencia, obtenemos los siguientes corolarios:

Corolario 6.74.1: En la situación 6.66, se cumple que $\mathfrak{d}_{C/A} = \mathfrak{d}_{B/A}^{[F:L]}\, \mathfrak{N}_{L/K}(\mathfrak{d}_{F/L})$.

Corolario 6.74.2: En la situación 6.66, se cumple que

$$\mathfrak{d}_{B/A} = \prod_{\mathfrak{P}\in \operatorname{Spec} B} \mathfrak{d}_{\mathfrak{P}},$$

donde $\mathfrak{d}_{\mathfrak{P}} := \mathfrak{d}_{\widehat{B_{\mathfrak{Q}}}/\widehat{A_{\mathfrak{p}}}} \cap A$.

Corolario 6.74.3: En la situación 6.66, un primo $\mathfrak{p} \in \operatorname{Spec} A$ se ramifica en B syss $\mathfrak{p} \mid \mathfrak{d}_{B/A}$.

Definición 6.75: En la situación 6.66 se dice que la extensión de anillos $B \supseteq A$ es ***no ramificada*** si todos los primos $\mathfrak{p} \in \operatorname{Spec} A$ no se ramifican en B.

Corolario 6.75.1: En la situación 6.66, la extensión B/A es no ramificada syss $\mathfrak{d}_{B/A} = A$.

Notas históricas

La definición de *lugar* fue originalmente dada por Ostrowski. Uno puede dotar a los lugares de una topología (similar a la que uno puede dar al espectro de un anillo) lo que resulta en un objeto llamado *superficie de Zariski-Riemann*.

Los cuerpos globales son un objeto curioso en cuanto que históricamente la clasificación precede a la axiomatización. Ésta última fue originalmente anunciada el 23 de abril de 1943 en un congreso de la Sociedad Matemática Estadounidense por Emil Artin, y más tarde publicado por Artin y Whaples [**67**] (1945). Se le atribuye a Artin el haber promulgado el paralelo entre la aritmética de los cuerpos numéricos con los cuerpos del tipo $\mathbb{F}_{p^n}(t)$; aunque éstas observaciones heurísticas ya fueron sugeridas originalmente por Dedekind y Gauss.

7

Fracciones continuas

Ya habíamos visto en el primer capítulo la idea de la representación de números por bases, pero ésto tiene un par de problemas: El primero es que elegir algo como el número 10 es considerablemente arbitrario, podríamos haber elegido 2 ó cualquier otro en éste sentido. El segundo problema es que, como vimos, las representaciones no son únicas, pues $0.\overline{9} = 1$, y ésto aplica para cualquier base empleando el último dígito, por ejemplo, en base 5 se cumple que $(0.\overline{4})_5 = 1$ y así, por ende, podríamos sospechar que, si en lugar de emplear una base finita utilizaramos una «base infinita», dado que no hay un último dígito el problema se vería resuelto.

7.1 Introducción

Definición 7.1 – *Fracción continua*: Dadas dos sucesiones $(a_n)_{n=0}$, $(b_n)_{n=1}^{\infty} \in \mathbb{C}$ se define la siguiente sucesión $(c_n)_{n=0}^{\infty} \in \mathbb{C}$:

$$c_0 := a_0, \quad c_1 := a_0 + \frac{b_1}{a_1}, \quad c_2 := a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2}}, \ \cdots$$

a la sucesión $(c_n)_{n\in\mathbb{N}}$ se le dicen ***aproximantes***.[a] También añadimos

un número ∞ (sin signo) que satisface lo siguiente:

$$\frac{z}{0} = \infty, \qquad \frac{z}{\infty} = 0, \qquad a \pm \infty = \infty$$

Finalmente, si c_n converge a un límite L se admiten las siguientes notaciones:

$$L = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}} = a_0 + \frac{b_1}{a_1} + \frac{b_2}{a_2} + \cdots = a_0 + \operatorname*{\mathrm{K}}_{n=1}^{\infty} \frac{b_n}{a_n}$$

La última es notación de Gauss y favoreceremos ésta.

[a] Khinchin sugiere los términos *convergentes* y *aproximantes*, preferimos el segundo para evitar confusiones, aunque otros autores en español tienden a optar por el primero.

Las notaciones están hechas para abreviar espacio, pero no dicen mucho sobre la sucesión real, pues notemos que a pesar de su parecido con la suma, aquí el orden sí importa y deben hacerse desde derecha a izquierda, por ejemplo:

$$\begin{aligned} \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{5}\right) &= \frac{1}{2} + \frac{1}{3 + \frac{1}{5}} \\ &= \frac{1}{2} + \frac{5}{16} = \frac{1}{2 + \frac{5}{16}} = \frac{16}{37} \end{aligned}$$

mientras que

$$\begin{aligned} \left(\frac{1}{2} + \frac{1}{3}\right) + \frac{1}{5} &= \frac{1}{2 + \frac{1}{3}} + \frac{1}{5} \\ &= \frac{3}{7} + \frac{1}{5} = \frac{3}{7 + \frac{1}{5}} = \frac{15}{36}. \end{aligned}$$

Teorema 7.2: Dadas las sucesiones $(a_n)_{n=0}^{\infty}, (b_n)_{n=1}^{\infty}$, entonces sus aproximantes $(c_n)_{n=0}^{\infty}$ se pueden calcular mediante la fórmula $c_n = p_n/q_n$, donde éstos se calcular recursivamente por

$$\begin{aligned} p_{-1} = 1, \quad p_0 = a_0, \qquad & q_{-1} = 0, \quad q_0 = 1 \\ p_n = a_n p_{n-1} + b_n p_{n-2}, \qquad & q_n = a_n q_{n-1} + b_n q_{n-2} \end{aligned}$$

Demostración: La demostración es por inducción:

$$c_0 = a_0 = \frac{a_0}{1}$$

Y suponiendo que aplica para toda sucesión entonces se tiene que

$$\begin{aligned} c_{n+1} &= a_0 + \frac{b_1}{a_1} + \cdots + \frac{b_n}{a_n} + \frac{b_{n+1}}{a_{n+1}} \\ &= a_0 + \frac{b_1}{a_1} + \cdots + \frac{b_n}{a_n + \frac{b_{n+1}}{a_{n+1}}} \\ &= a_0 + \frac{b_1}{a_1} + \cdots + \frac{b_n a_{n+1}}{a_n a_{n+1} + b_{n+1}} = \frac{p_{n+1}}{q_{n+1}} = \frac{p'_n}{q'_n}. \end{aligned}$$

donde p'_n, q'_n representan los valores dados por las nuevas sucesiones en donde el último término está cambiado. Por inducción se tiene que

$$\begin{aligned} p'_n &= a'_n p_{n-1} + b'_n p_{n-2} = (a_n a_{n+1} + b_{n+1}) p_{n-1} + b_n a_{n+1} p_{n-2} \\ &= (a_n p_{n-1} + b_n p_{n-2}) a_{n+1} - b_n p_{n-2} a_{n+1} + b_{n+1} p_{n-1} + b_n a_{n+1} p_{n-2} \\ &= a_{n+1} p_n + b_{n+1} p_{n-1} = p_{n+1}. \end{aligned}$$

y reemplazando las p's por q's nos queda la misma igualdad para q_{n+1}. □

Teorema 7.3: Dadas las sucesiones $(a_n)_{n=0}^{\infty}, (b_n)_{n=1}^{\infty}$ y la sucesión $(r_n)_{n=0}^{\infty} \in \mathbb{C}_{\neq 0}$ con $r_0 = 1$, entonces

$$a_0 + \mathop{\mathrm{K}}_{n=1}^{N} \frac{b_n}{a_n} = r_0 a_0 + \mathop{\mathrm{K}}_{n=1}^{N} \frac{r_{n-1} r_n b_n}{r_n a_n}.$$

de modo que una converge syss la otra lo hace y comparten límite.

Pista: Basta probar por inducción que sus aproximantes son de la forma $c_n = r_n p_n / r_n q_n$. □

Teorema 7.4 – *Fracción continua de Euler*: Sea $(t_n)_{n=0}^{\infty} \in \mathbb{C}_{\neq 0}$, entonces

$$\sum_{n=0}^{N} t_0 \cdots t_n = \frac{t_0}{1} + \frac{-t_1}{1+t_1} + \cdots + \frac{-t_n}{1+t_n},$$

de modo que una converge syss la otra lo hace y comparten límite. Más

aún se cumple que

$$1+\sum_{n=0}^{N} t_0\cdots t_n = \frac{1}{1}+\frac{-t_0}{1+t_0}+\frac{-t_1}{1+t_1}+\cdots = \frac{1}{1}+\mathop{\mathrm{K}}_{n=0}^{N}\frac{-t_n}{1+t_n}.$$

Demostración: Vamos a probarlo por inducción sobre N. El caso $N=0$ es trivial y

$$t_0+t_0t_1 = t_0(1+t_1) = \frac{t_0}{\frac{1+t_1-t_1}{1+t_1}} = \frac{t_0}{1+\frac{-t_1}{1+t_1}} = \frac{t_0}{1}+\frac{-t_1}{1+t_1}.$$

Si asumimos que se cumple para N, notemos que

$$\sum_{n=0}^{N+1} t_0\cdots t_n = \sum_{n=0}^{N-1} t_0\cdots t_n + t_0\cdots t_N(1+t_{N+1}).$$

Si $t_{N+1}=-1$, entonces $a_{N+1}=1+t_{N+1}=0$ y

$$c_{N+1} = \frac{a_{N+1}p_N+b_{N+1}p_{N-1}}{a_{N+1}q_N+b_{N+1}q_{N-1}} = \frac{p_{N-1}}{q_{N-1}} = c_{N-1}.$$

Si $t_{N+1}\neq -1$, entonces $a_{N+1}\neq 0$ y aplicamos la hipótesis de inducción a la sucesión $t_0,\ldots,t_{N-1},t'_N$, donde $t'_N = t_N(1+t_{N+1})$ y notamos que

$$\sum_{n=0}^{N+1} t_0\cdots t_n = \frac{t_0}{1}+\frac{-t_1}{1+t_1}+\cdots+\frac{-t'_N}{1+t'_N}$$

donde

$$\begin{aligned}\frac{-t'_N}{1+t'_N} &= \frac{-t_N(1+t_{N+1})}{1+t_N(1+t_{N+1})}\\ &= \frac{-t_N}{1+t_N+\frac{1}{1+t_{N+1}}-1} = \frac{-t_N}{1+t_N}+\frac{-t_{N+1}}{1+t_{N+1}}.\end{aligned}$$

Para la segunda identidad basta notar que

$$1+\frac{t_0}{1+F} = \frac{1+F+t_0}{1+F} = \frac{1}{1-\frac{t_0}{1+t_0+F}} = \frac{1}{1}+\frac{-t_0}{1+t_0+F}$$

que aplica para todo F (incluyendo $F=-1$ o $F=\infty$), así que basta reemplazar por el resto de términos para obtener la identidad buscada. □

Ejemplo $\exp(x) = \dfrac{1}{1} + \dfrac{-x/1}{1+x/1} + \dfrac{-x/2}{1+x/2} + \dfrac{-x/3}{1+x/3} + \cdots$. Nótese que ya habíamos visto que

$$\exp(x) = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}$$

dónde cada término en la sumatoria puede verse como la multiplicación de x/n, de modo que por la fracción continua de Euler se cumple que

$$\exp(x) = \frac{1}{1 + \underset{n=1}{\overset{\infty}{\mathrm{K}}} \dfrac{-x/n}{1+x/n}}, \qquad \forall x \in \mathbb{C}_{\neq 0}$$

También podemos emplear $-x$ para obtener y elevar ambos lados a (-1) para tener que:

$$\exp(x) = 1 + \underset{n=1}{\overset{\infty}{\mathrm{K}}} \frac{x/n}{1-x/n}$$

Luego podemos ajustar según el teorema por $r_n = n$:

$$\exp(x) = 1 + \frac{x}{1-x} + \frac{x}{2-x} + \frac{2x}{3-x} + \frac{3x}{4-x} + \cdots$$

7.2 Fracciones continuas simples

Definición 7.5: Dada una sucesión $(a_n)_{n=0}$ posiblemente finita (por ello obviamos el punto de final) de números naturales no nulos, donde a_0 se permite como cualquier entero (incluyendo al cero) se denota

$$[a_0; a_1, a_2, \dots] = a_0 + \underset{n=1}{\overset{}{\mathrm{K}}} \frac{1}{a_n}$$

lo que se considera una ***fracción continua simple***. Claramente el punto-coma sirve para denotar una idea de parte entera.

De momento las fracciones continuas simples son sólo un subconjunto de las generalizadas, pero veremos que son mucho más.

En primer lugar una consecuencia del primer teorema que vimos:

Proposición 7.6: Sea $[a_0; a_1, a_2, \dots]$, entonces sus aproximantes $(c_n)_{n=0}$ satisfacen que $c_n = p_n/q_n$ donde p_n, q_n son enteros determinados recursivamente por:

$$p_{-1} = 1, \quad p_0 = a_0, \qquad q_{-1} = 0, \quad q_0 = 1$$

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}$$

Proposición 7.7: Si $(c_n)_{n=0}$ son los aproximantes de $[a_0; a_1, a_2, \dots]$ y $c_n = p_n/q_n$, entonces se comprueba que $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$, o equivalentemente,

$$c_n - c_{n+1} = \frac{(-1)^{n+1}}{q_n q_{n+1}}.$$

Demostración: Naturalmente es por inducción, en el caso $n = 0$ se reduce a ver que

$$p_0 q_1 - p_1 q_0 = a_0 a_1 - (a_1 a_0 + 1) = -1.$$

Y el caso $n + 1$ se da pues

$$\begin{aligned} p_{n+1}q_{n+2} - p_{n+2}q_{n+1} &= p_{n+1}(a_{n+2}q_{n+1} - q_n) + (a_{n+2}p_{n+1} - p_n)q_{n+1} \\ &= p_{n+1}q_n - p_n q_{n+1} = (-1)(-1)^{n+1}. \end{aligned}$$ □

Corolario 7.7.1: Toda fracción continua simple infinita converge.

Proposición 7.8: Todo número real x admite una representación como fracción continua simple:

$$x = [a_0; a_1, a_2, a_3, \dots]$$

donde $t_0 := x$ y $a_0 = \lfloor x \rfloor$ y el resto de dígitos se construye por recursión:

$$t_{n+1} := \frac{1}{t_n - a_n}, \quad a_{n+1} = \lfloor t_{n+1} \rfloor$$

donde se subentiende que la fracción termina en a_n si $a_n = t_n$.

Los términos t_n se ven como desplazar la fracción continua:

$$t_0 = [a_0; a_1, a_2, \dots], \quad t_1 := [a_1; a_2, a_3, \dots], \quad t_2 = [a_2; a_3, a_4 \dots], \quad \dots$$

Lema 7.9: Dada una fracción continua simple cuyos aproximantes son $(p_n/q_n)_{n=0}^{\infty}$, entonces la sucesión q_n es estrictamente creciente.

Teorema 7.10: Un número es irracional syss tiene una fracción continua simple infinita asociada.

Demostración: $\Longrightarrow$. Por contrarrecíproca queda que si un número tiene una fracción continua simple finita entonces es racional lo que es trivial.

$\Longleftarrow$. Sea $\alpha := [a_0; a_1, a_2, \dots]$ y supongamos por contradicción que converge a un número racional p/q (siendo p, q coprimos). Si $c_n = (p_n/q_n) \to p/q$ entonces por el lema existe N tal que para todo $n \geq N$ se cumple que $q_n > q$. Luego se cumple que

$$|\alpha - c_n| \leq |c_{n+1} - c_n| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n q}$$
$$|\alpha - c_n| = \left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \frac{|pq_n - p_n q|}{q_n q} \geq \frac{1}{q_n q}.$$

donde $|pq_n - p_n q| \geq 1$ pues $c_n \neq \alpha$. □

Teorema 7.11: Un número irracional posee una única fracción continua simple asociada.

Demostración: Sean $[a_0; a_1, \dots] = [b_0; b_1, \dots] =: x$ dos expansiones en fracción continua simple de un mismo número irracional x, luego x no es entero y de hecho $a_0 < x < a_0 + 1$, luego

$$a_0 = \lfloor [a_0; a_1, a_2, \dots] \rfloor = \lfloor [b_0; b_1, b_2, \dots] \rfloor = b_0,$$

y luego notamos que $\frac{1}{x - a_0} = [a_1; a_2, \dots] = [b_1; b_2, \dots]$ y empleamos el mismo truco inductivamente, notando que nunca puede ser entero porque x es irracional, para concluir que $a_n = b_n$ para todo n. □

De éste modo podemos hablar de *los* aproximantes de una fracción continua simple. Ésto será útil pues claramente los aproximantes nos otorgan buenas aproximaciones racionales para números irracionales, pero el recíproco también es cierto (cfr. teorema 7.24).

Uno puede mejorar el teorema anterior un poco. En expansión base $b \geq 2$, veíamos que un número tenía una expansión periódica asociada si era racional; vamos a responder el qué signfica tener expansión periódica, pero veamos un par de lemas primero.

Lema 7.12: Sea α un real irracional con $\alpha = [a_0; a_1, a_2, \dots]$ y sean t_n como en la proposición 7.8. Entonces, para todo n se tiene lo siguiente:

$$\alpha = t_0, \qquad \alpha = \frac{t_1 a_0 + 1}{t_1}, \qquad \alpha = \frac{t_n p_{n-1} + p_{n-2}}{t_n q_{n-1} + q_{n-2}}.$$

Pista: Aplique inducción. □

Definición 7.13: Una fracción continua simple $\alpha = [a_0; a_1, a_2, \dots]$ se dice ***eventualmente periódica*** si existen $n_0 \in \mathbb{N}$ y $m > 0$ tal que $a_{n+m} = a_n$ para todo $n \geq n_0$. Si $n_0 = 0$, decimos que (la fracción continua simple de) α es ***puramente periódica***.

Teorema 7.14: Para un número irracional α son equivalentes:

1. Su fracción continua simple es eventualmente periódica.
2. α es algebraico cuadrático, vale decir, es raíz de un polinomio cuadrático.

Demostración: $1 \implies 2$. Sea

$$\alpha = [b_0; b_1, \dots, b_m, a_1, a_2, \dots, a_n, a_1, \dots].$$

Definiendo $\beta := [a_1, a_2, \dots]$ nótese que $t_n = \beta$ por hipótesis, de modo que el lema anterior nos da que

$$\beta = \frac{\beta p_{n-1} + p_{n-2}}{\beta q_{n-1} + q_{n-2}} \iff q_{n-1}\beta^2 + (q_{n-2} - p_{n-1})\beta - p_{n-2} = 0,$$

donde cada $p_i, q_i \in \mathbb{Z}$ son aproximantes, lo que prueba que β es cuadrático.

Realizando un procedimiento similar podemos despejar a α como $\alpha = f(\beta)/g(\beta)$ donde los polinomios son lineales, de modo que $\alpha \in \mathbb{Q}(\beta)$ y, siendo irracional, necesariamente es cuadrático también.

$2 \implies 1$. Sea α con polinomio minimal $ax^2 + bx + c = a(x - \alpha)(x - \beta) \in \mathbb{Z}[x]$. Defínase

$$g(x, y) := ax^2 + bxy + cy^2 = (x, y) \cdot \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

En notación de la proposición 7.8 con $\kappa := (q_n t_{n+1} - q_{n-1})^{-1} \neq 0$, tenemos que

$$\begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \kappa \cdot \begin{bmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{bmatrix} \cdot \begin{pmatrix} t_{n+1} \\ 1 \end{pmatrix} =: \kappa \cdot M \cdot \begin{pmatrix} t_{n+1} \\ 1 \end{pmatrix}.$$

Luego si definimos la siguiente matriz

$$\begin{bmatrix} A_n & B_n/2 \\ B_n/2 & C_n \end{bmatrix} := M^t \cdot \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \cdot M,$$

vemos que su determinante es el mismo que del polinomio $f(x)$, pues $|\det M| = 1$ por la proposición 7.7.

Además:

$$A_n t_{n+1}^2 + B_n t_{n+1}^2 + C_n = (t_{n+1}, 1) \cdot \begin{bmatrix} A_n & B_n/2 \\ B_n/2 & C_n \end{bmatrix} \cdot \begin{pmatrix} t_{n+1} \\ 1 \end{pmatrix}$$
$$= \kappa^2(\alpha, 1) \cdot \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ 1 \end{pmatrix} = \kappa^2 g(\alpha, 1) = 0.$$

Luego $g_n(x) := A_n x^2 + B_n x + C_n$ tiene una raíz t_{n+1}. Ahora bien, $A_n = f(p_n, q_n)$ (¿por qué?) y, por lo tanto, $C_n = A_{n-1}$. Nótese que

$$\left|\beta - \frac{p_n}{q_n}\right| \leq |\beta - \alpha| + \left|\alpha - \frac{p_n}{q_n}\right| \leq |\beta - \alpha| + \frac{1}{q_n^2} \leq |\beta - \alpha| + 1,$$

de modo que para todo $n \geq 1$ se cumple que

$$|A_n| = |f(p_n, q_n)| = a q_n^2 \left|\alpha - \frac{p_n}{q_n}\right| \left|\beta - \frac{p_n}{q_n}\right| \leq a(|\beta - \alpha| + 1)a + \sqrt{d},$$

donde $a|\beta - \alpha| = \sqrt{d}$ por la fórmula cuadrática.

Como los A_n's y C_n's son enteros esto nos a lo sumo finitas soluciones, y como $B_n^2 = d + 4A_nC_n$ esto nos da finitas posibilidades para B_n también. Así, hay finitos polinomios g_n's, cada uno con dos raíces, por lo tanto, hay alguna raíz que se repite infinitas veces, digamos $t_m = t_n$ con $m < n$. Pero la expansión de $t_m = [a_m; a_{m+1}, \ldots, a_{n-1}, t_n]$, así que la fracción continua simple de t_m es periódica. □

Proposición 7.15: Sea $\alpha \in \mathbb{Q}(\sqrt{d})$ un número real cuadrático y denotemos por $\overline{()}$ la conjugación. Entonces la fracción continua simple de α es puramente periódica syss $\alpha > 1 > -\overline{\alpha} > 0$.

Demostración: $\Longrightarrow$. Escribamos $\alpha = [\overline{a_0; a_1, \ldots, a_m}]$, donde la barra denota que $a_{m+1} = a_0$ y así (¡no confundir con conjugación!). Por definición de fracción continua simple tenemos que $\lfloor \alpha \rfloor = a_0 = a_{m+1} > 0$, por lo que $\alpha > 1$. Empleando el lema obtenemos que

$$\alpha = \frac{\alpha p_{m-1} + p_{m-2}}{\alpha q_{m-1} + q_{m-2}},$$

de modo que definiendo $f(x) := q_{m-1}x^2 + (q_{m-2} - p_{m-1})x - p_{m-2}$, tenemos que $f(\alpha) = 0 = f(\overline{\alpha})$. Basta notar que $f(0) = -p_{m-2} < 0$ y que

$$f(-1) = (q_{m-1} - q_{m-2}) + (p_{m-1} - p_{m-2}) > 0,$$

de modo que, por el teorema del valor intermedio, $\overline{\alpha} \in (-1, 0)$ como se quería probar.

$\Longleftarrow$. Denotemos por $\beta := -\overline{\alpha}$, por α_n el real tal que $\alpha = [a_0; \dots, a_{n-1}, \alpha]$ y β_n lo mismo con β. Nótese que $\alpha_n > a_n \geq 1$ y veamos que $0 < \beta_n < 1$ por inducción: el caso base $n = 0$ es obvio y tomando conjugados vemos que

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} \iff -\beta_n = a_n - \frac{1}{\beta_{n+1}}.$$

Luego, por hipótesis inductiva, a_n es un entero en $(1/\beta_{n+1} - 1, 1/\beta_{n+1})$, luego $a_n = \lfloor 1/\beta_{n+1} \rfloor$, de modo que $1/\beta_{n+1} > 1$ como se quería ver.

Ahora, como la fracción continua de α es eventualmente periódica, tenemos que $\alpha_n = \alpha_m$ para algunos $n < m$, donde elegimos $n > 0$ minimal. Tomando conjugados tenemos que $\beta_n = \beta_m$ y, por tanto, $a_{n-1} = \lfloor 1/\beta_n \rfloor = \lfloor 1/\beta_m \rfloor = a_{m-1}$, de lo que se sigue que $\alpha_{n-1} = \alpha_{m-1}$ lo que contradice la minimalidad de n. Es decir, necesariamente $n = 0$. □

Un teorema de D. N. Lehmer **[94]** dice que además, la fracción es capicúa (i.e., se lee igual al derecho que al revés)

Expansión de e. Veamos que e es irracional deduciendo que su fracción continua simple es

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots] = [1; 0, 1, 1, 2, 1, 1, 4, 1, \dots];$$

éste es el método descrito por Cohn **[74].** Sabemos, por el teorema principal, que el patrón en las aproximantes de la fracción continua de la derecha es

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2}, & q_{3n} &= q_{3n-1} + q_{3n-2} \\ p_{3n+1} &= 2np_{3n} + p_{3n-1}, & q_{3n+1} &= 2nq_{3n} + q_{3n-1} \\ p_{3n+2} &= p_{3n+1} + p_{3n}, & q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Definamos las siguientes integrales:

$$\begin{aligned} A_n &:= \int_0^1 e^x \frac{x^n(x-1)^n}{n!}\,\mathrm{d}x \\ B_n &:= \int_0^1 e^x \frac{x^{n+1}(x-1)^n}{n!}\,\mathrm{d}x \\ C_n &:= \int_0^1 e^x \frac{x^n(x-1)^{n+1}}{n!}\,\mathrm{d}x \end{aligned}$$

Lema 7.16: Para todo $n \geq 0$ se cumple que

$$A_n = q_{3n}e - p_{3n},\ B_n = p_{3n+1} - q_{3n+1}e,\ C_n = p_{3n+2} - q_{3n+2}e.$$

DEMOSTRACIÓN: Aplicaremos inducción sobre n: Caso $n = 0$: Notemos que $p_0/q_0 = 1/1, p_1/q_1 = 1/0$ y que $p_2/q_2 = 2/1$ así que para aplicar inducción basta probar que

$$A_0 = \int_0^1 e^x\,\mathrm{d}x = e-1, \quad B_0 = \int_0^1 xe^x\,\mathrm{d}x = [xe^x]_0^1 - \int_0^1 e^x\,\mathrm{d}x = e-(e-1) = 1.$$

y el caso restante saldrá de un caso probado más abajo. Caso $n+1$: Comenzaremos por ver un par de identidades

$$\begin{aligned} B_n &= \int_0^1 x^{n+1}e^x \frac{(x-1)^n}{n!}\,\mathrm{d}x \\ &= \left[x^{n+1}e^x\frac{(x-1)^{n+1}}{(n+1)!}\right]_0^1 - \int_0^1 \frac{(x-1)^{n+1}}{(n+1)!}((n+1)x^ne^x + x^{n+1}e^x)\,\mathrm{d}x \\ &= -\int_0^1 \frac{e^x x^n(x-1)^{n+1}}{n!}\,\mathrm{d}x - \int_0^1 \frac{e^x x^{n+1}(x-1)^{n+1}}{(n+1)!}\,\mathrm{d}x = -C_n - A_{n+1}. \end{aligned}$$

$$B_n + C_n = \int_0^1 \frac{e^x x^n(x-1)^n}{n!}(2x-1)\,\mathrm{d}x = 2B_n - A_n,$$

las cuales se reordenan a $A_{n+1} = -B_n - C_n$ y $C_n = B_n - A_n$ (nótese que de la última se deduce que $C_0 = B_0 - A_0 = 2-e$). La relación $B_n = -2nA_n + C_{n-1}$ sale de que

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(e^x\frac{x^n(x-1)^{n+1}}{n!}\right) = e^x\frac{x^n(x-1)^{n+1}}{n!} + e^x\frac{x^{n-1}(x-1)^{n+1}}{(n-1)!} + e^x\frac{(n+1)x^n(x-1)^n}{n!}$$

Nótese que al término en azul podemos factorizar un término $(x-1)$ para obtener

$$e^x\frac{x^{n-1}(x-1)^{n+1}}{(n-1)!} = -e^x\frac{x^{n-1}(x-1)^n}{(n-1)!} + e^x\frac{nx^n(x-1)^n}{n!}$$

Lo mismo se puede hacer en el término en rojo lo que da

$$e^x\frac{x^n(x-1)^{n+1}}{n!} = e^x\frac{x^{n+1}(x-1)^n}{n!} - e^x\frac{x^n(x-1)^n}{n!}$$

Reemplazando todo en la ecuación original nos queda

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(e^x\frac{x^n(x-1)^{n+1}}{n!}\right) = e^x\frac{x^{n+1}(x-1)^n}{n!} + (2n)e^x\frac{x^n(x-1)^n}{n!} - e^x\frac{x^{n-1}(x-1)^n}{(n-1)!}$$

Integrando a ambos lados nos queda la relación restante. Con ellas se puede deducir el caso inductivo. □

Teorema 7.17: $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \dots]$ Se cumple que

$$e = [1; 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots] = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots].$$

En consecuencia, e es irracional.

Pista: Basta comprobar que $A_n, B_n, C_n \to 0$. □

La proposición 7.19 da una demostración más sencilla de la irracionalidad de e, pero nuestro teorema da otra clase de información interesante. Una consecuencia es que e tampoco es algebraico cuadrático, pues su fracción continua simple no es periódica.

7.3 Aproximaciones diofánticas y la ecuación de Pell

Teorema 7.18 – *Teorema de aproximación de Dirichlet*: Sea α un número irracional y $M > 0$. Entonces existen $u, v \in \mathbb{Z}$ con $0 < v \leq M$ tales que

$$\left|\alpha - \frac{u}{v}\right| < \frac{1}{vM} \leq \frac{1}{v^2}.$$

Demostración: Considere los $M + 1$ números $\{0 \cdot \alpha, 1 \cdot \alpha, \dots, M\alpha\}$, y la aplicación $f(x) := x - \lfloor x \rfloor$ que otorga la parte fraccionaria o decimal de los números, de modo que $f(j\alpha) \in [0, 1)$. Ahora particionemos el conjunto $[0, 1)$ en M subintervalos:

$$\left[\tfrac{0}{M}, \tfrac{1}{M}\right), \quad \left[\tfrac{1}{M}, \tfrac{2}{M}\right), \quad \cdots, \quad \left[\tfrac{M-1}{M}, \tfrac{M}{M}\right).$$

Por el principio del palomar, se cumple que existen $0 \leq i < j \leq M$ distintos con $f(i\alpha), f(j\alpha)$ en el mismo subintervalo. Luego

$$\frac{1}{M} > |f(j\alpha) - f(i\alpha)| = |(j - i)\alpha - \lfloor j\alpha \rfloor + \lfloor i\alpha \rfloor|,$$

definiendo $v := (j - i)$ y $u := \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor$ se verifica el enunciado. □

Nótese que el teorema anterior no solo nos da la existencia, sino que además deben ser infinitas estas fracciones buenas u/v. En efecto si fijamos una aproximación u/v, entonces definimos $\epsilon := |v\alpha - u| > 0$ y eligiendo M tal

que $1/M < \epsilon$, tenemos que la proxima aproximación u'/v' ha de tener un mayor denominador.

A consecuencia del teorema de Dirichlet podemos redemostrar:

Corolario 7.18.1: Sea $n > 0$ entero tal que -1 es un residuo cuadrático módulo n. Entonces n es suma de dos cuadrados.

Demostración: Sea $r^2 \equiv -1 \pmod{n}$, luego por el teorema de aproximación de Dirichlet existe $v < \sqrt{n} = M$ y $u \in \mathbb{Z}$ tales que

$$\left|-\frac{r}{n} - \frac{u}{v}\right| < \frac{1}{v\sqrt{n}}.$$

Multiplicando por vn vemos que $a := rv + un$ tiene $|a| < \sqrt{n}$. Nótese que $a \equiv rv\ (n)$, de modo que $a^2 + v^2 \equiv r^2v^2 + v^2 \equiv 0\ (n)$ y $0 < a^2 + v^2 < n + n = 2n$, por lo que necesariamente $a^2 + v^2 = n$. □

A consecuencia tenemos el siguiente criterio sencillo de irracionalidad:

Corolario 7.18.2: Sea α un número real. Entonces α es irracional syss para todo $\epsilon > 0$ existen $u/v \in \mathbb{Q}$ tales que $0 < |\alpha v - u| < \epsilon$.

Demostración: $\Longleftarrow$. Por contrarrecíproca, si $\alpha = a/b$ es racional, entonces $va - ub$ es siempre un entero y por tanto $|va - ub| \geq 1 > 0$. Luego

$$0 < |v\alpha - u| \geq \frac{1}{b}.$$

$\Longrightarrow$. Basta elegir $1/M < \epsilon$ en el teorema de aproximación de Dirichlet. □

Empleando esto, demos ejemplos de números irracionales:

Proposición 7.19: Sea $(g_n)_n$ una sucesión creciente y no acotada de números naturales con $g_1 \geq 1$, y sea $(z_n)_n$ una sucesión de 0s y 1s tal que $z_n = 1$ para infinitos n's. Entonces el número

$$\alpha := \sum_{n=1}^{\infty} \frac{z_n}{g_1 g_2 \cdots g_n} = \frac{z_1}{g_1} + \frac{z_2}{g_1 g_2} + \frac{z_3}{g_1 g_2 g_3} + \cdots$$

es irracional. En particular, $e = \sum_{n=1}^{\infty} \frac{1}{n!}$ es irracional.

Demostración: Definamos los enteros

$$G_N := g_1 g_2 \cdots g_N, \qquad F_N := G_N \sum_{n=1}^{N} \frac{z_n}{G_n}.$$

Entonces

$$\begin{aligned} 0 < \left|\alpha - \frac{F_N}{G_N}\right| &= \frac{1}{G_N} \sum_{n=N+1}^{\infty} \frac{z_n}{g_{N+1} \cdots g_n} \\ &\leq \frac{1}{G_N}\left(\frac{1}{g_{N+1}} + \frac{1}{g_{N+1}^2} + \cdots\right) = \frac{1}{G_N(g_{N+1}-1)}. \end{aligned} \tag{7.1}$$

Como $g_{N+1} \to \infty$, entonces para todo ϵ eventualmente tendremos que $g_{N+1} - 1 > 1/\epsilon$ y aplicamos el corolario anterior. □

Hay varias modificaciones al teorema anterior e incluiremos algunas:

Proposición 7.20: Sean $\alpha_1, \ldots, \alpha_r$ números reales y $M > 0$ un entero. Entonces existen $u_1, \ldots, u_r \in \mathbb{Z}$ con $0 < v \leq M^r$ tales que

$$\forall 1 \leq j \leq r \quad \left|\alpha_j - \frac{u_j}{v}\right| < \frac{1}{vM^r} \leq \frac{1}{v^{r+1}}.$$

Intercambiando el rol del numerador y denominador, Dirichlet probó:

Proposición 7.21: Sean $\alpha_1, \ldots, \alpha_r$ números reales y $M > 0$ un entero. Entonces existen $u \in \mathbb{Z}$ y $v_1, \ldots, v_r \in \mathbb{Z}$ no todos nulos donde cada $|v_j| \leq M^{1/r}$ tales que

$$\left|\sum_{j=1}^{r} \alpha_j v_j - u\right| < \frac{1}{M}.$$

Finalmente, Kronecker dio una generalización simultánea:

Teorema 7.22 (de aproximación de Dirichlet multidimensional): Sean $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{m,r}$ números reales donde $m, r > 0$ son enteros fijos, y sean $M > 0$ otro entero. Entonces existen m enteros $u_1, \ldots, u_m$ y r enteros $v_1, \ldots, v_r$ (no todos nulos) con cada $|v_j| < M^{m/r}$ tales que

$$\forall 1 \leq j \leq m \quad \left|\sum_{k=1}^{r} \alpha_{jk} v_k - u_j\right| < \frac{1}{M}.$$

Demostración: La m-tupla

$$\left(\sum_{k=1}^{r}\alpha_{1k}v_k - \left\lfloor\sum_{k=1}^{r}\alpha_{1k}v_k\right\rfloor, \ldots, \sum_{k=1}^{r}\alpha_{mk}v_k - \left\lfloor\sum_{k=m}^{r}\alpha_{1k}v_k\right\rfloor\right)$$

yace en el cubo $[0,1)^m$ que se descompone en M^m subcubos.

Para poder aplicar el principio del palomar deben haber más r-tuplas $(v_1,\ldots,v_r)$ que subcubos. Si decidimos que $0 \leq v_j \leq P$, entonces hay $(P+1)^r$ tuplas y queremos que $(P+1)^r > M^m$ o equivalentemente, $P+1 > M^{m/r}$, por lo que $P := \lfloor M^{m/r}\rfloor$ basta. Finalmente, concluimos como en el teorema original de Dirichlet. □

El teorema de aproximación de Dirichlet nos dice que podemos aproximar bien a los números irracionales, pero no nos otorga, de buenas a primeras, un método eficiente para encontrar buenas aproximaciones.

De momento ya sabemos que la expansión en fracción continua simple de un irracional α es única, lo que nos permite hablar sin ambigüedad de *los* aproximantes de α. Podemos caracterizarles parcialmente por lo siguiente:

Teorema 7.23 – *Criterio de Legendre*: Sea $\alpha \in \mathbb{R}$ un número irracional y sea $p, q \in \mathbb{Z}$ enteros tales que

$$\alpha - \frac{p}{q} = \frac{\theta}{q^2}, \qquad |\theta| < 1.$$

Sean $p/q = [a_0; a_1, \ldots, a_n]$ y supongamos que $\operatorname{sign}\theta = (-1)^n$. Entonces p/q es un aproximante de α syss

$$|\theta| \leq \frac{q_n}{q_n + q_{n-1}},$$

(donde q_{n-1} es aproximante p/q.)

Demostración: Definamos β tal que

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}},$$

de modo que

$$\frac{\theta}{q_n^2} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\beta q_n + q_{n-1})},$$

por lo que

$$|\theta| = \frac{q_n}{\beta q_n + q_{n-1}}.$$

Despejando tenemos que $\beta = (q_n - |\theta| q_{n-1})/|\theta| q_{n-1}$ y como $0 < |\theta| < 1$ vemos que $\beta > 0$.

Si $\beta \geq 1$, entonces $\alpha = [a_0; a_1, \ldots, a_n, \beta]$ lo que prueba que p_n/q_n son aproximantes. Si $0 < \beta < 1$, entonces $\lfloor a_n + 1/\beta \rfloor =: a_n + c$ con $c > 0$, de modo que $\alpha = [a_0; a_1, \ldots, a_n + c, \ldots]$, por lo que $[a_0; a_1, \ldots, a_n]$ no es un aproximante de α. Esto prueba la equivalencia del enunciado. □

Teorema 7.24: Sean $\alpha \in \mathbb{R}$ un número irracional.

1. Sean $(c_n)_{n\in\mathbb{N}}$ los aproximantes de α. Entonces para todo n (al menos) uno de los dos aproximantes $p/q \in \{c_n, c_{n+1}\}$ satisface que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{7.2}$$

   En consecuencia, hay infinitas aproximaciones racionales que satisfacen la desigualdad (7.2).

2. Sean p, q enteros coprimos que satisfacen (7.2), entonces p/q es un aproximante de α.

Demostración:

1. Por la proposición 7.7, tenemos que si c_n es un aproximante de α, se cumple que $|c_n - c_{n+1}| = 1/q_n q_{n+1}$, pero como α está entre c_n y c_{n+1} concluimos que

$$|\alpha - c_n| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2},$$

   puesto que q_n es una sucesión estrictamente creciente. Ésto se puede mejorar aún más notando que

$$|\alpha - c_n| + |\alpha - c_{n+1}| = |c_n - c_{n+1}| = \frac{1}{q_n q_{n+1}},$$

   y ahora, por la desigualdad media geométrica-media cuadrática (cf. **[2,** Teo. 6.68]) sabemos que $xy < (x^2 + y^2)/2$ si $0 < x < y$, luego se concluye que

$$|\alpha - c_n| + |\alpha - c_{n+1}| = \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}.$$

Luego, al menos alguno de las dos restas, digamos c_n, satisface $|\alpha - c_n| < 1/(2q_n^2)$.

2. Empleando que $q_{n-1} < q_n$ para los aproximantes de una fracción continua, tenemos que

$$\frac{q_n}{q_n + q_{n-1}} > \frac{q}{q+q} = \frac{1}{2}.$$

De modo que podemos aplicar el criterio de Legendre. □

Teorema 7.25 (Hurwitz): Sea α un real irracional y sean $(c_n)_{n\in\mathbb{N}}$ sus aproximantes. Entonces para todo n, uno de los aproximantes $p/q \in \{c_n, c_{n+1}, c_{n+2}\}$ satisface que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

En consecuencia, infinitas fracciones reducidas satisfacen la desigualdad anterior.

Demostración: Sean p_n, q_n los numeradores y denominadores correspondientes de c_n. Con la notación del lema anterior es fácil comprobar que

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha'_{n+1}q_n + q_{n-1})} = \frac{1}{q_n^2(\alpha'_{n+1} + \beta_{n+1})},$$

donde $\beta_{n+1} := q_{n-1}/q_n$. Basta probar que $\alpha'_j + \beta_j > \sqrt{5}$ para algún $j \in \{n, n+1, n+2\}$.

Supongamos que no se satisface para $j \in \{n, n+1\}$. Como $\alpha'_n = a_n + 1/\alpha'_{n+1}$ y

$$\frac{1}{\beta_{n+1}} = \frac{q_n}{q_{n-1}} = \frac{a_n q_{n-1} + q_{n-2}}{q_{n-1}} = a_n + \beta_n,$$

de modo que

$$\frac{1}{\alpha'_{n+1}} + \frac{1}{\beta_{n+1}} = \alpha'_n + \beta_n \leq \sqrt{5}.$$

Luego, concluimos que

$$1 = \frac{1}{\alpha'_{n+1}}\alpha'_{n+1} \leq \left(\sqrt{5} - \frac{1}{\beta_{n+1}}\right)(\sqrt{5} - \beta_{n+1}) = 5 - \sqrt{5}\left(\frac{1}{\beta_{n+1}} + \beta_{n+1}\right) + 1,$$

lo que nos da que $\frac{1}{\beta_{n+1}} + \beta_{n+1} < \sqrt{5}$, donde la desigualdad estricta sale del hecho de que β_{n+1} es racional. Como $\beta_{n+1} < 1$, se deduce de que $\beta_{n+1} > \frac{1}{2}(\sqrt{5} - 1)$.

Análogamente vemos que $\beta_{n+2} > \frac{1}{2}(\sqrt{5}-1)$, por lo que

$$a_{n+1} = \frac{1}{\beta_{n+2}} - \beta_{n+1} < \sqrt{5} - (\beta_{n+2} + \beta_{n+1}) < \sqrt{5} - (\sqrt{5}-1) = 1,$$

lo cual es absurdo. □

La constante en el teorema de Hurwitz es aguda:

Proposición 7.26: Para todo $A > \sqrt{5}$ existe un α real irracional para el que la desigualdad $|\alpha - p/q| < 1/Aq^2$ solo admite finitas soluciones.

Demostración: Elijamos $\alpha := \frac{1}{2}(\sqrt{5}-1)$ y supongamos que

$$\alpha = \frac{p}{q} + \frac{\delta}{q^2}, \qquad |\delta| < \frac{1}{A} < \frac{1}{\sqrt{5}}.$$

Multiplicando por q y reordenando obtenemos

$$\frac{\delta}{q} - \frac{1}{2}\sqrt{5}q = \frac{\delta}{q} - \left(\frac{1}{2}q + p + \frac{\delta}{q}\right) = -\frac{1}{2}q - p.$$

Luego, tomando cuadrados tenemos que

$$\frac{\delta^2}{q^2} - \sqrt{5}\delta = \left(\frac{\delta}{q} - \frac{1}{2}\sqrt{5}q\right)^2 - \frac{5q^2}{4} = pq + p^2 - q^2.$$

Como $|\delta| < 1/\sqrt{5}$ vemos que para q suficientemente grande el lado izquierdo tiene valor absoluto < 1, de modo que $pq + p^2 - q^2 = 0$, o equivalentemente $(2p+q)^2 = 5q^2$ lo cual es absurdo pues $\sqrt{5}$ es irracional. □

§7.3.1 El teorema y los números de Liouville.

Teorema 7.27 (de aproximación de Liouville): Sea $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ un número algebraico de grado d. Entonces existe $C > 0$ tal que toda fracción $u/v \in \mathbb{Q}$ satisface que

$$\left|\alpha - \frac{u}{v}\right| \geq \frac{C}{v^d}.$$

Demostración: Sea $f(x) = c_d x^d + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ el polinomio minimal de α (es decir, los coeficientes son coprimos y el c_d «limpia denominadores»). Entonces $f(x) = (x-\alpha)g(x)$, donde $g(x) \in \mathbb{Q}[x]$. Ahora bien,

la función $|g(x)|$ alcanza un máximo M en el compacto $[\alpha-1, \alpha+1]$ y, por tanto, para toda fracción $u/v \in \mathbb{Q}$ se tiene que

$$|f(u/v)| = \left|\alpha - \frac{u}{v}\right| \cdot |g(u/v)| \leq M \left|\alpha - \frac{u}{v}\right|,$$

y nótese que $v^d|f(u/v)|$ es un entero, de modo que $|f(u/v)| \geq 1/v^d$ pues $f(x)$ no tiene raíces racionales. Así, tomando $C := \text{mín}\{1, 1/M\}$ tenemos el enunciado. □

Corolario 7.27.1: Sea α un irracional algebraico de grado d. Entonces existen a lo más finitas fracciones $u/v \in \mathbb{Q}$ tales que

$$\left|\alpha - \frac{u}{v}\right| < \frac{1}{v^{d+1}}.$$

Demostración: Basta notar que de existir infinitas, el denominador no está acotado y escoger $q > 1/C$, donde C es la constante del teorema anterior. □

Liouville empleó su teorema para dar el primer ejemplo de un número trascendente:

Ejemplo 7.28: El número

$$\lambda := \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0{,}11000100000000000000000001...$$

es trascendente.

En efecto, sea $c_n := \sum_{j=1}^{n} 10^{-j!}$ los cuales satisfacen que $\lim_n c_n = \lambda$. Luego, nótese que, con $v_n := 10^{n!}$, tenemos que $u_n := v_n c_n$ es entero y ésta fracción satisface que

$$\begin{aligned}\left|\lambda - \frac{u_n}{v_n}\right| &= \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \cdots < \sum_{j=0}^{\infty} \frac{1}{10^{(n+1)!+j}} \\ &= \frac{1}{10^{(n+1)!}} \cdot \frac{1}{1-1/10} < \frac{1}{10^{(n+1)!}} < \frac{1}{v_n^n}.\end{aligned}$$

Ahora sí, λ es irracional (pues su expansión decimal no es periódica) y, si fuese algebraico, tendría un grado d que acote las aproximaciones, pero claramente u_n/v_n son infinitas aproximaciones «buenas» lo que es absurdo. ⌟

Definición 7.29: Se dice que un real irracional α es un ***número de Liouville*** si para cada $j \geq 1$ natural existe una fracción reducida u/v tal que $|\alpha - u/v| < 1/v^j$. Se denota por $\mathcal{L}$ el conjunto de los números de Liouville.

El mismo argumento prueba que los números de Liouville son todos trascendentes, aunque el recíproco es falso. Exhibir un contraejemplo no es fácil, pero podemos dar una prueba indirecta.

Definición 7.30: Sea $\varphi\colon \mathbb{N} \to (0,1]$ una función y sea α un irracional. Se dice que φ es ***aproximante para*** α si existen infinitas fracciones $u/v \in \mathbb{Q}$ tales que $|\alpha v - u| < \varphi(v)$. Denotamos por $A(\varphi)$ el conjunto de reales para los cuales φ es aproximante.

Teorema 7.31 (Khinchin): Sea $\varphi\colon \mathbb{N} \to (0,1]$ una función.

1. El conjunto $A(\varphi)$ es no numerable.
2. El conjunto $A(\varphi)$ es denso.
3. Si $\sum_{q=1}^{\infty} \varphi(q) < \infty$, entonces $A(\varphi)$ tiene medida (de Lebesgue) nula.

Demostración:

1. Sea $Z' := \mathrm{Func}(\mathbb{N}, \{0,1\})$, es decir, el conjunto de las sucesiones binarias. Definamos $Z \subseteq Z'$ como las sucesiones que tienen infinitos 1's. Sea $2 < g_1 \leq g_2 \leq g_3 \leq \cdots$ una sucesión de naturales creciente tal que $\lim_n g_n = \infty$, entonces definimos la función

$$\begin{aligned} \psi_{\boldsymbol{g}}\colon Z &\longrightarrow \mathbb{R} \\ \boldsymbol{z} = (z_n)_n &\longmapsto \sum_{n=1}^{\infty} \frac{z_n}{g_1 g_2 \cdots g_n}. \end{aligned}$$

   Si fijamos $\boldsymbol{z} \in Z$ podemos definir las aproximaciones

$$G_N := q_1 q_2 \cdots q_N, \qquad F_N := G_N \sum_{n=1}^{N} \frac{z_n}{G_n}.$$

   Entonces, la desigualdad (7.1) nos da que

$$0 < \left| \psi_{\boldsymbol{q}}(\boldsymbol{z}) - \frac{F_N}{G_N} \right| \leq \frac{1}{G_N(q_{N+1} - 1)}.$$

Ahora bien, si rellenamos con $z_{N+1} = z_{N+2} = \cdots = z_{N+r-1} = 0$ podemos mejorar la desigualdad por $\frac{1}{G_N(g_{N+r}-1)}$, por lo que basta elegir el r suficientemente grande de modo que $\frac{1}{g_{N+r}-1} < \varphi(G_N)$.

Finalmente, es fácil notar que cada elección de $\boldsymbol{g} := (g_n)_{n\in\mathbb{N}}$ nos da un valor distinto y siempre nos otorga al menos un elemento de $A(\varphi)$ (dado por rellenar con suficientes ceros). Luego tenemos una inyección desde el conjunto de $\boldsymbol{q}$'s hasta $A(\varphi)$ y un mero argumento de cardinalidad nos dice que hay $\mathfrak{c}$ distintos $\boldsymbol{q}$'s.

2. Basta notar que, con la notación anterior, a un elemento $\psi_{\boldsymbol{q}}(\boldsymbol{z}) \in A(\varphi)$ podemos sumarle racionales de la forma a/G_N, donde $a \in \mathbb{Z}$ y $N \in \mathbb{N}$ varían, para obtener un elemento de $A(\varphi)$ y este conjunto de racionales es denso. También, el lector puede realizar el ejercicio de probar que $A(\varphi) + \mathbb{Q} = A(\varphi)$ en general y emplear que $A(\varphi) \neq \varnothing$ por nuestra demostración anterior.

3. Fijemos $N, g \in \mathbb{N}$. Si $\in A(\varphi) \cap [-g, g]$, entonces ha de existir una fracción u/v con $v \geq N$ tal que $|\alpha - u/v| < \varphi(v)/v$, es decir,

$$\alpha \in \left(\frac{u-\varphi(v)}{v}, \frac{u+\varphi(v)}{v}\right).$$

En consecuencia, $|u| < |\alpha|v + \varphi(v) \leq 1 + gv$, por lo que

$$A(\varphi) \cap [-g, g] \subseteq \bigcap_{N=1}^{\infty} \bigcup_{v=N}^{\infty} \bigcup_{|u|\leq 1+gv} \left(\frac{u-\varphi(v)}{v}, \frac{u+\varphi(v)}{v}\right),$$

por lo que, denotando la medida de Lebesgue por μ, tenemos que

$$\begin{aligned}\mu\big(A(\varphi) \cap [-g, g]\big) &\leq \sum_{v=N}^{\infty} \sum_{|u|\leq 1+gv} 2\frac{\varphi(v)}{v} = \sum_{v=N}^{\infty} 2(3+2gv)\frac{\varphi(v)}{v} \\ &\leq 16g \sum_{v=N}^{\infty} \varphi(v),\end{aligned}$$

lo cual con $N \to \infty$ converge a 0. □

Corolario 7.31.1: El conjunto $\mathcal{L} \subseteq \mathbb{R}$ es denso, no numerable y de medida nula.

Demostración: Basta notar que los elementos de $\mathcal{L}$ pertenecen todos a cada $A(\varphi_j)$ donde $\varphi_j(v) := \frac{1}{v^j}$, por lo que $\mathcal{L}$ tiene medida nula.

Nótese que al intersectar densos no numerables podemos perder susodichas propiedades, por lo que hay que ser cautelosos. Replicando el mismo argumento del ejemplo 7.28, pero con otra base, vemos que el número

$$\sum_{n=1}^{\infty} \frac{a_n}{b^{n!}}$$

con $0 \leq a_n < b$ y $b \geq 2$ fijo son trascendentes. Incluso con $b = 2$ obtenemos no numerables irracionales dados por la libertad de elegir la sucesión $(a_n)_{n\in\mathbb{N}}$. Además, es claro que $\mathcal{L} + \mathbb{Q} = \mathcal{L}$, de modo que es denso. □

Y finalmente un resultado divertido expuesto en **[82]:**

Teorema 7.32 (Erdős): $\mathcal{L} + \mathcal{L} = \mathbb{R}$.

Demostración: Sea $\alpha \in \mathbb{R}$. Como $\mathbb{Q}+\mathcal{L} = \mathcal{L}$, vemos que si $\alpha - \lfloor\alpha\rfloor = \beta+\gamma$, con $\beta, \gamma \in \mathcal{L}$, entonces $\alpha = \beta + (\gamma + \lfloor\alpha\rfloor)$ satisface que $\gamma + \lfloor\alpha\rfloor \in \mathcal{L}$. Así que, sea α dado por expansión en base 2:

$$\alpha = \sum_{n=1}^{\infty} \frac{a_n}{2^n},$$

con $0 \leq a_n < 2$. Definimos

$$\beta := \sum_{n=1}^{\infty} \frac{b_n}{2^n}, \qquad \gamma := \sum_{n=1}^{\infty} \frac{c_n}{2^n},$$

donde, fijado $m \geq 1$ tal que $m! \leq n < (m+1)!$, definimos $b_n = a_n$ y $c_n = 0$ si m es par, y $b_n = 0, c_n = a_n$ si m es impar. Queda al lector verificar que β, γ son números de Liouville. □

§7.3.2 La irracionalidad de $\zeta(2)$ y $\zeta(3)$. En ésta sección seguimos el artículo de Beukers **[14].**

En las siguientes demostraciones emplearemos $V(n) := \text{mcm}\{1, 2, \ldots, n\}$.

Proposición 7.33: El número

$$\zeta(2) := \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \sum_{k=1}^{\infty} \frac{1}{n^2}.$$

es irracional.

Demostración: Para un complejo $|z| < 1$ tenemos que la serie geométrica

$$\frac{z^r}{1-z} = z^r + z^{r+1} + z^{r+2} + \cdots$$

Si tenemos $x, y \in (0,1)$, entonces $z = xy$ nos permite deducir lo siguiente:

$$\begin{aligned} I_{rr} := \int_0^1 \int_0^1 \frac{x^r y^r}{1-xy}\,\mathrm{d}x\,\mathrm{d}y &= \int_0^1 \left(\frac{y^r}{r+1} + \frac{y^{r+1}}{r+2} + \cdots\right)\mathrm{d}y \\ &= \frac{1}{(r+1)^2} + \frac{1}{(r+2)^2} + \cdots, \end{aligned}$$

de modo que

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{r^2} + I_{rr}.$$

o despejando, tenemos que $I_{rr} = \frac{\alpha\zeta(2)+\beta}{V(r)^2}$, donde $\alpha, \beta \in \mathbb{Z}$.

Si ahora definimos

$$P_n(x) := \frac{1}{n!}\frac{\mathrm{d}^n}{\mathrm{d}x^n}\big(x^n(1-x)^n\big),$$

entonces se puede notar que $P_n(x)$ es un polinomio con coeficientes enteros (¿por qué?), y luego

$$\int_0^1 \int_0^1 \frac{(1-y)^n P_n(x)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = \frac{a_n\zeta(2) + b_n}{V(n)^2},$$

donde a_n, b_n son enteros. Si integramos parcialmente respecto a x en el lado derecho tenemos

$$\frac{a_n\zeta(2) + b_n}{V(n)^2} = (-1)^n \int_0^1 \int_0^1 \frac{y^n(1-y)^n x^n(1-x)^n}{(1-xy)^{n+1}}\,\mathrm{d}x\,\mathrm{d}y.$$

Vamos a acotar el integrando. Para ello, vamos a calcular el máximo valor en el intervalo $x \in [0,1]$ buscando valores críticos, de lo que

$$\frac{y(1-y)x(1-x)}{1-xy} \leq \left(\frac{\sqrt{5}-1}{2}\right)^5.$$

Así, tenemos que

$$0 < \left| \int_0^1 \int_0^1 \frac{y^n(1-y)^n x^n(1-x)^n}{(1-xy)^{n+1}}\,\mathrm{d}x\,\mathrm{d}y \right|$$

$$= \frac{|a_n\zeta(2) + b_n|}{V(n)^2} \leq \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \int_0^1 \int_0^1 \frac{\mathrm{d}x\,\mathrm{d}y}{1-xy}$$
$$= \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \zeta(2).$$

Así que, basta probar que

$$\lim_n V(n)^2 \left(\frac{\sqrt{5}-1}{2}\right)^{5n} = 0.$$

Ahora bien, nótese que $V(n) \leq n^{\pi(n)}$ y empleando las aproximaciones de Chebychev tenemos que

$$\pi(n) \leq (\log 3) \cdot \frac{n}{\log n},$$

por lo que podemos concluir pues

$$V(n)^2 \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \leq 3^n \cdot \left(\frac{\sqrt{5}-1}{2}\right)^{5n} \approx 0{,}2705^n. \qquad \square$$

Corolario 7.33.1: Hay infinitos primos.

Demostración: De lo contrario, empleando el producto de Euler

$$\zeta(2) = \prod_p \frac{1}{1-1/p^2},$$

notamos que a la derecha tenemos un producto finito de racionales y, por tanto, el lado izquierdo es racional. $\square$

Corolario 7.33.2: π^2 es irracional.

Vamos a emplear un método similar para concluir lo siguiente:

Teorema 7.34 (Apéry): El número $\zeta(3)$ es irracional.

Demostración: Nótese que

$$\int_0^1 \int_0^1 \frac{\log(xy)}{1-xy}(xy)^r \,\mathrm{d}x\,\mathrm{d}y = \int_0^1 \int_0^1 \sum_{j=0}^{\infty} (\log x + \log y) x^{r+j} y^{r+j} \,\mathrm{d}x\,\mathrm{d}y$$

$$= \int_0^1 \sum_{j=0}^{\infty} \left(-\frac{y^{r+j}}{(r+j+1)^2} + \frac{(\log y) y^{r+j}}{r+j+1} \right) \mathrm{d}y$$
$$= -2 \sum_{j=0}^{\infty} \frac{1}{(r+j+1)^3} = -2 \left(\zeta(3) - 1 - \frac{1}{2^3} - \cdots - \frac{1}{r^3} \right).$$

y análogamente si $r > s$ es fácil comprobar que

$$I_{rs} := \int_0^1 \int_0^1 \frac{\log(xy)}{1-xy} x^r y^s \, \mathrm{d}x \, \mathrm{d}y = \frac{-1}{r-s} \left(\frac{1}{(s+1)^2} + \cdots + \frac{1}{r^2} \right),$$

de modo que, I_{rs} es siempre un número racional si $\zeta(3)$ es racional.

Nuevamente, definiendo

$$P_n(x) := \frac{1}{n!} \frac{\mathrm{d}^n}{\mathrm{d}x^n} \big(x^n (1-x)^n \big),$$

entonces se puede notar que

$$\int_0^1 \int_0^1 \frac{-\log(xy)}{1-xy} P_n(x) P_n(y) \, \mathrm{d}x \, \mathrm{d}y = \frac{a_n \zeta(3) + b_n}{V(n)^3},$$

donde a_n, b_n son enteros.

Empleando la siguiente identidad

$$\frac{-\log(xy)}{1-xy} = \int_0^1 \frac{1}{1-(1-xy)z} \, \mathrm{d}z,$$

tenemos que

$$\frac{a_n \zeta(3) + b_n}{V(n)^3} = \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x) P_n(y)}{1-(1-xy)z} \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}z,$$

ahora integramos n veces respecto a x y obtenemos que

$$= \int_0^1 \int_0^1 \int_0^1 \frac{(xyz)^n (1-x)^n P_n(y)}{(1-(1-xy)z)^{n+1}} \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}z.$$

Mediante la sustitución

$$w := \frac{1-z}{1-(1-xy)z} \iff 1 - w = \frac{xyz}{1-(1-xy)z},$$

podemos reescribir

$$\frac{a_n \zeta(3) + b_n}{V(n)^3} = \int_0^1 \int_0^1 \int_0^1 (1-x)^n (1-w)^n \frac{P_n(y)}{1-(1-xy)w} \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}w,$$

ahora integramos n veces respecto a y y obtenemos que

$$= \int_0^1 \int_0^1 \int_0^1 \frac{x^n(1-x)^n y^n(1-y)^n w^n(1-w)^n}{(1-(1-xy)w)} \,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}w.$$

Nuevamente procedemos a acotar el integrando:

$$\frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w} \leq (\sqrt{2}-1)^4,$$

y entonces

$$\begin{aligned}\frac{a_n\zeta(3)+b_n}{V(n)^3} &= (\sqrt{2}-1)^{4n}\int_0^1\int_0^1\int_0^1 \frac{1}{1-(1-xy)w}\,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}w \\ &= (\sqrt{2}-1)^{4n}\int_0^1\int_0^1 \frac{-\log(xy)}{1-xy}\,\mathrm{d}x\,\mathrm{d}y = 2\zeta(3)\cdot(\sqrt{2}-1)^{4n},\end{aligned}$$

reordenando tenemos que $0 < |a_n\zeta(3)+b_n| = 2\zeta(3)V(n)^3(\sqrt{2}-1)^{4n}$. Empleando la misma desigualdad de Chebyshev, vemos que

$$2V(n)^3(\sqrt{2}-1)^{4n} = 2\cdot 27^n\cdot(\sqrt{2}-1)^{4n} \approx 2(0{,}7948)^n \to 0. \qquad \square$$

El lector notará los fuertes paralelos entre la demostración para $\zeta(2)$ y $\zeta(3)$, ¿admitirá una generalización para $\zeta(4)$ y $\zeta(5)$? La respuesta es que no, o al menos no el método empleado; ya en la última demostración vimos que $27(\sqrt{2}-1)^4 \approx 0{,}7948 < 1$; pero ya en casos superiores éste factor se pasa del 1.

Conjetura 7.35: Se creen:

1. Los valores $\zeta(5), \zeta(7), \zeta(9), \ldots$ son irracionales.
2. Los valores $\zeta(n)$ son trascendentes para todo $n > 1$ entero.
3. Los valores $\pi, \zeta(3), \zeta(5), \zeta(7), \ldots$ son ($\mathbb{Q}$-)algebraicamente independientes.

Claramente 3 $\implies$ 2 $\implies$ 1. Hay gente que cree que, similar al caso par, $\zeta(2n+1)$ se puede escribir como π^{2n+1} con sus respectivos errores; no obstante, una conjetura de Grothendieck implica la propiedad 3, por lo que se opta por ésta última.

Indudablemente es curioso que además de $\zeta(3)$ se desconozca la irracionalidad de otros valores $\zeta(2n+1)$.

§7.3.3 La ecuación de Pell. Ahora veremos cómo emplear fracciones continuas para calcular eficientemente la ecuación de Pell. En ésta sección fijaremos un natural $D > 0$ que no es un cuadrado y nos enfocaremos en la ecuación de Pell:

$$x^2 - Dy^2 = 1, \tag{7.3}$$

y diremos que las ***soluciones triviales*** son las de la forma $(\pm 1, 0)$. En primer lugar queremos encontrar soluciones no triviales de la ecuación de Pell:

Lema 7.36: Existe un entero k con $1 \leq |k| \leq 1+2\sqrt{D}$ tal que la ecuación diofántica $x^2 - Dy^2 = k$ tiene infinitas soluciones enteras.

Demostración: Como $\sqrt{D}$ es irracional, por el teorema de Dirichlet, existen infinitos $u/v \in \mathbb{Q}$ con $(u; v) = 1$ y $1 \leq v$ tales que

$$\left|\sqrt{D} - \frac{u}{v}\right| < \frac{1}{v^2},$$

o equivalentemente, $|u - v\sqrt{D}| < 1/v$. Nótese que

$$\begin{aligned} |u^2 - v^2 D| = |u - v\sqrt{D}|\,|u + v\sqrt{D}| &< \frac{1}{v}(|u - v\sqrt{D}| + 2v\sqrt{D}) \\ &< \frac{1}{v^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D}, \end{aligned}$$

donde empleamos desigualdad triangular. Finalmente, concluimos por una variación del principio de palomar. □

Teorema 7.37: La ecuación de Pell siempre posee soluciones no triviales.

Demostración: Por el lema anterior, elijamos k de modo que la ecuación diofántica $x^2 - Dy^2 = k$ posee infinitas soluciones. Consideramos dos soluciones distintas $(a_1, b_1), (a_2, b_2)$ positivas con

$$a_1 \equiv a_2, \qquad b_1 \equiv b_2 \pmod{k},$$

las cuales siempre existen puesto que hay finitas posibilidades de congruencias e infinitas soluciones. Definamos:

$$A + B\sqrt{D} := (a_1 - b_1\sqrt{D})(a_2 + b_2\sqrt{D}) = (a_1 a_2 - b_1 b_2 D) + (a_1 b_2 - a_2 b_1)\sqrt{D},$$

de modo que $A^2 - B^2 D = \mathrm{Nm}(A + B\sqrt{D}) = k^2$.

Afirmamos que $B \neq 0$: de lo contrario, existiría $\lambda \in \mathbb{Q}_{\neq 0}$ tal que $a_1 = \lambda a_2$, $b_1 = \lambda b_2$ y tal que

$$k = a_2^2 - b_2^2 D = \lambda^2(a_1^2 - b_1^2 D) = \lambda^2 k,$$

por lo que $\lambda = \pm 1$. Como las soluciones son positivas, entonces $\lambda = 1$, pero eso es absurdo pues elegimos las soluciones distintas.

Además nótese que como $a_1 \equiv a_2$ y $b_1 \equiv b_2$ (k) se cumple que

$$A \equiv a_1^2 - b_1^2 D = k \equiv 0, \qquad B \equiv a_1 b_1 - a_1 b_1 = 0 \pmod{k}.$$

luego existen u, v enteros tales que $A = ku, B = kv$ y finalmente:

$$k^2 = A^2 - B^2 D = k^2(u^2 - v^2 D) \iff 1 = u^2 - v^2 D,$$

donde $v \neq 0$ pues $B \neq 0$ por lo que es una solución no trivial. □

Está claro que las soluciones de la ecuación de Pell (a, b) son exactamente los números algebraicos $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ de norma 1. De modo que podemos definir

$$\mathcal{P}_D := \{a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}] : a^2 - b^2 D = 1\}$$

el cual es un grupo con la multiplicación.

Teorema 7.38: $\mathcal{P}_D \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Demostración: Nótese que $\mathcal{P}_D \subseteq \mathbb{Z}[\omega]^\times$ el cual es el anillo de enteros de $\mathbb{Q}(\sqrt{D})$. Una solución no trivial de $\mathcal{P}_D$ es también una unidad no trivial de $\mathbb{Z}[\omega]$, luego tiene una unidad fundamental $\eta > 1$ (teo. 4.32). Hay dos posibilidades, o bien la unidad fundamental es tal que $\mathrm{Nm}(\eta) = -1$, en cuyo caso, los elementos de $\mathcal{P}_D$ son exactamente las potencias pares de η, i.e., potencias de $\epsilon := \eta^2$; o bien la unidad fundamental ya es de norma 1, en cuyo caso, las soluciones de Pell son ya las potencias de $\epsilon := \eta$. En ambos casos se obtiene que $\mathcal{P}_D = \{\pm\epsilon^n : n \in \mathbb{N}\} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

Teorema 7.39: Sea $d > 0$ libre de cuadrados y sea $\omega \in \mathbb{Z}[\sqrt{d}]$ con coordenadas positivas tal que $\mathrm{Nm}(\omega) = 1$. Dada una solución de la ecuación de Pell generalizada $x^2 - dy^2 = n$ existen $a, b, k \in \mathbb{Z}$ tales que $x + y\sqrt{d} = (a + b\sqrt{d})\omega^k$ con

$$|a| \leq \frac{\sqrt{|n|}(\sqrt{\omega} + 1/\sqrt{\omega})}{2}, \qquad |b| \leq \frac{\sqrt{|n|}(\sqrt{\omega} + 1/\sqrt{\omega})}{2\sqrt{d}}.$$

DEMOSTRACIÓN: Para $\alpha \in \mathbb{Z}[\sqrt{d}]_{\neq 0}$ definamos $L(\alpha) = (\log|\alpha|, \log|\overline{\alpha}|) \in \mathbb{R}^2$. Claramente para α, β arbitrarios se tiene $L(\alpha\beta) = L(\alpha) + L(\beta)$. Nótese que $L(2) = (\log 2)(1,1)$ y $L(\omega) = (\log\omega)(1,-1)$ son $\mathbb{R}$-linealmente independientes, de modo que

$$L(x + y\sqrt{d}) = c_1(1,1) + c_2 L(\omega) = (c_1 + c_2', c_1 - c_2'),$$

para algunos $c_1, c_2 \in \mathbb{R}$ y donde $c_2' = c_2 \log\omega$. Sumando coordenadas obtenemos que

$$c_1 = \frac{\log|x + y\sqrt{d}| + \log|x - y\sqrt{d}|}{2} = \frac{\log|n|}{2}.$$

Ahora bien, elijamos k el entero más cercano a c_2 de modo que $\delta := k - c_2 \in (-1/2, 1/2)$, luego tendremos que

$$L(x + y\sqrt{d}) = \frac{\log|n|}{2}(1,1) + L(\omega^k) + \delta L(\omega),$$

y definimos $a + b\sqrt{d} := (x + y\sqrt{d})\omega^{-k}$, donde

$$L(a + b\sqrt{d}) = (\log(\sqrt{|n|}) + \delta\log\omega, \log(\sqrt{|n|}) - \delta\log\omega).$$

Y, por tanto, alguno de los dos números $|a + b\sqrt{d}|, |a - b\sqrt{d}|$ está acotado por $\sqrt{|n|}\omega^{1/2} = \sqrt{|n|\omega}$ y el otro por $\sqrt{|n|}\omega^0 = \sqrt{|n|}$. Así tenemos

$$|a| = \frac{|(a + b\sqrt{d}) + (a - b\sqrt{d})|}{2}, \qquad |a| = \frac{|(a + b\sqrt{d}) - (a - b\sqrt{d})|}{2\sqrt{d}}.$$

Definamos $s := \text{máx}\{|a + b\sqrt{d}|, |a - b\sqrt{d}|\}$, entonces ambos números son $s, |n|/s$ con algún orden. Además vimos que alguno de los dos números es $> \sqrt{|n|}$ y el otro es $< \sqrt{|n|\omega}$; como s es el máximo, tenemos que $\sqrt{|n|} < s < \sqrt{|n|}\omega$. Un cálculo de las derivadas permite deducir que la función $t \mapsto t + |n|/t$ es creciente para $t \geq \sqrt{|n|}$, de modo que

$$|a| \leq \frac{1}{2}\left(s + \frac{|n|}{s}\right) \leq \frac{1}{2}\left(\sqrt{|n|\omega} + \frac{|n|}{\sqrt{|n|\omega}}\right) = \frac{\sqrt{|n|}(\sqrt{\omega} + 1/\sqrt{\omega})}{2}.$$

Y similarmente con $|b\sqrt{d}|$ por lo que dividiendo por $\sqrt{d}$ da las cotas del enunciado. □

Ahora que hemos asegurado la existencia de soluciones no triviales de la ecuación de Pell, veamos cómo encontrarlas.

Teorema 7.40: Sea $D > 0$ libre de cuadrados, $|n| < \sqrt{D}$ entero y $x, y > 0$ enteros tales que $x^2 - Dy^2 = n$. Entonces x/y ocurren como aproximantes en la fracción continua simple de $\sqrt{D}$.

Demostración: Considere primero el caso con $n > 0$. Como $x - y\sqrt{D} > 0$, entonces vemos que $x + y\sqrt{D} > 2y\sqrt{D}$ y, por tanto

$$0 < x - y\sqrt{D} = \frac{n}{x + y\sqrt{D}} < \frac{\sqrt{D}}{2y\sqrt{D}} = \frac{1}{2y},$$

luego dividiendo ambos lados por y tenemos que $|x/y - \sqrt{D}| < 1/(2y^2)$, por lo que es un aproximante por el teorema 7.24.

Si $n < 0$, entonces $Dy^2 - x^2 = |n|$ luego

$$y^2 - \frac{1}{D}x^2 = \frac{|n|}{D} > 0 \implies y > \frac{x}{\sqrt{D}}.$$

Se sigue que

$$y - \frac{x}{\sqrt{D}} = \frac{|n|}{D(y + x/\sqrt{D})} < \frac{|n|}{2D(x/\sqrt{D})} < \frac{1}{2x},$$

dividiendo por x llegamos a la misma conclusión. □

Ejercicio 7.41: Resuelva (con ayuda de un ordenador) la ecuación generalizada de Pell $x^2 - 103y^2 = 2$.

Solución: En primer lugar calcularemos la fracción continua simple de $\sqrt{103}$. Empleando que $\lfloor\sqrt{103}\rfloor = 10$, podemos calcular que a_1 viene dado por la parte entera de

$$t_1 := \frac{1}{\sqrt{103} - 10} = \frac{1}{\sqrt{103} - 10} \cdot \frac{\sqrt{103} + 10}{\sqrt{103} + 10} = \frac{1}{3}(\sqrt{103} + 10),$$

como $10 < \sqrt{103} < 11$ vemos que $20/3 < t_1 < 21/3 = 7$, así que $a_1 = 6$.

Reiterando el proceso podemos obtener la siguiente tabla:

n	-1	0	1	2	3	4	5	6
a_n		10	6	1	2	1	1	9
p_n	1	10	61	71	203	274	477	4567
q_n	0	1	6	7	20	27	47	450
$p_n^2 - 103q_n^2$		-3	13	-6	9	-11	2	-11

Y prosiguiendo obtendremos dos piezas fundamentales de información: que $(477, 47)$ es la solución minimal de $x^2 - 103y^2 = 2$ y que la solución fundamental de $x^2 - 103y^2 = 1$ se corresponde a $\omega := 227528 + 22419\sqrt{103}$. Nótese que por el teorema anterior, ésta solución debía aparecer como aproximante y, de haber más, también deberían aparecer.

Finalmente, un cálculo nos da que:

$$\frac{\sqrt{2}(\sqrt{\omega} + 1/\sqrt{\omega})}{2} = 477$$

por lo que todas las soluciones de la Pell generalizada son de la forma:

$$\pm(477 + 47\sqrt{103}) \cdot (227528 + 22419\sqrt{103})^k. \qquad \square$$

§7.3.4 La ecuación de Markoff. La ecuación de Pell terminó por «resolverse» dando un algoritmo para iterar entre todas las soluciones, el siguiente es otro ejemplo en el mismo espíritu:

Teorema 7.42: Considere la ***ecuación de Markoff*** dada por

$$x^2 + y^2 + z^2 = 3xyz. \tag{7.4}$$

Entonces:

1. Dada una solución (a, b, c) de (7.4), entonces $(a, b, 3ab - c)$ es otra solución.
2. Todas las soluciones positivas no triviales a la ecuación de Markoff están generadas por $(1, 1, 1)$ empleando la regla del inciso anterior, reordenando coordenadas o cambiando signo a dos coordenadas.

Demostración:

1. Es un mero cálculo.
2. Por casos:
   (a) Si $x = y = z$: entonces $3x^2 = 3x^3$ implica que $x \in \{0, 1\}$ y descartamos la trivial.
   (b) Si $x = y \neq z$: entonces $2x^2 + z^2 = 3x^2 z$ implica que $x^2 \mid z^2$ y, por tanto, $x \mid z$. Sea $z = wx$, luego tenemos la ecuación $2 + w^2 = 3wx$. Nótese que, en consecuencia, $w \mid 2$ y como $z \neq x$, necesariamente $w = 2$ lo que nos da la solución $(1, 1, 2)$ dada por aplicar la regla a $(1, 1, 1)$.

(c) Si $x < y < z$: Basta probar que $3xy - z < z$ para poder aplicar un argumento inductivo.
Mirando la ecuación de Markoff en $\mathbb{Z}[x, y][z]$ podemos obtener la solución

$$2z_{\pm} = 3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}.$$

De darse el caso z_- nótese que

$$8x^2y^2 - 4x^2 - 4y^2 = 4x^2(y^2 - 1) + 4y^2(x^2 - 1) > 0,$$

de modo que

$$x^2y^2 < 9x^2y^2 - 4(x^2 + y^2) \iff 2z_- < 3xy - xy = 2xy.$$

No obstante, como z es el mayor, vemos que $3xyz_- = x^2 + y^2 + z_-^2 < 3z_-^2$ por lo que $xy < z_-$ lo cual es absurdo.
Así que se da el caso z_+ y vemos que $3xy - z_+ = z_- < z_+$ como se quería probar. □

Definición 7.43: Una solución (a, b, c) de (7.4) con coordenadas estrictamente positivas se dice una ***terna de Markoff***. Un número x que pertenece a alguna terna de Markoff se dice un ***número de Markoff***.

Hay una variedad de razones por las cuales los matemáticos tienen interés en las ternas y números de Markoff. De partida, el teorema anterior permite construir una estructura a raíz de las ternas (desordenadas) de Markoff, llamado un árbol de Markoff. Otra razón es que el mismo Markoff demostró que las ternas de Markoff tenían relación a un cierto tipo de formas cuadráticas.

Teorema 7.44 (Frobenius): Se cumplen:

1. Los números de una terna de Markoff son coprimos dos a dos.
2. Todo número de Markoff impar es $\equiv 1 \pmod 4$.
3. Todo número de Markoff par es $\equiv 2 \pmod 8$.

Demostración:

1. Sea (a, b, c) una terna de Markoff. Nótese que si $d \in \mathbb{N}$ es tal que divide a dos de tres números, entonces por la ecuación (7.4) vemos que divide al restante, de modo que $(a; b) = (a; c) = (b; c) = (a; b; c)$. Finalmente, aplicando el teorema anterior, notamos que

$$(a; b; c) = (a; b; 3ab - c) = \cdots = (1; 1; 1) = 1.$$

2. y 3. Nótese que como $c(3ab-c) = a^2+b^2$, entonces c no puede ser múltiplo de 4. Más aún, para cada $p \mid c$, tenemos que $a^2 + b^2 \equiv 0\ (p)$, donde $p \nmid ab$, de modo que -1 es un residuo cuadrático módulo p y, por tanto, $p = 2$ o $p \equiv 1$ (mód 4). Así todo factor primo impar p de c satisface $p \equiv 1$ (mód 4) y de aparecer el 2, lo hace una única vez. □

El siguiente teorema es original de Zhang **[110]:**

Teorema 7.45 (Y. Zhang): Un número de Markoff par c satisface $c \equiv 2$ (mód 32).

Demostración: Sea (a, b, c) una terna de Markoff donde c es par y a, b son impares. Entonces $(a-b)/2$ es par y $c/2 \equiv 1\ (4)$ por el teorema de Frobenius, luego

$$\left(\frac{a-b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 = ab \cdot \frac{3c-2}{4}.$$

Como c es coprimo con a y b, y $c/2$ es coprimo con $(3c-2)/4$ (¿por qué?); de modo que $c/2$ es coprimo con $ab(3c-2)/4$ y, en consecuente, con $(a-b)/2$. Ahora bien, $ab(3c-2)/4$ es un impar y suma de dos cuadrados coprimos, luego todos sus factores primos son $\equiv 1\ (4)$ (teorema 4.21 y siguiente), de modo que $(3c-2)/4 \equiv 1\ (4)$, o equivalentemente, $c \equiv 2\ (16)$.

Así $3c+2 \equiv 8\ (16)$ implica que $(3c+2)/8$ es impar y un mero cálculo da

$$\left(\frac{a+b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 = 2ab \cdot \frac{3c+2}{8}.$$

Aplicamos el mismo procedimiento verificando que $c/2$ es coprimo con $(3c+2)/8$, de lo que se sigue que $(3c+2)/8 \equiv 1\ (4)$ y, en consecuente, $c \equiv 2$ (32). □

El teorema es agudo pues $(1, 1, 2)$ y $(1, 13, 34)$ son ternas de Markoff, de modo que $2, 34$ son pares de Markoff.

La gran pregunta sobre la ecuación de Markoff, aún abierta es la siguiente:

Conjetura de unicidad de Markoff 7.46: Sean $(a_1, b_1, c_1), (a_2, b_2, c_2)$ un par de ternas de Markoff donde $a_i \leq b_i \leq c_i$ para $i \in \{1, 2\}$. Si $c_1 = c_2$, entonces $a_1 = a_2$ y $b_1 = b_2$.

Esta conjetura lleva más de un siglo sin resolución y, como otros problemas diofánticos ya estudiados, lleva un historial de demostraciones fallidas. Diremos que el número de Markoff c en la conjetura es ***único*** si la conjetura es cierta para c.

Lema 7.47: Sea $m \in \{p^n, 2p^n\}$ para algún $n \geq 1$ y p primo impar. Entonces, para todo r coprimo con m, la ecuación $x^2 + r = 0 \pmod{m}$ tiene a lo más una única solución con $0 < x < m/2$.

Pista: Se sigue de que dicho m tiene raíces primitivas por el teorema 2.29. □

Teorema 7.48: Un número de Markoff c es único si $3c+2$ o $3c-2$ es de la forma $p^n, 4p^n$ u $8p^n$ para algún p primo impar y $n \geq 1$.

Demostración: Sean (a, b, c) y $(\tilde{a}, \tilde{b}, c)$ dos ternas de Markoff, donde $a \leq b \leq c$ y $\tilde{a} \leq \tilde{b} \leq c$. Dividimos por subcasos:

(a) Si c es impar: Si $3c - 2 = p^n =: m$, entonces $(b-a)^2 + c^2 = abm \equiv 0 \pmod{m}$. Como $(c; 3c-2) = 1$ y como

$$0 < b - a < \frac{c}{2} - 1 < \frac{3c-2}{2} = \frac{m}{2},$$

entonces aplicamos el lema anterior para concluir que $b - a = \tilde{b} - \tilde{a}$. Igualando

$$ab(3c-2) = (b-a)^2 + c^2 = (\tilde{b} - \tilde{a})^2 + c^2 = 3\tilde{a}\tilde{b}c = \tilde{a}\tilde{b}(3c-2),$$

Así, $ab = \tilde{a}\tilde{b} =: d$; luego vemos que $\{a, b\}$ y $\{\tilde{a}, \tilde{b}\}$ son soluciones de $(d/x - x)^2 + c^2 = dc$.

Si $3c+2 = p^n =: m$, entonces empleamos la ecuación $(b+a)^2 + c^2 = abm$ de forma análoga.

(b) Si c es par: Por el teorema de Y. Zhang tenemos que $3c - 2 \equiv 4 \pmod{32}$ y $3c + 2 \equiv 8 \pmod{32}$. Así que, si $3c - 2 = 4p^n$, empleamos la ecuación

$$\left(\frac{b-a}{2}\right)^2 + \left(\frac{c}{2}\right)^2 = abp^n \equiv 0 \pmod{p^n}.$$

Y si $3c + 2 = 8p^n$, empleamos la ecuación

$$\left(\frac{b+a}{2}\right)^2 + \left(\frac{c}{2}\right)^2 = 2abp^n \equiv 0 \pmod{2p^n}$$

ambas de forma análoga al caso de c impar. □

7.4 El problema de Waring

En 1770, el matemático inglés **Edward Waring** escribió para sí en sus *Meditationes Algebraicæ*:

> Todo entero es igual a la suma de no más de 9 cubos. Además, todo entero es la suma de no más de 19 potencias cuartas y *así sucesivamente...*[1]

Esta última frase, «así sucesivamente...» ha sido interpretado como el ***problema de Waring***: dado un natural $k \geq 1$ existe un número $g \geq 1$ tal que todo entero $n \in \mathbb{Z}$ se puede escribir como suma de g potencias k-ésimas, es decir, tal que

$$\exists a_i \in \mathbb{Z} \qquad n = a_1^k + a_2^k + \cdots + a_g^k. \tag{7.5}$$

En ésta sección presentaremos una prueba elemental para este hecho. En primer lugar, obsérvese que los números más problemáticos para ésta afirmación son valores «pequeños» de a, ya que habrían pocas potencias con las que jugar; por ejemplo $n = b^k - 1$ con b «pequeño». Esto obstaculiza las cotas que podamos dar para g, por lo que es conveniente hacer las siguientes dos definiciones:

Definición 7.49: Sea $k \geq 1$ entero. Denotamos por $g(k)$ al mínimo cardinal (*a priori*, posiblemente ∞) tal que para todo $n \in \mathbb{Z}$ se satisfaga (7.5). Denotamos por $G(k)$ al mínimo cardinal tal que para todo n *suficientemente grande* se satisface (7.5).

Si $g(k) < \infty$, entonces las consideraciones previas sugieren que $G(k)$ es bastante menor que $g(k)$ para k suficientemente grande. Nótese que, en los capítulos previos hemos ya deducido que $g(2) = G(2) = 4$ (teorema de Lagrange).

Ahora vamos a introducir las siguientes definiciones:

Definición 7.50: Sea $k \geq 1$ entero. Para n suficientemente grande, sean:

$$N := \lfloor n^{1/k} \rfloor, \qquad v := 1/100, \qquad P := N^v.$$

Dados $1 \leq a \leq q \leq P$ con b, q coprimos, se definen los ***arcos mayores***:

$$\mathfrak{M}(q, a) := \{\alpha \in \mathbb{R} : |\alpha - a/q| \leq N^{v-k}\}.$$

[1] *Every integer is equal to the sum of not more than 9 cubes. Also every integer is the sum of not more than 19 fourth powers, and so on...*

Denotamos por $\mathscr{U} := (N^{v-k}, 1 + N^{v-k}]$ una traslación del intervalo semiabierto unitario y se definen los ***arcos menores***:

$$\mathfrak{m}(q,a) := \mathscr{U} \setminus \mathfrak{M}(q,a).$$

De no haber ambigüedad sobre la elección del par a, q, obviaremos los paréntesis en los arcos.

Nótese que, pese a llamarse «arcos», en realidad son intervalos.

Vamos a introducir una técnica de conteo, llamada las *sumas trigonómetricas*. Denotaremos $e(\alpha) := \exp(2\pi \mathrm{i}\alpha)$ y, dado un conjunto finito $b_1 < \cdots < b_N$ de naturales, definiremos

$$f(\alpha) := \sum_{j=1}^{N} e(\alpha b_j),$$

de modo que, dado $s \geq 1$ entero, se satisface que

$$f(\alpha)^s = \sum_{m=0}^{sb_N} R_s(m) e(\alpha m);$$

donde $R_s(m)$ denota la cantidad de maneras de escribir m como suma de s elementos de b_j's. Ahora bien, la teoría clásica de Fourier dice que

$$\int_0^1 e(\alpha m)\,\mathrm{d}\alpha = \int_0^1 \exp(2\pi m \mathrm{i}\cdot t)\,\mathrm{d}t = \begin{cases} 1, & m = 0, \\ 0, & m \neq 0. \end{cases}$$

De modo que

$$\int_0^1 f(\alpha)^s e(-\alpha n)\,\mathrm{d}\alpha = R_s(n).$$

Aplicando todo lo anterior para $b_j := j^k$ con $N = \lfloor n^{1/k} \rfloor$, obtenemos lo siguiente:

$$R_s(n) = \int_{\mathfrak{M}} f(\alpha)^s e(-\alpha n)\,\mathrm{d}\alpha + \int_{\mathfrak{m}} f(\alpha)^s e(-\alpha n)\,\mathrm{d}\alpha.$$

Notas históricas

El resultado de que $\zeta(3)$ sea irracional fue original de Apéry **[12]** (1979) y fue rápidamente sustituído por el método de las integrales de Beukers **[14].**

Se contaba que cuando Apéry presentó su solución original en los Días Aritméticos (*Journées Arithmétiques*) de Luminy, los estudiantes estaban inquietos con la pizarra que se llenaba de relaciones crípticas entre fracciones continuas, y que al acabar era como si la respuesta se revelase por milagro. Indudablemente no eran los estudiantes los únicos desorientados, también así lo estaban los colegas, por lo que la demostración con integrales de Beukers rapidamente tomó terreno y, además, también alumbro el por qué la demostración de Apéry solo aplicaba en los casos de $\zeta(2)$ y $\zeta(3)$.

El nombre «ecuaciones de Pell» es desafortunado y se debe al propio L. Euler quien le acredita las ecuaciones a John Pell; según Weil, esto podría deberse a que en el texto de *Álgebra* de Wallis, el nombre de Pell aparece en repetidas ocasiones, pero no en relación a las ecuaciones que llevan su nombre. Cuando D es relativamente pequeño, se pueden encontrar ingeniosamente soluciones a la ecuación de Pell y, tras descubrir la operación de grupo, generar más soluciones; por ello, la ecuación de Pell debería atribuirse mejor al indio Brahamgupta quién resolvió la ecuación $x^2 - 92y^2 = 1$ y descubrió completamente la ley de grupo en las soluciones. Otro gran aporte de la matemática hindú es el famoso método *chakravala* que hemos omitido aquí por ser menos eficiente que las aproximaciones por fracción continua, pero que resultó uno de los más eficaces algoritmos en la historia; su autoría se debate entre Bhaskara II (c. 1150) o Shankar Shukla.

Además de los indios, los griegos también aportaron a la ecuación, Teón de Esmirna (c. 130 a.C.) descubrió la ley de grupo para la ecuación $x^2 - 2y^2 = \pm 1$ y Diofanto resolvió las ecuaciones con $D \in \{26, 30\}$. Una situación divertida que vincula a los griegos con las ecuaciones de Pell es el *problema del ganado de Arquimedes* que plantea calcular el número del ganado del dios Helios mediante una serie de restricciones que eventualmente se reducen a resolver una ecuación de Pell con $D = 2^2 \cdot 609 \cdot 7766 \cdot 4657^2$; el problema tardó siglos en resolverse y no se pudo sino mediante computador, pero esto no se corresponde tanto en su dificultad, sino en que los números elegidos son demasiado grandes como para efectuar las cuentas a mano.[2]

Otros matemáticos emplean la terminología «ecuación de Pell-Fermat» que es más apropiada, pero preservamos la terminología anticuada por ser más común. Fermat redescubrió el problema en 1657. El recuento histórico de la ecuación de Pell es de Williams **[10].**

[2]De hecho, se cree que en cierto modo Aristóteles sabía que, tras los despejes apropiados, se escondía una ecuación de Pell astronómica y que intencionalmente propuso el problema en respuesta a otros trabajos griegos con números grandes.

Referencias

74. COHN, H. A Short Proof of the Simple Continued Fraction Expansion of e. *Amer. Math. Mon.* doi:10.2307/27641837 (2006).

82. ERDŐS, P. Representations of real numbers as sums and products of Liouville numbers. *Michigan Math. J.* **9,** 59-60. https://old.renyi.hu/~p_erdos/1962-18.pdf (1962).

90. KHINCHIN, A. *Continued Fractions* (University of Chicago Press, 1964).

94. LEHMER, D. N. A Theorem in Continued Fractions. *Ann. Math.* **2,** 146-147. doi:10.2307/2007192 (1900).

110. ZHANG, Y. Congruence and uniqueness of certain Markoff numbers. *Acta Math.* **128,** 295-301. doi:10.4064/aa128-3-7 (2007).

Otros recursos.

1. CUEVAS, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).

2. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

3. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).

4. LIU, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

5. WILSON, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. BRIESKORN, E. y KNORRER, H. *Plane Algebraic Curves* trad. por STILLWELL, J. (Birkhäuser Verlag, 1981).

7. DICKSON, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

8. NEWTON, I. *The Correspondence of Isaac Newton* (ed. TURNBULL, H. W.) (Cambridge University Press, 1960).

9. ROQUETTE, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

10. WILLIAMS, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. BENNETT, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. Alford, W. R., Granville, A. y Pomerance, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).
12. Apéry, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. Barnes, E. S. y Swinnerton-Dyer, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. Beukers, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).
15. Bombieri, E. y Vaaler, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).
16. Cassels, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).
17. Catalan, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).
18. Chao, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).
19. Chatland, H. y Davenport, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).
20. Clark, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).
21. De Bessy, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
22. Dedekind, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).
23. Dickson, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).
24. Dirichlet, G. L. en *G. Lejeune Dirichlet's Werke* (ed. Kronecker, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.
25. Euler, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).
26. Euler, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).

27. EULER, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).

28. GAUSS, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.

29. HARPER, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

30. HENSEL, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).

31. HENSEL, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. HYYRÖ, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. INKERI, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. INKERI, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. KAUSLER, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. KELLER, W. y RICHSTEIN, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. KÜRSCHÁK, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. LANG, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. LEGENDRE, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. LEHMER, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. MAHLER, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. MIGNOTTE, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. MINKOWSKI, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. MOTZKIN, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. NAGELL, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. Northcott, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. Ochem, P. y Rao, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. Oppenheim, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. Ostrowski, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. Ostrowski, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. Ostrowski, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. Ostrowski, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. Ostrowski, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. Perron, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. Rédei, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. Rella, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. Remak, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. Roth, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. Rychlík, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. Rychlík, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. Siegel, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. Tate, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 305-347.

63. Verger-Gaugry, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

8

Introducción a los cuerpos ciclotómicos

En éste capítulo introducimos una de las herramientas fundamentales en el estudio de extensiones de cuerpo: las raíces de la unidad. Una extensión ciclotómica[1] será una extensión generada por raíces de la unidad y prueba ser particularmente útil en el estudio del Último Teorema de Fermat.

8.1 Extensiones ciclotómicas y teoría de Kummer

Definición 8.1: Dado un cuerpo K y $n > 0$, se define:

$$\mu_n(K) := \{\alpha \in K : \alpha^n = 1\} \leq G^\times.$$

Los elementos de $\mu_n(K)$ se dicen ***raíces n-ésimas de la unidad***.

Teorema 8.2: Sea $\operatorname{car} k = p$ y L/k el cuerpo de escisión de $f(x) := x^n - 1$. El conjunto de las n-ésimas raíces de la unidad $\mu_n(L)$ con la multiplicación conforma un grupo cíclico. Más aún:

(a) Si $p \nmid n$ (incluyendo $p = 0$), entonces $|\mu_n(L)| = n$.

(b) Si $n = p^r m$ con $p \nmid m$, entonces $\mu_n(L) = \mu_m(L)$.

En el caso (a), los generadores de $\mu_n(L)$ se dicen n-ésimas raíces ***primitivas*** de la unidad.

[1] gr. /'ci.klos/: círculo, μ /to'mi/: cortar. 'Al rededor del círculo'.

Demostración: En el caso (a): Como $f(x)$ es separable, puesto que su derivada nx^{n-1} tiene solo raíces nulas, se concluye que efectivamente hay n raíces distintas de la unidad. En el caso (b): Vemos que, por el sueño del aprendiz, $f(x) = (x^m)^{p^r} - 1 = (x^m - 1)^{p^r}$, de modo que $\mu_n(L)$ se corresponde con las m-ésimas raíces de la unidad y nos reducimos al caso (a). □

Por ejemplo: claramente el 1 no es una raíz n-ésima de la unidad primitiva, excepto para $n = 1$. El -1 es la única raíz segunda primitiva de la unidad e $\mathrm{i} := \sqrt{-1}$ es una raíz cuarta primitiva de la unidad.

Definición 8.3: Sea k un cuerpo, el cuerpo de escisión L_n del polinomio $x^n - 1$ se llama la ***n-ésima extensión ciclotómica***. Más generalmente, K se dice una ***extensión ciclotómica*** si existe n tal que $L_n/K/k$ son extensiones de cuerpos.

A lo largo de éste libro, denotaremos por ζ_n a una raíz n-ésima primitiva de la unidad en L_n. Si k tiene característica 0, entonces seremos más explícitos y

$$\zeta_n := e^{2\pi/n\,\mathrm{i}} \in \mathbb{C}.$$

Definición 8.4: Sea K/k una extensión de Galois. K se dice una ***extensión cíclica*** (resp. ***abeliana***) si $\mathrm{Gal}(K/k)$ es cíclico (resp. abeliano).

Teorema 8.5: Sea k un cuerpo. Entonces:

1. La n-ésima extensión ciclótomica es una extensión cíclica.

2. Toda extensión ciclotómica K/k es abeliana.

Demostración: Basta ver que si L_n es la n-ésima extensión ciclotómica, entonces ésta es abeliana (pues las subextensiones también). Podemos suponer que $\mathrm{car}\, k \nmid n$ de modo que L_n es separable y por ende admite una raíz primitiva $\zeta := \zeta_n$ tal que $L = k(\zeta)$. Luego todo $\sigma \in \mathrm{Gal}(L/k)$ está determinado por adónde manda ζ y sus conjugados son de la forma ζ^j y es fácil notar que si $\sigma\zeta = \zeta^a$ y $\tau\zeta = \zeta^b$, entonces $\sigma\tau\zeta = \sigma\zeta^b = \zeta^{ab} = \tau\sigma\zeta$. □

De ésta demostración se desprenden fácilmente dos consecuencias:

Teorema 8.6: Si k es un cuerpo finito y K/k es una extensión finita, entonces K/k es una extensión cíclica.

Demostración: Nótese que la extensión $K := \mathbb{F}_{p^n}$ de $\mathbb{F}_p$ corresponde al cuerpo de escisión de $x^{p^n} - x = x(x^{p^n-1} - 1)$, por lo que es una extensión ciclotómica y, por lo tanto, cíclica. Luego, basta notar que todo cociente de un grupo cíclico es también cíclico para concluir. □

Lema 8.7: Sea $\zeta := \zeta_n \in K$, entonces todas las raíces n-ésimas primitivas de K son exactamente las de la forma ζ^j donde j, n son coprimos.

Teorema 8.8: Sea $K_n := \mathbb{Q}(\zeta_n)$. La extensión $K_n/\mathbb{Q}$ es de Galois y $\mathrm{Gal}(K_n/K)$ es isomorfo a $U_n := (\mathbb{Z}/n\mathbb{Z})^\times$.

Definición 8.9: Se define el n-ésimo ***polinomio ciclotómico*** como

$$\Phi_n(x) := \prod_{\substack{j=1 \\ (j;n)=1}}^{n} (x - \zeta_n^j) \in \mathbb{C}[x].$$

De momento sabemos poco del polinomio ciclotómico exceptuando por tres detalles triviales: El primero es que todas las raíces de Φ_n son exactamente las raíces n-ésimas primitivas de la unidad, el segundo es que $\Phi_n \mid (x^n - 1)$ y el tercero es que Φ_p concuerda con nuestra antigua definición de «Φ_p». La segunda observación se puede mejorar a:

Proposición 8.10: Sea $n > 0$, entonces

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Reordenando la ecuación anterior se obtiene que

$$\Phi_n(x) = \frac{x^n - 1}{\displaystyle\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)}.$$

Ésto puede parecer trivial, pero es de hecho lo que nos permite calcular los

polinomios ciclotómicos:

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

Una curiosidad de la teoría de números es que los factores pequeños parecen solo constar de coeficientes «± 1», sin embargo, es sabido que el polinomio ciclotómico $\Phi_{105}(x)$ posee un «-2» y es la primera vez que sucede. Se puede demostrar que los coeficientes son arbitrariamente grandes para un índice arbitrariamente grande.

Teorema 8.11: Para todo $n > 0$ se cumplen:

1. $\Phi_n(x)$ es mónico, tiene grado $\phi(n)$ y está en $\mathbb{Z}[x]$.
2. Φ_n es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$, de modo que Φ_n es el polinomio minimal de ζ_n sobre $\mathbb{Q}$.
3. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es un cuerpo de Galois de grado $\phi(n)$ que es, de hecho, el cuerpo de escisión de $x^n - 1$.

Demostración: Para la primera es trivial que Φ_n sea mónico y de grado $\phi(n)$. Probar que $\Phi_n \in \mathbb{Z}[x]$ se demuestra por inducción fuerte empleando nuestro conocimiento sobre el caso primo. El inciso 3 es equivalente al 2, que es el que vamos a probar.

Para ello, veremos lo siguiente: Sea $\omega := \zeta_n$ y sea $f(x) \in \mathbb{Q}[x]$ su polinomio minimal. Si p es un número primo tal que $p \nmid n$, entonces ω^p también es raíz de $f(x)$. Como todo número coprimo a n se obtiene multiplicando primos que no dividen a n, entonces al comprobar ésto veremos que necesariamente f tiene por raíces a todas las raíces n-ésimas primitivas de la unidad, por lo que $f = \Phi_n$.

Definamos $h(x)$ tal que $x^n - 1 = f(x)h(x)$, y supongamos, por contradicción, que ω^p no es raíz de $f(x)$. Entonces ω^p es raíz de $h(x)$, es decir, ω es raíz de $h(x^p)$ y como f es el polinomio minimal de ω se cumple que existe

$g \in \mathbb{Q}[x]$ tal que

$$h(x^p) = f(x)g(x).$$

Y como h, f tienen coeficientes enteros, entonces g también. Luego, podemos llevar la igualdad anterior a $\mathbb{F}_p$ y notar que $h(x^p) \equiv h(x)^p$ (mód p), por lo que $[\omega]$ es raíz común de f y h, por lo que f, h no son coprimos. Pero $x^n - 1 = f(x)h(x)$ también en $\mathbb{F}_p[x]$, y la derivada es nx^{n-1} el cual no es cero puesto que $p \nmid n$; por lo que no tiene raíces repetidas, pero acabamos de ver que $[\omega]$ está repetida, lo cual es absurdo. □

Teorema 8.12: Sea k un cuerpo. Todo subgrupo finito de $k^\times$ es cíclico.

Demostración: Sea $G \leq k^\times$ finito. Por el teorema fundamental de los grupos abelianos (cfr. [**1,** teo. 1.71]) se da que

$$G \cong C_{a_1} \times \cdots \times C_{a_n},$$

donde cada $a_i \mid a_{i+1}$, de modo que para todo $g \in G$ se cumple que $g^{a_n} = 1$. Considere el polinomio $f(x) := x^{a_n} - 1 \in k[x]$, cada elemento de G es raíz de $f(x)$ y $f(x)$ tiene a lo más a_n raíces. Así que $n = 1$ y G es cíclico. □

Teorema 8.13 – *Teorema 90 de Hilbert*: Sea k un cuerpo con una raíz primitiva n-ésima de la unidad ω, y sea K/k una extensión cíclica de grado n. Si $\sigma \in \mathrm{Gal}(K/k)$ es un generador, entonces existe $a \in K^\times$ tal que $\sigma(a) = \omega a$.

Demostración: Como σ es un k-automorfismo de K entonces en un endomorfismo de K como k-espacio vectorial, luego tiene un polinomio característico asociado $\psi_\sigma(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x]$ tal que

$$0 = \psi(\sigma) = \sigma^n + a_{n-1}\sigma^{n-1} + \cdots + a_0 = 1 + a_{n-1}\sigma^{n-1} + \cdots + a_0,$$

(pues $\sigma^n = 1$), pero como $1, \sigma, \ldots, \sigma^{n-1}$ son endomorfismos linealmente independientes por el lema de independencia de Dedekind (cfr. [**1,** lema 4.49]), luego necesariamente $\psi(x) = x^n - 1$.

Finalmente, el enunciado equivale a ver que ω es un valor propio de σ, y todo valor propio es una raíz del polinomio característico, así que es claro. □

Definición 8.14: Una extensión de cuerpos K/k se dice ***pura*** si $K = k(\sqrt[n]{a})$ para algún $a \in k$ y $n > 0$.

Proposición 8.15: Sea k un cuerpo que contiene una n-ésima raíz primitiva de la unidad ω.

1. Para todo $a \in k^\times$, la extensión pura $K := k(\sqrt[n]{a})$ es cíclica y su grado $m := [K : k]$ corresponde al orden de $[a] \in k^\times/k^{\times n}$.

2. Dada una extensión cíclica K/k de grado n, se cumple que $K = k(\sqrt[n]{a})$ es pura. Además el orden de $[a] \in k^\times/k^{\times n}$ es exactamente n.

Demostración:

1. Denotando $\beta := \sqrt[n]{a}$, se cumple que las raíces de $x^n - a$ son $\omega^j\beta$ donde $0 \leq j < n$. Para todo $\sigma \in \mathrm{Gal}(K/k)$ vemos que $\sigma(\beta) = \omega^j\beta$ para algún j que es único módulo n. Por lo tanto, determina un monomorfismo de grupos $\mathrm{Gal}(K/k) \to \mathbb{Z}/n\mathbb{Z}$ y, por ello, $\mathrm{Gal}(K/k)$ se identifica con un subgrupo (cíclico) de $\mathbb{Z}/n\mathbb{Z}$.

   Ahora fijamos σ un generador de $\mathrm{Gal}(K/k)$ y j tal que $\sigma(\beta) = \omega^j\beta$. Anotemos $a^{r/n} := \beta^r$ para $r \in \mathbb{Z}$. Es fácil probar que

   $$a^{r/n} \in k^\times \iff a^r \in k^{\times n}.$$

   Luego, como $\sigma(a^{1/n}) = \omega^j a^{1/n}$, vemos que $\sigma(a^{r/n}) = \omega^{jr}a^{r/n}$, por lo que si $a^{r/n} \in k^\times$, ha de cumplirse que $n \mid jr$ y viceversa dado que K/k es una extensión de Galois. Luego, dado que $m > 0$ es el mínimo natural tal que $a^{m/n} \in k^\times$, luego es fácil concluir que el orden de σ también es m.

2. Sea $\sigma \in \mathrm{Gal}(K/k)$ un generador. Por el teorema 90 de Hilbert sea β tal que $\sigma(\beta) = \omega\beta$, de modo que $\sigma(\beta^n) = \omega^n\beta^n = \beta^n$. Como la extensión es de Galois, entonces $\beta^n =: a \in k^\times$. Claramente $k(\beta) \subseteq K$; para probar la inclusión recíproca basta demostrar que $[k(\beta) : k] = n$. En efecto, el monomorfismo determinado por $\omega^j \mapsto \omega^j$ es un isomorfismo, de modo que $\mathrm{Gal}(k(\beta)/k) \cong \mathbb{Z}/n\mathbb{Z}$ y sabemos que $[k(\beta) : k] = |\mathrm{Gal}(k(\beta)/k)|$ (cfr. [**1,** teo. 4.50]). □

Corolario 8.15.1: Sea p primo y sea k un cuerpo que contiene una raíz p^2-ésima primitiva de la unidad. Las extensiones de Galois K/k de grado p (que son cíclicas) son extensiones puras.

Teorema 8.16: Sea $\mathrm{car}\, k = p \neq 0$, y sea $f_a(x) := x^p - x - a \in k[x]$.

1. Si $f_a(x)$ no tiene raíces en k y γ es una raíz, entonces $k(\gamma)$ es cíclica de grado p.

2. Si K/k es una extensión cíclica de grado p, entonces $K = k(\gamma)$ donde γ es raíz de $f_a(x)$ para algún $a \in k$.

Demostración:

1. Basta notar que si γ es raíz y $b \in \mathbb{F}_p$, entonces $\gamma + b$ es raíz de $f_a(x)$ (por el sueño del aprendiz y el pequeño teorema de Fermat); ésto nos otorga todas las p raíces del polinomio.

2. Como K es cíclica, sea $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Por el lema de independencia de Dedekind existe $\beta \in K$ tal que $\sum_{i=1}^{p} \sigma^i(\beta) \neq 0$. Definamos

$$\delta := \sigma\beta + 2\sigma^2\beta + \cdots + (p-1)\sigma^{p-1}\beta.$$

Luego se tiene que $\delta - \sigma\delta = \sigma\beta + \sigma^2\beta + \cdots + \sigma^{p-1}\beta - (p-1)\beta = \sum_{i=1}^{p} \sigma^i(\beta) \neq 0$, de modo que $\delta \notin k$ y necesariamente $K = k(\delta)$ (puesto que un grupo de orden p es simple). Es fácil notar que $\sigma^i\delta - \sigma^{i+1}\delta = \delta - \sigma\delta =: f$, por lo que, los conjugados de δ son $\delta, \delta+f, \ldots, \delta+(p-1)f$. Definamos $\gamma := \delta/f$ y nótese que sus conjugados son $\gamma, \gamma+1, \ldots, \gamma+(p-1)$. Más aún

$$a := \gamma \cdot (\gamma-1) \cdots \big(\gamma-(p-1)\big) = \mathrm{Nm}_{K/k}(\gamma) \in k.$$

Nótese que $b \in \mathbb{F}_p$ syss es raíz de $x^p - x = \prod_{b\in\mathbb{F}_p}(x-b)$, de lo que se sigue que $\gamma^p - \gamma = a$, o equivalentemente, que γ es raíz de $f_a(x) \in k[x]$. □

Lema 8.17: Sea p primo y sea k un cuerpo que contiene una raíz p^2-ésima primitiva de la unidad. Toda extensión de Galois K/k de grado p está contenido en una extensión L/k cíclica de grado p^2.

Demostración: Por el corolario anterior, $K = k(\sqrt[p]{a})$ para algún $a \in k^\times$. Sea $L := k(a^{1/p^2}) \supseteq K$; como L es una extensión pura, entonces es cíclica (proposición 8.15), donde el grado $g := [L : k]$ es el orden de $[a] \in k^\times/k^{\times p^2}$, el que divide a p^2. Si $g = p$, entonces $a^p = b^{p^2}$ para algún $b \in k$, por lo que, $(a/b^p)^p = 1$ y luego $a = b^p\omega^j$, donde ω es una raíz primitiva p-ésima de la unidad. Nótese, no obstante, que ω y b tienen raíces p-ésimas, así que a tiene raíz p-ésima lo que es absurdo. En conclusión, $g \neq p$, y como $g > 1$ y $g \mid p^2$, vemos que $g = p^2$. □

Lema 8.18: Sea p un primo y sea k un cuerpo con $\mathrm{car}\, k \neq p$. Si k^{alg}/k es una extensión de Galois de grado p, entonces $p = 2$ y $k^{\mathrm{alg}} = k(\sqrt{-1})$.

Demostración: Sea $K := k^{\mathrm{alg}}$. Como $\operatorname{car} K \neq p$, entonces K contiene una raíz p-ésima primitiva de la unidad ω. Nótese que ω es raíz del polinomio:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in k[x],$$

de modo que $k(\omega)/k$ es una extensión de grado g con $g \mid p - 1$. Como $K/k(\omega)/k$ son extensiones de cuerpo y $[K : k] = p$ que es coprimo con $(p - 1)$, entonces $g = 1$ y $\omega \in k$.

Nótese que k no contiene una raíz p^2-ésima primitiva de la unidad, de lo contrario el lema anterior nos daría una extensión L/K de grado p lo que contradice que K es algebraicamente cerrado. Luego $\omega^{1/p} \notin k$ y claramente $K = k(\omega^{1/p})$.

Sea $\sigma \in \mathrm{Gal}(K/k)$ un generador del grupo. Se tiene que $\sigma(\omega^{1/p}) = \omega^j \omega^{1/p}$ para algún j. Definamos $\zeta := \omega^j$, el cual ha de ser otra raíz p-ésima primitiva de la unidad.

Si p es impar, entonces vemos que

$$\mathrm{Nm}_{K/k}(\omega^{1/p}) = (\omega^{1/p})(\zeta\omega^{1/p}) \cdots (\zeta^{p-1}\omega^{1/p}) = \zeta^{\frac{p(p-1)}{2}}\omega = \omega,$$

puesto que $p \mid \frac{p(p-1)}{2}$ si p es impar. Luego, como la norma es multiplicativa y K es algebraicamente cerrado, vemos que $\mathrm{Nm}_{K/k}(\omega^{1/p^2})$ es una raíz p-ésima de ω que está en k, lo cual es absurdo. En conclusión, $p = 2$ y luego $\omega = -1$. □

Teorema 8.19: Sea k un cuerpo de $\operatorname{car} k = 0$ y suponga que k^{alg}/k es una extensión finita de Galois. Entonces o bien $k^{\mathrm{alg}} = k$ o bien $k^{\mathrm{alg}} = \sqrt{-1}$. Equivalentemente, si G es un grupo finito de automorfismos de un cuerpo algebraicamente cerrado K, entonces o bien $G = \{1\}$ o bien $G \cong \mathbb{Z}/2\mathbb{Z}$ y su cuerpo fijado k es tal que $K = k(\sqrt{-1})$.

Demostración: Nótese que ambas afirmaciones son equivalentes puesto que en una extensión de Galois K/k, el cuerpo fijado por $\mathrm{Gal}(K/k)$ es precisamente k. Fijaremos $K := k^{\mathrm{alg}}$.

Si $[K : k]$ tuviera algún factor primo p, entonces el teorema de Cauchy para grupos (cfr. **[1,** teo. 1.93**]**) nos dice que habría un elemento $\sigma \in \mathrm{Gal}(K/k)$ de orden p, luego el cuerpo fijado L por el subgrupo $\langle\sigma\rangle$ sería tal que L^{alg}/L fuese una extensión de Galois de grado p. Luego $[K : k]$ ha de ser una potencia de 2.

Supongamos que $K/k(\sqrt{-1})$ no fuese una extensión trivial, entonces existiría $\sigma \in \mathrm{Gal}(K/k(\sqrt{-1}))$ de orden 2, y sea L el cuerpo fijado por $\langle\sigma\rangle$. Luego

$[K : L] = 2$ y $\sqrt{-1} \in L$, lo que es absurdo por el lema anterior. Por ende, $K = k(\sqrt{-1})$ como se quería ver. □

La llamada *teoría de Artin-Schreier* se encarga principalmente del estudio de cuerpos formalmente reales (que poseen algun ordenamiento) y permite concluir que la clausura algebraica C de un cuerpo R es una extensión finita syss R es formalmente real y $C = R(\sqrt{-1})$, sin restricciones (*a priori*) sobre la característica de R; *a posteriori*, todos los cuerpos formalmente reales tienen característica 0.

Definición 8.20: Una extensión de cuerpos K/k se dice una ***extensión de Kummer n-ésima*** si:

EK1. K/k es una extensión finita de Galois.

EK2. k contiene una raíz n-ésima primitiva de la unidad.

EK3. $\mathrm{Gal}(K/k)$ es un grupo abeliano de exponente n.[2]

En el teorema fundamental de la teoría de Galois (cfr. [**1,** teo. 4.52, inciso 5]) podemos concluir que en una torre de extensiones de Galois los grupos de Galois satisfacen una relación con cocientes. Ésto es suficiente para concluir que polinomios resolubles generan extensiones con grupos resolubles, pero para nuestros propósitos necesitamos explicitar el cómo combinar los grupos de Galois.

Proposición 8.21: Sea k un cuerpo y K, L dos extensiones finitas de k.

1. Si K/k es de Galois, entonces $K \vee L/L$ también y
$$\mathrm{Gal}(K \vee L/L) \cong \mathrm{Gal}(K/K \cap L).$$
2. Si K/k y L/k son de Galois, entonces $K \vee L/k$ también y
$$\mathrm{Gal}(K \vee L/k) \cong \{(\sigma, \tau) \in \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k) : \sigma|_{K\cap L} = \tau|_{K\cap L}\}.$$

Demostración:

1. Como K/k es finita y de Galois, entonces K es el cuerpo de escisión de un polinomio separable $f(x) \in k[x]$ (cfr. [**1,** teo. 4.24]), luego es fácil

[2] Un grupo G se dice de exponente m si $g^m = 1$ para todo $g \in G$.

ver que $K \vee L/L$ es el cuerpo de escisión del mismo polinomio, que también es separable sobre L; luego es de Galois.

Podemos definir el siguiente homomorfismo de grupos:

$$\begin{aligned} \varphi\colon \operatorname{Gal}(K \vee L/L) &\longrightarrow \operatorname{Gal}(K/K \cap L) \\ \sigma &\longmapsto \sigma|_K, \end{aligned}$$

y hay que probar que es un isomorfismo. Claramente φ es inyectivo, veamos que es suprayectivo: para ello, nótese que $H := \operatorname{Img} \varphi \leq \operatorname{Gal}(K/K \cap L)$ induce un cuerpo fijado $E := F(H)$, de modo que por el teorema fundamental de la teoría de Galois (cfr. **[1,** teo. 4.52**]**) se cumple que $\operatorname{Gal}(K/E) = H$. Nótese que $K \cap L \subseteq E \subseteq K$ y como $E \subseteq K \vee L$ está fijado por $\operatorname{Gal}(K \vee L/L)$, entonces $E \subseteq L$, luego $E = K \cap L$ como se quería probar.

2. $K \vee L/k$ es de Galois puesto que podemos entender K, L como generados por polinomios separables $f(x), g(x)$ y luego la extensión $K \vee L$ está generada por el polinomio $f(x) \cdot g(x)$.

   Considere el homomorfismo:

$$\begin{aligned} \varphi\colon \operatorname{Gal}(K \vee L/k) &\longrightarrow \operatorname{Gal}(K/k) \times \operatorname{Gal}(L/k) \\ \sigma &\longmapsto (\sigma|_K, \sigma|_L). \end{aligned}$$

   Es inyectivo (¿por qué?) y va a parar en algún subgrupo H de

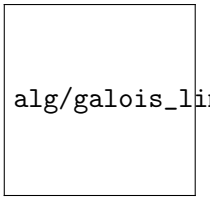
$$G := \{(\sigma, \tau) \in \operatorname{Gal}(K/k) \times \operatorname{Gal}(L/k) : \sigma|_{K \cap L} = \tau|_{K \cap L}\}.$$

   Nótese que H tiene $[K \vee L : k]$ elementos y que G tiene

$$|G| = [K : K \cap L][L : k] = [K \vee L : L][L : k] = [K \vee L : k]$$

   elementos, así que ha de tratarse de un isomorfismo. □

El inciso 2 de la proposición anterior, puede ilustrarse por los siguientes diagramas categoriales:

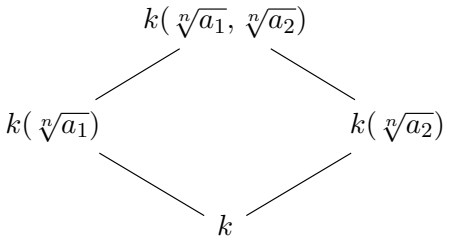


Proposición 8.22: Sea k un cuerpo que contiene una raíz n-ésima primitiva de la unidad y sea K/k una extensión finita de cuerpos. Son equivalentes:

1. K/k es de Kummer n-ésima.
2. Existen $a_1, \ldots, a_m \in k^\times$ tales que $K = k(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m})$.

Demostración: $2 \implies 1$. Es claro que K es de Galois en este caso, así que se satisfacen EK1 y EK2. También es claro que $\mathrm{Gal}(K/k)$ es un grupo de exponente n, así que falta probar que es abeliano.

Nótese que para cada j se tiene que $k(\sqrt[n]{a_i})/k$ es una extensión cíclica, luego es de Kummer. Así, tenemos el siguiente diagrama de retículos:



donde cada extensión de cuerpos es de Galois sobre la anterior, de modo que por la proposición anterior, vemos que

$$\mathrm{Gal}(k(\sqrt[n]{a_1}, \sqrt[n]{a_2})/k) \leq \mathrm{Gal}(k(\sqrt[n]{a_1})/k) \times \mathrm{Gal}(k(\sqrt[n]{a_2})/k),$$

donde el producto directo de grupos abelianos es abeliano. Aplicando inductivamente éste argumento concluimos EK3.

$1 \implies 2$. Si $\mathrm{Gal}(K/k)$ es abeliano, entonces por el teorema fundamental de los grupos abelianos (cfr. [**1,** teo. 1.71]) vemos que

$$\mathrm{Gal}(K/k) \cong C_{\alpha_1} \times \cdots \times C_{\alpha_m}$$

donde cada $\alpha_i \mid n$ (pues el grupo es de exponente n). Luego considere el subgrupo

$$H_i := \prod_{j \neq i} C_{\alpha_j} \leq \mathrm{Gal}(K/k),$$

que tendrá un subcuerpo fijado E_i. Por el teorema fundamental de la teoría de Galois, tenemos que $\mathrm{Gal}(E_i/k) \cong C_i$ así que, como las extensiones cíclicas (de exponente n) son puras tenemos que $E_i = k(\sqrt[n]{a_i})$. Finalmente, también por el teorema fundamental de la teoría de Galois, vemos que

$$K = F(1) = F\left(\bigcap_{i=1}^{m} H_i\right) = \bigvee_{i=1}^{m} E_i = k(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m}). \qquad \square$$

8.2 Enteros ciclotómicos

Teorema 8.23: Sea p primo, $q := p^r$ para algún r y $\theta := \zeta_q$. Sea $K := \mathbb{Q}(\theta)$ y $A := \mathcal{O}_K$.

1. El elemento $\pi := 1-\theta$ es primo en A y $pA = (\pi A)^{\phi(q)}$ con $f(\pi A/\mathbb{Z}) = 1$.
2. Si $q > 2$, entonces (p) tiene índice de ramificación $e := \phi(q) > 1$ y es el único primo de $\mathbb{Z}$ que se ramifica en A.
3. $A = \mathbb{Z}[\theta]$.
4. El discriminante $\mathfrak{d}(\theta) = \pm p^c$ (con $c = p^{r-1}(rp-r-1)$), donde $\operatorname{sign}\mathfrak{d}(\theta) = +1$ syss $p \equiv 1 \pmod 4$ o $q = 2^r$ con $r > 2$.

Demostración: Comencemos por el cálculo

$$\Phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = t^{p-1} + t^{p-2} + \cdots + 1, \qquad t = x^{p^{r-1}}.$$

Nótese que $\theta = \zeta_q$ (y en general, cada ζ_n) es entero por ser raíz de $\Phi_n(x) \in \mathbb{Z}[x]$ que es mónico. Además es trivialmente invertible en A. Nótese que

$$u_j := \frac{1-\theta^j}{1-\theta} = 1 + \theta + \cdots + \theta^{j-1}$$

es entero (por ser suma de enteros), además $u_p = 0$ y $u_{j_1} = u_{j_2}$ syss $j_1 \equiv j_2$ (p). Así, si $p \nmid j$, entonces θ^j es también una q-ésima raíz de la unidad primitiva, luego el mismo método aplica y u_j^{-1} es una suma de potencias de θ_j; así que $u_j^{-1} \in A$.

Ahora evaluamos $\Phi_q(x)$ en $x = 1$:

$$p = \Phi_q(1) = \prod_{\substack{j=1\\(j;p)=1}}^{q} (1-\theta^j) = \prod_{\substack{j=1\\(j;p)=1}}^{q} (1-\theta)u_j = \pi^{\phi(q)}u,$$

donde $u \in A^\times$ es el producto de los u_j's. De éste modo vemos que $\mathrm{Nm}_{K/\mathbb{Q}}(\pi) = p$, por lo que π es primo y también vemos que $pA = (\pi A)^{\phi(q)}$.

Nótese que si $q = 2$, entonces $\theta = -1$ y el resto de incisos es trivial, por lo que asumimos que $q > 2$. Enumeremos las raíces q-ésimas primitivas de la unidad como $\theta = \theta_1, \ldots, \theta_{\phi(q)}$ de modo que

$$\Phi_q(x) = \prod_{j=1}^{\phi(q)} (x - \theta_j).$$

Derivando la expresión, obtenemos

$$\Phi_q'(\theta_i) = \prod_{\substack{j=1\\ j\neq i}}^{n} (\theta_i - \theta_j),$$

y derivando por definición, obtenemos

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{x^q-1}{x^{q/p}-1}\right)\Big|_{x=\theta_i} = \left.\frac{qx^{q-1}(x^{q/p}-1)-(x^q-1)(\frac{q}{p}x^{q/p-1})}{(x^{p/q}-1)}\right|_{x=\theta_i} = \frac{p^r\theta_i^{-1}}{\theta_i^{p^{r-1}}-1}.$$

Definiendo $\omega := \zeta_p$, entonces mientras $1 \leq i \leq \phi(q)$ se satisface que $\theta_i^{p^{r-1}}$ recorre el conjunto $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ cubriendo cada elemento $\phi(q)/(p-1) = p^{r-1}$ veces. De éste modo, vemos que

$$\prod_{i=1}^{\phi(q)} \Phi_q'(\theta_i) = \frac{p^{r\phi(q)}\,\mathrm{Nm}_{K/\mathbb{Q}}(\theta_i)^{-1}}{\left(\prod_{j=1}^{p-1}(1-\omega^j)\right)^{p^{r-1}}}.$$

El producto del denominador es

$$\prod_{j=1}^{p-1}(\omega^j - 1) = (-1)^{p-1}\prod_{j=1}^{p-1}(1-\omega^j) = (-1)^{p-1}\Phi_p(1) = (-1)^{p-1}p.$$

Empleando una técnica similar, obtenemos que

$$\mathrm{Nm}_{K/\mathbb{Q}}(\theta) = (-1)^{\phi(q)}\Phi_q(0) = (-1)^{\phi(q)}.$$

Recopilando todo en la fórmula del teorema 4.80, tenemos

$$\mathfrak{d}(\theta) = (-1)^s \frac{p^{r\phi(q)}(-1)^{\phi(q)}}{((-1)^{p-1}p)^{p^{r-1}}} = (-1)^{s+\phi(q)-(p-1)p^{r-1}}p^c,$$

donde $s = \frac{\phi(q)(\phi(q)-1)}{2}$ y c es la constante descrita en el enunciado. El lector puede verificar las comprobaciones sobre el signo.

Por el teorema 4.79 sabemos que $\mathfrak{d}(\theta)A = p^cA \subseteq \mathbb{Z}[\theta]$, queremos probar la otra inclusión. En primer lugar, como $f(\pi A/\mathbb{Z}) = 1$, entonces $A/\pi A = \mathbb{Z}/p\mathbb{Z}$. Nótese que

$$\frac{\mathbb{Z}[\theta]}{\mathbb{Z}[\theta]\cap\pi A} \leq \frac{A}{A\cap\pi A} \cong \frac{\mathbb{Z}}{p\mathbb{Z}},$$

luego $\mathbb{Z}[\theta]/(\mathbb{Z}[\theta] \cap \pi A)$ es un subanillo de $\mathbb{F}_p$ y es no trivial, así que es igual a $\mathbb{F}_p$. De ésto se concluye que

$$\mathbb{Z}[\theta] + \pi A = A. \tag{8.1}$$

Multiplicando ambos lados por π (y empleando que $\pi \in \mathbb{Z}[\theta]$), obtenemos que

$$\pi A = \pi\mathbb{Z}[\theta] + \pi^2 A \subseteq \mathbb{Z}[\theta] + \pi^2 A,$$

sustituyendo en (8.1) obtenemos que $\mathbb{Z}[\theta]+\pi^2 A = A$. Iterando por inducción podemos probar que

$$\mathbb{Z}[\theta] + \pi^t A = A, \qquad t \in \mathbb{N}.$$

Evaluando en $t = c\phi(q)$ y empleando que $pA = (\pi A)^{\phi(q)}$, tenemos que

$$A = \mathbb{Z}[\theta] + \pi^{c\phi(q)} A = \mathbb{Z}[\theta] + p^c A \subseteq \mathbb{Z}[\theta],$$

de lo que concluimos la igualdad.

Finalmente como $A = \mathbb{Z}[\theta]$, entonces $\mathfrak{d}(A/\mathbb{Z}) = \mathfrak{d}(\theta)\mathbb{Z}$ por lo que el único primo que se ramifica es p como afirmamos. □

Nos introduciremos al caso general:

Proposición 8.24: Sea $m > 1$ un entero. Un primo racional p no se ramifica en el anillo de enteros de $\mathbb{Q}(\zeta_m)$ si $p \nmid m$.

Demostración: Definamos $\theta := \zeta_m$, $K := \mathbb{Q}(\theta)$ y $A := \mathcal{O}_K$. Es claro que $\mathbb{Z}[\theta] \subseteq A$, pero aún no podemos probar que se alcanza igualdad. Existe un polinomio $h(x) \in \mathbb{Z}[x]$ tal que

$$x^m - 1 = \Phi_m(x)h(x),$$

luego derivaremos a ambos lados para calcular $\mathfrak{d}(\theta)$:

$$mx^{m-1} = \Phi_m'(x)h(x) + \Phi_m(x)h'(x), \qquad m\theta^{m-1} = \Phi_m(\theta)h(\theta)$$
$$m^{[K:\mathbb{Q}]} = \pm \operatorname{Nm}_{K/\mathbb{Q}}\big(\Phi_m(\theta)\big) \operatorname{Nm}_{K/\mathbb{Q}}\big(h(\theta)\big),$$

donde empleamos que $\operatorname{Nm}_{K/\mathbb{Q}}(\theta)$ es una raíz de la unidad, luego es ± 1. Así, sin necesidad de calcular deducimos que $\mathfrak{d}(\theta)\mathbb{Z} \subseteq m^{\phi(m)}\mathbb{Z}$ y sabemos que $\mathfrak{d}(\theta)\theta \subseteq \mathfrak{d}(A/\mathbb{Z})$, por lo que si $p\mathbb{Z} \not\supseteq m$ vemos que $p\mathbb{Z} \not\supseteq \mathfrak{d}(A/\mathbb{Z})$. □

Teorema 8.25: Sea $m > 1$ un entero, entonces:

1. $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times = U_m$.
2. El anillo de enteros de $\mathbb{Q}(\zeta_m)$ es $\mathbb{Z}[\zeta_m]$.
3. Un primo p se ramifica en $\mathbb{Z}[\zeta_m]$ syss $p \mid m$

Demostración:

1. Un elemento $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ necesariamente permuta las raíces m-ésimas primitivas de la unidad, de modo que está determinado por $\sigma(\zeta_m) = \zeta_m^j$, donde j ha de ser un elemento de U_m. Ésto construye un monomorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ en U_m, y como tienen la misma cantidad de elementos, ha de ser un isomorfismo.
2. Ya vimos el caso cuando m es potencia de un primo, así que probaremos el caso general por inducción fuerte. Sea $m = qn$, donde q es potencia de primo y $(n; q) = 1$. Entonces $\mathbb{Q}(\zeta_q)$ y $\mathbb{Q}(\zeta_n)$ son extensiones de $\mathbb{Q}$ linealmente disjuntas y sus discriminantes (respecto a $\mathbb{Z}$) son coprimos (pues son divisibles por distintos primos), así que por el corolario 4.82.1 vemos que su anillo de enteros es $\mathbb{Z}[\zeta_q, \zeta_n] = \mathbb{Z}[\zeta_m]$.
3. Se deduce del mismo corolario. □

Lema 8.26: Sea p primo, n entero tal que $p \nmid n$ y $a \in \mathbb{Z}$ coprimo a p. Entonces $p \mid \Phi_n(a)$ syss el orden de a en U_p es n.

Demostración: $\Longrightarrow$. Como $x^n - 1 = \prod_{d|n} \Phi_d(x)$, se verifica que $\Phi_n(a) \equiv 0 \pmod p$ implica que $a^n \equiv 1 \ (p)$. Sea j el orden de a en U_p, luego $j \mid n$ por lo anterior. Por contradicción supongamos que $j < n$, entonces

$$0 \equiv a^j - 1 \equiv \prod_{d|j} \Phi_d(a) \pmod p,$$

de modo que $\Phi_{d_0}(a) \equiv 0 \ (p)$ para un $d_0 < n$. Es decir,

$$a^n - 1 = \Phi_n(a)\Phi_{d_0}(a) \cdots \equiv 0 \pmod{p^2}.$$

Ahora bien, como $f(a+p) \equiv f(a) \ (p)$ para todo polinomio $f(x)$, vemos que $\Phi_n(a+p) \equiv \Phi_{d_0}(a+p) \equiv 0 \ (p)$, por lo que

$$0 \equiv (a+p)^n - 1 \equiv a^n + npa^{n-1} - 1 \equiv npa^{n-1} \pmod{p^2},$$

pero como $p \nmid na$ ésto último es absurdo.

$\Longleftarrow$. Nuevamente se comprueba que $a^n - 1 \equiv 0 \ (p)$, por lo que $\Phi_d(a) \equiv 0 \ (p)$ para algún $d \mid n$. Pero, por la deducción anterior, vemos que si $d < n$, entonces el orden de a en U_p sería d; luego necesariamente $d = n$. □

En la demostración hemos visto también que $p \nmid \Phi_n(a)$ para a múltiplo de p, así que podemos quitar esa restricción de la hipótesis.

Proposición 8.27: Sea p primo y n entero tal que $p \nmid n$. Entonces, $p \mid \Phi_n(a)$ para algún $a \in \mathbb{Z}$ syss $p \equiv 1 \pmod{n}$.

Demostración: Si $p \mid \Phi_n(a)$, entonces $a^n \equiv 1 \ (p)$ por lo que $n \mid p - 1$ y $p \equiv 1 \ (n)$. Recíprocamente, si $n \mid p - 1$, entonces existe un elemento $a \in U_p$ de orden n, puesto que U_p es un grupo cíclico. □

Ésto permite deducir un caso particular del teorema de Dirichlet:

Corolario 8.27.1: Para $n > 2$, hay infinitos primos p con $p \equiv 1 \pmod{n}$.

Demostración: Sean $p_1, \ldots, p_r$ finitos primos $\equiv 1 \ (n)$. Defínase $M := np_1 \cdots p_r$ y sea $N \in \mathbb{Z}_{\neq 0}$ arbitrario, entonces $\Phi_n(NM) \equiv \Phi_n(0) = \pm 1 \pmod{M}$, por lo que $\Phi_n(NM)$ es coprimo a los p_i's, y luego un divisor primo $q \mid \Phi_n(NM)$ no estaba en la lista y necesariamente satisface que $q \equiv 1 \ (n)$ por la proposición anterior. □

Nótese que como $\Phi_2(x) = x + 1$, ésta demostración engloba la clásica prueba de Euclides.

Lema 8.28: Sea p primo y $n > 2$ entero tal que $p \nmid n$. Sea $\mathfrak{p} \lhd \mathbb{Z}[\zeta_n]$ un primo que contenga a p, entonces las raíces n-ésimas de la unidad son distintas mód$\mathfrak{p}$.

Demostración: Basta probar que para todo $0 < i < n$ se cumple que $1 \not\equiv \zeta_n^i \pmod{p}$ y para ello, basta notar que

$$\prod_{j=1}^{n-1}(x - \zeta_n^j) = \frac{x^n - 1}{x - 1} = 1 + x + \cdots + x^{n-1},$$

lo que aplicándolo en $x = 1$ nos da

$$\prod_{j=1}^{n-1}(1 - \zeta_n^j) = n \not\equiv 0 \pmod{p}. \qquad \square$$

Teorema 8.29: Sea p primo y $n > 2$ entero tal que $p \nmid n$. Sea f el mínimo entero tal que $p^f \equiv 1 \pmod{n}$, entonces (p) se escinde en $g = \phi(n)/f$ primos en $\mathbb{Z}[\zeta_n]$, cada uno con grado de inercia f. En particular, p se escinde completamente (i.e., $f = 1$) syss $p \equiv 1 \ (n)$.

Demostración: Sea $\mathfrak{p} \lhd \mathbb{Z}[\zeta_n]$ primo tal que $\mathfrak{p} \mid (p)$, entonces $k := \mathbb{Z}[\zeta_n]/\mathfrak{p}$ es un cuerpo de característica p y, por lo tanto, admite un endomorfismo de Frobenius $\mathrm{Frob}_k(x) \equiv x^p \pmod{\mathfrak{p}}$ (definido en k) cuyo orden en k es el grado de la extensión $[k : \mathbb{F}_p] = f(\mathfrak{p}/p)$. Si queremos considerar $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tal que al restringir y proyectar en k coincida en Frob_k, notamos que el lema anterior obliga a que $\sigma_p(\zeta_n) = \zeta_n^p$, de modo que

$$\mathrm{Frob}_k^f = \mathrm{Id} \iff \sigma_p^f(\zeta_n) = \zeta_n \iff \zeta_n^{p^f} = \zeta_n \iff p^f \equiv 1 \quad (n).$$

Finalmente, recordando que $e = 1$ (p se escinde) por el teorema 8.25 y aplicando el teorema 4.65.1, vemos que $fg = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ lo que concluye el enunciado. □

Dado un cuerpo numérico K, denotamos por K^+ su clausura real.

Introducir el concepto de *clausura real*.

Proposición 8.30: Dado $n > 2$ entero, $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Demostración: Es fácil probar que $\mathbb{Q}(\zeta_n)$ no es formalmente real (en general, las únicas raíces de la unidad de un cuerpo formalmente real son ± 1), y que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ sí lo es. Basta probar que $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ es una extensión cuadrática para concluir. Para ello, nótese que ζ_n es raíz de $x^2 - (\zeta_n + \zeta_n^{-1})x + 1$. □

Teorema 8.31: Sea $n > 2$ entero. El anillo de enteros de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ es $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Demostración: Definamos $\omega := \zeta_n + \zeta_n^{-1}$. Dado un entero algebraico $\alpha = a_0 + a_1\omega + \cdots + a_N\omega^N \in \mathbb{Q}(\omega)$ con $N \leq \phi(n)/2 - 1$ y con $a_i \in \mathbb{Q}$, podemos suponer sin perdida de generalidad que $a_i \in \mathbb{Z}$ para $i < N$ y $a_N \notin \mathbb{Z}$ (¿por qué?). Podemos eliminar los índices anteriores para reducirnos al caso de $\alpha = a_N\omega^N$ y multiplicamos por ζ_n^N para obtener:

$$\zeta_n^N \alpha = a_N + \binom{N}{1} a_N \zeta_n^2 + \cdots + a_N \zeta_n^{2N},$$

el cual es un entero algebraico, así que yace en $\mathbb{Z}[\zeta_n]$. Como $2N \leq \phi(n)-2 < \phi(n)-1$, entonces $\{1, \zeta_n, \ldots, \zeta_n^{2N}\}$ es un subconjunto de una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n]$, de modo que necesariamente $a_N \in \mathbb{Z}$ como se quería ver. □

§8.2.1 Último Teorema de Fermat para primos regulares.

Teorema 8.32 (Kronecker): Sea α un entero algebraico con conjugados $\alpha = \alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que $|\alpha_i| \leq 1$. Entonces α es una raíz de la unidad.

Demostración: Sea $r > 1$ un entero, definamos

$$f_r(x) := \prod_{i=1}^{n} (x - \alpha_i^r).$$

Nótese que para todo monomorfismo $\sigma\colon K \to \mathbb{C}$, donde $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, se cumple que $\sigma f_r(x) = f_r(x)$, así que $f_r(x) \in \mathbb{Q}[x]$. Más aún, sus coeficientes están generados por los α_i's, así que $f_r(x) \in \mathbb{Z}[x]$.

Como los α_i's tienen valor absoluto ≤ 1, es fácil comprobar que el coeficiente que acompaña a x^j en f_r tiene valor absoluto $\leq \binom{n}{j}$, de modo que hay finitas opciones para f_r, lo que prueba que α tiene finitas potencias distintas, con lo que se concluye que es una raíz de la unidad. □

Proposición 8.33: Sea $p > 2$ primo, y sea $\omega := \zeta_p$. Dado $\epsilon \in \mathbb{Z}[\omega]^\times$, existen $\epsilon' \in \mathbb{Q}(\omega + \omega^{-1})$ y $r \in \mathbb{Z}$, tales que $\epsilon = \omega^r \epsilon'$.

Demostración: Denotemos por $\overline{()}\colon \mathbb{C} \to \mathbb{C}$ la conjugación compleja clásica y nótese que $\omega^{-1} = \bar{\omega}$. Claramente $\bar{\epsilon}$ también es una unidad de $\mathbb{Z}[\omega]$ y así $\alpha := \epsilon/\bar{\epsilon}$ es un entero algebraico cuyos conjugados tienen todos valor absoluto 1 (¿por qué?), por lo que, por el teorema anterior, $\alpha = \pm\omega^m$.

Veremos que $\alpha = +\omega^m$: Por contradicción, si no, entonces escribamos $\epsilon = b_0 + b_1\omega + \cdots + b_{p-1}\omega^{p-1}$ para algunos $b_i \in \mathbb{Z}$. Definiendo $\pi := 1 - \omega$, el cual vimos es un primo, satisface que $\omega \equiv 1 \pmod{\pi}$ y que

$$\epsilon \equiv b_0 + b_1 + \cdots + b_{p-1} \equiv b_0 + b_1\bar{\omega} + \cdots + b_{p-1}\bar{\omega}^{p-1} \equiv \bar{\epsilon} \pmod{\pi},$$

así, $\epsilon \equiv \bar{\epsilon} = -\omega^m\epsilon \equiv -\epsilon\ (\pi)$, con lo que $2\epsilon \equiv 0\ (\pi)$. Ya vimos que $\pi \mid p$, por lo que $2 \notin (\pi)$, por lo que $\epsilon \in (\pi)$, por ser ideal primo, lo que es absurdo pues ϵ es una unidad.

Así $\alpha = \omega^m$ y podemos elegir r tal que $2r \equiv m\ (p)$ y definamos $\epsilon' := \omega^{-r}\epsilon$. Entonces es fácil verificar que $\overline{\epsilon'} = \epsilon'$, por lo que se satisface el enunciado. □

Definición 8.34: Sea p un primo, denotamos por h_p al número de clases de $h_{\mathbb{Z}[\zeta_p]}$. El primo p se dice ***regular*** si $p \nmid h_p$, de lo contrario se dice ***irregular***.

De momento no tenemos muchas técnicas para calcular números de clase y verificar cuáles primos son regulares o no, por lo que los siguientes resultados motivarán ese desarrollo.

Teorema 8.35: El caso I del Último Teorema de Fermat se verifica para primos regulares.

Demostración: El enunciado, escrito a la larga, es el siguiente: no existen soluciones (a, b, c) no triviales de

$$a^p + b^p = c^p, \qquad p \nmid abc,$$

con p primo regular. El caso $p = 3$ ya está cubierto en su totalidad, así que supondremos $p \geq 5$.

Supongamos que $a \equiv b \equiv -c \pmod{p}$, entonces $c^p = a^p + b^p \equiv -2c^p \ (p)$, pero $p \nmid 3c$ lo que es absurdo. Así que podemos reescribir la ecuación, por ejemplo como $a^p + (-c)^p = (-b)^p$ de tal modo que $a \not\equiv b \ (p)$. Desde ahora en adelante trabajaremos en $A := \mathbb{Z}[\zeta_p]$ y denotaremos $\zeta := \zeta_p$.

(i) Veremos que los ideales $(a + \zeta^i b)$ son coprimos con $0 \leq i \leq p - 1$. Por contradicción, sea $\mathfrak{p} \lhd A$ primo tal que

$$a + \zeta^i b \in \mathfrak{p}, \qquad a + \zeta^j b \in \mathfrak{p}, \qquad i \neq j.$$

Entonces $(a+\zeta^i b)-(a+\zeta^j b) = (\zeta^i - \zeta^j)b \equiv 0 \ (\mathfrak{p})$, pero $\zeta^i - \zeta^j = u(1-\zeta)$, donde $u \in A^\times$, así que o bien $\mathfrak{p} = (1 - \zeta)$, o bien $b \in \mathfrak{p}$.

Realizando el mismo razonamiento con

$$\zeta^j(a + \zeta^i b) - \zeta^i(a + \zeta^j b) = (\zeta^i - \zeta^j)a \equiv 0 \pmod{\mathfrak{p}},$$

vemos que o bien $\mathfrak{p} = (1 - \zeta)$, o bien $a \in \mathfrak{p}$. Como a, b son coprimos (en $\mathbb{Z}$, luego también en A), entonces se concluye que $\mathfrak{p} = (1 - \zeta)$.

Empleando ésto, vemos que $a + b \equiv a + \zeta^i b \equiv 0 \ (\mathfrak{p})$ para todo i, pero $\mathfrak{p} \mid p$, así que $a + b \equiv 0 \ (p)$ y $c^p = a^p + b^p \equiv a + b \equiv 0 \ (p)$, lo cual es absurdo.

(ii) Para todo $\alpha \in \mathbb{Z}[\zeta]$ existe $d \in \mathbb{Z}$ tal que $\alpha^p \equiv d \pmod{p}$. En efecto, nótese que si $\alpha = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}$, entonces por el sueño del aprendiz:

$$\alpha^p \equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-1}\zeta^{p-1})^p = b_0^p + b_1^p + \cdots + b_{p-1}^p \pmod{p}.$$

(III) Si $\alpha = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}$ donde algún $b_j = 0$ y si $n \mid \alpha$, entonces $n \mid b_i$ para cada i. Basta notar que como $1+\zeta+\zeta^2+\cdots+\zeta^{p-1} = \Phi_p(\zeta) = 0$, entonces cualquier conjunto de $(p-1)$ elementos de $\{1, \zeta, \ldots, \zeta^{p-1}\}$ es base de A, y luego aplicar cocientes.

Con ésto estamos listos para seguir a la demostración. En primer lugar, considere la igualdad entre ideales:

$$\prod_{i=0}^{p-1}(a + \zeta^i b) = (c)^p,$$

como los ideales $(a+\zeta^i b)$ son coprimos dos a dos por (I), entonces $(a+\zeta^i b) = \mathfrak{a}_i^p$ para algún $\mathfrak{a}_i \lhd A$ distinto. Más aún, como $p \nmid h_p$, se comprueba que $\mathfrak{a}_i$ es principal (¿por qué?), de modo que $\mathfrak{a}_i = (\gamma_i)$. Así que $a + \zeta^i b = u_i \gamma_i^p$ donde $u_i \in A^\times$.

Fijemos $i = 1$ y obviemos los subíndices: $a+\zeta^i b = u\gamma^p$. Por la proposición anterior, $u = \zeta^r u'$ para algún $r \in \mathbb{Z}$, donde $u' \in \mathbb{Q}(\zeta + \zeta^{-1})$. Por (II), vemos que $\gamma^p \equiv d \ (p)$. Así que $a + \zeta b = \zeta^r u' \cdot \gamma^p \equiv \zeta^r u' d \ (p)$, y además

$$a + \zeta^{-1} b = \overline{a + \zeta b} = \zeta^{-r} u' \bar{\gamma}^p \equiv \zeta^{-r} u' \bar{d} = \zeta^{-r} u' d \pmod{p},$$

donde empleamos que $\bar{d} = d$ y $\bar{p} = p$. Con esto concluimos que $\zeta^r(a+\zeta^{-1}b) \equiv \zeta^{-r}(a + \zeta b) \ (p)$, o equivalentemente:

$$a + \zeta b - \zeta^{2r} a - \zeta^{2r-1} b \equiv 0 \pmod{p}. \tag{8.2}$$

Como $p \geq 5$ por hipótesis, tenemos que la propiedad (III) implicaría que $p \mid ab$ si los números $\{1, \zeta, \zeta^{2r}, \zeta^{2r-1}\}$ fuesen todos distintos, así que no lo son, pero $1 \neq \zeta$ y también $\zeta^{2r} \neq \zeta^{2r-1}$, lo que nos deja:

(a) $\underline{1 = \zeta^{2r}}$: La ecuación (8.2) ahora queda como $a + \zeta b - a - \zeta^{-1} b = \overline{\zeta b - \zeta^{-1} b} \equiv 0 \ (p)$, por lo que, por la propiedad (III) vemos que $p \mid b$ lo que es absurdo.

(b) $\underline{1 = \zeta^{2r-1}, \text{ o equivalentemente, } \zeta = \zeta^{2r}}$: La ecuación (8.2) ahora queda como $a+\zeta b-\zeta a-b = a-b+\zeta(b-a) \equiv 0 \ (p)$, por lo que, la propiedad (III) implica que $a \equiv b \ (p)$, pero ésto es absurdo por lo mencionado al comienzo de la demostración.

(c) $\underline{\zeta = \zeta^{2r-1}, \text{ o } \zeta^{2r} = \zeta^2}$: La ecuación (8.2) ahora queda como $a + \zeta b - \zeta^2 a - \zeta b = a - \zeta^2 a \equiv 0 \ (p)$, por lo que, por la propiedad (III) vemos que $p \mid a$ lo que es absurdo. □

8.3 Caracteres

La noción general que estamos estudiando es la siguiente:

Definición 8.36: Dado un grupo G llamamos su ***grupo dual*** a $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$.

Proposición 8.37: Sean G, H dos grupos abelianos.

1. $\widehat{G \times H} \cong \hat{G} \times \hat{H}$.
2. Si G es finito, entonces $\hat{G} \cong G$.

Demostración:

1. Dados $\chi \in \hat{G}, \psi \in \hat{H}$ podemos definir

$$\begin{aligned} \chi \cdot \psi \colon G \times H &\longrightarrow \mathbb{C}^\times \\ (a, b) &\longmapsto \chi(a)\psi(b). \end{aligned}$$

   Y luego definir $\Phi \colon \hat{G} \times \hat{H} \to \widehat{G \times H}$ dado por $\Phi(\chi, \psi) := \chi \cdot \psi$. Queda al lector verificar que Φ es un isomorfismo.

2. Como todo grupo abeliano finito es un producto de grupos cíclicos (finitos), basta probar que $\hat{C}_n \cong C_n$. En notación aditiva, nótese que para todo $a \in C_n$ y todo $\chi \in \hat{C}_n$ se cumple que $\chi(a) = \chi(a \cdot 1) = \chi(1)^a$, así que χ está completamente determinado por su valor en 1. Como 1 tiene orden n en C_n, se comprueba que $\chi(1)$ es una raíz n-ésima de la unidad, luego $\chi(1) = \zeta_n^{j_\chi}$ para un único entero j_χ módulo n; ésto determina el isomorfismo. □

Pese a que al inicio del capítulo fijamos ζ_n como una raíz n-ésima primitiva de la unidad bien específica, nótese que hay una elección detrás de ésta raíz, de modo que el isomorfismo no es canónico.

Proposición 8.38: Para todo grupo abeliano finito G se cumple que $\hat{\hat{G}} \cong G$.

Demostración: Fijado $g \in G$ definamos el siguiente homomorfismo:

$$\mathrm{ev}_g \colon \hat{G} \longrightarrow \mathbb{C}^\times$$

$$\chi \longmapsto \chi(g),$$

y nótese que $\mathrm{ev}_g \in \hat{\hat{G}}$. Ésto determina un homomorfismo $\Phi := \mathrm{ev}_- : G \to \hat{\hat{G}}$. Sea $H := \ker \Phi$, entonces $\hat{G}$ actúa fielmente sobre G/H mediante $\chi \cdot g := \mathrm{ev}_g(\chi) = \chi(g)$, pero por la proposición anterior $|\hat{G}| = |G| \leq |G/H|$, de modo que necesariamente $|H| = 1$ y Φ es inyectivo. Finalmente, empleando que $|\hat{\hat{G}}| = |\hat{G}| = |G|$ obtenemos que Φ es un isomorfismo. □

Definición 8.39: Sea G un grupo abeliano y $H \leq G$, definimos su ***complemento ortogonal***

$$H^\perp := \{\chi \in \hat{G} : \ker \chi \supseteq H\} \leq \hat{G}.$$

Proposición 8.40: Sea G un grupo abeliano y $H \leq G$. Se cumple que

$$H^\perp \cong \widehat{G/H}, \qquad \hat{H} \cong \hat{G}/H^\perp, \qquad (H^\perp)^\perp \cong H.$$

Demostración: Sea $\pi : G \to G/H$ la proyección canónica, el primer isomorfismo viene dado por

$$\begin{aligned} \widehat{G/H} &\longrightarrow H^\perp \\ \chi &\longmapsto \pi \circ \chi. \end{aligned}$$

El segundo viene de que el siguiente homomorfismo

$$\begin{aligned} \rho_H : \hat{G} &\longrightarrow \hat{H} \\ \chi &\longmapsto \chi|_H, \end{aligned}$$

tiene núcleo $H^\perp$ y falta probar la suprayectividad. Y el tercero viene del primero empleando que $\hat{\hat{G}} \cong G$. □

Cabe destacar que todos los isomorfismos son canónicos.

Definición 8.41: Un ***caracter de Dirichlet*** módulo n es un elemento $\chi \in \hat{U}_n$, es decir, un homomorfismo de grupos $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. Si $n \mid m$, entonces χ puede verse como un caracter módulo m mediante la composición:

$$U_m \twoheadrightarrow U_n \xrightarrow{\chi} \mathbb{C}^\times,$$

así que llamaremos ***conductor***, denotado f_χ, al mínimo entero f tal que χ es un caracter módulo f. Un caracter de Dirichlet módulo n se dice

primitivo si su conductor es n. Si $f_\chi \mid n$, decimos que χ tiene ***periodo*** n.

Nótese que el nombre *periodo* tiene sentido puesto que si $a \in U_n$ con $f_\chi \mid n$, entonces $\chi(a+n) = \chi(a)$.

Ejemplo.

- Para todo $n > 1$, nótese que podemos definir el caracter dado por el homomorfismo trivial, que es aquel que $\chi(a) = 1$ para todo $a \in U_n$. Éste caracter es el único de conductor 1.
- Es fácil comprobar que todo caracter de Dirichlet tiene por codominio a un grupo de raíces de la unidad. Luego si $\chi\colon U_n \to \mathbb{C}^\times$ es un caracter, podemos componerlo por la conjugación compleja y dar un caracter $\bar{\chi}(a) := \overline{\chi(a)} = \chi(a)^{-1}$.
- Fijemos $U_6 = \{1, 5\}$, de modo que podemos definir un caracter módulo 6 como $\chi(1) = 1$ y $\chi(5) = \chi(-1) = -1$. Es fácil comprobar que $f_\chi = 3$.

Definición 8.42: Sean χ, ψ dos caracteres de Dirichlet primitivos módulo n, m resp. Entonces sea

$$\begin{aligned} \gamma\colon U_{\mathrm{mcm}(n,m)} &\longrightarrow \mathbb{C}^\times \\ a &\longmapsto \chi(a)\psi(a). \end{aligned}$$

Denotamos por $\chi \cdot \psi$ al caracter primitivo asociado a γ.

Si $\chi\colon U_n \to \mathbb{C}^\times$ es un caracter de Dirichlet, entonces claramente $\chi \cdot \bar{\chi}$ es el caracter trivial. Ésto prueba que los caracteres de Dirichlet, con la operación $\cdot$ descrita anteriormente forman un grupo.

También es fácil comprobar que cuando n, m son coprimos, entonces ésta operación coincide con aquella que dimos en la prueba de que $\widehat{G \times H} \cong \hat{G} \times \hat{H}$, así que dado un caracter $\chi \in \hat{U}_n$ podemos expresarlo como

$$\chi = \prod_{p \mid n} \chi_p,$$

donde χ_p es un caracter módulo p^a, donde $a = \nu_p(n)$.

Definición 8.43: Un ***caracter de Galois*** es un homomorfismo de grupos $\chi\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to \mathbb{C}^\times$; claramente los caracteres de Dirichlet y de Galois están en biyección canónica, de modo que obviaremos apellidos. Si

χ es un caracter, entonces $\ker\chi$ es un grupo de automorfismos de $\mathbb{Q}(\zeta_n)$ y llamamos su ***cuerpo asociado*** al cuerpo fijado por $\ker\chi$.

Dado X un grupo finito de caracteres (i.e., un conjunto no vacío cerrado bajo $\cdot$ y $()^{-1}$), entonces sea n el mínimo común múltiplo de los conductores de los caracteres de X; luego podemos definir $H := \bigcap_{\chi\in X}\ker\chi \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ y luego el cuerpo fijado por dicho H se dice el ***cuerpo asociado*** al grupo X.

Claramente los caracteres de Dirichlet están en biyección canónica con los caracteres de Galois, pero identificar a los caracteres de una manera o de otra será útil más adelante.

Si X es un grupo de caracteres de Dirichlet, denotamos

$$X_p := \{\chi_p : \chi \in X\}.$$

Ahora procedemos a construir una biyección entre subgrupos de X y subcuerpos de K. Sea $L \subseteq K$ un subcuerpo, entonces definamos

$$\begin{aligned} H_L &:= \{\chi \in X : \ker\chi \supseteq \mathrm{Gal}(K/L)\} \\ &= \mathrm{Gal}(K/L)^\perp \cong \left(\frac{\mathrm{Gal}(K/\mathbb{Q})}{\mathrm{Gal}(K/L)}\right)^\wedge \cong \widehat{\mathrm{Gal}(L/\mathbb{Q})}. \end{aligned}$$

Recíprocamente, si $H \leq X$, entonces definimos

$$H^\perp := \{g \in \mathrm{Gal}(K/\mathbb{Q}) : \forall\chi \in H \quad \chi(g) = 1\},$$

y el subcuerpo L correspondiente es el subcuerpo fijado por $H^\perp$. Ésto comprueba:

Proposición 8.44: Sea X un grupo finito de caracteres con cuerpo asociado K. Existe una biyección entre subgrupos $G \leq X$ y subcuerpos $\mathbb{Q} \subseteq L \subseteq K$.

Teorema 8.45: Sea X un grupo finito de caracteres de Dirichlet con cuerpo asociado K. Para todo primo $p \in \mathbb{Z}$, su índice de ramificación en $\mathcal{O}_K$ es $e = |X_p|$.

Referencias

108. WASHINGTON, L. C. *Introduction to Cyclotomic Fields Graduate Texts in Mathematics* **83** (Springer-Verlag New York, 1982).

Parte II.

Geometría diofántica

9

Alturas

9.1 Alturas en el espacio proyectivo

Definición 9.1: Sea K un cuerpo global. Dado un punto proyectivo $P := [x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n_{K^{\text{alg}}}$, supongamos que $P \in \mathbb{P}^n_L$ (para L/K una extensión finita) y definamos su ***altura***:

$$h(P) = \sum_{v \in M_L} \max_j \{\log |x_j|_v\}.$$

A la función $h(\boldsymbol{x})$ se le llama ***altura logarítmica absoluta*** y a la función $H(\boldsymbol{x}) := e^{h(\boldsymbol{x})}$ le llamamos ***altura multiplicativa***.

Lema 9.2: Sea K un cuerpo global y $P \in \mathbb{P}^n_{K^{\text{alg}}}$. El valor de $h(P)$ no depende ni de la representación del punto, ni de la extensión de cuerpos.

Demostración: Sea $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n_L$ para una extensión finita L/K y sea $L' \supseteq L$ otra extensión finita. Entonces, aplicando el teorema 6.26, tenemos:

$$\sum_{w \in M_{L'}} \max_j \{\log |x_j|_w\} = \sum_{v \in M_L} \sum_{w|v} \max_j \{\log |x_j|_v\}.$$

Sea $\lambda \in L^\times$ de modo que $[x_0 : \cdots : x_n] = [\lambda x_0 : \cdots : \lambda x_n]$, entonces:

$$\sum_{v \in M_L} \max_j \{\log |\lambda x_j|_v\} = \sum_{v \in M_L} \log |\lambda|_v + \sum_{v \in M_L} \log |x_j|_v = h(P),$$

donde empleamos la fórmula del producto. □

Esto también induce una función de alturas sobre el espacio afín $\mathbb{A}^n_{K^{\mathrm{alg}}}$ empleando el encaje

$$(x_1, \ldots, x_n) \longmapsto [1 : x_1 : \cdots : x_n].$$

En particular, denotando $\log^+ t := \max\{0, \log t\}$ extendida por $\log^+(0) := 0$, entonces se sigue que la altura en el espacio afín es

$$\boldsymbol{x} := (x_1, \ldots, x_n) \in \mathbb{A}^n_L \quad h(\boldsymbol{x}) = \sum_{v \in M_L} \max_j \{\log^+ |x_j|_v\};$$

y, más en particular, la altura de un elemento separable $\alpha \in K^{\mathrm{sep}}$ es

$$h(\alpha) = \sum_{v \in M_L} \log^+ |\alpha|_v,$$

donde L/K es una extensión finita separable tal que $\alpha \in L$.

Un par de cálculos explícitos:

Proposición 9.3: Se cumplen:

1. Sea $x = a/b \in \mathbb{Q}^\times$ con a, b coprimos. Entonces $h(x) = \log \max\{|a|, |b|\}$.
2. Sea K un cuerpo numérico y $\alpha, \beta \in K$ con $\alpha\beta \neq 0$. Entonces:

$$h(\alpha/\beta) = \sum_{v \in M_K} \log^+ \max\{|\alpha|_v, |\beta|_v\}.$$

Si, además, α, β son enteros algebraicos, entonces

$$h(\alpha/\beta) \leq \sum_{v \in S_\infty} \log \max\{|\alpha|_v, |\beta|_v\} = \sum_{\sigma\colon K \to \mathbb{C}} \log \max\{|\sigma\alpha|, |\sigma\beta|\}.$$

Demostración:

1. Para el primero basta notar que si $a = p^r m$ con $p \nmid m$, entonces $|a|_p = p^{-r}$, de modo que $\log^+ |a|_p = 0$. Para b^{-1} tenemos que $\log^+ |b^{-1}|_\infty = 0$ y sobreviven el resto de valores.

2. Basta notar que $\max\{|\alpha/\beta|_v, 1\} = |\beta|_v^{-1} \max\{|\alpha|_v, |\beta|_v, 1\}$, de modo que

$$h(\alpha/\beta) = \sum_{v\in M_K} \log^+ \max\{|\alpha|_v, |\beta|_v\} - \log\left(\prod_{v\in M_K} |\beta|_v\right),$$

donde el segundo factor se anula por la fórmula del producto.

Si α, β son enteros algebraicos, entonces $\log \max\{|\alpha|_v, |\beta|_v\} \leq 0$ para todo lugar finito, de modo que sólo sobreviven los lugares al infinito. □

Teorema 9.4 (Kronecker): La altura de $\zeta \in (\mathbb{Q}^{\mathrm{alg}})^\times$ es 0 syss ζ es una raíz de la unidad.

El teorema de Kronecker es particular de $\mathbb{Q}$, más allá de su mera demostración.

Proposición 9.5: Sea K un cuerpo global y $P_1, P_2, \ldots, P_r \in \mathbb{A}^n_{K^{\mathrm{alg}}}$ puntos en el espacio afín. Entonces

$$h(P_1 + \cdots + P_r) \leq \begin{cases} \sum_{i=1}^n h(P_i), & \operatorname{car} K > 0 \\ \sum_{i=1}^n h(P_i) + \log r, & \operatorname{car} K = 0. \end{cases}$$

Demostración: Sean $P_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ y sea L/K una extensión finita tal que cada $P_i \in \mathbb{A}^n_L$. Por definición

$$h(P_1 + \cdots + P_r) = \sum_{v\in M_L} \max_j \{\log^+ |x_{1j} + x_{2j} + \cdots + x_{rj}|_v\}.$$

Vamos a acotar el último término según casos:

(a) Si v es ultramétrico:

$$|x_{1j} + x_{2j} + \cdots + x_{nj}|_v \leq \max_i \{|x_{ij}|_v\}.$$

(b) Si v es arquimediano:

$$|x_{1j} + x_{2j} + \cdots + x_{nj}|_v \leq |r|_v \max_i \{|x_{ij}|_v\}.$$

Agrupando los lugares arquimedianos, tenemos que

$$\sum_{v|\infty} \log |r|_v = \log |r|_\infty = \log r;$$

finalmente los dos casos del enunciado se deducen del hecho de que un cuerpo global posee lugares arquimedianos syss tiene característica 0. □

Proposición 9.6: Sea $P \in \mathbb{P}^n_{\mathbb{Q}^{\mathrm{alg}}}$. Entonces, para todo automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ se cumple que $h(P) = h(\sigma(P))$.

Lema 9.7: Sea K un cuerpo global, $\alpha \in K^{\mathrm{alg}}$ y $\lambda \in \mathbb{Q}$ un exponente. Entonces $h(\alpha^\lambda) = |\lambda| h(\alpha)$ y, en particular, $h(\alpha^{-1}) = h(\alpha)$.

Demostración: Si $\lambda > 0$ entonces se sigue de la definición, por tanto, basta probar el caso $\lambda = -1$. Sea L/K una extensión finita tal que $\alpha \in L^\times$. Para todo lugar $v \in M_L$ se tiene la siguiente fórmula:

$$\log |\alpha|_v = \log^+ |\alpha|_v - \log^+ |1/\alpha|_v$$

(¿por qué?), de modo que si sumamos sobre todos los lugares, por fórmula del producto tendremos que $0 = h(\alpha) - h(1/\alpha)$ como se quería probar. □

Corolario 9.7.1 (desigualdad fundamental): Sea K un cuerpo global y $S \subseteq M_K$ un conjunto finito de lugares. Para todo $\alpha \in K^\times$ se tiene que

$$-h(\alpha) \leq \sum_{v \in S} \log |\alpha|_v \leq h(\alpha).$$

Teorema 9.8 (desigualdad de Liouville): Sea L/K una extensión de cuerpos globales, $S \subseteq M_L$ un conjunto finito de lugares y sean $\alpha \in L, \beta \in K$ distintos. Entonces

$$(2H(\alpha)H(\beta))^{-[L:K]} \leq \prod_{w \in S} \|\alpha - \beta\|_w \leq (2H(\alpha)H(\beta))^{[L:K]}.$$

Demostración: Basta aplicar la proposición 9.5 seguido de la desigualdad fundamental. □

Definición 9.9: Sea K un cuerpo global y sea

$$f(t_1, \ldots, t_n) = f(\boldsymbol{t}) = \sum_\alpha c_\alpha \boldsymbol{t}^\alpha \in K[\boldsymbol{t}],$$

en notación multiíndice. Definimos su ***altura***

$$h(f) := \sum_{v \in M_K} \log |f|_v, \qquad |f|_v := \max_{\alpha}\{|c_\alpha|_v\}.$$

Nótese que $|f|_v = \|f\|_{(1,\dots,1)}$, en notación de §5.3.1, de modo que tenemos que $|fg|_v = |f|_v\,|g|_v$ por el teorema 5.49.

Lema 9.10: Sea K un cuerpo global y considere el ***encaje de Segre*** dado por

$$\begin{aligned} \sigma\colon \mathbb{P}^n_{K^{\mathrm{alg}}} \times \mathbb{P}^m_{K^{\mathrm{alg}}} &\longrightarrow \mathbb{P}^{(n+1)(m+1)-1}_{K^{\mathrm{alg}}} \\ (\boldsymbol{x}, \boldsymbol{y}) &\longmapsto \boldsymbol{x} \otimes \boldsymbol{y} := [x_i y_j]_{ij}, \end{aligned}$$

donde los pares (i,j) se ordenan lexicográficamente. Entonces

$$h(\boldsymbol{x} \otimes \boldsymbol{y}) = h(\boldsymbol{x}) + h(\boldsymbol{y}).$$

Demostración: Basta notar que $\max_{i,j}\{|x_i y_j|_v\} = \max_i\{|x_i|_v\}\cdot\max_j\{|y_j|_v\}$. □

Proposición 9.11: Sea K un cuerpo global y $f(t_1,\dots,t_n), g(s_1,\dots,s_m)$ polinomios en variables disjuntas. Entonces

$$h(f \cdot g) = h(f) + h(g).$$

Para estudiar $|f|_v$ con v arquimediano es necesario introducir un nuevo concepto:

Definición 9.12: Sean K un cuerpo numérico, $f(t_1,\dots,t_n) \in K[\boldsymbol{t}]$ un polinomio y fijemos $\sigma\colon K \hookrightarrow \mathbb{C}$ un monomorfismo. Entonces la ***medida de Mahler*** de f es:

$$M_\sigma(f) := \exp\left(\int_{\mathbb{T}^n} \log |f(e^{\mathrm{i}\theta_1},\dots,e^{\mathrm{i}\theta_n})|_v \,\mathrm{d}\mu_1 \cdots \mathrm{d}\mu_n\right),$$

donde $\mathbb{T} := \mathbb{S}^1 = \{e^{\mathrm{i}\theta} : 0 \le \theta \le 2\pi\}$ es la circunferencia unitaria con la medida $\mathrm{d}\mu = (1/2\pi)\mathrm{d}\theta$.

Nótese que no ponemos un subíndice al valor absoluto; esto se debe a que $\mathbb{C}$ ya se considera un cuerpo métrico *per se*, del mismo modo en que se presupone el valor absoluto sobre $\mathbb{Q}_p$.

Las siguientes dos propiedades son sencillas de probar, la segunda siendo un mero cálculo.

Lema 9.13: Sea K un cuerpo numérico.

1. Para todo $f, g \in K[\boldsymbol{t}]$ tenemos que $M(fg) = M(f)\,M(g)$.
2. Para todo $\alpha \in K$ tenemos que $M(t-\alpha) = \log^+ |\alpha|_v$.

Empleando el carácter multiplicativo y la factorización de términos lineales tenemos:

Proposición 9.14 (fórmula de Jensen): Sea K un cuerpo numérico y

$$f(t) = c(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n) \in K[t].$$

Entonces

$$\log M(f) = \log|c| + \sum_{j=1}^{n} \log^+ |\alpha_j|.$$

Proposición 9.15: Sea $\alpha \in \mathbb{Q}^{\mathrm{alg}}$ y sea $f(t) \in \mathbb{Z}[t]$ el polinomio minimal de α (donde limpiamos denominadores para obtener un polinomio primitivo). Entonces

$$\log M(f) = \deg\alpha \cdot h(\alpha),$$

en particular,

$$\log|\operatorname{Nm}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|_\infty \leq \deg\alpha \cdot h(\alpha).$$

Demostración: Sea $d := \deg\alpha$, sea K la clausura normal de $\mathbb{Q}(\alpha)$ y sea

$$f(t) = c(t-\alpha_1)\cdots(t-\alpha_d) \in K[t].$$

Si $G := \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_m\}$, entonces la lista $\{\sigma_1\alpha, \ldots, \sigma_m\alpha\}$ cuenta cada conjugado de α exactamente $[K:\mathbb{Q}]/d$ veces. Empleando que $|gh|_v = |g|_v\,|h|_v$ (teo. 5.49) tenemos que:

$$|c|_v \prod_{\sigma\in G} \max\{1, |\sigma\alpha|_v\}^{\frac{d}{[K:\mathbb{Q}]}} = 1$$

para todo lugar finito $v \in M_K \smallsetminus S_\infty$.

Por la proposición 9.6 tenemos que

$$[K:\mathbb{Q}]h(\alpha) = \sum_{\sigma\in G}\sum_{v\in M_K} \log^+ |\sigma\alpha|_v$$

$$
\begin{aligned}
&= \sum_{v|\infty} \sum_{\sigma\in G} \log^+ |\sigma\alpha|_v - \frac{[K:\mathbb{Q}]}{d} \sum_{v\nmid\infty} \log |c|_v \\
&= \frac{[K:\mathbb{Q}]}{d} \sum_{v|\infty} \left(\log |c|_v + \sum_{j=1}^{d} \log^+ |\alpha_j|_v \right), \\
&= \frac{[K:\mathbb{Q}]}{d} \sum_{\sigma\in \mathrm{Hom}(K,\mathbb{C})} \log M_\sigma(f) = \frac{[K:\mathbb{Q}]}{d} \log M(f).
\end{aligned}
$$

donde en la tercera línea hemos empleado la fórmula del producto y en la cuarta hemos empleado la fórmula de Jensen.

Para la parte de «en particular» empleamos que

$$
\sum_{v|\infty} \sum_{j=1}^{d} \log^+ |\alpha_j|_v = \log |\,\mathrm{Nm}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|_\infty. \qquad \square
$$

Como ejercicio, ¿dónde se empleó que $f(t)$ sea primitivo?

Definición 9.16: Sea $f(t) = \sum_{j=0}^{d} a_j x^j \in \mathbb{C}[t]$ un polinomio de una variable. Para $p \in [1,\infty) \subseteq \mathbb{R}$ definimos la ***norma*** ℓ_p:

$$
\ell_p(f) := \left(\sum_{j=0}^{d} |a_j|^p \right)^{1/p}, \qquad \ell_\infty(f) := \max_j \{|a_j|\} = |f|_\infty.
$$

Lema 9.17: Sea $f(t) = \sum_{j=0}^{d} a_j x^j \in \mathbb{C}[t]$ con $a_d \neq 0$. Entonces $M(f) \leq \ell_1(f)$ y, más aún,

$$
\binom{d}{\lfloor d/2 \rfloor}^{-1} \ell_\infty(f) \leq M(f) \leq \ell_2(f) \leq \sqrt{d+1}\,\ell_\infty(f).
$$

Demostración: Basta notar que $|f(e^{\mathrm{i}\theta})| \leq \ell_1(f)$ por desigualdad triangular para poder comprobar que $M(f) \leq \ell_1(f)$.

Empleando la desigualdad de Jensen (cfr. **[2]** teo. 9.23) se concluye que

$$
M(f) \leq \left(\int_{\mathbb{T}} |f(e^{\mathrm{i}\theta})|^2 \,\mathrm{d}\mu \right)^{1/2},
$$

y por la identidad de Parseval, tenemos que

$$
\ell_2(f) = \left(\sum_{j=0}^{d} |a_j|^2 \right)^{1/2} \leq \sqrt{d+1}\,\ell_\infty(f).
$$

Finalmente, factorizando

$$f(t) = a_d(t-\gamma_1)\cdots(t-\gamma_d) \in \mathbb{C}[t],$$

concluimos que, en notación multiíndice,

$$\left|\frac{a_r}{a_d}\right| = \left|\sum_{|\alpha|=r} \boldsymbol{\gamma}^\alpha\right| \leq \binom{d}{r} \prod_{j=0}^{d} \text{máx}\{1, |\gamma_j|\}.$$

Finalmente, por fórmula de Jensen

$$|a_r| \leq \binom{d}{r} M(f) \implies \ell_\infty(f) \leq \binom{d}{\lfloor d/2 \rfloor} M(f). \qquad \square$$

Teorema 9.18 – *Teorema de finitud de Northcott*: Dado $d \in \mathbb{N}$ y $r \geq 0$, entonces existen finitos números algebraicos $\alpha \in \mathbb{Q}^{\text{alg}}$ tales que $\deg \alpha \leq d$ y $h(\alpha) \leq r$. Más generalmente, existen finitos puntos proyectivos $P \in \mathbb{P}^n_{\mathbb{Q}^{\text{alg}}}$ con $h(P) \leq r$ y $\deg P \leq d$.

Nótese que es necesario acotar el grado, de lo contrario, las raíces de la unidad (que son infinitas) tienen altura 0.

Demostración: Sea α algebraico de grado d y $h(\alpha) \leq r$. Definiendo $H := e^r$, si $f(t) = \sum_{j=1}^{d} a_j x^j \in \mathbb{Z}[t]$ es el polinomio minimal de α, entonces $M(f) = H^d$. Por las desigualdades anteriores, tenemos que $\text{máx}_j\{|a_j|\} \leq 2^d M(f)$, de modo que los coeficientes de f están acotados por $(2H)^d$. Como f tiene $d+1$ coeficientes enteros, esto da lugar a

$$\left(2\lfloor (2H)^d \rfloor + 1\right)^{d+1}$$

polinomios, cada uno con a lo más d raíces, lo que da un total de

$$d\left(2\lfloor (2H)^d \rfloor + 1\right)^{d+1} \leq (5H)^{d^2+d}$$

posibilidades para α.

La parte de «más generalmente» se sigue trivialmente. $\square$

La demostración da una cota para la cantidad de puntos, pero se puede mejorar bastante.

Teorema 9.19 (Schanuel): Sea K un cuerpo numérico, sea $X \geq 0$ un número real y sea N_X la cantidad de puntos $x \in \mathbb{P}^{n-1}(K)$ tales que $H(x) \leq X$. Entonces

$$N_X = \frac{h}{\zeta_K(n)} c_n X^{nd} + \begin{cases} O(X \log X), & (d,n) = (1,2), \\ O(X^{nd-1}), & (d,n) \neq (1,2). \end{cases}$$

Donde

$$c_n := \left(\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|\Delta|}} \right)^n \frac{R}{w} n^r,$$

donde $d := [K : \mathbb{Q}]$ es el grado de la extensión, donde r_1, r_2 denotan la cantidad de lugares reales y complejos de K resp., donde $r := r_1 + r_2 - 1$ es el rango de las unidades, donde w es la cantidad de raíces de la unidad en K, y donde R, Δ, h son el regulador, el discriminante y el número de clases de $\mathcal{O}_K$ resp.

Lema 9.20: Sea $f(t_1, \ldots, t_n) \in \mathbb{C}[\boldsymbol{t}]$ un polinomio complejo multivariable y sea $d_j := \deg_{t_j}(f)$. Entonces:

$$M(f) \prod_{j=1}^{n} (d_j + 1)^{-1/2} \leq \ell_\infty(f) \leq M(f) \prod_{j=1}^{n} \binom{d_j}{\lfloor d_j/2 \rfloor}.$$

Demostración: La segunda desigualdad se demuestra igual que en el lema 9.17. Para la primera procedemos por inducción, escribiendo

$$f(\boldsymbol{t}, s) = \sum_{j=0}^{d_{n+1}} g_j(\boldsymbol{t}) s^j.$$

Por definición, tenemos que

$$\log M_{\boldsymbol{t},s}(f) := \int_{\mathbb{T}^n} \log M_s\big(f(e^{\mathrm{i}\theta_1}, \cdots, e^{\mathrm{i}\theta_n}, s)\big) \, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_n.$$

Y, por el lema 9.17 obtenemos

$$\begin{aligned} \log M(f) &\geq \int_{\mathbb{T}^n} \log \max_j \left\{ g_j(e^{\mathrm{i}\theta_1}, \cdots, e^{\mathrm{i}\theta_n}) \right\} \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_n - \log \binom{d_{n+1}}{\lfloor d_{n+1}/2 \rfloor} \\ &\geq \max_j \left\{ \int_{\mathbb{T}^n} \log g_j(e^{\mathrm{i}\theta_1}, \cdots, e^{\mathrm{i}\theta_n}) \, \mathrm{d}\mu_1 \cdots \mathrm{d}\mu_n \right\} - \log \binom{d_{n+1}}{\lfloor d_{n+1}/2 \rfloor}, \end{aligned}$$

de esto se concluye que

$$\binom{d_{n+1}}{\lfloor d_{n+1}/2 \rfloor} M(f) \geq \max_j \{M(g_j)\}$$

y concluimos por hipótesis inductiva. □

Lema 9.21: Sean $a \leq A, b \leq B$ y d números naturales. Entonces

$$\binom{A}{a}\binom{B}{b} \leq \binom{A+B}{a+b}, \qquad \binom{d}{\lfloor d/2 \rfloor}\sqrt{d+1} \leq 2^d.$$

Demostración: La primera desigualdad es una consecuencia de la identidad

$$(1+t)^A(1+t)^B = (1+t)^{A+B}.$$

Para la segunda desigualdad procedemos por inducción. Los casos $d = 0$ y $d = 1$ son triviales. Definiendo $C_d := \binom{d}{\lfloor d/2 \rfloor}\sqrt{d+1}$ se tiene que

$$\frac{C_{2m+1}}{C_{2m}} = 2\left(1 - \frac{1}{2m+2}\right)^{1/2} < 2, \quad \frac{C_{2m+2}}{C_{2m}} = 4\left(1 - \frac{1}{(2m+2)^2}\right)^{1/2} < 4.$$

Empleando estos dos casos se concluye la hipótesis inductiva. □

Lema 9.22 (Gelfond): Sean $g_1, \ldots, g_r \in \mathbb{C}[t_1, \ldots, t_n]$ y sea $f := g_1 \cdots g_r$. Entonces

$$2^{-d} \prod_{j=1}^{r} \ell_\infty(g_j) \leq \ell_\infty(f) \leq 2^d \prod_{j=1}^{r} \ell_\infty(g_j),$$

donde $d = \sum_{i=1}^{n} \deg_{t_i}(f)$.

Demostración: Sea $d_{ji} := \deg_{t_i}(g_j)$. Entonces, por inducción es fácil comprobar que

$$\ell_\infty(f) \leq C \prod_{j=1}^{r} \ell_\infty(g_j),$$

donde

$$C = \prod_{j=1}^{r-1} \prod_{i=1}^{n} (1 + d_{ji}) \leq 2^d.$$

Para la otra desigualdad, empleamos el lema 9.20 para obtener que

$$\prod_{j=1}^{r} \ell_\infty(g_j) \leq \left(\prod_{j=1}^{r} \prod_{i=1}^{n} \binom{d_{ji}}{\lfloor d_{ji}/2 \rfloor} \right) \left(\prod_{i=1}^{n} (1 + \textstyle\sum_{j=1}^{r} d_{ji})^{1/2} \right) \ell_\infty(f)$$
$$\leq \prod_{i=1}^{n} 2^{\deg_{t_i}(f)} \ell_\infty(f) = 2^d \ell_\infty(f). \qquad \square$$

Combinando el lema de Gelfond junto con el hecho de que $|f \cdot g|_v = |f|_v \, |g|_v$ (teo. 5.49) tenemos el siguiente resultado:

Teorema 9.23: Sean $g_1, \ldots, g_r \in \mathbb{Q}^{\mathrm{alg}}[t_1, \ldots, t_n]$, sea $f := g_1 \cdots g_r$ y sea $d := \sum_{i=1}^{n} \deg_{t_i}(f)$. Entonces

$$-d \log 2 + \sum_{j=1}^{r} h(g_j) \leq h(f) \leq d \log 2 + \sum_{j=1}^{r} h(g_j).$$

Notas históricas

El teorema de Northcott fue demostrado, en mayor generalidad, en Northcott [**46**] (1949).

La altura de los polinomios y la medida de Mahler fueron introducidas en Mahler [**41**] (1962). Relacionado a la medida de Mahler se incluye el siguiente resultado, conocido como la conjetura de D. H. Lehmer [**40**] (1933):

Para todo $\alpha \in (\mathbb{Q}^{\mathrm{alg}})^\times$ sea $f(t) \in \mathbb{Z}[t]$ su polinomio minimal y definamos $M(\alpha) := M(f)$. La proposición anterior indica que $M(\alpha) = H(\alpha)^{\deg \alpha}$.

Conjetura de Lehmer 9.24: Existe una constante $c > 1$ tal que para todo $\alpha \in (\mathbb{Q}^{\mathrm{alg}})^\times$ que no sea raíz de la unidad se tenga $M(\alpha) \geq c$.

La conjetura de Lehmer fue recientemente demostrada por Verger-Gaugry [**63**] (2017) quien encontró por constante $c = 1{,}016126...$

10

Geometría de los números

Éste capítulo pretende explorar varios tópicos en simultáneo. En primera instancia y tal como señala el título, queremos introducir la técnica de la *geometría de los números* de Minkowski, la cual es hoy estándar en cualquier libro moderno de teoría de números. Ésta disciplina ha tomado varias formas con el pasar del tiempo, pero nuestro enfoque pretende tocar también la introducción y utilización de los adèles e idèles como diccionario local-global; ello con inspiración de Cassels **[70].** Finalmente, una versión adélica del teorema de Minkowski también pavimenta el camino para presentar distintas mejoras al clásico lema de Siegel, principalmente siguiendo a Bombieri y Gubler **[69].**

10.1 Cuerpos localmente compactos y adèles

Gran parte de la combinación entre cuerpos y topología ya la detallamos en el capítulo anterior, pero aquí conviene revisar las aplicaciones de una topología pura y no solo de usos de las métricas.

Recuérdese lo siguiente:

Teorema 10.1: Sea G un grupo (topológico) localmente compacto. Entonces posee una medida de Borel no nula que es invariante por la izquierda, vale decir, tal que para toda función $f \in C_c(G;\mathbb{C})$ continua

de soporte compacto y todo $y \in G$ tenemos:

$$\int_G f(y \cdot x)\,\mathrm{d}\mu(x) = \int_G f(x)\,\mathrm{d}\mu(x).$$

Más aún, si ν satisface lo anterior, entonces $\nu = c\mu$ para algún $c \in \mathbb{R}_{>0}$.

Definición 10.2: Sea G un grupo topológico. Una medida de Borel no nula invariante por la izquierda se dice una ***medida de Haar (izquierda)***.

Corolario 10.2.1: Sea G un grupo localmente compacto y $H \trianglelefteq G$ un subgrupo normal cerrado. Sean μ, ν medidas de Haar sobre G, H resp. Entonces existe una única medida de Haar λ sobre el cociente G/H tal que

$$\forall f \in C_c(G;\mathbb{C}) \quad \int_G f(x)\,\mathrm{d}\mu(x) = \int_{G/H} \left(\int_H f(xy)\,\mathrm{d}\nu(x) \right) \mathrm{d}\lambda(\pi(y)).$$

El corolario anterior debería interpretarse geométricamente como una generalización del teorema de Fubini.

En general, la mayoría de libros suele citar los resultados generales de medidas de Haar porque uno está obligado a reconstruirlas explícitamente en los debidos contextos.

Definición 10.3: Sea G un grupo localmente compacto y $\sigma\colon G \to G$ un automorfismo en TopGrp.[1] Definimos el ***módulo*** de σ como el cociente $\mathrm{Mod}_G\,\sigma := \mu(\sigma[X])/\mu(X)$ donde μ es una medida de Haar sobre G y X es un conjunto medible con $0 < \mu(X) < \infty$. Obviaremos el subíndice «G» de no haber ambigüedad.

Nótese que como las medidas de Haar son únicas salvo constante, el módulo es independiente de la elección de μ.

Proposición 10.4: Sea G un grupo localmente compacto, y sean σ, τ automorfismos de G. Entonces:

1. Para todo conjunto medible S y toda función medible $f \in \mathscr{L}(G;\mathbb{R})$ se tiene:

$$\mu(\sigma[S]) = \mathrm{Mod}\,\sigma \cdot \mu(S),$$

[1] Vale decir, σ es un isomorfismo de grupos y un homeomorfismo de espacios topológicos.

$$\int_S f(\sigma^{-1}(x))\,\mathrm{d}\mu(x) = (\operatorname{Mod}\sigma)\cdot\int_{\sigma[S]} f(x)\,\mathrm{d}\mu(x).$$

2. $\operatorname{Mod}(\sigma\circ\tau) = \operatorname{Mod}\sigma\cdot\operatorname{Mod}\tau$.

3. Sea $H \trianglelefteq G$ un subgrupo normal cerrado y σ-invariante. Denotemos $\overline{\sigma}\in\operatorname{Aut}(G/H)$ el automorfismo inducido, entonces:

$$\operatorname{Mod}_G\sigma = \operatorname{Mod}_{G/H}(\overline{\sigma})\cdot\operatorname{Mod}_H(\sigma|_H).$$

Esto podemos emplearlo para el contexto de cuerpos topológicos:[2]

Definición 10.5: Sea K un cuerpo localmente compacto y sea $a\in K$. Se define $\operatorname{Mod}_K(a)$ como el módulo del automorfismo $x\mapsto ax$ (sobre el grupo $(K,+)$) si $a\neq 0$ y $\operatorname{Mod}_K(0) := 0$.

Proposición 10.6: Sea K un cuerpo localmente compacto. Entonces $\operatorname{Mod}_K\colon K\to\mathbb{R}$ es una función continua y $\operatorname{Mod}_K(ab) = \operatorname{Mod}_K(a)\cdot\operatorname{Mod}_K(b)$.

Demostración: Sea μ una medida de Haar (aditiva) sobre K y X un entorno compacto del 0. Para todo $a\in K$ y todo $\epsilon>0$, existe un entorno abierto $U\supseteq a\cdot X$ tal que $\mu(U)\leq\mu(aX)+\epsilon$. Sea W un entorno (abierto) de a tal que $WX\subseteq U$, entonces para todo $b\in W$ tenemos que

$$\operatorname{Mod}_K(b)\leq\operatorname{Mod}_K(a)+\mu(X)^{-1}\epsilon.$$

Empleando que $\operatorname{Mod}_K(a^{-1})^{-1} = \operatorname{Mod}_K(a)$ (¿por qué?), es fácil concluir una desigualdad recíproca similar y ver que es continua.

La última afirmación se sigue de la proposición anterior. □

Teorema 10.7: Sea K un cuerpo localmente compacto y no discreto. Para todo $\epsilon>0$, el conjunto $\overline{B}_\epsilon := \{a\in K : \operatorname{Mod}_K(a)\leq\epsilon\}$ es compacto.

Demostración: Sea C un compacto con $0\in\operatorname{Int}C$ y sea U un entorno tal que $U\cdot C\subseteq C$. Como K no es discreto, entonces existe $r\in U\cap C$ tal que $0<\operatorname{Mod}_K(r)<1$ y, por inducción, $r^n\in C$ para $n\in\mathbb{N}$. Como C es compacto, sea s un punto de acumulación de $\{r^n\}_{n\in\mathbb{N}}$ y, aplicando $\operatorname{Mod}_K(-)$, vemos que $\operatorname{Mod}_K(s)=0$, por lo que $s=0$ (¿por qué?).

[2]Más generalmente, Weil [**109**] considera el caso de espacios vectoriales topológicos sobre un anillo de división topológico. El lector interesado puede generalizar lo siguiente.

Sea $a \in \overline{B}_\epsilon$. Como $r^n a \to 0$, sea m el mínimo natural tal que $r^m a \in C$. Si $a \notin C$, entonces $r^{m-1}a \notin C$ y, por tanto, $r^m a \in C \smallsetminus rC$. Sea $S := \overline{C \smallsetminus rC}$, entonces $S \subseteq C$ es compacto y $0 \notin S$, así que $\delta := \text{ínf}\{\text{Mod}_K(x) : x \in S\} > 0$. Sea N el máximo entero tal que $\text{Mod}_K(r)^N \leq \delta/\epsilon$, entonces como $a \in \overline{B}_\epsilon \smallsetminus C$ tenemos que

$$\text{Mod}_K(r)^N \epsilon \leq \delta \leq \text{Mod}_K(r^m a) = \text{Mod}_K(r)^m \,\text{Mod}_K(a) \leq \text{Mod}_K(r)^m \epsilon.$$

Por tanto, $N \geq m$. Esto prueba que $\overline{B}_\epsilon \subseteq \bigcup_{j=0}^{N} r^{-j} C$ y es fácil ver que $\overline{B}_\epsilon$ es cerrado, por lo que es compacto. □

Por el teorema anterior, el lector podría sospechar que $\text{Mod}_K(-)$ se comporta como un valor absoluto, pero solo hasta cierto punto. Es fácil probar que para $\alpha \in \mathbb{C}^\times$ tenemos que $\text{Mod}_{\mathbb{C}}(\alpha) = |\alpha|^2$, la cual no es una función valor absoluto (¿por qué?).

Corolario 10.7.1: Sea K un cuerpo localmente compacto y no discreto. Entonces:

1. La familia $\{\overline{B}_r\}_{r>0}$ es una base de entornos cerrados del 0.
2. K es un espacio 1AN y un grupo métrico (posee una métrica que induce su topología invariante bajo $+$).
3. Se tiene que $\lim_n a^n = 0$ syss $\text{Mod}_K(a) < 1$.
4. Todo subcuerpo discreto de K es finito.

Demostración:

1. Sea C un compacto con $0 \in \text{Int}\, C$. Sea $\epsilon > \sup\{\text{Mod}_K(x) : x \in C\}$, de modo que $C \subseteq \overline{B}_\epsilon$. Defínase $S := \overline{\overline{B}_\epsilon \smallsetminus C}$ y sea $\delta := \text{ínf}\{\text{Mod}_K(x) : x \in S\} \leq \epsilon$. Finalmente, elíjase $0 < \gamma < \delta$ tal que $\overline{B}_\gamma \subseteq \overline{B}_\delta$ con $B_\gamma \cap S = \varnothing$; de modo que $B_\gamma \subseteq C$.
2. Esto es una aplicanción del teorema de Birkhoff-Kakutani.
3. Basta considerar la familia $\{\overline{B}_{r^n}\}_{n\in\mathbb{N}}$ con $r := \text{Mod}_K(a)$.
4. Sea $L \subseteq K$ discreto. Para todo $a \in L^\times$, nótese que $\text{Mod}_K(a) \leq 1$, puesto que de lo contrario el conjunto $\{a^{-n}\}_{n\in\mathbb{N}}$ tiene un punto de acumulación (el 0). Así, L es un subespacio discreto del compacto $\overline{B}_1$ y, por lo tanto, es finito. □

Teorema 10.8: Sea K un cuerpo localmente compacto y no discreto. Sea V un K-espacio vectorial topológico y $U \leq V$ un subespacio con base $\{v_1, \ldots, v_n\}$. Entonces la aplicación

$$(a_1, \ldots, a_n) \longmapsto \sum_{i=1}^{n} a_i v_i$$

es un isomorfismo y un homeomorfismo. Más aún, U es localmente compacto (como espacio) y es cerrado en V.

Corolario 10.8.1: Sea K un cuerpo localmente compacto y no discreto. Entonces todo K-espacio vectorial de dimensión finita posee una única topología de modo que sea un K-espacio vectorial topológico.

Corolario 10.8.2: Sea K un cuerpo localmente compacto, y sea V un K-espacio vectorial localmente compacto y no discreto. Entonces V tiene dimensión finita d y $\mathrm{Mod}_V(a) = \mathrm{Mod}_K(a)^d$.

Corolario 10.8.3: Sea K un cuerpo localmente compacto no discreto y sea $A\colon V \to V$ un endomorfismo sobre un espacio vectorial de dimensión finita. Entonces $\mathrm{Mod}_V(A) = \mathrm{Mod}_K(\det A)$.

Esta demostración depende de la conmutatividad de K.

Proposición 10.9: Sea K un cuerpo localmente compacto no discreto. La aplicación $\mathrm{Mod}_K\colon K^\times \to \mathbb{R}_{>0}$ induce un homomorfismo abierto en un subgrupo cerrado de $(\mathbb{R}_{>0}, \cdot)$.

Teorema 10.10: Sea K un cuerpo localmente compacto no discreto. Entonces existe una constante $C > 0$ tal que para todo $a, b \in K$:

$$\mathrm{Mod}_K(a+b) \leq C \,\mathrm{máx}\{\mathrm{Mod}_K(a), \mathrm{Mod}_K(b)\}.$$

Además, C está dado por

$$C := \sup\{\mathrm{Mod}_K(1+a) : \mathrm{Mod}_K(a) \leq 1\},$$

y si $C \leq 1$, entonces $\Gamma := \mathrm{Img}(\mathrm{Mod}_K|_{K^\times}) \subseteq \mathbb{R}_{>0}$ es discreto.

§10.1.1 Adèles.

Definición 10.11: Sea K un cuerpo global y sea $S \supseteq M_K^\infty$ un conjunto finito de lugares de K que contenga los lugares infinitos. Se define el siguiente anillo:

$$K_{\mathbb{A}}(S) := \prod_{v \in S} K_v \times \prod_{v \notin S} \mathfrak{o}_v,$$

con la suma y multiplicación coordenada a coordenada. Esta descripción hace que $K_{\mathbb{A}}(S)$ sea un anillo (topológico) localmente compacto.[3] De manera conjuntista, $K_{\mathbb{A}}(S)$ corresponde al conjunto de adèles (cfr. def. 6.37) $\boldsymbol{a}$ tales que $|a|_v \leq 1$ para todo $v \notin S$.

Se define el anillo de adèles como:[4]

$$K_{\mathbb{A}} := \bigcup_{\substack{M_K^\infty \subseteq S \subseteq M_K \\ |S| < \infty}} K_{\mathbb{A}}(S),$$

con la topología en la cual cada $K_{\mathbb{A}}(S)$ es un subanillo abierto.

Tenemos la inclusión natural $K \hookrightarrow K_{\mathbb{A}}$ dada por la función diagonal $a \mapsto (a)_{v \in M_K}$. Esto vuelve a K un subgrupo (aditivo) de $K_{\mathbb{A}}$

Teorema 10.12: Sea K un cuerpo global. Entonces:

1. El subconjunto $K \subseteq K_{\mathbb{A}}$ es un subgrupo (aditivo) cerrado discreto.
2. Si $\operatorname{car} K = 0$, sea $\{\omega_1, \ldots, \omega_n\}$ una $\mathbb{Z}$-base de $\mathcal{O}_K$ y sea

$$\Omega_\infty := \left\{ \boldsymbol{a} \in \prod_{v|\infty} K_v \cong K \otimes_{\mathbb{Q}} \mathbb{R} : \boldsymbol{a} = \sum_{j=1}^{n} \omega_j \otimes r_j \quad r_j \in [0,1) \right\},$$

(donde empleamos el teorema 6.26).

Si $\operatorname{car} K \neq 0$, entonces $\Omega_\infty := \{0\}$. El subconjunto

$$\Omega := \Omega_\infty \times \prod_{v \nmid \infty} \mathfrak{o}_v \subseteq K_{\mathbb{A}}(M_K^\infty),$$

es un dominio fundamental para $K_{\mathbb{A}}/K$, es decir, cada clase de equivalencia en $K_{\mathbb{A}}/K$ tiene exactamente un representante en Ω.

[3] En efecto, cada $\mathfrak{o}_v$ es compacto, luego el producto lo es por el teorema de Tychonoff. Cada K_v es localmente compacto y solo tomamos un producto finito de ellos.

[4] Esta es notación de Weil [**109,** pág. 59] y Bombieri y Gubler [**69,** pág. 604]. La notación estándar es $\mathbb{A}_K$, pero optamos por $K_{\mathbb{A}}$ para evitar confusión con el espacio afín.

3. En consecuencia, $K_{\mathbb{A}}/K$ es un grupo compacto.

Demostración:

1. Empleando que las traslaciones son homeomorfismos, basta ver que el 0 está aislado. Elíjase un lugar $w \in M_K$, entonces

$$U := \{a \in K_w : |a|_w < 1\} \times \prod_{v \neq w} \{a \in K_v : |a|_v \leq 1\}$$

es un entorno del 0 y, por la fórmula del producto, $K \cap U = \{0\}$.

2. Primero veamos la existencia de representantes. Sea $\boldsymbol{a} \in K_{\mathbb{A}}$, entonces el conjunto de lugares (finitos) S tales que $|a|_v > 1$ es finito. Considerando el conjunto $\{a_v : v \in S\}$, por el teorema de aproximación, tenemos que existe $b \in K$ tal que $|a_v - b|_v < 1$ para todo $v \in S$. Reemplazando $\boldsymbol{a}$ con $\boldsymbol{a} - b$ podemos suponer que $\boldsymbol{a} \in K_{\mathbb{A}}(M_K^\infty)$. Defínase

$$(a_v)_{v|\infty} = \sum_{j=1}^{n} \omega_j \otimes r_j$$

con $r_j \in \mathbb{R}$. Luego, existen $c_j \in \mathbb{Z}$ tales que $0 \leq r_j - c_j < 1$ para cada j, de modo que $\boldsymbol{a} - \sum_{j=1}^n \omega_j \otimes c_j$ es un representante de $\boldsymbol{a}$ en Ω.

Sean $\boldsymbol{a}, \boldsymbol{b} \in \Omega \subseteq K_{\mathbb{A}}(M_K^\infty)$ tales que $\boldsymbol{c} := \boldsymbol{a} - \boldsymbol{b} \in K$. Denotemos $(a_v)_{v|\infty} = \sum_{j=1}^n \omega_j \otimes a_j, (b_v)_{v|\infty} = \sum_{j=1}^n \omega_j \otimes b_j$. Como $\boldsymbol{c} \in K_{\mathbb{A}}(M_K^\infty)$, entonces $c_v \in \mathfrak{o}_v$ para todo lugar finito, de modo que $c \in \mathcal{O}_K$ y, por lo tanto,

$$c = \sum_{j=1}^{n} \omega_j \otimes (a_j - b_j)$$

satisface que $a_j - b_j \in (-1, 1)$ sea entero, por tanto $a_j = b_j$. □

Definición 10.13: Sea K un cuerpo numérico y sea $v \in M_K$. Definimos la normalización β_v de la medida de Haar sobre K_v:

(a) Si $K_v = \mathbb{R}$, entonces β_v es la medida de Lebesgue usual.

(b) Si $K_v = \mathbb{C}$, entonces β_v es el doble de la medida de Lebesgue usual.

(c) Si $K_v \supseteq \mathbb{Q}_p$, entonces

$$\beta_v(\mathfrak{o}_v) = |\mathfrak{d}(K_v/\mathbb{Q}_p)|_p^{1/2}.$$

Sobre $K_{\mathbb{A}}(S)$ definimos:

$$\beta_S := \prod_{v\in S} \beta_v \times \prod_{v\notin S} \beta_v|_{\mathfrak{o}_v}.$$

Los cuales son compatibles entre sí y se pegan en una medida de Haar β sobre el anillo de adèles $K_{\mathbb{A}}$.

Proposición 10.14: Sea K un cuerpo numérico. La medida de Haar sobre $K_{\mathbb{A}}/K$ satisface que $\beta_{K_{\mathbb{A}}/K}(K_{\mathbb{A}}/K) = 1$.

Demostración: Como Ω (definido como antes) es un dominio fundamental, basta verificar que $\beta(\Omega) = 1$. Por definición:

$$\beta(\Omega) := \left(\prod_{v|\infty} \beta_v\right)(\Omega_\infty) \cdot \prod_p \prod_{v|p} |\mathfrak{d}(K_v/\mathbb{Q}_p)|_p^{1/2}.$$

Nótese que para un lugar u sobre $\mathbb{Q}$ tenemos que

$$|\mathfrak{d}(K/\mathbb{Q})|_u := \prod_{v|u} |\mathfrak{d}(K_v/\mathbb{Q}_u)|_v,$$

y por la fórmula del producto, concluimos que

$$\prod_p \prod_{v|p} |\mathfrak{d}(K_v/\mathbb{Q}_p)|_p^{1/2} = |\mathfrak{d}(K/\mathbb{Q})|^{-1/2}.$$

Ahora estudiemos la parte arquimediana. En primer lugar, nótense que hay $r + 2s$ encajes complejos $\sigma\colon K \to \mathbb{C}$, donde r son encajes reales y $2s$ son encajes imaginarios (vienen de a pares por la conjugación compleja). Denotando $\overline{()}$ para la conjugación compleja, ordenemos los monomorfismos así:

$$\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}, \sigma_{r+s+1} := \overline{\sigma_{r+s}}, \ldots, \sigma_{r+2s} = \overline{\sigma_{r+s}}$$

donde los σ_i's son los reales para $1 \le i \le r$.

Sea $d := [K : \mathbb{Q}]$, entonces $K \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_{v|\infty} K_v \cong \mathbb{R}^d$ y $d = r + 2s$. Para $\alpha \in K$ definimos el siguiente vector

$$\boldsymbol{v}(\alpha) := (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \operatorname{Re}\sigma_{r+1}(\alpha), \operatorname{Im}\sigma_{r+1}(\alpha), \ldots, \operatorname{Re}\sigma_{r+s}(\alpha), \operatorname{Im}\sigma_{r+s}(\alpha)).$$

Sea $\omega_1, \ldots, \omega_d$ una $\mathbb{Z}$-base de $\mathcal{O}_K$; entonces la medida de Lebesgue de Ω_∞ en $\mathbb{R}^d$ está dada por

$$\left|\det[\boldsymbol{v}(\omega_1), \ldots, \boldsymbol{v}(\omega_n)]\right| = 2^{-s}\left|\det[\sigma_i(\omega_j)]_{ij}\right|,$$

donde en el lado derecho se emplean todos los encajes complejos. Nótese que el 2^{-s} sale del hecho de la matriz de la derecha tiene entradas del tipo $\sigma_{r+s}(\omega) = \operatorname{Re}\sigma_{r+s}(\omega) + \operatorname{Im}\sigma_{r+s}(\omega)$ y del tipo $\overline{\sigma}_{r+s}(\omega) = \operatorname{Re}\sigma_{r+s}(\omega) - \operatorname{Im}\sigma_{r+s}(\omega)$; al sumar ambas filas obtendremos $2\operatorname{Re}\sigma_{r+s}\omega, \operatorname{Im}\sigma_{r+s}\omega$ por lo que sale un «2» por cada encaje imaginario.

Finalmente, basta notar que $\left|\det[\sigma_i(\omega_j)]_{ij}\right| = \sqrt{|\mathfrak{d}(K/\mathbb{Q})|}$ para concluir, ya que el factor 2^{-s} se cancela con nuestras normalizaciones de $\beta_{\mathbb{C}}$. □

Corolario 10.14.1: Sea K un cuerpo global. Existen reales $\delta_v > 0$ para cada lugar $v \in M_K$ con $\delta_v = 1$ para todos salvo finitos v's, de modo que el subconjunto $W \subseteq K_{\mathbb{A}}$ de adèles $\boldsymbol{\gamma} \in W$ que satisfacen $|\gamma_v|_v \leq \delta_v$ posee la siguiente propiedad: todo adèle $\boldsymbol{\alpha} \in K_{\mathbb{A}}$ puede descomponerse como

$$\boldsymbol{\alpha} = \beta + \boldsymbol{\gamma}, \qquad \beta \in K, \boldsymbol{\gamma} \in W.$$

Demostración: Esto se sigue de que el cociente $K_{\mathbb{A}}/K$ tenga medida de Haar finita, así que el W del enunciado no es más que un conjunto de representantes del cociente. □

10.2 Los teoremas de Minkowski

Lema 10.15: Sea K un cuerpo numérico y $v \in M_K$ un lugar finito. Fijado un natural n denótese $E_v := K_v^n$. Para un $\mathfrak{o}_v$-submódulo Λ de E_v son equivalentes:

1. Λ es abierto y compacto dentro de E_v.
2. Λ es un $\mathfrak{o}_v$-submódulo finitamente generado y $K_v\langle\Lambda\rangle = E_v$.

Lema 10.16: Sea $\Lambda \leq \mathbb{R}^n$ un subgrupo (aditivo). Son equivalentes:

1. Λ es discreto y $\mathbb{R}^n/\Lambda$ es compacto (como grupo topológico).
2. Λ es discreto y $\mathbb{R}\langle\Lambda\rangle = \mathbb{R}^n$.
3. Λ es un $\mathbb{Z}$-módulo libre y posee una $\mathbb{Z}$-base que es también una $\mathbb{R}$-base de $\mathbb{R}^n$.

Definición 10.17: Sea K un cuerpo numérico y $v \in M_K$ un lugar (sin especificar). Fijado un natural n, denótese $E_v := K_v^n$. Un subgrupo $\Lambda \leq E_v$ se dice un K_v-***reticulado*** si:

(a) Cuando v es un lugar finito, Λ es abierto y compacto dentro de E_v.

(b) Cuando v es un lugar al infinito, Λ es discreto y E_v/Λ es compacto.

Sea A un dominio íntegro con $K := \operatorname{Frac} A$. Un ***A-reticulado*** dentro de K^n es un A-submódulo libre $\Lambda \leq K^n$ tal que $K\langle\Lambda\rangle = K^n$.

Proposición 10.18: Sea K un cuerpo numérico y fijemos un K-espacio vectorial $E := K^n$. Se cumplen:

1. Si Λ es un $\mathcal{O}_K$-reticulado en E, entonces $\Lambda_v := \overline{\Lambda} \subseteq E_v$ es un K_v-reticulado para todo lugar finito v y además $\Lambda_v = \mathfrak{o}_v^n$ solo para finitos lugares v.

2. Si $\{\Lambda_v\}_{v\in M_K^0}$ es una familia de K_v-reticulados en E_v tales que $\Lambda_v = \mathfrak{o}_v^n$ solo para finitos lugares; entonces existe un único $\mathcal{O}_K$-reticulado Λ tal que $\overline{\Lambda} = \Lambda_v \subseteq E_v$. Además, dicho Λ viene dado por:

$$\Lambda = \bigcap_{v\in M_K\smallsetminus M_K^\infty} (\Lambda_v \cap E).$$

Veamos una especie de resultado inverso. Si consideramos los lugares infinitos en vez de los finitos, notamos primero que M_K^∞ es un conjunto finito, por lo que $E_\infty := \prod_{v\in M_K^\infty} E_v$ es un $\mathbb{R}$-espacio vectorial de dimensión finita.

Proposición 10.19: La imagen Λ_∞ de un K-reticulado Λ bajo el encaje diagonal $E \hookrightarrow E_\infty$ es un $\mathbb{R}$-reticulado.

Definición 10.20: Sea K un cuerpo numérico y $\boldsymbol{x} \in K_\mathbb{A}$ un adèle. Dado $\lambda \in \mathbb{R}$ se denota

$$(\lambda\boldsymbol{x})_v := \begin{cases} \lambda x_v, & v \mid \infty, \\ x_v, & v \nmid \infty. \end{cases}$$

Dada una tupla de adèles $\boldsymbol{y} := (\boldsymbol{y}^1, \ldots, \boldsymbol{y}^N) \in K_\mathbb{A}^N$, se denota $\lambda\boldsymbol{y} := (\lambda\boldsymbol{y}^1, \ldots, \lambda\boldsymbol{y}^N)$. Para un lugar $v \mid \infty$, un subconjunto $S_v \subseteq E_v$ se dice ***simétrico*** si $-S_v = S_v$.

Para cada lugar arquimediano $v \mid \infty$, sean $S_v \subseteq E_v$ abiertos no vacíos, acotados, convexos, simétricos y sea Λ un $\mathcal{O}_K$-reticulado en E. Se denota

$$S_\mathbb{A}^\Lambda := \prod_{v\mid\infty} S_v \times \prod_{v\nmid\infty} \Lambda_v \subseteq E_\mathbb{A}.$$

Para $1 \leq n \leq N$ se define el ***n*-ésimo mínimo sucesivo** como

$$\lambda_n := \text{ínf}\{t > 0 : tS \text{ contiene } n \text{ vectores } K\text{-linealmente independientes de } \Lambda\}.$$

Se denota por μ_n al supremo de los $\mu \geq 0$ tales que para todo $\boldsymbol{x}, \boldsymbol{y} \in \mu S_{\mathbb{A}}^{\Lambda}$ con $\boldsymbol{x} - \boldsymbol{y} \in E$, las últimas $N - n + 1$ coordenadas de $\boldsymbol{x}$ e $\boldsymbol{y}$ coinciden.

Es claro que

$$0 < \lambda_1 \leq \cdots \leq \lambda_N < \infty, \qquad 0 \leq \mu_1 \leq \cdots \leq \mu_N < \infty.$$

Lema 10.21: Sea K un cuerpo numérico y $N \geq 1$. Considere el homomorfismo

$$\begin{aligned} \Phi_n \colon E_{\mathbb{A}} = K_{\mathbb{A}}^N &\longrightarrow (K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n} \\ \boldsymbol{x} &\longmapsto (\overline{\boldsymbol{x}}_1, \ldots, \overline{\boldsymbol{x}}_n, \boldsymbol{x}_{n+1}, \ldots, \boldsymbol{x}_N). \end{aligned}$$

Para cada $v \in M_K^{\infty}$, sean $T_v \subseteq E_v$ abiertos no vacíos, acotados, convexos y simétricos, sea Λ un $\mathcal{O}_K$-reticulado en E y sea $T := T_{\mathbb{A}}^{\Lambda}$. Para todo $\mu \geq 1$ real, tenemos que

$$\text{Vol}(\Phi_n[\mu T]) \geq \mu^{d(N-n)} \,\text{Vol}(\Phi_n[T]).$$

Aquí, Vol es cualquier medida de Haar sobre el codominio $(K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n}$. El teorema también podría reformularse adecuadamente en términos del módulo de la función $\boldsymbol{x} \mapsto \Phi_n(\mu \boldsymbol{x})$.

Demostración: Supongamos primero que $n = N$. Como Φ_n es un homomorfismo y las medidas de Haar son invariantes bajo traslaciones, para cada $\boldsymbol{y}$ podemos suponer que $T - \boldsymbol{y}$ contiene al origen y, por convexidad, $\mu(T - \boldsymbol{y}) \supseteq T - \boldsymbol{y}$. Así que $\text{Vol}(\Phi_n[\mu T]) \geq \text{Vol}(\Phi_n[T])$.

Supongamos que $n < N$, e identifiquemos $K_{\mathbb{A}}^N = K_{\mathbb{A}}^n \times K_{\mathbb{A}}^{N-n}$. Dado $\boldsymbol{y} \in K_{\mathbb{A}}^{N-n}$ denotése

$$T(\boldsymbol{y}) := \{\boldsymbol{w} \in K_{\mathbb{A}}^n : (\boldsymbol{w}, \boldsymbol{y}) \in T\}.$$

Denotando por $\overline{\boldsymbol{w}}, \boldsymbol{y}$ las variables en $(K_{\mathbb{A}}/K)^n$ y en $K_{\mathbb{A}}^{N-n}$ resp., por el teorema de Fubini tenemos que

$$\text{Vol}(\Phi_n[\mu T]) = \int_{K_{\mathbb{A}}^{N-n}} \mathrm{d}\boldsymbol{y} \int_{\Phi_n[(\mu T)(\boldsymbol{y})]} \mathrm{d}\overline{\boldsymbol{w}}.$$

Con el cambio de variables $\boldsymbol{y} = \mu\boldsymbol{z}$ obtenemos que

$$\operatorname{Vol}(\Phi_n[\mu T]) = \mu^{d(N-n)} \int_{K_{\mathbb{A}}^{N-n}} \operatorname{Vol}\left(\Phi_n[(\mu T)(\mu\boldsymbol{z})]\right) \mathrm{d}\boldsymbol{z},$$

pero $(\mu T)(\mu\boldsymbol{z}) = \mu \cdot T(\boldsymbol{z})$; así que, aplicando el caso $N = n$, obtenemos que

$$\operatorname{Vol}\left(\Phi_n[(\mu T)(\mu\boldsymbol{z})]\right) \geq \operatorname{Vol}(\Phi_n[T(\boldsymbol{z})]).$$

Así concluimos pues

$$\operatorname{Vol}(\Phi_n[\mu T]) \geq \mu^{d(N-n)} \int_{K_{\mathbb{A}}^{N-n}} \operatorname{Vol}(\Phi_n[T(\boldsymbol{z})]) \, \mathrm{d}\boldsymbol{z} = \mu^{d(N-n)} \operatorname{Vol}(\Phi_n[T]).$$

□

Teorema 10.22 (Davenport-Estermann): Sea K un cuerpo numérico de grado d y $N \geq 1$. Para cada $v \in M_K^\infty$, sean $T_v \subseteq E_v$ abiertos no vacíos, acotados, convexos y simétricos, y sea Λ un $\mathcal{O}_K$-reticulado en E. Entonces

$$(\mu_1 \cdots \mu_N)^d \operatorname{Vol}(T_{\mathbb{A}}^\Lambda) \leq 1.$$

Aquí «Vol» es realmente la medida producto de β sobre el espacio de adèles $K_{\mathbb{A}}$.

Demostración: Queremos aplicar el lema anterior de manera inductiva, para lo que denotamos por

$$\Phi_n^N \colon K_{\mathbb{A}}^N \longrightarrow (K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n},$$
$$\Psi_n := \mathrm{Id}_{(K_{\mathbb{A}}/K)^n} \times \Phi_1^{N-n} \colon (K_{\mathbb{A}}/K)^n \times K_{\mathbb{A}}^{N-n} \longrightarrow (K_{\mathbb{A}}/K)^{n+1} \times K_{\mathbb{A}}^{N-n-1}.$$

De modo que $\Phi_{n+1}^N = \Phi_n^N \circ \Psi_n$, abreviaremos Φ_n^N por Φ_n.

Veamos que Ψ_n es inyectiva en $\Phi_n[\mu_{n+1}T]$. Sean $\boldsymbol{x}, \boldsymbol{y} \in \mu_{n+1}T$ tales que $\Phi_{n+1}(\boldsymbol{x}) = \Phi_{n+1}(\boldsymbol{y})$. Esto significa que $\boldsymbol{x}_j = \boldsymbol{y}_j$ para todo $j > n+1$ y que $\boldsymbol{x}_j - \boldsymbol{y}_j \in K$ para todo $j \leq n+1$; en particular, $\boldsymbol{x} - \boldsymbol{y} \in K^N$. Así, por definición de μ_{n+1} concluimos que $\boldsymbol{x}_{n+1} = \boldsymbol{y}_{n+1}$, vale decir, que $\Phi_n(\boldsymbol{x}) = \Phi_n(\boldsymbol{y}_n)$.

Ahora, empleando las medidas de Haar normalizadas y la unicidad del teorema 10.1 concluimos que

$$\operatorname{Vol}(\Phi_n[\mu_{n+1}T]) = \operatorname{Vol}(\Phi_{n+1}[\mu_{n+1}T]),$$

y, aplicando el lema anterior con $T' = \mu_n T$ y $\mu' := \mu_{n+1}/\mu_n$, obtenemos que

$$\operatorname{Vol}(\Phi_N[\mu_N T]) = \operatorname{Vol}\left(\Phi_{N-1}\left[\frac{\mu_N}{\mu_{N-1}}\mu_{N-1}T\right]\right) \geq \left(\frac{\mu_N}{\mu_{N-1}}\right)^d \operatorname{Vol}(\Phi_{N-1}[\mu_{N-1}T])$$

$$\geq \prod_{n=1}^{N-1} \left(\frac{\mu_{n+1}}{\mu_n}\right)^{d(N-n)} \operatorname{Vol}(\Phi_1[\mu_1 T]) \geq (\mu_1 \cdots \mu_N)^d \operatorname{Vol}(T),$$

donde en el último paso empleamos el lema como $\operatorname{Vol}(\Phi_0[\mu_1 T]) \geq \mu_1^{dN} \operatorname{Vol}(T)$. Finalmente, notemos que Φ_n llega al cociente $(K_{\mathbb{A}}/K)^N$ que es compacto, por lo que su medida de Haar total normalizada es 1. □

Teorema 10.23 (Minkowski-McFeat): Sea K un cuerpo numérico de grado d y $N \geq 1$. Para cada $v \in M_K^\infty$, sean $S_v \subseteq E_v$ abiertos no vacíos, acotados, convexos y simétricos, y sea Λ un $\mathcal{O}_K$-reticulado en E. Denotando $S := \prod_{v|\infty} S_v \times \prod_{v\nmid\infty} \Lambda_v \subseteq E_{\mathbb{A}}$ se tiene

$$(\lambda_1 \cdots \lambda_N)^d \operatorname{Vol}(S) \leq 2^{dN}.$$

Más aún, si para cada lugar imaginario $v \in M_K^\infty$ se cumple que S_v es $\mathbb{C}$-simétrico (i.e. para todo $|\zeta| = 1$ se satisface que $\zeta \cdot S_v = S_v$), entonces tenemos la siguiente cota:

$$\frac{2^{dN}\pi^{sN}}{(N!)^r\big((2N)!\big)^s} |\mathfrak{d}(K/\mathbb{Q})|^{-N/2} \leq (\lambda_1 \cdots \lambda_N)^d \operatorname{Vol} S, \tag{10.1}$$

donde r, s denotan la cantidad de lugares reales e imaginarios de K resp.

Demostración: Sea $\gamma \in \mathrm{GL}_N(K_{\mathbb{A}})$ una matriz invertible que determina un automorfismo lineal de $E_{\mathbb{A}}$. Se puede verificar que

$$\prod_{v \in M_K} \|\det \gamma\|_v = 1,$$

de modo que no afecta el volumen de S y, así, suponer que $\lambda_n S$ contiene a la base canónica $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ de $E_{\mathbb{A}}$.

Aplicando el teorema de Davenport-Estermann basta probar que $\mu_n \geq \frac{1}{2}\lambda_n$. Procedemos por inducción sobre n. Sean $\boldsymbol{x}, \boldsymbol{y} \in \frac{1}{2}\lambda_n S$ tales que $\boldsymbol{x} - \boldsymbol{y} \in E$ y, como S es convexo y simétrico, entonces

$$\boldsymbol{x} - \boldsymbol{y} = \frac{1}{2}(2\boldsymbol{x}) + \frac{1}{2}(-2\boldsymbol{y}) \in \lambda_n S.$$

Si $n = 1$ y $\lambda > \lambda_1$, entonces $\lambda S \cap E$ contiene a $\boldsymbol{e}_1$, es discreto y relativamente compacto, así que $\overline{\lambda_1 S} \subseteq E_{\mathbb{A}}$ contiene a $\boldsymbol{e}_1$, de modo que $\lambda_1 S$ no y $\boldsymbol{x} = \boldsymbol{y}$, comprobando que $\mu_1 \geq \frac{1}{2}\lambda_1$. Si $n \geq 2$ entonces, por hipótesis inductiva, podemos suponer que $\lambda_n > \lambda_{n-1}$. Así $\overline{\lambda_{n-1} S} \subseteq \lambda_n S$ y, como $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{n-1}, \boldsymbol{x} -$

$\boldsymbol{y} \in \lambda_n S$ y, por tanto, $\boldsymbol{x} - \boldsymbol{y}$ deben ser combinación lineal de $\boldsymbol{e}_1, \dots, \boldsymbol{e}_{n-1}$; comprobando así que $\boldsymbol{x}_j = \boldsymbol{y}_j$ para $j \geq n$.

Probaremos ahora el «más aún». Para cada lugar al infinito $v \in M_K^\infty$ defínase

$$S'_v := \left\{ \boldsymbol{t} \in E_v : \sum_{j=1}^{N} \lambda_j |t_j|_v < 1 \right\}.$$

Así, por simetría (incluída la $\mathbb{C}$-simetría cuando v es imaginario) concluimos que $S'_v \subseteq S_v$. Sea

$$S' := \prod_{v \in M_K^\infty} S'_v \times \prod_{v \in M_K^0} \mathfrak{o}_v^N.$$

Es claro que $S' \subseteq S$, por lo que $\operatorname{Vol}(S') \subseteq \operatorname{Vol} S$; finalmente solo calculamos las medidas de Haar:

$$\beta_v^N(S') = \begin{cases} \dfrac{2^N}{N!}(\lambda_1 \cdots \lambda_N)^{-1}, & v \text{ es un lugar real,} \\ \dfrac{(4\pi)^N}{(2N)!}(\lambda_1 \cdots \lambda_N)^{-2}, & v \text{ es un lugar imaginario,} \\ |\mathfrak{d}(K_v/\mathbb{Q}_p)|_p^{N/2}, & v \in M_K^0. \end{cases}$$

Donde los dos primeros cálculos son ejercicios para el lector (calcular volumenes de esferas y cubos salvo transformación lineal) y el último es por definición de (la normalización) β_v. También, recuérdese que $r + 2s = d$. □

Aplicando el teorema anterior con $K = \mathbb{Q}$, donde M_K^∞ solo consiste del lugar arquimediano usual «∞» obtenemos:

Teorema 10.24 – *Teoremas de Minkowski*: Sea $N \geq 1$ un natural. Sea $S_\infty \subseteq \mathbb{R}^N$ un abierto no vacío, acotado, convexo y simétrico, y sea $\Lambda_\infty \subseteq \mathbb{R}^N$ un $\mathbb{R}$-reticulado (i.e. un subgrupo aditivo discreto generado por una $\mathbb{R}$-base).

Primero Supongamos que

$$\operatorname{Vol}(S_\infty) > 2^N \operatorname{Vol}(\Lambda_\infty),$$

entonces S_∞ contiene un punto de Λ_∞ distinto del origen. Aquí $\operatorname{Vol}(\Lambda_\infty)$ denota la medida de Lebesgue de un dominio fundamental de $\mathbb{R}^N$ respecto a la acción por traslación de Λ_∞.[5]

Segundo Definiendo λ'_n con $1 \leq n \leq N$ como el ínfimo $t > 0$ tal

que tS_∞ posee n vectores $\mathbb{R}$-linealmente independientes en Λ_∞, obtenemos que

$$\lambda'_1 \cdots \lambda'_N \operatorname{Vol}(S_\infty) \leq 2^N \operatorname{Vol}(\Lambda_\infty).$$

10.3 Aplicaciones

§10.3.1 Finitud del grupo de clases y el grupo de S-unidades.

Lema 10.25: Sea K un cuerpo global, existe una constante real $C > 0$ con la siguiente propiedad: si $\boldsymbol{a} \in K_{\mathbb{A}}$ es un adèle tal que $\prod_{v \in M_k} |a_v|_v > C$, entonces existe un adèle principal $\beta \in K \subseteq K_{\mathbb{A}}$ no nulo tal que

$$\forall v \in M_k \qquad |\beta|_v \leq |a_v|_v.$$

Demostración: Sea $c \geq 0$ la medida de Haar (en $K_{\mathbb{A}}$) del conjunto de adèles $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ tales que

$$\begin{cases} |\gamma_v|_v \leq 1/2, & v \mid \infty, \\ |\gamma_v|_v \leq 1, & v \nmid \infty. \end{cases}$$

Esta constante c satisface que $0 < c < \infty$ (pues solo hay finitos lugares arquimedianos), entonces veamos que $C := 1/c$ sirve.

El conjunto T de adèles $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ tales que

$$\begin{cases} |\gamma_v|_v \leq \frac{1}{2}|\alpha_v|_v, & v \mid \infty, \\ |\gamma_v|_v \leq |\alpha_v|_v, & v \nmid \infty, \end{cases}$$

tiene medida de Haar $c\prod_{v \in M_K} |\alpha_v|_v > c \cdot C = 1$, de modo que al pasar al cociente $K_{\mathbb{A}} \to K_{\mathbb{A}}/K$ hay al menos dos puntos $\boldsymbol{\gamma}, \boldsymbol{\delta} \in T$ con la misma imagen (pues la medida de Haar del cociente es 1), por lo que $\beta := \boldsymbol{\gamma} - \boldsymbol{\delta} \in K \subseteq K_{\mathbb{A}}$ satisface

$$|\beta|_v = |\gamma_v - \delta_v|_v \leq |\alpha_v|_v. \qquad \square$$

Corolario 10.25.1: Sea K un cuerpo global y fijemos un lugar $v_0 \in M_K$. Sean $\delta_v > 0$ reales para cada $v \neq v_0$, donde $\delta_v = 1$ para todos salvo finitos v's. Entonces existe $\beta \in K^\times$ tal que

$$\forall v \neq v_0 \qquad |\beta_v| \leq \delta_v.$$

[5]Esta es la notación de Bombieri y Gubler **[69,** pág. 615], mientras que P. L. Clark **[73,** pág. 7] emplea *covolúmen*.

Teorema 10.26 (de aproximación fuerte): Sea K un cuerpo global y fijemos un lugar $v_0 \in M_K$. Sea $\mathcal{A}$ la proyección del anillo de adèles $K_{\mathbb{A}}$ que borra la coordenada v_0. Entonces la imagen de K es densa en $\mathcal{A}$.

Otra manera de leer éste resultado es que dado un adèle cualquiera, éste se puede aproximar tanto como se quiera por un adèle principal salvo por una coordenada.

Demostración: El enunciado equivale al siguiente: sea $S \subseteq M_K$ un conjunto finito de lugares con $v_0 \notin S$, sean $\epsilon > 0$ y $\alpha_v \in K_v$ para cada $v \in S$; entonces existe un adèle principal $\beta \in K$ tal que

$$\forall v \in S, w \notin S \cup \{v_0\}, \qquad |\alpha_v - \beta_v|_v \leq \epsilon, \quad |\beta_w|_w \leq 1.$$

Ahora bien, por el corolario 10.14.1 existen δ_v's y un conjunto $W \subseteq K_{\mathbb{A}}$ de los adèles con $|\theta_v|_v \leq \delta_v$, de modo que todo adèle $\boldsymbol{\varphi} \in K_{\mathbb{A}}$ se descompone

$$\boldsymbol{\varphi} = \boldsymbol{\theta} + \gamma, \qquad \boldsymbol{\theta} \in W, \gamma \in K. \tag{10.2}$$

Ahora bien, por el corolario anterior existe $\lambda \in K^\times$ tal que

$$\forall v \in S, w \notin S \cup \{v_0\}, \qquad |\lambda|_v \leq \delta_v^{-1}\epsilon, \quad |\lambda|_w \leq \delta_w^{-1}.$$

Así, escogiendo $\boldsymbol{\varphi} := \lambda^{-1}\boldsymbol{\alpha}$ y multiplicando la igualdad (10.2) por λ obtenemos que

$$\boldsymbol{\alpha} = \boldsymbol{\psi} + \beta, \qquad \boldsymbol{\psi} \in \lambda W, \beta \in K,$$

que es precisamente lo que se quería probar. □

Definición 10.27: Sea K un cuerpo global. Los elementos del grupo multiplicativo del anillo de adèles $K_{\mathbb{A}}^\times$ se denominan ***idèles***, esto equivale a dar un adèle $\boldsymbol{\alpha} \in K_{\mathbb{A}}$ cuyas coordenadas son todas no nulas y tal que $|\alpha_v|_v = 1$ para todos salvo finitos lugares v's. Los elementos $\beta \in K^\times \subseteq K_{\mathbb{A}}^\times$ se denominan ***idèles principales***.

El conjunto de idèles se denota I_K y lo dotamos de la topología inicial inducida por la función:

$$I_K \to K_{\mathbb{A}} \times K_{\mathbb{A}}, \qquad \boldsymbol{x} \mapsto (\boldsymbol{x}, \boldsymbol{x}^{-1}),$$

la cual convierte a I_K en un grupo topológico. Sobre el grupo de idèles tenemos el siguiente homomorfismo multiplicativo:

$$|\,|\colon I_K \to (\mathbb{R}_{>0}, \cdot), \qquad \boldsymbol{x} \mapsto \prod_{v \in M_K} |x_v|_v,$$

denotaremos por I_K^0 a su núcleo.

El ***grupo de clases de idèles*** de K es el cociente topológico $\mathrm{Cl}_K := I_K/K^\times$. La fórmula del producto se traduce en que $K^\times \subseteq I_K^0$, de modo que el homomorfismo se factoriza en $||\colon \mathrm{Cl}_K \to \mathbb{R}_{>0}$; y denotamos por $\mathrm{Cl}_K^0 = I_K^0/K^\times$ a su núcleo.

La topología sobre I_K no es la topología subespacio de $K_\mathbb{A}$ y, *a priori*, Cl_K no es un grupo topológico (aunque sí es un grupo y sí posee una topología).

Proposición 10.28: Sea K un cuerpo global. El subgrupo de idèles principales $K^\times \leq I_K$ forma un subgrupo discreto (en la topología de I_K). En consecuente, $K^\times \leq_f I_K$ es un subgrupo cerrado y Cl_K es un grupo topológico.

Demostración: Basta factorizar

$$\begin{aligned} K^\times &\longrightarrow K^\times \times K^\times \overset{i}{\hookrightarrow} K_\mathbb{A} \times K_\mathbb{A} \\ a &\longmapsto (a, a^{-1}) \end{aligned}$$

donde i es la inclusión canónica. Como $K^\times$ es discreto en la topología de $K_\mathbb{A}$, esta factorización muestra que $K^\times$ también lo es en la topología de I_K. □

Lema 10.29.A: Sea K un cuerpo global. El conjunto I_K^0 es cerrado en $K_\mathbb{A}$ y su $K_\mathbb{A}$-topología subespacio coincide con su I_K-topología subespacio.

Demostración: Sea $\boldsymbol{a} \in K_\mathbb{A}$ tal que $\boldsymbol{a} \notin I_K^0$, queremos encontrar un $K_\mathbb{A}$-entorno de $\boldsymbol{a}$. Veamos por casos:

(a) $\prod_{v\in M_K} |a_v|_v < 1$: Sea $S \subseteq M_K$ el subconjunto de lugares $v \in M_K$ tales que $|a_v|_v > 1$, el cual es finito. Entonces el conjunto W de adèles $\boldsymbol{\gamma} \in K_\mathbb{A}$ tales que

$$\forall v \in S, w \notin S, \qquad |\gamma_v - \alpha_v|_v < \epsilon,\ |\gamma_w|_w \leq 1 \tag{10.3}$$

es $K_\mathbb{A}$-abierto. Agregando lugares a S y eligiendo $\epsilon > 0$ suficientemente pequeño, podemos asegurar que W no corte a I_K^0.

(b) $\prod_{v\in M_K} |a_v|_v =: C > 1$:[6] Existe un subconjunto finito $S \subseteq M_K$ y un número $\epsilon > 0$ tales que:

[6] ¿Por qué habría de existir este producto infinito?

- Si $v \in M_K$ es tal que $|a_v|_v > 1$, entonces $v \in S$.
- Si $v \notin S$ y $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ satisface $|\gamma_v|_v < 1$, entonces $|\gamma_v|_v \leq \frac{1}{2}C$.
- Si $v \in S$ y $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ satisface $|\gamma_v - \alpha_v|_v < \epsilon$, entonces $1 < \prod_{v\in S} |\gamma_v|_v < 2C$.

Entonces el conjunto W de adèles $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ tales que satisfacen (10.3) es un $K_{\mathbb{A}}$-entorno de $\boldsymbol{a}$.

Así, sabemos que I_K^0 es cerrado en $K_{\mathbb{A}}$.

Sea $W \subseteq I_K^0$ un conjunto que contiene a un idèle $\boldsymbol{a} \in I_K^0$. Si W es $K_{\mathbb{A}}$-abierto, entonces contiene a un $K_{\mathbb{A}}$-entorno de $\boldsymbol{a}$ cuyos elementos $\boldsymbol{\gamma}$ satisfacen (10.3) para algún $S \subseteq M_K$ finito y $\epsilon > 0$. Esto contiene al I_K-entorno de $\boldsymbol{a}$ cuyos elementos $\boldsymbol{\gamma}$ satisfacen

$$\forall v \in S, w \notin S \qquad |\gamma_v - \alpha_v|_v < \epsilon,\ |\gamma_w|_w = 1. \tag{10.4}$$

Supongamos que W es I_K-abierto, es decir, contiene a la intersección con un I_K-entorno H de $\boldsymbol{a}$ cuyos elementos $\boldsymbol{\gamma}$ satisfacen (10.4) para un conjunto S que contiene a los lugares arquimedianos M_K^∞ y los lugares v's tales que $|a_v|_v \neq 1$. Si achicamos $\epsilon > 0$ lo suficiente, entonces para todo $\boldsymbol{\gamma} \in H$ se cumplirá que

$$2^{-1} < \prod_{v\in M_K} |\gamma_v|_v < 2.$$

La intersección $H \cap I_K^0$ es la misma que la del $K_{\mathbb{A}}$-entorno dado por (10.3), de modo que es $K_{\mathbb{A}}$-abierto. □

Teorema 10.29: Sea K un cuerpo global. El grupo Cl_K^0 es compacto.

Demostración: Por el lema anterior, basta probar que existe un subconjunto compacto $W \subseteq K_{\mathbb{A}}$ tal que la restricción de la proyección $W \cap I_K^0 \to \mathrm{Cl}_K^0$ siga siendo sobreyectiva. Sea $C > 0$ la constante dada en el lema 10.25, y sea $\boldsymbol{\alpha} \in I_K$ un idèle con $\prod_{v\in M_K} |\alpha_v|_v > C$; sea W el conjunto de los $\boldsymbol{\gamma} \in K_{\mathbb{A}}$ tales que

$$\forall v \in M_K \qquad |\gamma_v|_v \leq |\alpha_v|_v.$$

Claramente W es compacto y para todo idèle $\boldsymbol{\beta} \in I_K^0$ existe un idèle principal $\lambda \in K^\times$ tal que

$$\forall v \in M_K \qquad |\lambda|_v \leq |\beta_v^{-1}\alpha_v|_v,$$

es decir, $\lambda\boldsymbol{\beta} \in W$ como se quería ver. □

Corolario 10.29.1: Sea K un cuerpo global. El grupo de clases de ideales $\mathrm{Cl}(\mathcal{O}_K)$ del anillo de enteros $\mathcal{O}_K$ es finito.

Demostración: Sea $I_{\mathcal{O}_K}$ el grupo de ideales fraccionarios de $\mathcal{O}_K$. Recuérdese que, por el primer teorema de Ostrowski, existe una biyección entre lugares finitos e ideales primos de $\mathcal{O}_K$; con ella construyamos el siguiente homomorfismo:

$$I_K^0 \longrightarrow I_{\mathcal{O}_K}, \qquad \boldsymbol{a} \longmapsto \prod_{\mathfrak{p}\in \mathrm{Spec}\,\mathcal{O}_K} \mathfrak{p}^{\nu_{\mathfrak{p}}(a_{\mathfrak{p}})}.$$

Dotando a $I_{\mathcal{O}_K}$ de la topología discreta, vemos que la función es continua y es fácil ver que es sobreyectiva. La imagen de los idèles principales $K^\times$ cae en el subgrupo de ideales fraccionarios principales $P_{\mathcal{O}_K}$, de modo que tomando cocientes a ambos lados obtenemos un homomorfismo continuo sobreyectivo $\mathrm{Cl}_K^0 \to \mathrm{Cl}(\mathcal{O}_K)$ y, como Cl_K^0 es compacto y $\mathrm{Cl}(\mathcal{O}_K)$ es discreto, concluimos que $\mathrm{Cl}(\mathcal{O}_K)$ es finito. □

El corolario anterior *per se* ya es una bonita consecuencia de las nociones de adèles e idèles, pero combinándolo con técnicas de la geometría de los números podemos mejorar bastante.

Definición 10.30: Sea k un cuerpo con un conjunto de lugares M (que supondremos es M_k cuando k sea global), y sea $S \subset M$ un subconjunto de lugares que contiene a los arquimedianos. Se denota

$$\mathfrak{o}_{S,k} := \bigcap_{v\in M\smallsetminus S} \mathfrak{o}_v = \{a \in k : \forall v \notin S \quad |a|_v \leq 1\}.$$

De no haber ambigüedad sobre los signos, obviaremos el subíndice «k». Como los lugares $v \notin S$ son no arquimedianos, la desigualdad ultramétrica prueba que $\mathfrak{o}_S$ es un anillo. Los elementos de su grupo de unidades se llaman ***S-unidades*** de k:

$$U_{S,k} := \mathfrak{o}_{S,k}^\times = \{a \in k : \forall v \notin S \quad |a|_v = 1\}.$$

Ejemplo. Sea K un cuerpo numérico.

- Las M_K^∞-unidades de K son precisamente las unidades de su anillo de enteros $\mathcal{O}_K$.
- Sea $\mathfrak{p} = \pi\mathcal{O}_K \in \mathrm{Spec}(\mathcal{O}_K)$. Las $M_K^\infty \cup \{\mathfrak{p}\}$-unidades son productos de unidades de $\mathcal{O}_K$ con potencias enteras de π.

Teorema 10.31 – *Teorema de las unidades de Dirichlet-Chevalley-Hasse*: Sea K un cuerpo numérico y sea $M_K^\infty \subseteq S \subseteq M_K$ un conjunto finito de lugares. Entonces el grupo de S-unidades de K es el producto directo entre un grupo finito (que corresponde a las raíces de la unidad de K) y a un grupo abeliano libre de rango $|S| - 1$. En particular, $U_{K,S}$ es finitamente generado.

Demostración: Consideremos el homomorfismo

$$\lambda\colon U_{K,S} \longrightarrow \mathbb{R}^{|S|}, \qquad a \longmapsto \log |a|_v.$$

El núcleo de λ serían los elementos $a \in K^\times$ tales que $|a|_v = 1$ para todos los lugares; o equivalentemente, serían números algebraicos de altura nula, pero un teorema de Kronecker nos dice que las raíces de la unidad son las únicas que satisfacen aquello. La imagen de λ cae en el $\mathbb{R}$-subespacio vectorial

$$\left\{ \boldsymbol{x} \in \mathbb{R}^{|S|} : \sum_{v \in S} x_v = 0 \right\}$$

el cual tiene ($\mathbb{R}$-)dimensión $s - 1$. Más aún, generan $\mathbb{R}$-linealmente dicho espacio, puesto que la imagen de I_S^0 lo hace.

Finalmente, la imagen $\lambda[U_{K,S}]$ es discreta, puesto que para toda tupla de constantes $0 < c_v < C_v$ para cada $v \in S$, el conjunto de S-unidades $\eta \in U_{K,S}$ que satisfacen

$$\forall v \in S \qquad c_v \leq |\eta|_v \leq C_v$$

es finito, ya que es la intersección entre un conjunto compacto del grupo de idèles I_K y el subgrupo discreto $K^\times$. □

§10.3.2 Aplicaciones: sumas de cuadrados.

Teorema 10.32: Un primo $p \equiv 1 \pmod 4$ es suma de dos cuadrados.

Demostración: Por el criterio de Euler sabemos que -1 es un residuo cuadrático si $p \equiv 1 \pmod 4$, de modo que $1 + m^2 \equiv 0 \pmod p$ para algún $m \in \mathbb{Z}$. Consideremos $\boldsymbol{u} = (1, m)$ y $\boldsymbol{v} = (0, p)$ los cuales son linealmente independientes y generan el reticulado $\Lambda = \boldsymbol{u}\mathbb{Z} + \boldsymbol{v}\mathbb{Z}$, cuyos paralelepípedos fundamentales tienen área p. Sea $\boldsymbol{w} = a\boldsymbol{u} + b\boldsymbol{v} \in \Lambda$, nótese que

$$\|\boldsymbol{w}\|^2 = a^2 + (am + bp)^2 \equiv a^2 + (am)^2 = a^2(1 + m^2) \equiv 0 \pmod p.$$

Considere $X = B_{\sqrt{2p}}(\vec{0})$, la bola de radio $\sqrt{2p}$. Luego $\mu(X) = 2\pi p > 4p$ por lo que posee un punto $\boldsymbol{w}$ de Λ tal que $p \mid \|w\|^2$ y $\|\boldsymbol{w}\|^2 < 2p$, luego $\|\boldsymbol{w}\|^2 = p$ y p es la suma de dos cuadrados. □

Otra aplicación es la siguiente, propuesta por Ankeny **[66]:**

Teorema 10.33: Todo número que no es de la forma $4^a(8n + 7)$ con $a, n \in \mathbb{N}$ es una suma de tres cuadrados.

Demostración: Es fácil notar que basta verlo para $a = 0$. Sea $m = p_1 \cdots p_r$ libre de cuadrados, veamos la demostración por casos:

(a) Caso $m \equiv 3 \pmod 8$: En primer lugar, por el teorema de Dirichlet, podemos encontrar un primo q tal que

$$\forall i \ \left(\frac{-2q}{p_i}\right) = 1, \qquad q \equiv 1 \pmod 4.$$

Luego, elaborando los símbolos de Jacobi se obtiene que

$$\begin{aligned} 1 &= \prod_{i=1}^{r} \left(\frac{-2q}{p_i}\right) = \prod_{i=1}^{r} \left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) \\ &= \left(\frac{-2}{m}\right) \prod_{i=1}^{r} \left(\frac{p_i}{q}\right) = \left(\frac{-2}{m}\right)\left(\frac{m}{q}\right) = \left(\frac{-2}{m}\right)\left(\frac{-m}{q}\right) = \left(\frac{-m}{q}\right). \end{aligned}$$

En consecuente, existe un $b > 0$ impar tal que $b^2 \equiv -m \pmod q$, o equivalentemente, existe $\bar{h}$ tal que

$$b^2 - \bar{h}q = -m, \tag{10.5}$$

analizando la misma fórmula mód 4 se obtiene que $1 - \bar{h}q \equiv 1 \pmod 4$, de lo que se deduce que $\bar{h}$ es múltiplo de 4 y $4h = \bar{h}$.

Como $-2q$ es un residuo cuadrático mód m, entonces $(-2q)^{-1}$ también lo es y, por tanto, existe un entero t tal que $t^2 \cdot (-2q) \equiv 1 \pmod m$. Luego considere

$$\begin{aligned} R(x, y, z) &:= 2tqx + tby + mz \\ S(x, y, z) &:= \sqrt{2q}x + \frac{b}{\sqrt{2q}}y \\ T(x, y, z) &:= \sqrt{\frac{m}{2q}}y \end{aligned}$$

las cuales son transformaciones lineales y es fácil notar que el conjunto C de los (x, y, z)'s tales que $R^2 + S^2 + T^2 < 2m$ es convexo. En coordenadas (R, S, T), el conjunto tiene medida $\frac{4}{3}\pi(2m)^{3/2}$ y el determinante de las transformaciones lineales descritas es $m^{3/2}$ de modo que la medida de C, en coordenadas (x, y, z), es $\frac{1}{3}2^{7/2}\pi \approx 11{,}84 > 8$; por lo cual, tomando el reticulado $\Lambda = \boldsymbol{e}_1\mathbb{Z} + \boldsymbol{e}_2\mathbb{Z}$ vemos que C contiene un punto de coordenadas enteras (x_1, y_1, z_1) con imágenes R_1, S_1, T_1. Nótese que dicha solución satisface lo siguiente:

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= (2tqx_1 + tby_1 + mz_1)^2 + \left(\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1\right)^2 \\ &\quad + \left(\sqrt{\frac{m}{2q}}y_1\right)^2 \\ &\equiv t^2(2qx_1 + by_1)^2 + \frac{1}{\sqrt{2q}}(2qx_1 + by_1)^2 \equiv 0 \pmod{m}, \end{aligned}$$

por la definición de t. Más aún,

$$\begin{aligned} R_1^2 + S_1^2 + T_1^2 &= R_1^2 + \left(\sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1\right)^2 + \left(\sqrt{\frac{m}{2q}}y_1\right)^2 \\ &= R_1^2 + \frac{1}{2q}\left((2qx_1 + by_1)^2 + my_1^2\right) \\ &= R_1^2 + 2\underbrace{(qx_1^2 + bx_1y_1 + hy_1^2)}_{=:v}, \end{aligned}$$

luego $v \in \mathbb{Z}$ y como $R_1^2 + S_1^2 + T_1^2 \in \mathbb{Z}$ concluimos que $R_1 \in \mathbb{Z}$. Lo anterior se reduce a ver que $m \mid R_1^2 + 2v$, pero como $R_1^2 + 2v < 2m$, entonces necesariamente

$$R_1^2 + 2v = m. \tag{10.6}$$

Sea p un primo impar tal que $\nu_p(v) = 2n + 1$ es impar (posiblemente puede no existir).

I) Si $p \nmid m$: entonces como $m \equiv R_1^2 \pmod{p}$ se tiene que

$$\left(\frac{m}{p}\right) = +1,$$

es fácil notar que

$$4qv = (2qx_1 + by_1)^2 + my_1^2,$$

si $p \mid q$ entonces, por (10.5), se cumple que $\left(\frac{-m}{p}\right) = 1$.
Si $p \nmid q$ entonces, la ecuación anterior se traduce en que

$$p^{2n+1} \parallel e^2 + mf^2,$$

de lo que se concluye que $\left(\frac{-m}{p}\right) = 1$, ésto debido a que la potencia del p es impar.
En cualquier caso $\left(\frac{-m}{p}\right) = 1$, combinado al hecho de que $\left(\frac{m}{p}\right) = +1$, se concluye que $\left(\frac{-1}{p}\right) = 1$ y $p \equiv 1 \pmod 4$.

II) Si $p \mid m$: Entonces por (10.6) se concluye que $p \mid R_1$ y notando que

$$m = R_1^2 + \frac{1}{2q}\big((2qx_1 + by_1)^2 + my_1^2\big),$$

notamos que $p \mid 2qx_1 + by_1$. Como m está libre de cuadrados, entonces $m/p \not\equiv 0 \pmod p$ y la ecuación anterior se reescribe a

$$\frac{1}{2q}\frac{m}{p}y_1^2 \equiv \frac{m}{p} \pmod p \iff y_1^2 \equiv 2q \ (p) \implies \left(\frac{2q}{m}\right) = 1,$$

pero recordemos que $\left(\frac{-2q}{m}\right) = 1$ de modo que $\left(\frac{-1}{p}\right) = 1$ y $p \equiv 1 \pmod 4$.

En consecuencia, todos los primos impares que dividen a v con valuación impar son $\equiv 1 \pmod 4$ Luego, $2v$ es una suma de dos cuadrados y como $m = R_1^2 + 2v$, entonces m es suma de tres cuadrados.

(b) Caso $m \equiv 1, 2, 5, 6 \pmod 8$: Nuevamente, por el teorema de Dirichlet podemos escoger un primo q tal que para todo p_i divisor primo impar de m se cumpla que $\left(\frac{-q}{p_i}\right) = 1$, que $q \equiv 1 \pmod 4$ y que, si m es par, entonces

$$m = 2\bar{m}, \qquad \left(\frac{-2}{q}\right) = (-1)^{\frac{\bar{m}-1}{2}}, \qquad (-q)t^2 \equiv 1 \pmod{p_i},$$

siguiendo el mismo despeje se concluye que $\left(\frac{-m}{q}\right) = 1$ con lo que

$$b^2 - qh = -m,$$

y definiendo

$$R(x, y, z) := tqx + tby + mz,$$

$$S(x,y,z) := \sqrt{q}x + \frac{b}{\sqrt{q}}y,$$
$$T(s,y,z) := \sqrt{\frac{m}{q}}y.$$

Luego procedemos de manera análoga al caso anterior. □

Definición 10.34: Los números triangulares son aquellos de la forma

$$\frac{n(n+1)}{2}$$

para algún $n \in \mathbb{N}$.

Teorema 10.35 (Eureka): Todo número natural puede escribirse como suma de tres números triangulares.

El nombre se debe a que cuando Gauss probó el teorema escribió:

$$! \quad \text{num} = \triangle + \triangle + \triangle.$$

Demostración: Sea n un natural. Nótese que $8n + 3 \equiv 3$ (8) de modo que el teorema anterior nos dice que se puede escribir como suma de tres cuadrados:

$$x_1^2 + x_2^2 + x_3^2 = 8n + 3 \equiv 3 \pmod 8.$$

Los cuadrados módulo 8 son $0, 1$ y 4; de modo que necesariamente $x_i^2 \equiv 1$ (mód 8). Luego, se sigue cada x_i es impar y de la forma $2m_i+1$, y finalmente

$$\begin{aligned}\sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} &= \frac{1}{8}\sum_{i=1}^{3}(4m_i^2 + 4m_i + 1 - 1) \\ &= \frac{1}{8}\left(-3 + \sum_{i=1}^{3}(2m_i+1)^2\right) = \frac{1}{8}(-3 + 8n + 3) = n.\end{aligned}$$ □

10.4 El lema de Siegel

El lema de Siegel da una cota efectiva y útil para una solución de un sistema de ecuaciones lineales en $\mathbb{Z}$ en términos de las entradas. Si en lugar de «en $\mathbb{Z}$» contemplásemos las ecuaciones viviendo posiblemente en un anillo de S-enteros nos percatamos que da una cota de una solución de un sistema de matrices en términos de *alturas*. Si finalmente, un sistema de ecuaciones

lo vemos como una subvariedad lineal de un espacio proyectivo, entonces el «sistema de ecuaciones lineales» es ahora un punto en una variedad grassmanniana y la solución es un punto en la subvariedad lineal.

§10.4.1 Alturas en las variedades grassmannianas. Esta sección pretende tanto dar un ejemplo más concreto de alturas, como servir de introducción a la teoría de Arakelov. Aquí $\mathbb{Q}$ es siempre un cuerpo global con su conjunto estándar de valores absolutos $M_{\mathbb{Q}}$, y $M_{\mathbb{Q}^{\mathrm{alg}}}$ es el conjunto de lugares en $\mathbb{Q}^{\mathrm{alg}}$ que extienden a lugares de $M_{\mathbb{Q}}$ sin normalizar.

Definición 10.36: Sea $\boldsymbol{x} \in \mathbb{A}^n(\mathbb{Q}^{\mathrm{alg}})$. Dado un lugar $v \in M_{\mathbb{Q}^{\mathrm{alg}}}$ se define su altura multiplicativa como

$$H_v(\boldsymbol{x}) = \begin{cases} \max_j |x_j|_v, & v \nmid \infty, \\ \left(\sum_{j=1}^n |x_j|_v^2\right)^{1/2}, & v \mid \infty, \end{cases}$$

(de modo que si $\boldsymbol{x} \in \mathbb{A}^n(\mathbb{Q})$ y $v \mid p$, entonces coincide con $H_p(\boldsymbol{x})$.) Dado un cuerpo numérico $K \supseteq \mathbb{Q}^{\mathrm{alg}}$, un punto $\boldsymbol{x} \in \mathbb{A}^n(K)$ y dados $v \mid w \mid p$ (en la torre $\mathbb{Q}^{\mathrm{alg}}/K/\mathbb{Q}$) se define

$$H_w(\boldsymbol{x}) := H_v(\boldsymbol{x})^{[K_w:\mathbb{Q}_p]/[K:\mathbb{Q}]}.$$

Finalmente, dado un punto $P \in \mathbb{P}^n(K)$ que en una carta afín viene representado por $\boldsymbol{x} \in \mathbb{A}^n(K)$, se define

$$h_{\mathrm{Ar}}(P) := \sum_{w \in M_K} \log H_w(\boldsymbol{x}),$$

y se define $H_{\mathrm{Ar}}(P) := \exp h_{\mathrm{Ar}}(P)$.

Observación 10.36.1: La altura global de Arakelov h_{Ar} es la altura global inducida por el haz inversible $\mathscr{O}_{\mathbb{P}^n}(1)$ con la M-métrica de Fubini-Study (i.e., si $u \nmid \infty$ entonces la u-métrica es la trivial y si $u \mid \infty$, entonces es la u-métrica de Fubini-Study).

Definición 10.37: Sea F un cuerpo numérico y fijemos $K := F^{\mathrm{alg}}$. Dado un L-subespacio lineal $W \subseteq K^n$ de dimensión $m \leq n$, entonces W se corresponde canónicamente al punto cerrado

$$P_w := \left[\bigwedge^m W\right] \in \mathbb{P}_K\left(\left(\bigwedge^m K^n\right)^\vee\right) \cong \mathrm{Grass}_{m,n}$$

de modo que denotamos $h_{\mathrm{Ar}}(W) := h_{\mathrm{Ar}}(P_W)$. Si $A \in \mathrm{Mat}_{m\times n}(K)$ es una matriz de orden $m \times n$ de rango $m \leq n$, denotaremos por $h_{\mathrm{Ar}}(A)$ a la altura del subespacio generado por sus filas.

Más generalmente, si $A \in \mathrm{Mat}_{m\times n}(K)$ es una matriz (posiblemente con $m > n$) de rango r, denotamos por $h_{\mathrm{Ar}}^{\mathrm{fila}}(A) := h_{\mathrm{Ar}}(\bigwedge^r W)$, donde W es el K-subespacio lineal de K^n generado por las filas de A y $\bigwedge^r W$ es visto como un punto en el espacio proyectivo $\mathbb{P}_K(\bigwedge^r K^n)$.

Observación 10.37.1: Podemos explicitar el cálculo de h_{Ar} sobre matrices. Sea $K := \mathbb{Q}^{\mathrm{alg}}$ y sea $A \in \mathrm{Mat}_{m\times n}(K)$ una matriz de rango $m \leq n$ y definamos

$$\mathcal{J} := \{I \subseteq \{1, \ldots, n\} \text{ de cardinalidad } m\}.$$

Denotemos por A_I la submatriz de A de orden $m \times m$ constituida por las filas de $I \in \mathcal{J}$. Entonces el punto asociado a A en $\mathbb{P}(\bigwedge^m K^n)$ tiene por coordenadas $\det(A_I)$. Para $u \in M_{\mathbb{Q}^{\mathrm{alg}}}$ tenemos que

$$H_u(A) = \begin{cases} \max_{I\in\mathcal{J}}\{|\det(A_I)|_u\}, & u \nmid \infty, \\ \left(\sum_{I\in\mathcal{J}} |\det(A_I)|_u^2\right)^{1/2}, & u \mid \infty. \end{cases}$$

Sea $F \subseteq K$ un cuerpo numérico tal que $A \in \mathrm{Mat}_{m\times n}(F)$. Dado w en M_F tal que $u \mid w$ en $\mathbb{Q}^{\mathrm{alg}}$ y tal que $w \mid p$ para $p \in M_{\mathbb{Q}}$, definimos

$$H_w(A) := H_u(A)^{[F_w:\mathbb{Q}_p]/[F:\mathbb{Q}]}.$$

Finalmente, se satisface que

$$h_{\mathrm{Ar}}(A) = \sum_{w\in M_F} \log H_w(A).$$

De esto es claro que, dado $G \in \mathrm{GL}_n(\mathbb{Q}^{\mathrm{alg}})$, se satisface que $h_{\mathrm{Ar}}(AG) = h_{\mathrm{Ar}}(A)$.

Proposición 10.38: Sea $A \in \mathrm{Mat}_{m\times n}(\mathbb{Q}^{\mathrm{alg}})$ una matriz de rango $m \leq n$ y sea $u \in M_{\mathbb{Q}^{\mathrm{alg}}}^{\infty}$ un lugar arquimediano. Entonces $H_u(A) = |\det(AA^*)|_u^{1/2}$, donde $A^* = \overline{A}^t$ es la conjugada de la traspuesta de A.

Demostración: Sin perdida de generalidad podemos suponer que u es un lugar complejo y que $A \in \mathrm{Mat}_{m\times n}(\mathbb{C})$. El enunciado ahora se reduce a la clásica fórmula de Binet:

$$\det(A^*A) = \sum_{I\in\mathcal{J}} |\det(A_I)|^2.$$

Identifiquemos a A con su transformación lineal $L\colon \mathbb{C}^m \to \mathbb{C}^n$ en base canónica, con adjunta L^*. Por funtorialidad

$$\bigwedge^m(L) \circ \bigwedge^m(L^*) = \bigwedge^m(L \circ L^*).$$

Relativo a la base canónica, $\bigwedge^m(L)$ (resp. $\bigwedge^m(L^*)$) posee una única fila (resp. columna) cuyas entradas son $\det(A_I)$ (resp. $\overline{\det(A_I)}$), donde $I \in \mathcal{J}$. En consecuencia, $\bigwedge^m(L \circ L^*)$ es una única matriz con entrada $\det(AA^*)$. □

Corolario 10.38.1: Sea K un cuerpo numérico y $A \in \mathrm{Mat}_{m\times n}(K)$ una matriz de rango $r > 0$. Denotando por $H(A)$ a la altura canónica de la matriz vista como un punto en $\mathcal{P}_K^{nm-1}$, entonces

$$H_{\mathrm{Ar}}^{\mathrm{fila}}(A) \leq \left(\sqrt{n}H(A)\right)^r.$$

Demostración: Esto significa que hay r columnas de A que son K-linealmente independientes, por lo que existe una submatriz $A' \in \mathrm{Mat}_{r\times n}(K)$ tal que $H_{\mathrm{Ar}}^{\mathrm{fila}}(A) = H_{\mathrm{Ar}}(A')$; haciendo la sustitución podemos sustituir A con A' y m con r. Separemos a A en dos submatrices complementarias B, C de ordenes $m_1 \times n$ y $m_2 \times n$ resp. Entonces para $v \in M_K^0$ se comprueba por definición que

$$H_v(A) \leq H_v(B)\, H_v(C),$$

empleando la desigualdad triangular (¿por qué?). Si $v \in M_K$ es arquimediano, entonces empleando la proposición anterior tenemos que $H_u(A) = |\det(A\,A^*)|_u^{1/2}$, y $A\,A^*$ se puede expandir como matriz por bloques a lo que se reduce a la desigualdad de Fischer:

$$\det \begin{vmatrix} B\,B^* & C\,B^* \\ B\,C^* & C\,C^* \end{vmatrix} \leq \det(B\,B^*)\det(C\,C^*).$$

Así pues, $H_v(A) \leq H_v(B)\,H_v(C)$ también se satisface en este caso. Luego, tendremos que $h_{\mathrm{Ar}}(A) \leq h_{\mathrm{Ar}}(B) + h_{\mathrm{Ar}}(C)$. □

Proposición 10.39: Sea $K := \mathbb{Q}^{\mathrm{alg}}$, sea W un K-subespacio vectorial no nulo de K^n y sea $W^\perp$ su anulador en $(K^n)^\vee$. Entonces $h_{\mathrm{Ar}}(W^\perp) = h_{\mathrm{Ar}}(W)$.

Demostración: Sea $V := K^n$, todo elemento $\boldsymbol{x} \in \bigwedge^m(V)$ determina una transformación lineal $\psi(\boldsymbol{x})\colon \boldsymbol{y} \mapsto \boldsymbol{x} \wedge \boldsymbol{y}$, desde $\bigwedge^{n-m}(V) \to \bigwedge^n(V)$, es decir, determina un elemento $\varphi(\boldsymbol{x}) \in \bigwedge^n(V) \otimes \bigwedge^{n-m}(V^\vee)$. El homomorfismo

$$\varphi\colon \bigwedge^m(V) \longrightarrow \bigwedge^n(V) \otimes \bigwedge^{n-m}(V^\vee)$$

es un isomorfismo que manda cada elemento de la base canónica de $\bigwedge^m(V)$ a un elemento de la base canónica de $\bigwedge^n(V)\otimes\bigwedge^{n-m}(V^\vee)$ multiplicado por ± 1. Mediante este isomorfismo, la recta $\bigwedge^m(W)$ se manda a la recta $\bigwedge^n(V)\otimes\bigwedge^{n-m}(W^\perp)$; por lo que las coordenadas de $[\bigwedge^m(W)]\in\mathbb{P}\left(\bigwedge^m(V)\right)$ son, salvo signo, las coordenadas de $\left[\bigwedge^{n-m}(W^\perp)\right]\in\mathbb{P}\left(\bigwedge^{m-n}(V^\vee)\right)$. □

Corolario 10.39.1: Sea K un cuerpo numérico y $A\in\mathrm{Mat}_{m\times n}(K)$ una matriz de rango m. La altura de Arakelov del espacio de soluciones $\boldsymbol{y}\cdot A=\vec{0}$ es $h_{\mathrm{Ar}}(A)$.

§10.4.2 Variaciones sobre un tema de Siegel.

Lema 10.40 (Siegel, 1929): Sea $A=[a_{ij}]_{ij}\in\mathrm{Mat}_{N\times M}(\mathbb{Z})$ una matriz no nula, donde $N>M$. Sea $B>0$ tal que cada $a_{ij}\leq B$, entonces existe $\boldsymbol{x}\in\mathbb{Z}^N$ no nulo tal que $\boldsymbol{x}\cdot A=\vec{0}$ con

$$\max_i|x_i|\leq\lfloor(NB)^{\frac{M}{N-M}}\rfloor.$$

Demostración: Sin perdida de generalidad supongamos que A no posee columnas nulas. Para un natural $k>0$ (sin fijar aún) definamos

$$T:=\{\boldsymbol{x}\in\mathbb{Z}^N:\forall i\quad 0\leq x_i\leq k\},$$

el cual posee $(k+1)^N$ puntos. Sean S_m^+,S_m^- la suma de las entradas positivas y negativas resp. de la m-ésima columna de A. Así, para $\boldsymbol{x}\in T$ definiendo $\boldsymbol{y}:=\boldsymbol{x}\cdot A$ vemos que

$$kS_m^-\leq y_m\leq kS_m^+.$$

Sea entonces

$$T':=\{\boldsymbol{y}\in\mathbb{Z}^M:\forall m\quad kS_m^-\leq y_m\leq kS_m^+\}.$$

Sea $B_m:=\max_i|a_{i,m}|$, entonces $S_m^+-S_m^-\leq NB_m$ de modo que T' posee $\prod_{m=1}^M(NkB_m+1)$ elementos. Queremos aplicar el principio del palomar, es decir, buscamos un k tal que

$$\prod_{m=1}^M(NkB_m+1)<(k+1)^N.$$

Así, elíjase k como la parte entera de $\prod_{m=1}^M(NB_m)^{\frac{1}{N-M}}$ y, empleando que $NkB_m+1<NB_m(k+1)$, se concluye que la desigualdad está satisfecha.

Finalmente por el principio del palomar existen $\boldsymbol{y}, \boldsymbol{z} \in T$ tales que $\boldsymbol{y}Z = \boldsymbol{z}A$ y, por tanto, $\boldsymbol{x} := \boldsymbol{y} - \boldsymbol{z}$ satisface que $\boldsymbol{x} \cdot A = \vec{0}$ y $\max_i |x_i| \leq k$ como se quería. □

La condición $N > M$ asegura que siempre $\boldsymbol{x} \cdot A = \vec{0}$ admita soluciones enteras no triviales. La parte interesante del lema es, por supuesto, la cota para una solución.

Es tangible la conexión entre el lema de Siegel y los problemas atacados en la teoría de Minkowski; así que procedemos a emplear el teorema de Minkowski-McFeat para obtener una reformulación y mejora del lema de Siegel en forma de una desigualdad de puntos y grassmannianos.

Primero fijemos la siguiente notación:

Situación 10.41: Sea $K/\mathbb{Q}$ un cuerpo numérico de grado d, sean $1 \leq m \leq n$ enteros y sea $A \in \mathrm{Mat}_{m\times n}(K)$ una matriz de rango m. Para cada $v \in M_K$ denotemos por $Q_v^n \subseteq K_v^n$ el cubo unitario de volumen 1, más precisamente:

$$Q_v^n := \begin{cases} \max_{j=1}^n\{\|x_j\|_v\} < \frac{1}{2}, & K_v = \mathbb{R}, \\ \max_{j=1}^n\{\|x_j\|_v\} < \frac{1}{2\pi}, & K_v = \mathbb{C}, \\ \max_{j=1}^n\{\|x_j\|_v\} \leq 1, & v \nmid \infty. \end{cases}$$

También para cada $v \in M_K$ denotamos

$$S_v := \{\boldsymbol{y} \in K_v^m : \boldsymbol{y} \cdot A \in Q_v^n\} \subseteq K_v^m.$$

Y construimos

$$\Lambda := \{\boldsymbol{x} \in K^m : \forall v \in M_K^0\ \boldsymbol{x} \in S_v\}.$$

Observación 10.41.1: En la situación anterior, recordando que las transformaciones lineales $L\colon \boldsymbol{y} \mapsto \boldsymbol{y} \cdot A$ son continuas, tenemos que S_v es la preimagen de Q_v^n bajo L, por lo que cada S_v es inmediatamente un abierto no vacío y acotado. Si v es arquimediano entonces también es fácil verificar que S_v es convexo y simétrico.

Lema 10.42: En la situación 10.41 para $v \in M_K^\infty$ se satisface que

$$\beta_v(S_v) \geq \|\det(A\,A^*)\|_v^{-1/2},$$

donde $A^* = \overline{A}^t$ es la matriz conjugada traspuesta de A.

Lema 10.43: En la situación 10.41, para $v \in M_K^0$ tal que $v \mid p$ con $p \in M_{\mathbb{Q}}^0$, se satisface que

$$\beta_v(S_v) = |D_{K_v/\mathbb{Q}_p}|_p^{m/2} \left(\max_I \{ \| \det(A_I) \|_u \} \right)^{-1},$$

donde I recorre los subconjuntos de $\{1, \ldots, n\}$ de cardinalidad m y A_I es la submatriz de $m \times m$ de A con las columnas de índice en I.

Proposición 10.44: En la situación 10.41, existe una K-base $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m \in \mathbb{A}^n(K)$ de la imagen de A tal que

$$\prod_{j=1}^m H(\boldsymbol{x}_j) \leq \left(\frac{2}{\pi}\right)^{ms/d} |D_{K/\mathbb{Q}}|_\infty^{m/2d} H_{\mathrm{Ar}}(A),$$

donde s es la cantidad de lugares complejos de K.

Demostración: Agrupando los lemas anteriores y la proposición 10.38 se obtiene que

$$\prod_{v \in M_K} \beta_v(S_v) \geq H_{\mathrm{Ar}}(A)^{-d} \cdot \prod_{p \in M_{\mathbb{Q}}^0} \prod_{v \mid p} |D_{K_v/\mathbb{Q}_p}|_p^{m/2} = H_{\mathrm{Ar}}(A)^{-d} \cdot |D_{K/\mathbb{Q}}|_\infty^{-m/2},$$

por lo que, el teorema de Minkowski-McFeat nos dice que

$$\lambda_1 \cdots \lambda_m \leq 2^m |D_{K/\mathbb{Q}}|_\infty^{m/2d} H_{\mathrm{Ar}}(A).$$

Ahora queremos estimar los mínimos sucesivos respecto al reticulado Λ. Si $\boldsymbol{y} \in K^m$ es un punto en $\lambda S \cap \Lambda$ para algún $\lambda > 0$, definamos $\boldsymbol{x} := \boldsymbol{y} \cdot A$. Por definición de $S := \prod_{v \mid \infty} S_v$ tenemos que $\max_j \|x_j\|_v < \lambda/2$ si $K_v = \mathbb{R}$, que $\max_j \|x_j\|_v < \lambda^2/(2\pi)$ si $K_v = \mathbb{C}$ y $\max_j \|x_j\|_v \leq 1$ si $v \nmid \infty$; así pues

$$H(\boldsymbol{y} \cdot A) < \frac{\lambda}{2} \left(\frac{2}{\pi}\right)^{s/d}.$$

Por definición de mínimos sucesivos, existen vectores K-linealmente independientes $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m \in K^m$ tales que cada $\boldsymbol{y}_j \in \lambda_j \overline{S}$ con $1 \leq j \leq m$, por lo que definiendo $\boldsymbol{x}_j := \boldsymbol{y}_j \cdot A$ vemos que se satisface el enunciado. □

Teorema 10.45 (lema de Siegel-Bombieri-Vaaler): Sea K un cuerpo numérico de grado d y sea $A \in \mathrm{Mat}_{m \times n}(K)$ una matriz de rango $m \leq n$. Entonces, el núcleo $\ker A$ posee una K-base $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{n-m} \in \mathfrak{o}_K^m$ tal que

$$\prod_{\ell=1}^{n-m} H(\boldsymbol{x}_\ell) \leq |D_{K/\mathbb{Q}}|^{\frac{n-m}{2d}} H_{\mathrm{Ar}}(A).$$

Demostración: Sea A' una matriz de orden $(n-m)\times m$ cuyas filas forman una base de $\ker A$. Claramente A' tiene rango $n-m$ y $\mathrm{Im}(A') = \ker(A)$, de modo que $H_{\mathrm{Ar}}(A') = H_{\mathrm{Ar}}(A)$ por el corolario 10.39.1. Ahora bien, aplicando la proposición anterior a A' vemos que existe una K-base $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-m}$ de $\ker A$ tal que

$$\prod_{\ell=1}^{n-m} H(\boldsymbol{x}_\ell) \le \left(\frac{2}{\pi}\right)^{ms/d} |D_{K/\mathbb{Q}}|^{m/2d} H_{\mathrm{Ar}}(A),$$

y finalmente concluimos puesto que $2 < \pi$. □

Mediante la cota del corolario 10.38.1 obtenemos la siguiente consecuencia:

Corolario 10.45.1: Sea K un cuerpo numérico de grado d y sea $A \in \mathrm{Mat}_{m\times n}(K)$ una matriz de rango m. Entonces $\ker A$ posee una K-base $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-m} \in \mathfrak{o}_K^m$ tal que

$$\prod_{\ell=1}^{n-m} H(\boldsymbol{x}_\ell) \le |D_{K/\mathbb{Q}}|^{\frac{n-m}{2d}} \big(\sqrt{N} H(A)\big)^m.$$

En consecuencia, existe un punto $\boldsymbol{x} \in \mathfrak{o}_K^m$ tal que $\boldsymbol{x}\cdot A = \vec{0}$ con

$$H(\boldsymbol{x}) \le |D_{K/\mathbb{Q}}|^{1/2d} \big(\sqrt{N} H(A)\big)^{\frac{m}{n-m}}.$$

Aquí vemos que la versión de Bombieri-Vaaler mejora el lema de Siegel original cambiando el «N» por «$\sqrt{N}$».

Teorema 10.46 – *Lema de Siegel relativo*: Sea K un cuerpo numérico de grado d, sea F/K una extensión finita de grado r, sea $A \in \mathrm{Mat}_{m\times n}(F)$ una matriz con entradas en F y supongamos que $rm < n$. Entonces existen $n-rm$ vectores K-linealmente independientes $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{n-rm} \in \mathfrak{o}_K^m$ tales que

$$\forall \ell \quad \boldsymbol{x}_\ell \cdot A = \vec{0}$$

y

$$\prod_{\ell=1}^{n-rm} H(\boldsymbol{x}_\ell) \leq |D_{K/\mathbb{Q}}|^{\frac{n-rm}{2d}} \prod_{j=1}^{m} H_{\mathrm{Ar}}(A_{j,*})^r.$$

Notas históricas

El nombre «teorema de Minkowski-McFeat» es no estándar. En realidad, ésta es una reformulación adélica (original de McFeat [**95**]) de lo que se conoce en el folclore como el «segundo teorema de Minkowski». Los teoremas que se siguen de él corresponden a la formulación original del alemán **Hermann Minkowski** (1864-1909) publicados en el libro póstumo [**43**] (1896).

El lema de Siegel fue demostrado originalmente en [**61**] (1929). El lema de Bombieri-Vaaler fue probado en [**15**] (1983).

Ahora procedemos a hacer un breve recuento de la historia de los adèles, según Roquette [**9,** págs. 191 s.]. En primer lugar, Claude Chevalley introdujo la noción de los idèles como una herramienta para la teoría de cuerpos de clase; el primer registro fue la carta a Edmund Hasse del 20 de junio de 1935, y más tarde se dieron a conocer en el encuentro anual de la Sociedad Matemática Alemana el 12 de septiembre de 1938. Inspirados en Chevalley, André Weil introdujo los adèles (bajo el nombre de *diferenciales*) en un artículo de 1938 publicado en la revista Crelle acerca de una demostración del teorema de Riemann-Roch; en simultáneo, Emil Artin y George Whaples introdujeron la noción de adèle (bajo el nombre de *vector de valuación*) en [**67**]**.** Los nombres *idèle* y *adèle* tomaron fuerza gracias a algunas reseñas de Hasse, y al libro de Weil [**109**]**.** Estos también fueron una herramienta fundamental en la tesis de Tate [**62**] 1967.

Referencias

66. Ankeny, N. C. Sums of three squares. *Proc. Amer. Math. Soc.* doi:10.1090/S0002-9939-1957-0085275-8 (1957).

69. Bombieri, E. y Gubler, W. *Heights in Diophantine Geometry* (Cambridge University Press, 2006).

70. Cassels, J. W. S. *Global fields* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 42-84.

73. Clark, P. L. *Geometry of numbers with applications to Number Theory* http://alpha.math.uga.edu/~pete/geometryofnumbers.pdf (2015).

95. McFeat, R. B. *Geometry of numbers in adèle spaces* PhD (University of Adelaide, 1969).

Otros recursos.

1. Cuevas, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).
2. Cuevas, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).
3. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).
5. Wilson, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. Brieskorn, E. y Knorrer, H. *Plane Algebraic Curves* trad. por Stillwell, J. (Birkhäuser Verlag, 1981).
7. Dickson, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).
8. Newton, I. *The Correspondence of Isaac Newton* (ed. Turnbull, H. W.) (Cambridge University Press, 1960).
9. Roquette, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).
10. Williams, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. Bennett, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. Alford, W. R., Granville, A. y Pomerance, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).
12. Apéry, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.
13. Barnes, E. S. y Swinnerton-Dyer, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).
14. Beukers, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).

15. BOMBIERI, E. y VAALER, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).
16. CASSELS, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).
17. CATALAN, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).
18. CHAO, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).
19. CHATLAND, H. y DAVENPORT, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).
20. CLARK, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).
21. De BESSY, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).
22. DEDEKIND, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).
23. DICKSON, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).
24. DIRICHLET, G. L. en *G. Lejeune Dirichlet's Werke* (ed. KRONECKER, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.
25. EULER, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).
26. EULER, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).
27. EULER, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).
28. GAUSS, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.
29. HARPER, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).
30. HENSEL, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).
31. HENSEL, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. Hyyrö, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. Inkeri, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. Inkeri, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. Kausler, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. Keller, W. y Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. Kürschák, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. Lang, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. Legendre, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. Lehmer, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. Mahler, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. Mignotte, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. Minkowski, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. Motzkin, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. Nagell, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. Northcott, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. Ochem, P. y Rao, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. Oppenheim, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. Ostrowski, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. Ostrowski, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. OSTROWSKI, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. OSTROWSKI, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. OSTROWSKI, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. PERRON, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. RÉDEI, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. RELLA, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. REMAK, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. ROTH, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. RYCHLÍK, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. RYCHLÍK, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. SIEGEL, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. TATE, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. CASSELS, J. W. S. y FRÖHLICH, A.) (Academic Press, 1967), 305-347.

63. VERGER-GAUGRY, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

11

Aproximación diofántica

Ya en la sección §7.3 vimos un primer vistazo a resultados de aproximación diofántica, siendo el teorema de Liouville el punto de partida. En éste capítulo se busca proseguir en el mismo tópico y ahondar en dos de los resultados más importantes de la geometría diofántica: el teorema de Roth y el teorema del subespacio de Schmidt.

11.1 El teorema de Roth

Recomendamos al lector leer el enunciado del teorema 11.8 más adelante en la pág. 409 para orientarse mejor a lo largo de ésta demostración. La estrategia que se sigue es esencialmente la misma detrás del teorema de aproximación de Dirichlet, solo que Roth necesitó introducir una nueva clase de maquinaria para atacar los pasos principales.

Sean $\boldsymbol{m} := (m_1, \dots, m_n), \boldsymbol{\mu} := (\mu_1, \dots, \mu_n)$ un par de multiíndices de igual longitud, denotaremos:

$$|\boldsymbol{m}| = m_1 + \cdots + m_n, \qquad \binom{\boldsymbol{m}}{\boldsymbol{\mu}} = \prod_{j=1}^{n} \binom{m_j}{\mu_j}.$$

Así mismo, dada una tupla de variables $\boldsymbol{x} = (x_1, \dots, x_n)$, denotamos

$$\partial_{\boldsymbol{\mu}} := \frac{1}{\mu_1! \cdots \mu_n!} \frac{\partial^{|\boldsymbol{\mu}|}}{\partial x_1^{\mu_1} \cdots \partial x_n^{\mu_n}}.$$

Es fácil ver que

$$\partial_{\boldsymbol{\mu}} \boldsymbol{x}^{\boldsymbol{m}} = \binom{\boldsymbol{m}}{\boldsymbol{\mu}} \boldsymbol{x}^{\boldsymbol{m}-\boldsymbol{\mu}}. \tag{11.1}$$

Definición 11.1: Sea k un cuerpo de $\operatorname{car} k = 0$, sea $m \geq 1$ un entero y $\boldsymbol{d} := (d_1, \ldots, d_m) \in \mathbb{R}^m_{>0}$ una tupla de «pesos». Dado un polinomio $f(\boldsymbol{x}) \in k[x_1, \ldots, x_m]$ y un punto afín $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_m) \in \mathbb{A}^m(k)$, definimos el ***índice*** de f en $\boldsymbol{\alpha}$ como

$$\text{índ}(f; \boldsymbol{d}; \boldsymbol{\alpha}) := \min_{\boldsymbol{\mu}} \left\{ \frac{\mu_1}{d_1} + \cdots + \frac{\mu_m}{d_m} : \partial_{\boldsymbol{\mu}} f(\boldsymbol{\alpha}) \neq 0 \right\}$$

Corolario 11.1.1: Sea k un cuerpo de $\operatorname{car} k = 0$ y sea $\boldsymbol{d} := (d_1, \ldots, d_m) \in \mathbb{R}^m_{>0}$. Sean $f, g \in k[x_1, \ldots, x_m]$ un par de polinomios y $P \in \mathbb{A}^m(k)$ un punto afín. Entonces:

1. $\text{índ}(f + g; \boldsymbol{d}; P) \geq \min\{\text{índ}(f; \boldsymbol{d}; P), \text{índ}(g; \boldsymbol{d}; P)\}$.
2. $\text{índ}(f \cdot g; \boldsymbol{d}; P) = \text{índ}(f; \boldsymbol{d}; P) + \text{índ}(g; \boldsymbol{d}; P)$.
3. Dado un multiíndice $\boldsymbol{\mu}$, se satisface que

$$\text{índ}(\partial_{\boldsymbol{\mu}} f; \boldsymbol{d}; P) = \text{índ}(f; \boldsymbol{d}; P) - \frac{\mu_1}{d_1} - \cdots - \frac{\mu_m}{d_m}.$$

Proposición 11.2 (criterio del wronskiano): Sea k un cuerpo de $\operatorname{car} k = 0$ y sean $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$ un conjunto de n polinomios en m variables. El conjunto $f_1, \ldots, f_n$ es k-linealmente independientes syss algún wronskiano generalizado

$$W_{\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n}(x_1, \ldots, x_m) := \det[\partial_{\boldsymbol{\mu}_i} f_j]_{i,j}$$

no es un polinomio nulo para algún $|\boldsymbol{\mu}_j| < j$.

Demostración: $\Longleftarrow$. Procedemos por contrarrecíproca. Si $f_1, \ldots, f_n$ son k-linealmente dependientes, entonces $\partial_{\boldsymbol{\mu}} f_1, \ldots, \partial_{\boldsymbol{\mu}} f_n$ también para cualquier multiíndice $\boldsymbol{\mu}$; luego es claro que todos los wronskianos son nulos.

$\Longrightarrow$. Supongamos que $f_1, \ldots, f_n$ son k-linealmente independientes. Considere la sustitución de Kronecker $(x_1, \ldots, x_m) \mapsto (t, t^d, \ldots, t^{d^{m-1}})$, donde t es una nueva indeterminada. Sobre los monomios en $k[\boldsymbol{x}]$ con grados parciales $< d$, esta sustitución es inyectiva, por lo que escogemos d mayor que los

grados parciales de todos los $f_1, \ldots, f_n$. Así pues, los f_j's son k-linealmente independientes syss los polinomios

$$\Phi_j(t) := f_j(t, t^d, \ldots, t^{d^{m-1}})$$

son k-linealmente independientes. Ahora bien, para un conjunto de polinomios $\Phi_1, \ldots, \Phi_n$ en una sola variable t, es fácil ver que éstos son k-linealmente independientes syss el wronskiano

$$W(t) := \det \left[\frac{\mathrm{d}^{i-1}}{\mathrm{d}t^{i-1}} \Phi_j \right]_{i,j}$$

es no nulo. Por la regla de la cadena existen ciertos polinomios $a_{\boldsymbol{\mu},i}(t; d, m) \in \mathbb{Q}[t]$ tales que

$$\frac{\mathrm{d}^{i-1}}{\mathrm{d}t^{i-1}} \Phi_j = \sum_{|\boldsymbol{\mu}|<i} a_{\boldsymbol{\mu},i}(t; d, m) \partial_{\boldsymbol{\mu}} f_j(t, \ldots, t^{d^{m-1}}).$$

Así, vemos que el wronskiano $W(t)$ es una combinación lineal de wronskianos generalizados $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n}(t, t^d, \ldots, t^{d^{m-1}})$. Finalmente, si $W(t)$ no es el polinomio nulo, entonces necesariamente algún wronskiano generalizado tampoco. □

Teorema 11.3 (lema de Roth): Sea $f(x_1, \ldots, x_m) \in \mathbb{Q}^{\mathrm{alg}}[\boldsymbol{x}]$ de grados parciales acotados por $d_1, \ldots, d_m$ con cada $d_j \geq 1$. Sea $P \in \mathbb{A}^m(\mathbb{Q}^{\mathrm{alg}})$ un punto afín y sea $0 < \sigma \leq 1/2$ tales que:

(a) Los pesos $d_1, \ldots, d_m$ «decrecen rápidamente», vale decir, $d_{j+1} \leq \sigma d_j$ para cada $1 \leq j < m$.

(b) El punto P satisface que

$$\min_{j=1}^{m} \{d_j h(P_j)\} \geq \frac{h(f) + 4md_1}{\sigma}.$$

Entonces $\mathrm{índ}(f; \boldsymbol{d}; P) \leq 2m\sigma^{2^{1-m}}$.

Demostración: Para simplificar notación, fijaremos el punto P y los grados $\boldsymbol{d} := (d_1, \ldots, d_m)$, de modo que $\mathrm{índ}(f) := \mathrm{índ}(f; \boldsymbol{d}; P)$.

Procedemos por inducción sobre m. Para el caso $m = 1$ nótese que $(x - P)^{d\,\mathrm{índ}(f)}$ es un factor de f, vale decir, existe $g(x) \in \mathbb{Q}^{\mathrm{alg}}[x]$ tal que $f =$

$(x-P)^{d\,\mathrm{índ}(f)}\cdot g$. Entonces, por el teorema 9.23, tenemos que $d\log 2+h(f)\geq d\,\mathrm{índ}(f)h(P)+h(g)\geq d\,\mathrm{índ}(f)h(P)$. Así que

$$2\sigma>\sigma\geq\frac{h(f)+4d}{dh(P)}>\frac{h(f)+d\log 2}{dh(P)}\geq\mathrm{índ}(f).$$

Para el caso general descompongamos

$$f(\boldsymbol{x})=\sum_{j=0}^{s}f_j(x_1,\dots,x_{m-1})g_j(x_m),$$

donde $s\leq d_m$ y donde $f_0,\dots,f_s$ y $g_0,\dots,g_s$ son conjuntos de polinomios $\mathbb{Q}^{\mathrm{alg}}$-linealmente independientes resp. Por el criterio del wronskiano, esto se traduce en los dos wronskianos generalizados

$$U(x_1,\dots,x_{m-1}):=\det[\partial_{\boldsymbol{\mu}_i}f_j]_{i,j},\qquad V(x_m):=\det[\partial_\nu g_j]_{\nu,j=0}^{s}$$

no sean polinomios nulos, donde cada $|\boldsymbol{\mu}_i|\leq s\leq d_m$. Multiplicando los determinantes, obtenemos

$$W(x_1,\dots,x_m):=\det[\partial_{\boldsymbol{\mu}_i,\nu}f]_{i,j}=U(x_1,\dots,x_{m-1})V(x_m).$$

Como $d_{j+1}\leq\frac{1}{2}d_j$, entonces $d_1+\cdots+d_m\leq 2d_1$.

Ahora bien, como U,V tienen variables disjuntas, tenemos que $h(U)+h(V)=h(W)$. Los grados parciales de U,V están acotados por $\big((s{+}1)d_1,\dots,(s{+}1)d_{m-1}\big)$ y por $(s+1)d_m$ resp. Finalmente, expandiendo el determinante W en término de sus entradas, donde σ recorre permutaciones del conjunto $\{0,\dots,s\}$, obtenemos que

$$h(W)=\sum_{v\in M_{\mathbb{Q}}}\max_{\sigma}\left\{\log\left|\prod_{j=0}^{s}\partial_{\boldsymbol{\mu}_j,\sigma(j)}f\right|_v\right\}+\log((s+1)!).$$

Ahora, para separar el producto, empleamos el lema de Gauss para lugares no arquimedianos y el lema de Gelfond para los lugares arquimedianos, lo que nos da

$$h(W)\leq\sum_{v\in M_{\mathbb{Q}}}\max_{\sigma}\left\{\sum_{j=0}^{s}\log|\partial_{\boldsymbol{\mu}_j,\sigma(j)}f|_v\right\}+(s+1)(d_1+\cdots+d_m)\log 2+\log((s+1)!).$$

Ahora, recordemos que sobre un monomio $\boldsymbol{x}^{\boldsymbol{\alpha}}$ la derivada parcial actúa como $\partial_{\boldsymbol{\mu}}\boldsymbol{x}^{\boldsymbol{\alpha}} = \binom{\boldsymbol{\alpha}}{\boldsymbol{\mu}}\boldsymbol{x}^{\boldsymbol{\alpha}-\boldsymbol{\mu}}$, donde el coeficiente multinomial es un producto de coeficientes binomiales. Si v es no arquimediano, se comprueba que $|\partial_{\boldsymbol{\mu}}\boldsymbol{x}^{\boldsymbol{\alpha}}|_v = 1$, pero si v es arquimediano, entonces

$$|\partial_{\boldsymbol{\mu}}\boldsymbol{x}^{\boldsymbol{\alpha}}|_\infty \leq 2^{d_1}\cdots 2^{d_m}.$$

Así, obtenemos la cota

$$\begin{aligned} h(W) \leq \sum_{j=0}^{s} \big(h(f) + (d_1+\cdots+d_m)\log 2\big) \\ + (s+1)((d_1+\cdots+d_m)\log 2 + \log(d_m+1)), \end{aligned}$$

empleando que $(d_1+\cdots+d_m) \leq 2d_1$ y que $\log(d_m+1) \leq d_m \leq \frac{1}{2}d_1$, se reduce a $h(W) < (s+1)(h(f)+4d_1)$.

Procedemos a acotar $\operatorname{índ}(W)$, primero nótese que

$$\begin{aligned} \operatorname{índ}(\partial_{\boldsymbol{\mu},\nu} f) &\geq \operatorname{índ}(f) - \frac{\mu_1}{d_1} - \cdots - \frac{\mu_{m-1}}{d_{m-1}} - \frac{\nu}{d_m} \\ &\geq \operatorname{índ}(f) - \frac{d_m}{d_{m-1}} - \frac{\nu}{d_m} \geq \operatorname{índ}(f) - \frac{\nu}{d_m} - \sigma. \end{aligned}$$

Además, como el índice es positivo, $\operatorname{índ}(\partial_{\boldsymbol{\mu},\nu} f) \geq \max\{\operatorname{índ}(f) - \nu/d_m, 0\} - \epsilon$, donde $\epsilon \in \{0, \sigma\}$. Nuevamente, expandiendo el determinante y empleando las propiedades de $\operatorname{índ}(-)$ obtenemos

$$\begin{aligned} \operatorname{índ}(W) &\geq \min_{\sigma} \left\{ \sum_{j=0}^{s} \operatorname{índ}(\partial_{\boldsymbol{\mu}_j,\sigma(j)} f) \right\} \\ &\geq \min_{\sigma} \left\{ \sum_{j=0}^{s} \big(\max\{\operatorname{índ}(f) - \sigma(j)/d_m, 0\} - \sigma \big) \right\} \\ &= \sum_{j=0}^{s} \big(\max\{\operatorname{índ}(f) - j/d_m, 0\} - \sigma \big) \\ &\geq (s+1)\min\left\{ \frac{1}{2}\operatorname{índ}(f), \frac{1}{2}\operatorname{índ}(f)^2 \right\} - (s+1)\sigma, \end{aligned}$$

donde la última desigualdad se deduce de que

$$\sum_{j=0}^{s} \max\{t - j/s, 0\} \geq (s+1)\max\left\{ \frac{t}{2}, \frac{t^2}{2} \right\}.$$

Ahora, empleando que $\text{índ}(W) = \text{índ}(U) + \text{índ}(V)$ y la hipótesis inductiva concluimos que

$$\text{índ}(U) \leq 2(m-1)(s+1)\sigma^{2^{2-m}}, \qquad \text{índ}(V) \leq (s+1)\sigma.$$

Por lo que,

$$\text{mín}\{\text{índ}(f), \text{índ}(f)^2\} \leq 4(m-1)\sigma^{2^{2-m}} + 4\sigma.$$

En cualquier caso, $\text{índ}(f) \leq m$, por tanto

$$\text{índ}(f)^2 \leq 4m(m-1)\sigma^{2^{2-m}} + 4m\sigma \leq 4m^2\sigma^{2^{2-m}},$$

tal y como se quería probar. □

El nombre del resultado dentro de la literatura técnica es «lema de Roth»; no obstante, lo dejamos como teorema, ya que las ideas involucradas tienen un alcance significativo.

Describamos ahora el contexto bajo el cual formularemos el teorema de Roth:

Situación 11.4: Sea K un cuerpo semiglobal, $S \subseteq M_K$ un subconjunto finito. Para cada $v \in S$, elijamos una única extensión $|\,|_v$ en K^{alg} y un elemento algebraico $\alpha_v \in K^{\text{alg}}$.

Definición 11.5: En la situación 11.4, para todo $\beta \in K^{\text{alg}}$ se define

$$\Lambda(\beta) := \prod_{v \in S} \text{mín}\{1, |\beta - \alpha_v|_v\}.$$

Si $\Lambda(\beta) < 1$, diremos que β es una ***aproximación no trivial***. Para una aproximación no trivial β definimos el punto

$$\boldsymbol{p}(\beta) := \big(\log \text{mín}\{1, |\beta - \alpha_v|_v\} / \log \Lambda(\beta)\big)_{v \in S} \in [0,1]^S.$$

Fijado $N \geq 1$ entero, podemos dividir el cubo $[0,1]^S$ en $N^{|S|}$ subcubos semiabiertos de largo $1/N$ (más precisamente, en traslaciones de $[0,1/N)^S$). Una ***clase de aproximaciones de largo*** $1/N$ es el conjunto de aproximaciones no triviales en un mismo subcubo.

Dado un subcubo que contenga un punto $\boldsymbol{x}$, el ***vértice sudeste*** es

$$\boldsymbol{\lambda} = (\lambda_v)_{v \in S} := \big(\lfloor N x_v \rfloor / N\big)_{v \in S}.$$

Denotaremos el subcubo como $Q(\boldsymbol{\lambda})$ y por $\mathcal{C}(\boldsymbol{\lambda}; N) \subseteq Q(\boldsymbol{\lambda})$ a la clase de aproximación de largo $1/N$.

Se sigue de la definición:

Corolario 11.5.1: En la situación 11.4, para cada $\beta \in \mathcal{C}(\boldsymbol{\lambda}; N)$ y cada $v \in S$ se satisfacen:

$$\Lambda(\beta)^{\lambda_v+1/N} < \text{mín}\{1, |\beta - \alpha_v|_v\} \leq \Lambda(\beta)^{\lambda_v}, \tag{11.2}$$

$$1 - \frac{|S|}{N} \leq \sum_{v\in S} \lambda_v \leq 1. \tag{11.3}$$

Demostración: La primera identidad es expandir la definición. Para la segunda empleamos que $\mathcal{C}(\boldsymbol{\lambda}; N)$ es no vacía, ya que contiene al β del enunciado, y por tanto, existe un punto $\boldsymbol{x}$ en el correspondiente subcubo, cuyas coordenadas suman $\sum_{v\in S} x_v = 1$. Como las coordenadas de $\boldsymbol{\lambda}$ son mínimas en el subcubo, tenemos la desigualdad $\sum_{v\in S} \lambda_v \leq 1$; como el subcubo tiene largo $1/N$ concluimos la restante. □

Ojo que la segunda igualdad se cumple, precisamente porque la clase $\mathcal{C}(\boldsymbol{\lambda}; N)$ es no vacía.

Definición 11.6: Sea K un cuerpo semiglobal. Una sucesión $(\beta_1, \ldots, \beta_m) \in K^m$ se dice (L, M)-***independiente***, donde $L \geq 0$ y $M \geq 2$ son números reales, si $h(\beta_1) \geq L$ y cada $h(\beta_{j+1}) \geq Mh(\beta_j)$ para $1 \leq j < m$.

Corolario 11.6.1: Sea K un cuerpo numérico. Todo conjunto infinito de K contiene sucesiones infinitas (L, M)-independientes para todo $L \geq 0$ y $M \geq 2$.

Demostración: Esto se sigue del teorema de finitud de Northcott. □

Definición 11.7: Dado un entero $m \geq 1$ y un real $t \geq 0$, se dentota

$$\mathcal{V}_m(t) := \{\boldsymbol{x} \in [0, 1]^m : x_1 + \cdots + x_m \leq t\} \subseteq \mathbb{R}^m,$$

y se denota $V_m(t) := \text{Vol}\, \mathcal{V}_m(t)$. Dado $\boldsymbol{t} \in \mathbb{R}^n_{\geq 0}$, defínase

$$V_m(\boldsymbol{t}) := \sum_{j=1}^{n} V_m(t_j).$$

Lema 11.8.A: En la situación 11.4, la cantidad de clases de aproximación

de largo $1/N$ (no vacíos) es menor o igual a

$$\binom{N+|S|}{|S|} < 2^{N+|S|}.$$

Demostración: Sea $\mathcal{C}(\boldsymbol{\lambda}; N)$ una clase de aproximación no vacía. El vértice satisface que $n_v := N\lambda_v \geq 0$ sean todos enteros y empleando (11.3) obtenemos

$$\sum_{v\in S} n_v \leq N.$$

Este es un problema combinatorio, cuya cantidad de soluciones viene descrita en el enunciado. □

Lema 11.8.B: Dado un entero $m \geq 1$ y $0 \leq \epsilon \leq 1/2$, entonces

$$V_m\big((1/2-\epsilon)m\big) \leq \exp(-6m\epsilon^2).$$

Lema 11.8.C: Sea K un cuerpo numérico y F/K una extensión finita de grado r. Sean $\boldsymbol{\alpha}_1 := (\alpha_{11}, \ldots, \alpha_{1m}), \ldots, \boldsymbol{\alpha}_n \in F^m$ vectores de puntos y sea $\boldsymbol{t} \in \mathbb{R}^n_{\geq 0}$ tal que $rV_m(\boldsymbol{t}) < 1$. Para todos enteros suficientemente grandes $d_1, \ldots, d_m$, existe un polinomio $f(\boldsymbol{x}) \in K[x_1, \ldots, x_m]$ no nulo con grados parciales menores que $d_1, \ldots, d_m$, tal que:

1. El índice está acotado por $\text{índ}(f; \boldsymbol{d}; \boldsymbol{\alpha}_i) \geq t_i$ para $1 \leq i \leq n$.

2. La altura de f está acotada por

$$h(f) \leq \frac{r}{1 - rV_m(\boldsymbol{t})} \sum_{i=1}^{n} \sum_{j=1}^{m} V_m(t_i)\big(h(\alpha_{ij}) + \log 2 + o(1)\big)d_j,$$

donde el $o(1)$ es cuando $d_j \to \infty$ para $1 \leq j \leq m$.

Demostración: Sean $\boldsymbol{i} := (i_1, \ldots, i_m), \boldsymbol{j} := (j_1, \ldots, j_m) \in \mathbb{N}^m$ un par de multiíndices. Sea $f(\boldsymbol{x}) := \sum_{\boldsymbol{j}} p_{\boldsymbol{j}} \boldsymbol{x}^{\boldsymbol{j}}$ un polinomio arbitrario, sin fijar, y considere el sistema de ecuaciones

$$\partial_{\boldsymbol{i}} f(\boldsymbol{\alpha}_\ell) = 0, \qquad \text{donde} \quad \frac{i_1}{d_1} + \cdots + \frac{i_\ell}{d_\ell} < t_\ell.$$

Esto determina un sistema lineal en los coeficientes $p_{\boldsymbol{j}}$, por lo que tenemos

$$N := (d_1+1)\cdots(d_m+1) \sim d_1 \cdots d_m$$

variables, mientras que el número de ecuaciones es

$$M \sim V_m(\boldsymbol{t}) d_1 \cdots d_m;$$

así, cuando $d_i \to \infty$ se satisface que $N > rM$.

Los coeficientes del sistema lineal son

$$\mathcal{A} := \left[\binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{\alpha}_\ell^{\boldsymbol{j}-\boldsymbol{i}} \right]_{(\boldsymbol{i},\ell),\boldsymbol{j}},$$

donde las filas están indexadas por $(\boldsymbol{i}, \ell)$ y las columnas por $\boldsymbol{j}$. Ahora aplicamos el lema de Siegel relativo, lo que nos da una solución $\boldsymbol{x}$ tal que

$$H(\boldsymbol{x}) \leq |D_{K/\mathbb{Q}}|^{1/2r} \left(\sqrt{N} \prod_{(\boldsymbol{i},\ell)} H(\mathcal{A}_{(\boldsymbol{i},\ell),*}) \right)^{r/(N-rM)},$$

el vector fila $\mathcal{A}_{(\boldsymbol{i},\ell),*}$ tiene entradas $\binom{\boldsymbol{j}}{\boldsymbol{i}} \boldsymbol{\alpha}_\ell^{\boldsymbol{j}-\boldsymbol{i}}$ acotadas por

$$H(\mathcal{A}_{(\boldsymbol{i},\ell)}) \leq \prod_{j=1}^{m} \left(2H(\alpha_{\ell,j})\right)^{d_j},$$

la cual es una cota independiente de $\boldsymbol{i}$.

Nótese que para ℓ fijo hay $V_m(t) d_1 \cdots d_m$ elecciones para $\boldsymbol{i}$, de modo que el producto de las alturas $H(\mathcal{A}_{(\boldsymbol{i},\ell)})$ está acotado por:

$$\left(\prod_{\ell=1}^{s} \prod_{j=1}^{m} \left(2H(\alpha_{\ell,j})\right)^{d_j V_m(t_\ell)} \right)^{(1+o(1)) d_1 \cdots d_m}.$$

Finalmente, como $\boldsymbol{x}$ es el vector de coeficientes de $f(\boldsymbol{x})$, entonces la altura $H(\boldsymbol{x})$ es la altura $H(f)$. Cuando $d_j \to \infty$, el término $|D_{K/\mathbb{Q}}|^{1/2r}$ y $\sqrt{N}$ son despreciables, en cambio, $2^{d_j V_m(t_\ell)}$ sí es significativo, lo que nos da la cota del enunciado. □

La siguiente formulación es una generalización de Lang:

Teorema 11.8 – *Teorema de Roth, 1955*: Sea K un cuerpo numérico, $S \subseteq M_K$ un conjunto finito de lugares y L/K una extensión finita. Para cada $v \in S$ escojamos una extensión $V \mid v$ en L y un número

$\alpha_v \in L$. Para todo $\kappa > 2$ existen solo finitos $\beta \in K$ tales que

$$\Lambda(\beta) = \prod_{v \in S} \min\{1, |\beta - \alpha_v|_V\} \leq H(\beta)^{-\kappa}.$$

Demostración: Procedemos por contradicción, y supondremos que existen infinitos β's con $\Lambda(\beta) \leq H(\beta)^{-\kappa}$. Por finitud de Northcott, ello implica que hay infinitas aproximaciones no triviales y, por el principio del palomar, que hay una clase de aproximación $\mathcal{C}(\boldsymbol{\lambda}; N)$ con infinitos elementos.

(i) El polinomio auxiliar: Sea $D > 0$ un número real (sin fijar), $m \geq 1$ un entero (sin fijar), sea $\boldsymbol{\beta} := (\beta_1, \ldots, \beta_m) \in K^m$ una sucesión (L, M)-independiente en $\mathcal{C}(\boldsymbol{\lambda}; N)$ y defínanse $d_j := \lfloor D/h(\beta_j) \rfloor$ para $1 \leq j \leq m$. Sea $0 < \epsilon < 1/2$ (sin fijar) y defínase $\boldsymbol{t} := (t_v)_{v \in S}$ con $t_v := (1/2 - \epsilon)m$; por el lema 11.8.B se calcula que

$$rV_m(\boldsymbol{t}) = r|S|V_m\big((1/2 - \epsilon)m\big) < r|S|e^{-6m\epsilon^2} \leq \frac{1}{2},$$

donde la última desigualdad se satisface cuando fijamos

$$m > \frac{\log(2r|S|)}{6\epsilon^2}.$$

Ahora, podemos aplicar el lema 11.8.C, lo cual nos da un polinomio $f(\boldsymbol{x}) \in K[\boldsymbol{x}]$ no nulo con grados parciales menores que $d_1, \ldots, d_m$ y tal que

$$\text{índ}(f; \boldsymbol{d}; \boldsymbol{\alpha}) \geq \left(\frac{1}{2} - \epsilon\right) m,$$

$$h(f) \leq \left(\sum_{v \in S} \sum_{j=1}^{m} \frac{h(\alpha_v) + \log 2}{h(\beta_j)} \right) D + o(D)$$

donde empleamos que $rV_m(\boldsymbol{t})/(1 - rV_m(\boldsymbol{t})) < 1$ y que $d_j = D/h(\beta_j) + O(1)$. Sea

$$C_1 := |S| \left(\max_{v \in S}\{h(\alpha_v)\} + \log 2 \right),$$

entonces para $D \gg 0$ se obtiene que

$$h(f) \leq 2C_1 D/L,$$

donde $\sum_{j=1}^{m} 1/h(\beta_j) \leq 2/L$.

(II) El no anulamiento: En el paso anterior obtuvimos un polinomio $f(\boldsymbol{x})$ con «índice grande en $\boldsymbol{\alpha}$», ahora queremos ver que no se anula en $\boldsymbol{\beta}$. Para ello querremos aplicar el lema de Roth en el punto $\boldsymbol{\beta}$ con los grados d_j's, para lo cual fijaremos la sucesión de manera conveniente.

Sea $0 < \sigma \leq 1/2$ (sin fijar). Fijamos $\boldsymbol{\beta}$ como una sucesión (L, M)-independiente para D suficientemente grande, donde $M \geq 2/\sigma$ (con L sin fijar). Así, los grados parciales d_j's decrecen rápidamente. Empleando que $d_j h(\beta_j) \sim D$ y que $d_1 \leq D/h(\beta_1) \leq D/L$ obtenemos que

$$d_j h(\beta_j) \sim D \leq \frac{h(f) + 4md_1}{\sigma} \leq \frac{2C_1 + 4m}{\sigma L} \cdot D,$$

lo cual se satisface si fijamos $L \geq (2C_1 + 4m)\sigma^{-1}$. Aplicando el lema de Roth para f sobre $\boldsymbol{\beta}$ obtenemos que

$$\text{índ}(f; \boldsymbol{d}; \boldsymbol{\beta}) \leq 2m\sigma^{2^{1-m}}.$$

Fijemos $\sigma := \epsilon^{2^{m-1}}$, entonces se deduce que existe $\boldsymbol{\mu}$ tal que $\partial_{\boldsymbol{\mu}} f(\boldsymbol{\beta}) \neq 0$ y tal que

$$\sum_{j=1}^{m} \frac{\mu_j}{d_j} \leq 2m\epsilon.$$

Definiendo $g := \partial_{\boldsymbol{\mu}} f$ vemos que verifica:

- $g(\boldsymbol{\beta}) \neq 0$.
- $\text{índ}(g; \boldsymbol{d}; \boldsymbol{\alpha}_v) \geq (1/2 - 3\epsilon)m$ para todo $v \in S$, por el inciso 3 del corolario 11.1.1.
- $h(g) \leq 4C_1 D/L$. Para esto, basta notar que los coeficientes de g crecen por un factor de a lo más $2^{d_1 + \cdots + d_j} < 4^{d_1}$.

(III) La cota superior: Queremos acotar $\log |g(\boldsymbol{\beta})|_v$ para todo lugar $v \in M_K$. Definiendo

$$\epsilon_v := \begin{cases} [K_v : \mathbb{Q}_v]/[K : \mathbb{Q}], & v \mid \infty \\ 0, & v \nmid \infty \end{cases}$$

tenemos la siguiente cota trivial para $v \notin S$:

$$\log |g(\boldsymbol{\beta})|_v \leq \log |g|_v + \sum_{j=1}^{m} (\log^+ |\beta_j|_v + \epsilon_v o(1)) d_j, \tag{11.4}$$

donde $o(1) \to 0$ cuando $d_j \to \infty$.

Si $v \in S$, podemos hacerlo mejor. Primero, expándamos g como serie de Taylor centrada en $\boldsymbol{\alpha}_v$:

$$g(\boldsymbol{\beta}) = \sum_{\boldsymbol{j}} \partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v)(\beta_1 - \alpha_v)^{j_1} \cdots (\beta_m - \alpha_v)^{j_m}.$$

Por construcción de g, sabemos que

$$\frac{j_1}{d_1} + \cdots + \frac{j_m}{d_m} < \left(\frac{1}{2} - 3\epsilon\right) m \implies \partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v) = 0.$$

La cota trivial es, en este caso,

$$\log |\partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v)|_V \leq \log |g|_v + \sum_{\ell=1}^{m} \log^+ |\alpha_v|_V (d_\ell - j_\ell) + \epsilon_v (\log 2 + o(1)) d_\ell,$$

si en ella empleamos también la siguiente cota elemental

$$\log |a-b|_V \leq -\log^+ \left(\frac{1}{|a-b|_V}\right) + \log^+ |a|_V + \log^+ |b|_V + \epsilon_v \log 2,$$

obtenemos que

$$\begin{aligned} \log \left| \partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v) \prod_{\ell=1}^{m} (\beta_\ell - \alpha_v)^{j_\ell} \right|_V &\leq \log |g|_v - \sum_{\ell=1}^{m} j_\ell \log^+ \left(\frac{1}{|\beta_j - \alpha_v|_V}\right) \\ &\quad + \sum_{\ell=1}^{m} \big(\log^+ |\beta_\ell|_v + \log^+ |\alpha_v|_V + (\log 4 + o(1))\epsilon_v \big) d_\ell. \end{aligned}$$

Así pues, podemos estimar:

$$\begin{aligned} \log |g(\boldsymbol{\beta})|_v &= \log \left| \sum_{\boldsymbol{j}} \partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v) \prod_{\ell=1}^{m} (\beta_\ell - \alpha_v)^{j_\ell} \right|_V \\ &\leq \max_{\boldsymbol{j}} \log \left| \partial_{\boldsymbol{j}} g(\boldsymbol{\alpha}_v) \prod_{\ell=1}^{m} (\beta_\ell - \alpha_v)^{j_\ell} \right|_V + \epsilon_v \sum_{\ell=1}^{m} \log(d_\ell + 1) \\ &\leq -\underline{\min} \left\{ \sum_{\ell=1}^{m} j_\ell \log^+ \frac{1}{|\beta_j - \alpha_v|_V} \right\} + \log |g|_v \\ &\quad + \sum_{\ell=1}^{m} \big(\log^+ |\beta_\ell|_v + \log^+ |\alpha_v|_V + (\log 4 + o(1))\epsilon_v \big) d_\ell; \end{aligned} \tag{11.5}$$

donde $\underline{\text{mín}}$ es el mínimo sobre los multiíndices $\boldsymbol{j}$'s tales que

$$\frac{j_1}{d_1} + \cdots + \frac{j_m}{d_m} \geq \left(\frac{1}{2} - 3\epsilon\right) m. \tag{11.6}$$

Si ahora tomamos una sumatoria sobre todos los lugares $v \in M_K$ recogiendo (11.4), (11.5) y que $\sum_{v\in M_K} \epsilon_v = 1$, obtendremos

$$\sum_{v\in M_K} \log |g(\boldsymbol{\beta})|_v \leq -\sum_{v\in S} \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} j_\ell \log^+ \frac{1}{|\beta_j - \alpha_v|_V} \right\} + h(g) + \sum_{\ell=1}^{m} \left(h(\beta_\ell) + \sum_{v\in S} \log^+ |\alpha_v|_V + \log 4 + o(1) \right) d_\ell.$$

Además, ya sabemos que $h(g) \leq 4C_1 D/L$, que $d_\ell h(\beta_\ell) \sim D$, que $\sum_{\ell=1}^{m} d_\ell \leq 2d_1 \leq 2D/L + o(D/L)$; por lo que tenemos que

$$\sum_{v\in M_K} \log |g(\boldsymbol{\beta})|_v \leq h(g) - \sum_{v\in S} \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} j_\ell \log^+ \frac{1}{|\beta_j - \alpha_v|_V} \right\} + \left(m + \frac{C_2}{L} \right) D + o(D),$$

donde $C_2 := 4C_1 + 2\log 4 + 2|S|\,\text{máx}_{v\in S}\{\log^+ |\alpha_v|_V\}$.

Procedemos a acotar $\underline{\text{mín}}$. En primer lugar, recordemos que cada $\Lambda(\beta_\ell) \leq H(\beta_\ell)^{-\kappa}$ por hipótesis. En segundo lugar, recordemos que cada $\beta_\ell \in \mathcal{C}(\boldsymbol{\lambda}; N)$, por lo que empleando (11.2), se satisface que

$$\lambda_v \kappa h(\beta_\ell) \leq \lambda_v \log \frac{1}{\Lambda(\beta_\ell)} \leq \log^+ \frac{1}{|\beta_\ell - \alpha_v|_V}.$$

Luego

$$\begin{aligned} \sum_{v\in S} \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} j_\ell \log^+ \frac{1}{|\beta_\ell - \alpha_v|_V} \right\} &\geq \sum_{v\in S} \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} \lambda_v \kappa h(\beta_\ell) j_\ell \right\} \\ &= \kappa \left(\sum_{v\in S} \lambda_v \right) \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} h(\beta_\ell) d_\ell \frac{j_\ell}{d_\ell} \right\} \\ &\sim D\kappa \left(\sum_{v\in S} \lambda_v \right) \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} \frac{j_\ell}{d_\ell} \right\}. \end{aligned}$$

Finalmente (11.6) se traduce en

$$\underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} \frac{j_\ell}{d_\ell} \right\} \geq \left(\frac{1}{2} - 3\epsilon \right) m$$

y aplicando (11.3), se concluye:

$$\sum_{v \in S} \underline{\text{mín}} \left\{ \sum_{\ell=1}^{m} j_\ell \log^+ \frac{1}{|\beta_\ell - \alpha_v|_V} \right\} \geq \kappa \left(1 - \frac{|S|}{N} \right) \left(\frac{1}{2} - 3\epsilon \right) mD + o(D).$$

Empleando la cota del $\underline{\text{mín}}$, todo se resume en:

$$\sum_{v \in M_K} \log |g(\boldsymbol{\beta})|_v \leq -\kappa \left(1 - \frac{|S|}{N} \right) \left(\frac{1}{2} - 3\epsilon \right) mD + \left(m + \frac{C_2}{L} \right) D + o(D).$$

(iv) Cota inferior: Como $g(\boldsymbol{\beta}) \neq 0$, por la fórmula del producto:

$$\sum_{v \in M_K} \log |g(\boldsymbol{\beta})|_v = 0.$$

(v) Confrontar cotas: Dividiendo por mD cuando $D \to \infty$, las cotas se confrontan en:

$$-\kappa \left(1 - \frac{|S|}{N} \right) \left(\frac{1}{2} - 3\epsilon \right) + 1 + \frac{C_2}{mL} \geq 0,$$

que se reescribe como

$$\kappa \leq \left(1 + \frac{C_2}{L} \right) \left(1 - \frac{|S|}{N} \right)^{-1} \left(\frac{1}{2} - 3\epsilon \right)^{-1}.$$

Cuando $\epsilon \to 0$, $L \to \infty$ y $N \to \infty$, el lado derecho converge a 2, lo que contradice que $\kappa > 2$. □

Finalmente, con $K = \mathbb{Q}$ y $S = \{\infty\}$ obtenemos el enunciado clásico:

Corolario 11.8.1: Sea $\alpha \in \mathbb{R} \cap \mathbb{Q}^{\mathrm{alg}}$ un real algebraico. Para todo $\epsilon > 0$ existen finitas aproximaciones $u/v \in \mathbb{Q}$ tales que

$$\left|\alpha - \frac{u}{v}\right|_\infty \leq \frac{1}{v^{2+\epsilon}}.$$

Por supuesto, lo interesante es que tomando $\epsilon = 0$ existen infinitas aproximaciones por el teorema de Dirichlet.

Hay una extensión que resultará particularmente útil. Si en lugar de considerar $\alpha \in \mathbb{A}^1_{\mathbb{Q}}$ queremos una «extensión» a $\alpha \in \mathbb{P}^1_{\mathbb{Q}}$, podríamos definir para $\beta \neq 0$:

$$|\infty - \beta|_v := |\beta|_v^{-1}. \tag{11.7}$$

Esta extensión está justificada desde el siguiente punto de vista: al considerar $\beta \neq 0$, ambos α y β viven en la carta afín $\mathbb{A}^1_{\mathbb{Q}} \cong \{[x : y] : x \neq 0\} \subseteq \mathbb{P}^1_{\mathbb{Q}}$, donde el isomorfismo viene dado por $z \mapsto [1 : z]$, mediante el cual $\beta = [\beta : 1]$ se manda a $1/\beta$ y $\alpha \mapsto 0$.

Si ahora nos restringimos a la intersección de las dos cartas afines de $\mathbb{P}^1$ llegamos al grupo multiplicativo $(K^{\mathrm{alg}})^\times$, donde combinando un teorema de Roth común, con la definición de (11.7), se obtiene:

Corolario 11.8.2: Sea K un cuerpo numérico, sea $G \subseteq K^\times$ un grupo multiplicativo finitamente generado y sea $S \subseteq M_K$ un conjunto finito de lugares. Para todo $\epsilon > 0$ existen solo finitos $\gamma \in G$ tales que

$$\prod_{v \in S} |\gamma - 1|_v \leq H(\gamma)^{-\epsilon}. \tag{11.8}$$

Demostración: Sea $T \subseteq M_K$ un conjunto finito de lugares tal que $G \subseteq U_{K,T}$ y $S \subseteq T$. Fijemos una solución $\gamma \in G$ de (11.8). Ahora, defínanse T_0 el conjunto de los $v \in M_K$ tales que $|\gamma|_v < 1/2$, T_∞ el conjunto de los $v \in M_K$ tales que $|\gamma|_v > 2$ y $T_1 \subseteq S$ el conjunto de los $v \in S$ tales que $|\gamma - 1|_v < 1/2$. Nótese que $T_0, T_1, T_\infty \subseteq T$ y son disjuntos (¿por qué?); denotaremos por t_0, t_1, t_∞, t sus cardinalidades resp. Entonces

$$H(\gamma)^{-\epsilon} \geq \prod_{v \in T} |\gamma - 1|_v \geq \frac{1}{2^{t-t_1}} \prod_{v \in T_1} |\gamma - 1|_v \geq \frac{1}{2^t} \prod_{v \in T_1} |\gamma - 1|_v.$$

Ahora bien, si $v \in M_K$ es un lugar no arquimediano y $|\alpha|_v < 1$, entonces de las definiciones $|\alpha|_v \leq 1/2$, de modo que como $\gamma \in G$ es una T-unidad vemos que

$$\prod_{v \in T_0} |\gamma|_v = \prod_{v \in T_\infty} |\gamma|_v^{-1} = H(\gamma)^{-1}. \tag{11.9}$$

Sea $\Phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ la transformación lineal fraccionaria $x \mapsto \frac{x}{x+1}$ que manda $(0,1,\infty) \mapsto (0,1/2,1)$. Nótese que satisface lo siguiente:

$$\begin{aligned} |x-0|_v \leq \frac{1}{2} &\implies \frac{1}{2}|x-0|_v \leq |\Phi(x)-0|_v \leq 2|x-0|_v \\ |x-1|_v \leq \frac{1}{2} &\implies \frac{1}{2}|x-1|_v \leq \left|\Phi(x)-\frac{1}{2}\right|_v \leq 2|x-1|_v \\ |x-\infty|_v \leq \frac{1}{2} &\implies \frac{1}{2}|x-\infty|_v \leq |\Phi(x)-1|_v \leq 2|x-\infty|_v \end{aligned}$$

De modo que

$$\begin{aligned} &\prod_{v\in T_0} |\gamma|_v \cdot \prod_{v\in T_\infty} |\gamma|_v^{-1} \cdot \prod_{v\in T_1} |\gamma-1|_v \\ &\qquad\qquad \geq \frac{1}{2^t} \prod_{v\in T_0} |\Phi(\gamma)|_v \cdot \prod_{v\in T_\infty} |\Phi(\gamma)-1|_v \cdot \prod_{v\in T_1} \left|\Phi(\gamma)-\frac{1}{2}\right|_v, \end{aligned}$$

empleando ahora la igualdad (11.9) obtenemos que

$$\begin{aligned} &\prod_{v\in T_0} |\Phi(\gamma)|_v \cdot \prod_{v\in T_\infty} |\Phi(\gamma)-1|_v \cdot \prod_{v\in T_1} \left|\Phi(\gamma)-\frac{1}{2}\right|_v \\ &\qquad\qquad \leq H(\gamma)^{-2} 2^t \left(\prod_{v\in T_1} |\gamma-1|_v\right) \leq \frac{1}{H(\gamma)^{2+\epsilon}}. \end{aligned}$$

Y concluimos por una aplicación del teorema de Roth usual. □

11.2 Aplicaciones

§11.2.1 Digresión: recubrimientos y el teorema de Belyĭ. Antes de enunciar el teorema de Belyĭ aclaremos un poco de notación: denotamos por $\Gamma(2) \leq \mathrm{SL}_2(\mathbb{Z})$ el núcleo del homomorfismo $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_2)$ de reducción módulo 2. Recuérdese que ${}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$, así que denotamos por $\overline{\Gamma}(2)$ a la imagen de $\Gamma(2)$ en el cociente. Es sabido que las matrices de $\mathrm{SL}_2(\mathbb{Z})$ actúan sobre el semiplano complejo superior $\mathfrak{h} \subseteq \mathbb{C}$.

Lema 11.9 (Belyĭ): Sea $g\colon C_1 \to C_2$ un morfismo no constante entre curvas íntegras suaves sobre un cuerpo numérico K y sea $S \subseteq C_1(K^{\mathrm{alg}})$ un conjunto finito de puntos. Existe una aplicación racional no constante $h\colon C_2 \dashrightarrow \mathbb{P}^1_K$ tal que $f := g \circ h\colon C_1 \dashrightarrow \mathbb{P}^1_K$ es no ramificado fuera de $f^{-1}[\{0,1,\infty\}]$ y tal que $f[S] \subseteq \{0,1,\infty\}$.

Teorema 11.10 (de Belyĭ): Sea C una curva íntegra, proyectiva, suave sobre $\mathbb{C}$. Son equivalentes:

1. Existe una curva C' sobre $\mathbb{Q}^{\mathrm{alg}}$ tal que $C' \times_{\mathbb{Q}^{\mathrm{alg}}} \operatorname{Spec}\mathbb{C} \cong C$.
2. Existe una aplicación racional no constante $f\colon C \dashrightarrow \mathbb{P}^1_{\mathbb{C}}$ ramificada en a lo más tres puntos.
3. Existe un subgrupo de índice finito $G \leq \overline{\Gamma}(2)$ tal que $\mathfrak{h}/G$ es isomorfo a la analitificación de un abierto Zariski-denso $U \subseteq C$.

§11.2.2 Puntos S-enteros en variedades. La generalización natural de «soluciones enteras a ecuaciones diofánticas» se corresponde a «puntos enteros» de un esquema afín. Lo primero es esclarecer qué se entiende por «punto entero» ya que un esquema es en sí mismo una especie de «espacio abstracto, sin un sistema fijo de coordenadas».

Lema 11.11.A: Sea K un cuerpo global, sea $M_K^\infty \subseteq S \subseteq M_K$ un conjunto finito de lugares y sea $A := \mathfrak{o}_{K,S}$. Dada una una variedad afín X sobre K, para un conjunto de puntos racionales $T \subseteq X(K)$ son equivalentes:

1. Para toda función regular $f \in \Gamma(X, \mathscr{O}_X)$ existe $a \in K^\times$ tal que $f[T] \subseteq aA$.
2. Existe un A-esquema de tipo finito Y tal que:
   (a) $X = Y_K = Y \times_A \operatorname{Spec} K$.
   (b) Todo punto de T está en correspondencia con un punto A-valuado en $Y(A)$.[1]
3. Existe un A-esquema afín de tipo finito que satisface (a) y (b).

Demostración: $1 \implies 3$. Sea $j = (j_1, \ldots, j_n)\colon X \hookrightarrow \mathbb{A}^n_K$ un K-encaje cerrado, lo que se corresponde a un conjunto de funciones racionales $j_1, \ldots, j_n \in \Gamma(X, \mathscr{O}_X)$, de modo que existe $a \in K^\times$ tal que cada $j_i[T] \subseteq aA$. Nótese que

[1] Si el lector prefiere, la inclusión $A \hookrightarrow K$ induce un morfismo fijo $f\colon \operatorname{Spec} K \to \operatorname{Spec} A$ (o un punto K-valuado de A). La precomposición por f nos da una función $Y(A) \to Y(K)$ y, finalmente, el cambio de base $Y_K = X \to Y$ da, mediante la propiedad universal de los productos fibrados, una función $Y(K) \to X(K)$. Esta correspondencia $Y(A) \to X(K)$ establece una biyección con T.

$\Gamma(X, \mathscr{O}_X)$ es una K-álgebra y, por tanto, una A-álgebra. Definamos finalmente

$$B := A\left[\tfrac{1}{a}j_1, \ldots, \tfrac{1}{a}j_n\right] \subseteq \Gamma(X, \mathscr{O}_X),$$

entonces $Z := \operatorname{Spec} B$ es un A-esquema afín de tipo finito y su cambio de base es $Z_K = \operatorname{Spec}(B \otimes_A K)$. Que j sea un encaje cerrado se traduce en que los j_i's generen (como K-álgebra) a $\Gamma(X, \mathscr{O}_X)$ por lo que se comprueba lo exigido.

$3 \implies 2$. Trivial.

$2 \implies 1$. Sea $f \in \Gamma(X, \mathscr{O}_X) = \Gamma(Y, \mathscr{O}_Y) \otimes_A K$. Existe $b \in A$ no nulo tal que $fb \in \Gamma(Y, \mathscr{O}_Y)$ y, por la correspondencia, vemos que $f[T] \subseteq \frac{1}{b}A$. □

Definición 11.11 (Serre): En la situación anterior, decimos que $T \subseteq X(K)$ es un ***conjunto de puntos S-enteros*** o ***A-enteros*** si satisface las condiciones del lema anterior.

Así, el que un punto sea S-entero o no depende de la elección de un conjunto ambiente (por ejemplo, todo conjunto que consta de un solo punto es trivialmente S-entero). Esto es, a mi juicio, positivo ya que la definición ingenua de «punto con coordenadas S-enteras» depende de una elección de coordenadas (i.e., de un encaje cerrado $X \hookrightarrow \mathbb{A}^m_K$); mientras que el conjunto $\frac{1}{2}\mathbb{Z} \subseteq \mathbb{A}^1(\mathbb{Q})$ es $\mathbb{Z}$-entero.

Ejemplo. Sea K un cuerpo global, $M_K^\infty \subseteq S \subseteq K$ un conjunto finito de lugares y $A := \mathfrak{o}_{K,S}$. Sea $i\colon X \hookrightarrow \mathbb{A}^m_K$ un subesquema cerrado. El conjunto

$$X(K) \cap A^m \subseteq \mathbb{A}^m(K)$$

es un conjunto de puntos S-enteros, llamado el ***conjunto canónico*** (respecto a i).

La siguiente aplicación es original de Corvaja y Zannier **[77]:**

Teorema 11.12: Sea K un cuerpo global, $M_K^\infty \subseteq S \subseteq K$ un conjunto finito de lugares y $A := \mathfrak{o}_{K,S}$. Dada una curva afín C sobre K, denotemos por $\overline{C}$ su clausura proyectiva. Si $\overline{C} \smallsetminus C$ tiene al menos tres puntos, entonces todo conjunto de puntos S-enteros de C es finito.

Demostración: Sea $\widetilde{C}$ la normalización de $\overline{C}$; nótese que $|\widetilde{C} \smallsetminus C| \geq |\overline{C} \smallsetminus C|$, por lo que trabajaremos con $\widetilde{C}$ que es suave. Sean $q_1, \ldots, q_r \in \widetilde{C} \smallsetminus C$; pasando

a una extensión finita de K podemos suponer que cada $\Bbbk(q_i) = K$. Para todo entero N considere el K-espacio vectorial

$$V = V_N := \{f \in \Gamma(C, \mathscr{O}_C) : \operatorname{div} f \geq -N(q_1 + \cdots + q_r)\}$$

de dimensión finita d_N y sea $f_1, \ldots, f_d$ una base de V. Por el teorema de Riemann-Roch obtenemos que $d_N \geq Nr + 1 - g$, donde g es el género de $\widetilde{C}$.

Sea $X \subseteq C$ un conjunto infinito de puntos S-enteros. Dentro de X podemos construir una sucesión $(P_n \in X)_{n\in\mathbb{N}}$ de puntos distintos tales que para todo $v \in S$ la sucesión converge v-ádicamente a $P^v \in \widetilde{C}(K_v)$; sea S' el conjunto de puntos tales que $P^v \in \widetilde{C} \smallsetminus C$ y sea $S'' := S \smallsetminus S'$. Para $v \in S'$ sea $\{L_{1,v}, \ldots, L_{d,v}\}$ una K-base de V tal que cada

$$_{P^v}(L_{j,v}) \geq N - j + 1.$$

En general, sea $g \in K(\widetilde{C})$ con $q :=_{P^v} (g)$, entonces gt_v^{-q} es regular en P^v, es decir, $|t_v^{-q}(P_n)g(P_n)|$ es acotado y $|g(P_n)|_v \ll |t_v(P_n)|^q$; aplicándolo a $L_{j,v}$ obtenemos que $|L_{j,v}(P_n)|_v \ll |t_v(P_n)|_v^{j-1-N}$. Para $w \in S''$ sea $L_{j,w} := f_j$ nuestra base fijada al comienzo. Para cada $v \in S'$ sea $t_v \in K(\widetilde{C})$ un parámetro local de P^v, entonces se tiene que

$$\forall 1 \leq j \leq d, \qquad |L_{j,v}(P_n)|_v \ll |t_v(P_n)|_v^{j-1-N},$$

y que $|L_{j,w}(P_n)|_w \ll 1$ para todo $w \in S''$ (por defínción de X). En consecuencia

$$\begin{aligned}\prod_{v\in S}\prod_{j=1}^{d} |L_{j,v}(P_n)|_v &\ll \left(\prod_{v\in S'} |t_v(P_n)|_v\right)^{\frac{d}{2}(d-2N-1)} \\ &\leq \left(\prod_{v\in S'} |t_v(P_n)|_v\right)^{\frac{d}{2}((r-2)N-g)}.\end{aligned}$$

Ahora bien, cada f_j se anula en P^v con multiplicidad $\leq N$, de modo que $\max_j\{|f_j(P_n)|_v\} \ll |t_v(P_n)|_v^{-N}$ para $v \in S'$; en otras palabras

$$H(f_1(P_n) : \cdots : f_d(P_n)) \ll \left(\prod_{v\in S'} |t_v(P_n)|_v\right)^{-N},$$

lo que, confrontado a la cota anterior, nos da

$$\prod_{v\in S}\prod_{j=1}^{d} |L_{j,v}(P_n)|_v \ll H(f_1(P_n) : \cdots : f_d(P_n))^{-\frac{d}{2N}((r-2)N-g)}.$$

Para $N \geq g+1$ se cumple que $d \geq 2$, de modo que podemos aplicar el teorema del subespacio de Schmidt para concluir que los puntos proyectivos $[f_1(P_n) : \cdots : f_d(P_n)]$ están contenidos en una unión de subfibrados lineales propios de $\mathbb{P}^d_K$, pero esto es absurdo ya que los f_i's son K-linealmente independientes. □

Teorema 11.13 – *Teorema de Siegel, 1929*: Sea K un cuerpo global, $M_K^\infty \subseteq S \subseteq K$ un conjunto finito de lugares y $A := \mathfrak{o}_{K,S}$. Si C es una curva geométricamente íntegra afín sobre K con un conjunto infinito de puntos S-enteros, entonces la completación de su normalización $\widetilde{C}$ tiene género 0 y $\widetilde{C} \smallsetminus C$ tiene a lo más dos puntos.

Demostración: Supongamos que $\widetilde{C}$ tiene género $g \geq 1$, entonces si $\widetilde{C}_{\text{an}}$ denota su analitificación (i.e., la curva analítica compleja determinada por sus ecuaciones) ésta corresponde topológicamente a la superficie compacta de género g, de modo que $H_1(\widetilde{C}_{\text{an}}, \mathbb{Z}) \cong \mathbb{Z}^{2g}$. En $\mathbb{Z}^{2g}$ podemos encontrar un subgrupo normal N' de índice ≥ 3 al cual le corresponde un subgrupo normal $N \lhd \pi_1(\widetilde{C}_{\text{an}}, x)$ de índice ≥ 3 y, por correspondencia de Galois, tenemos un recubrimiento topológico $\widetilde{C}'_{\text{an}} \to \widetilde{C}_{\text{an}}$ de grado ≥ 3. Nótese que $\widetilde{C}'_{\text{an}}$ también ha de ser una superficie compacta, es decir, una superficie de Riemann; por correspondencia GAGA, esto se traduce en la existencia de un recubrimiento étale finito $\widetilde{C}' \to \widetilde{C}$ de grado ≥ 3. Ahora $\widetilde{C}' \smallsetminus C$ sí posee tres puntos. □

En particular, toda curva elíptica posee a lo más finitos puntos enteros (en el conjunto canónico).

§11.2.3 Las ecuaciones de S-unidades. Al siguiente resultado se le conoce como la «ecuación de S-unidades en dos variables»:

Teorema 11.14: Sea $G \subseteq \mathbb{Q}^{\text{alg}\,\times}$ un subgrupo multiplicativo finitamente generado (e.g., $G = \mathfrak{o}_{K,S}^\times$ donde K es numérico y $M_K^\infty \subseteq S \subseteq M_K$ es finito). La ecuación

$$u + v = 1$$

tiene finitas soluciones en $(u, v) \in G \times G$.

Demostración: Nótese que existe un cuerpo numérico K y un subconjunto finito de lugares $M_K^\infty \subseteq S \subseteq M_K$ tal que $G \subseteq \mathfrak{o}_{K,S}^\times$, de modo que no perdemos generalidad asumiendo que $G = \mathfrak{o}_{K,S}^\times$. Supongamos que tenemos infinitas soluciones $(u_n, v_n) \in (\mathfrak{o}_{K,S}^\times)^2$ tales que $H(v_n) \geq H(u_n)$; sea $T(u, v)$

el conjunto de lugares $w \in S$ tales que $|v|_w < 1$. Como S es finito, por principio del palomar, podemos suponer que el conjunto $T(u_n, v_n) =: T$ es el mismo para todas. Definiendo $\gamma_n := -u_n/v_n$ obtenemos que $\gamma_n - 1 = -v_n^{-1}$, de modo que

$$\prod_{w\in T} |\gamma_n - 1|_w = \prod_{w\in T} \frac{1}{|v_n|_w} = \prod_{w\in S} \max\{1, |v_n^{-1}|_w\} = H(v_n^{-1})^{-1} = H(v_n)^{-1}.$$

Ahora bien, como $H(\gamma_n) \leq H(u_n)H(v_n) \leq H(v_n)^2$ concluimos que

$$\prod_{w\in T} |\gamma_n - 1|_w \leq H(\gamma_n)^{-1/2}.$$

Pero esto contradice el corolario 11.8.2 del teorema de Roth. □

Una consecuencia de lo anterior es:

Teorema 11.15 (Thue-Mahler): Sea K un cuerpo numérico y $M_K^\infty \subseteq S \subseteq M_K$ un subconjunto finito de lugares. Sea $f(x, y) \in \mathfrak{o}_{K,S}[x, y]$ un polinomio homogéneo con al menos tres factores lineales no proporcionales en $K^{\mathrm{alg}}[x, y]$. Entonces existen finitas parejas $(u, v) \in \mathfrak{o}_{K,S}^2$ salvo factores en $K^\times$ tales que

$$f(u, v) \in \mathfrak{o}_{K,S}^\times.$$

Demostración: Factorizamos:

$$f(x, y) = \prod_{j=1}^{\ell} (\beta_j x - \alpha_j y)^{e_i} \in \mathbb{Q}^{\mathrm{alg}}[x, y],$$

donde los $\beta_j x - \alpha_j y$ son factores no asociados entre sí y cada $e_j \geq 1$. Tras extender a K podemos suponer que cada $\alpha_j, \beta_j \in K$ y que los $\beta_i\alpha_j - \beta_j\alpha_i$ son S-unidades para $i \neq j$. Sea (u, v) una solución de coeficientes S-enteros coprimos, entonces cada $u_j := \beta_j u - \alpha_j v$ es una S-unidad. Considerando los términos u_1, u_2, u_3 y despejando (pues los determinantes son unidades) obtenemos la relación lineal

$$a_1u_1 + a_2u_2 + a_3u_3 = 0,$$

despejando obtenemos una ecuación de S-unidades en dos variables, la cual solo admite finitas soluciones. □

La demostración, tal y como se puede apreciar, depende de la finitud de la ecuación de S-unidades. De momento, tal finitud la hemos probado mediante el teorema de Roth que es *inefectivo*;[2] no obstante, la teoría de formas lineales en logaritmos da una versión efectiva de la ecuación de S-unidades y, en consiguiente, una solución efectiva a las ecuaciones de Thue-Mahler.

Teorema 11.16: Sea K un cuerpo numérico y $M_K^\infty \subseteq S \subseteq M_K$ un subconjunto finito de lugares. Sea $f(x) \in \mathfrak{o}_{K,S}[x]$ un polinomio con al menos tres raíces simples[3] distintas en K^{alg}. Entonces la ecuación

$$v^2 = f(u)$$

admite solo finitas soluciones $(u, v) \in \mathfrak{o}_{K,S} \times K$.

Notas históricas

Las aproximaciones diofánticas podría decirse que comienzan con los resultados clásicos de Dirichlet y Liouville. El teorema de Dirichlet te dice que fijando un número real $\alpha \in \mathbb{R}$ existen infinitas aproximaciones $u/v \in \mathbb{Q}$ tales que

$$\left|\frac{u}{v} - \alpha\right|_\infty \leq \frac{1}{v^2}.$$

Una pregunta central durante medio siglo fue qué tan bueno podía escogerse el exponente de modo que siguiesen existiendo infinitas aproximaciones. Dado un número real α, denotaremos por $\tau(\alpha) > 0$ el mínimo real tal que para todo $e > \tau(\alpha)$ existan solo finitas aproximaciones $u/v \in \mathbb{Q}$ tales que

$$\left|\frac{u}{v} - \alpha\right|_\infty \leq \frac{1}{v^e}.$$

El teorema de Liouville dice que si $\alpha \in \mathbb{Q}^{\text{alg}}$ tiene grado $d := [\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$, entonces $\tau(\alpha) \leq d$. Similarmente, otros matemáticos en el siglo XX probaron las siguientes mejoras:

Liouville	1844	$\tau(\alpha) \leq d$
Thue	1909	$\tau(\alpha) \leq \frac{1}{2}d + 1$
Siegel	1921	$\tau(\alpha) \leq 2\sqrt{d}$
Gel'fond, Dyson	1947	$\tau(\alpha) \leq \sqrt{2d}$
Roth	1955	$\tau(\alpha) = 2$

[2] Vale decir, que no da indicios sobre la ubicación de las finitas soluciones, por ejemplo, con cotas de alturas.

[3] Recuérdese que una raíz α de $f(x)$ se dice *simple* si $(x-\alpha) \mid f(x)$, pero $(x-\alpha)^2 \nmid f(x)$.

El teorema de Roth fue probado en **[58]** y fue generalizado en términos de alturas por Lang **[38].** Nuestra demostración sigue a Corvaja **[75].**

Referencias

66. Ankeny, N. C. Sums of three squares. *Proc. Amer. Math. Soc.* doi:10.1090/S0002-9939-1957-0085275-8 (1957).

69. Bombieri, E. y Gubler, W. *Heights in Diophantine Geometry* (Cambridge University Press, 2006).

70. Cassels, J. W. S. *Global fields* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 42-84.

73. Clark, P. L. *Geometry of numbers with applications to Number Theory* http://alpha.math.uga.edu/~pete/geometryofnumbers.pdf (2015).

75. Corvaja, P. Autour du Théorème de Roth. *Mh. Math.* **124,** 147-175. doi:10.1007/bf01300617 (1997).

76. Corvaja, P. *Integral Points on Algebraic Varieties. An Introduction to Diophantine Geometry* (Springer-Verlag, 2016).

77. Corvaja, P. y Zannier, U. A subspace theorem approach to integral points on curves. *C. R. Acad. Sci. Paris, Ser. I* **334,** 267-271. doi:10.1016/S1631-073X(02)02240-9 (2002).

95. McFeat, R. B. *Geometry of numbers in adèle spaces* PhD (University of Adelaide, 1969).

9. Roquette, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

12

Curvas elípticas

12.1 Definición y ley de grupo

Definición 12.1: Sea k un cuerpo. Una ***curva elíptica*** sobre k es una curva (i.e., esquema algebraico de dimensión 1) íntegra, proyectiva y suave isomorfa a un cerrado de $\mathbb{P}^2_k = \mathrm{Proj}(k[u,v,w])$ dado por una ***ecuación de Weierstrass larga***:

$$E\colon \qquad v^2w + a_1uvw = u^3 + a_2u^2w + a_4uw^2 + a_6, \qquad a_1,\dots,a_6 \in k.$$

Dada una curva proyectiva mediante ecuaciones es fácil verificar que una curva *sea* elíptica, pero no tanto el que *no* lo sea. Sobre la carta afín $w = 1$ uno recupera la típica ecuación de Weierstrass con $(x,y) := (u/w, v/w)$.

Ejemplo. Considere la cúbica (proyectiva) de Fermat $C\colon u^3 + v^3 = w^3$. Es fácil verificar que efectivamente determina una subvariedad suave (e.g., por el criterio del jacobiano), pero a simple vista no parece dada por ecuación de Weierstrass. En primer lugar, aplicamos el cambio de variables $(u,v,w) \mapsto (u, v+w, w)$ y obtenemos que

$$u^3 + (v+w)^3 = w^3 \iff 3vw^2 + 3v^2w = -u^3 - v^3.$$

Pasando a la carta afín $v = 1$ con $(x,y) := (u/v, w/v)$, se obtiene la ecuación $3y^2+3y = -x^3-1$. Podemos multiplicar por 3^3 y ocupar $(x,y) \mapsto (-3x, -9y)$

para obtener la ecuación:

$$y^2 - 9y = x^3 - 27 \iff \left(y - \frac{9}{2}\right)^2 = x^3 - 27 + \frac{9^2}{2^2}.$$

La cual sí es una ecuación de Weierstrass con el cambio de variables $y \mapsto y - 9/2$. Por estética, puede multiplicar todo por 2^6 y obtener la ecuación $y^2 = x^3 - 2^4 \cdot 3^3$.

Nótese que los cambios de variables son todos válidos syss $\operatorname{car} k \notin \{2, 3\}$ (desde ahora denotado como $\operatorname{car} k \nmid 6$). Esto es recurrente en la teoría de curvas elípticas, especialmente las precauciones para característica 2.

Unos recordatorios geométricos de Liu **[4]:**

1. Sea $H := \mathbf{V}_+(f) \subseteq \mathbb{P}^n_k$ una hipersuperficie (i.e., un cerrado definido por una sola ecuación), donde $\deg f =: d$. Entonces su *género aritmético* es $p_a(H) = \binom{d-1}{n}$.

   a) En particular, si $n = 2$, entonces H es una curva en el plano definida por un polinomio homogéneo de grado d y su género aritmético es $\frac{(d-1)(d-2)}{2}$. Esta función crece como se describe en la tabla 12.1.

d	1	2	3	4	5	$\cdots$
$\frac{(d-1)(d-2)}{2}$	0	0	1	3	6	$\cdots$

Figura 12.1

   b) En consecuencia, toda curva elíptica tiene género aritmético 1.

2. Para una variedad proyectiva que es una intersección completa local (abrev., i.c.l.) las nociones de género aritmético y geométrico coinciden. En particular, una curva suave es i.c.l., de modo que no haremos más dicha distinción. Más aún, el género geométrico es un invariante birracional.

3. Una curva íntegra sobre k es elíptica syss es conexa, proyectiva, suave, de género 1 y con un punto k-racional (cfr. **[4,** pág. 286], cor. 7.5.4).

Del inciso 1.(a) se sigue de que toda curva suave proyectiva dada por una ecuación irreducible en el plano de grado 3 con un punto racional es una

curva elíptica. En particular, no es coincidencia que la cúbica proyectiva de Fermat sea una curva elíptica, sino que ya satisface las condiciones descritas anteriormente; por la tabla, esto no aplica para otras variedades de Fermat.

Una aplicación del criterio del jacobiano da lo siguiente:

Lema 12.2: Sea k un cuerpo.

1. La curva proyectiva dada en la carta afín $z = 1$ por la ecuación de Weierstrass larga:

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6$$

es suave syss

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0,$$

donde los b_i's son los llamados ***polinomios de división*** dados por

$$b_2 := a_1^2 + 4a_2, \qquad b_4 := 2a_4 + a_1a_3, \qquad b_6 := a_3^2 + 4a_6,$$
$$b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

2. Si $\operatorname{car} k \neq 2$, entonces la curva proyectiva dada en la carta afín $z = 1$ por la ecuación

$$y^2 = x^3 + ax + b$$

es suave syss

$$\Delta := -16(4a^3 + 27b^2) \neq 0.$$

En ambos casos, el Δ definido se llama el ***discriminante*** de la curva.

Pista: El caso que nos interesa es el segundo, donde notamos que el Δ es -16 multiplicado por el discriminante del polinomio x^3+ax+b. Finalmente, el discriminante de un polinomio es no nulo syss dicho polinomio es separable, vale decir, si no tiene raíces repetidas sobre su cuerpo de escisión, la cual es fácil de verificar que corresponde a la condición para que la curva no tenga puntos singulares.

El caso 1 también se demuestra con un cálculo detallado en Silverman **[105]**. □

El siguiente es un resultado de geometría algebraica:

Teorema 12.3 (Poincaré): Sea k un cuerpo y sea E una curva íntegra completa y suave sobre k con un punto racional distinguido $O \in E(k)$. Son equivalentes:

1. El género de E es 1, es decir, E es una curva elíptica.
2. La curva E admite una (única) estructura de grupo algebraico, de modo que O sea el neutro de E. En consecuencia, E será una variedad abeliana y, por tanto, la operación de grupo es abeliana.

La unicidad de la estructura se sigue del lema de rigidez.
Aquí aparecen dos términos posiblemente nuevos:

Definición 12.4: Sea k un cuerpo. Un ***grupo algebraico*** sobre k es un par $(G, \mathfrak{G})$, donde G es un esquema algebraico sobre k (e.g., una variedad algebraica) y $\mathfrak{G}\colon (\mathsf{Sch}/k)^{\mathrm{op}} \to \mathsf{Grp}$ es un funtor tal que G lo representa.

Una ***variedad abeliana*** sobre k es un grupo algebraico que es también una variedad proyectiva y suave.

En la práctica, esto significa que para esquema X sobre k (en particular para cada extensión de cuerpos K/k), los puntos X-valuados $G(X)$ tienen estructura de grupo y compatible entre ellos. Hay muchas equivalencias de qué significa ser una variedad abeliana y *a posteriori* las variedades abelianas resultan ser grupos algebraicos conmutativos, es decir, que sus puntos X-valuados $G(X)$ siempre son grupos abelianos.

Los siguientes resultados son folclóricos y varios se deducen del lema de rigidez:

Corolario 12.4.1: Sea A una variedad abeliana sobre un cuerpo k. Se cumplen:

1. A es un grupo algebraico conmutativo, i.e., para todo k-esquema X, los puntos X-valuados $A(X)$ son un grupo abeliano. En particular, para toda extensión de cuerpos K/k, los puntos K-racionales $A(K)$ lo son.
2. Dado un morfismo de k-esquemas $\varphi\colon A \to G$, donde G es un grupo algebraicos

Parte III.

Métodos analíticos

13

Formas modulares

En la sección sobre curvas elípticas complejas se realizó lo siguiente:

1. Vimos que una curva elíptica $E(\mathbb{C})$ puede, en ciertos casos, verse como un cociente analítico $\mathbb{C}/\Lambda$, para algún reticulado Λ.

2. A un punto $z \in \mathbb{C}$ con $\mathrm{Im}(z) > 0$ podemos asignarle el reticulado $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, los cuales son homotéticos a todos los reticulados posibles dentro de $\mathbb{C}$. Bajo esta asociación, podemos asignarle $z \mapsto j(E_{\mathbb{Z}+\tau\mathbb{Z}})$ la función que da el invariante j de la curva elíptica asociada.

3. Como el invariante j es efectivamente el mismo para curvas elípticas isomorfas, entonces dados dos τ_1, τ_2 con $\mathrm{Im}(\tau_1), \mathrm{Im}(\tau_2) > 0$ que generen el mismo reticulado, tenemos que $j(\tau_1) = j(\tau_2)$. Esto induce a que j, visto como una función compleja, posea una inusual cantidad de simetrías.

El objetivo de éste capítulo es perseguir estas observaciones y construir sobre éste tema. Formalmente, éste capítulo no depende de aquél de curvas elípticas, sino que solo se sirve del último como inspiración.

13.1 Acciones sobre el semiplano superior

Comenzaremos con ciertas propiedades generales de las acciones topológicas.

Definición 13.1: Sea G un grupo topológico, y sea X un espacio topológico (resp. una variedad analítica). Una ***acción topológica*** (resp. ***acción analítica***) de G sobre X es una aplicación

$$a\colon X \times G \longrightarrow X, \qquad (x, g) \longmapsto x \cdot g,$$

que satisface lo siguiente:

AT1 Para cada $g_0 \in G$, la endofunción $x \mapsto x \cdot g_0$ sobre X es continua (resp. holomorfa).

AT2 Para cada $g, h \in G$ y $x \in X$ se cumple que $(x \cdot g) \cdot h = x \cdot (gh)$.

AT3 Para cada $x \in X$ se cumple que $x \cdot 1 = x$.

También se dice que G ***actúa topológicamente*** (resp. ***analíticamente***) sobre X.

Se siguen las propiedades típicas de acciones como que, por ejemplo, por , las traslaciones $x \mapsto x \cdot g_0$ son homeomorfismos (resp. biholomorfismos) cuando X es un espacio topológico (resp. variedad analítica). También se preservan definiciones como las del estabilizador, órbitas y las definiciones de acción fiel y transitiva. Nótese que toda acción analítica es topológica.

La generalización del «teorema de órbita-estabilizador» en este contexto es el siguiente:

Teorema 13.2: Sea $G \curvearrowright X$ una acción topológica transitiva, donde G es un grupo localmente compacto 2AN y X es de Hausdorff localmente compacto. Entonces, para cada punto $x \in X$ la aplicación

$$\Phi\colon (G/\mathrm{Stab}_x)^+ \longrightarrow X, \qquad \mathrm{Stab}_x g \longmapsto x \cdot g$$

determina un homeomorfismo entre el espacio topológico cociente de clases laterales derechas G/Stab_x y X.

Demostración: Es claro que Φ es una biyección, por lo que basta probar que es una aplicación continua y abierta. La continuidad es clara, mientras que «ser abierta» equivale a que para todo abierto $U \subseteq G$ la imagen $xU \subseteq X$ sea abierta: dado un punto $x \cdot g \in xU$, existe un entorno $V \subseteq G$ del $1 \in G$ que tiene clausura compacta K, es simétrico (i.e., $K^{-1} = K$) y tal que $K^2 g \subseteq U$. Como G posee una base numerable, existe una sucesión $(g_n)_{n\in\mathbb{N}}$ en G tal que $G = \bigcup_{n\in\mathbb{N}} Kg_n$ y defínase $W_n := xKg_n$, de modo que $X = \bigcup_{n\in\mathbb{N}} W_n$.

Como X es de Hausdorff, cada W_n es un subconjunto compacto cerrado. Supongamos, por contradicción, que cada W_n tiene interior vacío. Como X es regular, podemos construir recursivamente abiertos $U_n \subseteq X$ no vacíos de clausura compacta tales que

$$\overline{U}_n \subseteq U_{n-1} \smallsetminus W_{n-1}, \qquad n \geq 2.$$

En particular, $\overline{U}_1 \supseteq \overline{U}_2 \supseteq \cdots$ Nótese que, por compacidad de $\overline{U}_1$, se cumple que $\bigcap_{n\in\mathbb{N}} \overline{U}_n \neq \varnothing$; pero esto es absurdo ya que $\bigcap_{n\in\mathbb{N}} \overline{U}_n$ no corta a ningún W_m y $X = \bigcup_{m\in\mathbb{N}} W_m$. Así, algún W_n tiene interior no vacío y basta con trasladar. □

Definición 13.3: Sea $a\colon G \curvearrowright X$ una acción topológica. Se dice que a es una ***acción propiamente discontinua*** si todo par de puntos distintos $x \neq y \in X$ posee entornos $U, V \subseteq X$ resp., tales que

$$|\{g \in G : U \cdot g \cap V \neq \varnothing\}| < \infty.$$

Corolario 13.3.1: Si $a\colon G \curvearrowright X$ es una acción topológica sobre un espacio X localmente compacto, entonces a es propiamente discontinua syss para todo par de subconjuntos compactos $A, B \subseteq X$ se cumple que

$$|\{g \in G : A \cdot g \cap B \neq \varnothing\}| < \infty.$$

Demostración: Como todo cubrimiento abierto de un compacto admite un subcubrimiento finito, vemos « $\Longrightarrow$ ». El recíproco «$\Longleftarrow$» es precisamente por definición de «localmente compacto». □

Lema 13.4.A: Si G es un grupo topológico y $\Gamma \leq G$ es un subgrupo discreto (i.e., cuya topología subespacio es la discreta), entonces $\Gamma \leq_f G$ es un subgrupo cerrado sin puntos de acumulación.

Demostración: Por definición de «discreto», existe un entorno $U \subseteq G$ del $1 \in G$ tal que $U \cap \Gamma = \{1\}$; como G es un grupo topológico, existe un subentorno simétrico V del 1 tal que $V^{-1}V \subseteq U$. En consecuencia, dados dos elementos distintos $\alpha \neq \beta \in \Gamma$ se cumple que $\alpha V \cap \beta V = \varnothing$.

Dado un elemento adherente $g \in \overline{\Gamma}$ y un $\alpha \in gV^{-1} \cap \Gamma$, vemos que $gV^{-1} \cap \Gamma = \{\alpha\}$, de modo que $g = \alpha \in \Gamma$. □

Teorema 13.4: Sea $G \curvearrowright X$ una acción topológica y sea $\Gamma \leq G$ un subgrupo. Supongamos que todos los estabilizadores de elementos de G son subgrupos compactos. Entonces son equivalentes:

1. El subgrupo Γ es discreto.

2. La acción (por restricción) $\Gamma \curvearrowright X$ es propiamente discontinua.

Lema 13.5: Sea $G \curvearrowright X$ una acción topológica. Supongamos que todo par de puntos $x, y \in X$ poseen entornos $x \in U \subseteq X$, $y \in V \subseteq X$ tales que $gU \cap V = \varnothing$ para todo $g \in G$ tal que $gx \neq y$. Entonces el espacio topológico cociente $G \setminus X$ es de Hausdorff.

Proposición 13.6: Si $G \curvearrowright X$ es una acción propiamente discontinua sobre un espacio de Hausdorff X. Entonces $G \setminus X$ es de Hausdorff.

En éste capítulo, trabajaremos principalmente con dos abiertos distinguidos del plano complejo $\mathbb{C}$ que son el ***semiplano superior*** y el ***disco unitario*** resp.:

$$\mathfrak{h} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}, \qquad \mathbb{D} := \{z \in \mathbb{C} : |z| < 1\}.$$

Tanto a $\mathfrak{h}$ como $\mathbb{D}$ los vamos a dotar de estructura de variedad analítica.

Definición 13.7: Sobre la esfera de Riemann $\mathbb{P}^1(\mathbb{C})$, podemos considerar las ***transformaciones de Möbius*** asociadas a matrices inversibles

$$\gamma := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R}), \qquad \gamma \cdot z := \frac{az+b}{cz+d}.$$

Las cuales determinan una acción analítica $\mathrm{GL}_2(\mathbb{R}) \curvearrowright \mathbb{P}^1(\mathbb{C})$.

Lema 13.8.A: Dado $\gamma \in \mathrm{GL}_2(\mathbb{R})$ y un punto $z \in \mathbb{C}$, se satisface que

$$\operatorname{Im}(\gamma \cdot z) = \frac{\det(\gamma) \operatorname{Im} z}{|cz+d|^2}. \tag{13.1}$$

En particular, $\mathfrak{h}$ es $\mathrm{GL}_2^+(\mathbb{R})$-estable.

El teorema del mapeo de Riemann nos dice que:

Lema 13.8.B: Las variedades $\mathfrak{h}$ y $\mathbb{D}$ son biholomorfas.

Recuérdese que

$$\mathrm{GL}_2^+(\mathbb{R}) := \{\gamma \in \mathrm{GL}_2(\mathbb{R}) : \det \gamma > 0\} \supseteq \mathrm{SL}_2(\mathbb{R}).$$

Dentro de $\mathrm{GL}_2^+(\mathbb{R})$ tenemos a todos los elementos de la forma λI_2 para $\lambda \in \mathbb{R}^\times$, donde I_2 es la matriz identidad; a estos elementos les llamaremos ***escalares*** y esto determina un monomorfismo canónico $\mathbb{R}^\times \hookrightarrow \mathrm{GL}_2^+(\mathbb{R})$. También será útil el grupo simétrico especial

$$\mathrm{SO}_2(\mathbb{R}) := \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} : 0 \leq \theta < 2\pi \right\} \subseteq \mathrm{SL}_2(\mathbb{R}).$$

Teorema 13.8: Se cumplen:

1. Para todo $z \in \mathfrak{h}$ existe un $\gamma \in \mathrm{SL}_2(\mathbb{R})$ tal que $\gamma \cdot \mathrm{i} = z$.
2. El homomorfismo ι induce un isomorfismo
$$\mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times \cong \mathrm{SL}_2(\mathbb{R})/\{\pm 1\} \cong \mathrm{Aut}_{\mathsf{An}}(\mathfrak{h}).$$
3. El grupo simétrico ortogonal $\mathrm{SO}_2(\mathbb{R}) = \{\gamma \in \mathrm{SL}_2(\mathbb{R}) : \gamma \cdot \mathrm{i} = \mathrm{i}\}$ es el estabilizador del i.

De esto extraemos dos consecuencias:

Corolario 13.8.1: El espacio de clases laterales (derechas) $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ es homeomorfo a $\mathfrak{h}$.

Demostración: Se sigue de aplicar el inciso 3 del teorema anterior al teorema 13.2. □

Corolario 13.8.2: La acción (canónica) de un subgrupo $\Gamma \leq \mathrm{Aut}_{\mathsf{An}}(\mathfrak{h})$ es propiamente discontinua sobre $\mathfrak{h}$ syss Γ es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$.

Demostración: Se sigue de aplicar el inciso 2 del teorema anterior al teorema 13.4. □

Para la siguiente definición, nótese que si $\gamma \in \mathrm{GL}_2(\mathbb{R})$ es un elemento escalar, entonces fija a todo $\mathfrak{h}$.

Definición 13.9: Sea $\gamma \in \mathrm{GL}_2(\mathbb{R}) \setminus \mathbb{R}^\times$ una matriz inversible no escalar, entonces su polinomio característico es

$$\psi(t) = \psi_\gamma(t) := t^2 - \mathrm{tr}(\gamma)\, t + \det\gamma \in \mathbb{R}[t].$$

el cual tiene discriminante $\delta := \mathrm{tr}(\gamma)^2 - 4\det\gamma$. Decimos que γ es un elemento ***elíptico*** (resp. ***parabólico***, ***hiperbólico***) si $\delta < 0$ (resp. $\delta = 0$, $\delta > 0$).

Como las raíces del polinomio característico corresponden a valores propios, vemos lo siguiente:

Corolario 13.9.1: Sea $\gamma \in \mathrm{GL}_2(\mathbb{R}) \smallsetminus \mathbb{R}^\times$ no escalar y considere la acción analítica $\mathrm{GL}_2(\mathbb{R}) \curvearrowright \mathbb{P}^1(\mathbb{C})$.

1. γ es elíptico syss el endomorfismo de γ (sobre $\mathbb{P}^1(\mathbb{C})$) tiene exactamente dos puntos fijos z_0 y $\overline{z}_0$, con $z_0 \in \mathfrak{h}$.
2. γ es parabólico syss γ tiene exactamente un punto fijo $z \in \mathbb{R} \cup \{\infty\}$.
3. γ es hiperbólico syss γ tiene exactamente dos punto fijos, ambos en $\mathbb{R} \cup \{\infty\}$.

Definición 13.10: Un ***grupo fuchsiano*** Γ es un subgrupo discreto de $\mathrm{SL}_2(\mathbb{R})$, siempre dotado de su acción canónica $\Gamma \curvearrowright \mathfrak{h}$; se denota

$$Z(\Gamma) := \Gamma \cap \{\pm 1\}.$$

Un punto $z \in \mathfrak{h} \cup \mathbb{R} \cup \{\infty\}$ se dice ***elíptico*** (resp. ***parabólico***, ***hiperbólico***) relativo a Γ si existe un elemento γ elíptico (resp. parabólico, hiperbólico) de Γ tal que z es un punto fijo de γ. Los puntos parabólicos respecto a Γ se dicen ***cúspides*** de Γ. Dados dos puntos $z, w \in \mathfrak{h} \cup \mathbb{R} \cup \{\infty\}$, denotaremos por Γ_z el estabilizador de z por $\Gamma \curvearrowright \mathfrak{h}$ y por $\Gamma_{z,w} := \Gamma_z \cap \Gamma_w$.

Teorema 13.11: Sea Γ un grupo fuchsiano.

1. Dado un punto elíptico $z \in \mathfrak{h}$ de Γ, entonces Γ_z es un grupo cíclico finito.
2. Dada una cúspide $x \in \mathbb{R} \cup \{\infty\}$ de Γ, entonces $\Gamma_x \subseteq \mathrm{SL}_2(\mathbb{R})_x^{(p)}$ y
$$\Gamma_x / Z(\Gamma) \cong \mathbb{Z}.$$
Además, dado $\sigma \in \mathrm{SL}_2(\mathbb{R})$ tal que $\sigma \cdot x = \infty$, se cumple que
$$\sigma \Gamma_x \sigma^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^m : m \in \mathbb{Z}, h > 0 \right\}$$
3. Si $\Gamma_{x,y} \neq Z(\Gamma)$ para $x \neq y \in \mathbb{R} \cup \{\infty\}$, se verifica que
$$\Gamma_{x,y} / Z(\Gamma) \cong \mathbb{Z}.$$

Corolario 13.11.1: Si Γ es un grupo fuchsiano y $\Gamma' \leq \Gamma$ es un subgrupo de índice finito, entonces las cúspides de Γ' son exactamente las misma de Γ.

Definición 13.12: Sea Γ un grupo fuchsiano. El conjunto de cúspides de Γ lo denotaremos P_Γ y denotaremos también:

$$\mathfrak{h}^* = \mathfrak{h}^*_\Gamma := \mathfrak{h} \cup P_\Gamma.$$

Dado $r > 0$ real, definimos

$$U_r := \{z \in \mathfrak{h} : \operatorname{Im} z > r\}, \qquad U_r^* := U_r \cup \{\infty\}.$$

Dotamos a $\mathfrak{h}^*$ de la siguiente topología: para un punto $z \in \mathfrak{h}$ consideramos una base de entornos usual de $\mathfrak{h}$ y para una cúspide $x \in P_\Gamma$ consideramos la base de entornos de la forma $\sigma^{-1}U_r^*$, donde $r > 0$ y σ recorre los elementos de $\mathrm{SL}_2(\mathbb{R})$ tales que $\sigma \cdot x = \infty$.

Proposición 13.13: Para todo grupo fuchsiano Γ, el espacio $\Gamma \setminus \mathfrak{h}^*$ es de Hausdorff.

Definición 13.14: Un elemento de $\Gamma \setminus \mathfrak{h}^*$ se dice un ***punto elíptico*** (resp. una ***cúspide***) si es la imagen de un punto elíptico (resp. una cúspide). Los puntos que no son ni elípticos ni cúspides se dicen ***ordinarios***.

Un grupo fuchsiano Γ se dice ***de primer tipo*** si $\Gamma \setminus \mathfrak{h}^*$ es compacto.

Teorema 13.15: Si Γ es un grupo fuchsiano de primer tipo, entonces $\Gamma \setminus \mathfrak{h}^*$ contiene solo finitos puntos elípticos y cúspides.

13.2 Formas automorfas

Definición 13.16: Sea $f\colon \mathfrak{h} \to \mathbb{P}^1(\mathbb{C})$ una función meromorfa y sea $k \in \mathbb{Z}$ un entero. Dado $\gamma := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2^+(\mathbb{R})$, se define

$$(f|_k\gamma)(z) := \frac{\det(\gamma)^{k/2} f(\gamma \cdot z)}{cz + d}.$$

Corolario 13.16.1: Sea $f\colon \mathfrak{h} \to \mathbb{P}^1(\mathbb{C})$ una función meromorfa y sea $k \in \mathbb{Z}$ un entero. Entonces:

1. Para todo $\alpha, \beta \in \mathrm{GL}_2^+(\mathbb{R})$ se cumple que $f|_k\alpha\beta = (f|_k\alpha)|_k\beta$.

2. Para una matriz escalar $\gamma = \lambda I_2 \in \mathrm{GL}_2^+(\mathbb{R})$ (con $\lambda \in \mathbb{R}^\times$), se cumple que $f|_k\gamma = (\operatorname{sign}\gamma)^k f$.

Definición 13.17: Sea Γ un grupo fuchsiano. Se dice que una función meromorfa $f\colon \mathfrak{h} \to \mathbb{P}^1(\mathbb{C})$ es una ***forma automorfa*** de peso k con respecto a Γ o una Γ***-forma automorfa*** de peso k si

$$\forall \gamma \in \Gamma \qquad f|_k\gamma = f.$$

Denotaremos por $\Omega_k(\Gamma)$ al conjunto de Γ-formas automorfas de peso k.

Corolario 13.17.1: Sea Γ un grupo fuchsiano y sea $k \in \mathbb{Z}$. Entonces:

1. $\Omega_k(\Gamma)$ es un $\mathbb{C}$-subespacio vectorial de $C^{\mathrm{an}}(\mathfrak{h}, \mathbb{P}^1(\mathbb{C}))$.
2. Si $\Gamma' \subseteq \Gamma$ es otro grupo fuchsiano, entonces $\Omega_k(\Gamma') \supseteq \Omega_k(\Gamma)$.
3. Dados $f \in \Omega_k(\Gamma)$ y $g \in \Omega_l(\Gamma)$ (con $l \in \mathbb{Z}$), entonces $f \cdot g \in \Omega_{k+l}(\Gamma)$.
4. Si k es impar y $-1 \in \Gamma$, entonces $\Omega_k(\Gamma) = \{0\}$.

Referencias

97. MIYAKE, T. *Modular forms* trad. por MAEDA, Y. (Springer-Verlag, 2006).

14

La conjetura de Catalan

14.1 Introducción y exponentes pares

El famoso problema que estudiaremos en detalle en éste capítulo es el siguiente: las soluciones de la ecuación diofántica

$$x^n - y^m = 1,$$

donde $n, m > 1$ son exclusivamente $3^2 - 2^3 = 1$. Ésto fue conjeturado por el belga Eugène Charles Catalan en 1842 en una carta a la revista alemana *Crelle* de matemáticas, y fue finalmente demostrado por el rumano Preda V. Milhăilescu en 2004,[1] 160 años después de la formulación del problema.

Lema 14.1: Sean A, B enteros coprimos y p un número primo.

1. Si p divide a uno de los números $\dfrac{A^p - B^p}{A - B}$ o $A - B$, entonces divide al restante.
2. Sea $d := \text{mcd}\left(\dfrac{A^p - B^p}{A - B}, A - B\right)$ entonces $d \in \{1, p\}$.
3. Si $p > 2$ y $d = p$, entonces:

$$\nu_p\left(\frac{A^p - B^p}{A - B}\right) = 1.$$

[1] Milhăilescu escribió el manuscrito en 2000 y lo mandó a revisar a Yuri Bilu, autor del libro principal que seguimos **[68].**

Demostración: En primer lugar, reescribamos:

$$\frac{A^p - B^p}{A - B} = \frac{((A-B)+B)^p - B^p}{A-B} = \sum_{j=1}^{p} \binom{p}{j} (A-B)^{j-1} B^{p-j}, \qquad (14.1)$$

como $p \mid \binom{p}{j}$ para $0 < j < p$, entonces

$$\frac{A^p - B^p}{A-B} \equiv (A-B)^{p-1} \pmod{p}.$$

Reescribiendo (14.1):

$$\frac{A^p - B^p}{A-B} = pB^{p-1} + (A-B)\sum_{j=2}^{p} \binom{p}{j} (A-B)^{j-2} B^{p-j},$$

como A, B son coprimos, entonces $(A-B), B$ también, por lo que como $d \mid pB^{p-1}$ concluimos que $d \mid p$.

Finalmente si asumimos que $p \mid A - B$ y $p > 2$, tenemos que:

$$\frac{A^p - B^p}{A-B} = pB^{p-1} + \binom{p}{2}(A-B)B^{p-2} + (A-B)^2 \sum_{j=3}^{p} \binom{p}{j} (A-B)^{j-3} B^{p-j},$$

de modo que $\frac{A^p - B^p}{A-B} \equiv pB^{p-1} \not\equiv 0 \pmod{p^2}$. □

Teorema 14.2 (Nagell): Sean $x, y > 0$ y $q \neq 2$ primo tales que $x^2 - y^q = 1$. Entonces $2 \mid y$ y $q \mid x$.

Demostración: Reescribamos $y^q = x^2 - 1 = (x-1)(x+1)$. Nótese que el máximo común divisor entre $(x-1), (x+1)$ es divisor de 2, así que si y fuese impar, tendríamos que $(x-1), (x+1)$ son coprimos con lo que $x - 1 = a^q, x + 1 = b^q$ y $b^q - a^q = 2$ lo cual es absurdo. Así pues, y es par.

Escribamos:

$$x^2 = \frac{y^q + 1}{y+1}(y+1),$$

donde $A = y$ y $B = -1$. Por el lema anterior, los factores tienen máximo común divisor 1 o q. Si $q \nmid x$, entonces los factores son coprimos y luego existen $a, b > 0$ tales que

$$y + 1 = a^2, \qquad \frac{y^q + 1}{y+1} = b^2, \qquad x = ab.$$

Como $x^2-y^q=1$, entonces $x+y^{\frac{q-1}{2}}\sqrt{y}$ es invertible en el anillo $A:=\mathbb{Z}[\sqrt{y}]$. Más aún, como $b^2-y=1$, entonces $a+\sqrt{y}$ es una unidad fundamental de A, por lo tanto, existe $n\in\mathbb{N}$ tal que

$$x+y^{\frac{q-1}{2}}\sqrt{y}=(a+\sqrt{y})^n,$$

Ahora bien, veamos congruencias modulares en A:

$$(a+\sqrt{y})^n\equiv a^n+na^{n-1}\sqrt{y}\pmod{y},$$

por lo que

$$na^{n-1}\equiv y^{\frac{q-1}{2}}\equiv 0\pmod{y}.$$

Ahora bien, y es par y a es impar, luego n es par.

Por otro lado

$$x=ab\equiv 0,\qquad y=a^2-1\equiv -1\pmod{a},$$

de modo que

$$(-1)^{\frac{q-1}{2}}\sqrt{y}\equiv x+y^{\frac{q-1}{2}}\sqrt{y}=(a+\sqrt{y})^n\equiv(-1)^{n/2}\pmod{a},$$

de modo que a divide a $1\pm\sqrt{y}$ en A y como $a=y+1>1$ ésto es absurdo. □

Teorema 14.3 (Ko Chao): La ecuación $x^2-y^q=1$, con $q\geq 5$ primo, no admite soluciones con $x,y>0$.

Demostración: Por el teorema anterior, x es impar y y es par.

(a) Si $x\equiv 3\pmod 4$: La igualdad $(x-1)(x+1)=y^q$ implica que

$$x+1=2^{q-1}a^q,\qquad x-1=2b^q.$$

Luego tenemos que:

$$2b^q+2=2^{q-1}a^q\iff a^q=\frac{b^q+1}{2^{q-2}}<b^q\implies a<b.$$

Además, nótese que

$$(b^2+2a)\frac{b^{2q}+(2a)^q}{b^2+2a}=b^{2q}+(2a)^q=\left(\frac{x-1}{2}\right)^2+2(x+1)=\left(\frac{x+3}{2}\right)^2.$$

Por el teorema anterior $q\mid x$ y como $q\geq 5$, entonces q no divide al lado izquierdo de la ecuación, de modo que los factores son coprimos y, por lo tanto, son cuadrados. En particular,

$$b^2+2a\geq(b+1)^2\iff 2a\geq(b+1)^2-b^2>2b,$$

por lo que $a>b$ lo que es absurdo.

(b) Si $x \equiv 1 \pmod 4$: Entonces $x - 1 = 2^{q-1}a^q$ y $x + 1 = 2b^q$, luego

$$b^{2q} - (2a)^q = \left(\frac{x-3}{2}\right)^2,$$

y procedemos de forma análoga. □

Al resultado anterior, le sumamos dos casos complementarios, probados anteriormente:

Teorema 14.4 (Euler): La ecuación $x^2 - y^3 = 1$ no tiene soluciones con $x, y > 0$ (cfr. ejercicio 2.59).

Teorema 14.5 (V. A. Lebesgue): Sea $p > 2$, entonces la ecuación diofántica $x^p - y^2 = 1$ sólo tiene por solución $(x, y) = (1, 0)$ (cfr. teorema 4.50).

Gracias a ésto, podemos reducirnos al caso de exponentes impares.

14.2 Relaciones de Cassels

Por la sección anterior, ahora trabajaremos con soluciones (hipotéticas) de

$$x^p - y^q = 1,$$

donde p, q son primos impares distintos, y $xy \neq 0$. A una tupla (x, y, p, q) que satisfaga lo anterior, diremos que forma un ***contraejemplo de Catalan***.

Definición 14.6: Para un real $\alpha \in \mathbb{R}$ y un natural j definimos por recursión:

$$\binom{\alpha}{0} := 1, \qquad \binom{\alpha}{j+1} := \binom{\alpha}{j}\frac{\alpha - j}{j+1}.$$

En particular, tenemos lo siguiente:

$$(1+t)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} t^n.$$

Lema 14.7: Sea $\alpha = a/b \in \mathbb{Q}$ con a, b coprimos, entonces:

1. Para todo $j \in \mathbb{N}$ existe un N suficientemente grande tal que $b^N \binom{\alpha}{j} \in \mathbb{Z}$.

2. Si q es primo tal que $q \mid b$, entonces para todo $j \in \mathbb{N}$:

$$\nu_q\binom{\alpha}{j} = -j\nu_q(b) - \nu_q(j!) > -j\nu_q(b) - \frac{j}{q-1};$$

en particular, la siguiente sucesión es decreciente:

$$0 = \nu_q\binom{\alpha}{0} > \nu_q\binom{\alpha}{1} > \nu_q\binom{\alpha}{2} > \cdots$$

Demostración: En primer lugar, nótese que para todo $j \in \mathbb{N}$:

$$\binom{\alpha}{j} = \frac{a \cdot (a-b) \cdots (a-(j-1)b)}{b^j j!},$$

como a, b son coprimos, entonces $a \not\equiv 0 \pmod{q}$, de modo que el denominador no es divisible por q, luego

$$\nu_q\binom{\alpha}{j} = -j\nu_q(b) - \nu_q(j!),$$

para la otra fórmula basta notar que

$$\nu_q(j!) = \left\lfloor \frac{j}{q} \right\rfloor + \left\lfloor \frac{j}{q^2} \right\rfloor + \cdots < \frac{j}{q} + \frac{j}{q^2} + \cdots = \frac{j}{q-1}. \qquad \square$$

Lema 14.8: Sea $\alpha \in \mathbb{R}$ y $m \in \mathbb{N}$. Entonces para todo $|t| < 1$ se cumple

$$\left|(1+t)^\alpha - \sum_{n=0}^{m}\binom{\alpha}{n}t^n\right| \leq \text{máx}\{1, (1+t)^{\alpha-m-1}\}\left|\binom{\alpha}{m+1}t^{m+1}\right|, \quad (14.2)$$

en particular con $m = 1$ obtenemos

$$|(1+t)^\alpha - 1| \leq \text{máx}\{1, (1+t)^{\alpha-1}\}|\alpha t|. \quad (14.3)$$

Demostración: Por la expansión de Taylor (cfr. **[2,** teo. 6.32]) en torno al intervalo $[-t, t]$, vemos que:

$$\begin{aligned}\left|(1+t)^\alpha - \sum_{n=0}^{m}\binom{\alpha}{n}t^n\right| &\leq \sup_{|\theta|\leq|t|}\left\{\frac{\mathrm{d}^{m+1}(1+x)^\alpha}{\mathrm{d}x^{m+1}}\Big|_{x=\theta}\right\}\frac{|t|^{m+1}}{(m+1)!} \\ &= \text{máx}\{1, (1+t)^{\alpha-m-1}\}\left|\binom{\alpha}{m+1}t^{m+1}\right|. \qquad \square\end{aligned}$$

Lema 14.9: Sea (x, y, p, q) un contraejemplo de Catalan, entonces

$$|y - x^{p/q}| \leq \frac{1{,}1}{q}|x|^{p/q-p}. \tag{14.4}$$

Demostración: En primer lugar, reescribamos lo que significa ser solución

$$y = (x^p - 1)^{1/q} = x^{p/q}(1 - x^{-p})^{1/q} =: x^{p/q}(1 + r),$$

donde $r := (1 - x^{-p})^{1/q} - 1$, luego con $\alpha := 1/q$ y $t := -x^{-p}$ obtenemos una cota mediante (14.3):

$$|r| \leq (1 - x^{-p})^{\frac{1-q}{q}} \left|\frac{1}{q}x^{-p}\right|.$$

Ahora bien, la lista de las potencias no triviales en orden creciente es $1, 4, 8, 9, 16, 25, \ldots$, de modo que $|x^p| > 16$, luego

$$(1 - x^{-p})^{\frac{1-q}{q}} = \left(\frac{1}{1 - x^{-p}}\right)^{\frac{q-1}{q}} < \left(\frac{1}{1 - 16^{-1}}\right)^{1} < 1{,}1. \qquad \square$$

Proposición 14.10: Sea (x, y, p, q) un contraejemplo de Catalan. Entonces:

$$\operatorname{mcd}\left(\frac{x^p - 1}{x - 1}, x - 1\right) = \begin{cases} p, & p \mid y, \\ 1, & p \nmid y. \end{cases}$$

Demostración: Basta reescribir

$$y^q = \frac{x^p - 1}{x - 1}(x - 1),$$

y aplicar el lema. $\square$

Nuestro objetivo será erradicar el caso segundo, forzando a que $p \mid y$.

Proposición 14.11: Sea (x, y, p, q) un contraejemplo de Catalan con $p < q$. Entonces $p \mid y$.

Demostración: Procedemos por contradicción. Por la proposición anterior, $\frac{x^p-1}{x-1}$ y $(x - 1)$ son coprimos y ambos son potencias q-ésimas. Sea $x - 1 = a^q$. Si $|a| = 1$, entonces $x = 2$ y luego $y = (x^p - 1)^{1/q} < 2$ pues $p < q$ y, por lo tanto, $y = 1$ lo que es absurdo.

Así, $|a| \geq 2$. Como $1+y^q = x^p = (1+a)^p$, entonces «y está cerca de a^p», formalmente:

$$x^{p/q} = (1+a^q)^{p/q} = a^p(1+a^{-q})^{p/q} =: a^p(1+r),$$

donde, por (14.3):

$$|r| = |(1+a^q)^{p/q-1}| \leq \text{máx}\{1,(1+a^q)^{\frac{p}{q}-1}\}\frac{p}{q}|a|^{-q} \leq (1-|a|^{-q})^{\frac{p}{q}-1}\frac{p}{q}|a|^{-q},$$

ahora bien

$$(1-|a|^{-q})^{\frac{p}{q}-1} \leq \frac{1}{1-2^{-3}} \approx 1{,}14285... < 1{,}15.$$

Con ésto concluimos que

$$|x^{p/q} - a^p| \leq 1{,}15|a|^{p-q} \leq 1{,}15 \cdot 2^{-1} < \frac{2}{3}.$$

Además, por (14.4) tenemos:

$$|y - x^{p/q}| \leq \frac{1{,}1}{q}|x|^{\frac{p}{q}-p} < \frac{1{,}1}{3}|x|^{1-p} < \frac{1{,}1}{3\cdot 2^2} \approx 0{,}0916... < 0{,}1.$$

Con ello, vemos que $|y - a^p| < 1$ y así $y = a^p$, pero la ecuación diofántica $x^p - (a^q)^p = 1$ no tiene soluciones, lo que es absurdo. □

Con ésto sacaremos una cota para x:

Lema 14.12 (Hyyrö): Sea (x,y,p,q) un contraejemplo de Catalan con $p > q$. Entonces $|x| \geq q^{p-1} + q$.

Demostración: Si (x,y,p,q) es un contraejemplo, entonces $(-y,-x,q,p)$ también con $q > p$ así que, por la proposición anterior, $q \mid x$. Ahora, como $x^p = \frac{y^q+1}{y+1} \cdot (y+1)$, entonces por el lema 14.1 vemos que

$$\frac{y^q+1}{y+1} = qa^p, \qquad y+1 = q^{p-1}b^p, \qquad x = qab,$$

con a, b coprimos. Reescribiendo la primera relación tenemos

$$q(a^p-1) = \frac{y^q+1}{y+1} - q = ((-y)^{q-1}-1) + \cdots + ((-y)^2-1) + ((-y)-1),$$

así pues $y+1 \mid q(a^p-1)$ y como $y+1 = q^{p-1}b^p$ concluimos que $a^p \equiv 1 \pmod{q^{p-2}}$.

Como $p > q$, entonces $p \nmid q^{p-3}(q-1)$ el cual es la cardinalidad de $(\mathbb{Z}/q^{p-2}\mathbb{Z})^\times$, por lo que se concluye que $a \equiv 1 \pmod{q^{p-2}}$.

Como $|y| \geq 2$ y $(y,q) \neq (2,3)$, entonces es fácil probar que:

$$\frac{y^q+1}{y+1} > q,$$

de modo que $a > 1$ y luego $a \geq q^{p-2}+1$. Finalmente,

$$|x| = qab \geq qa \geq q^{p-1}+q. \qquad \square$$

El siguiente teorema también aparece como *teorema de divisibilidad de Cassels*.

Teorema 14.13 (relaciones de Cassels): Si (x,y,p,q) es un contraejemplo de Catalan, entonces $p \mid y$ y simétricamente $q \mid x$.

Más aún, existen a, b no nulos y $u, v > 0$ tales que:

$$x-1 = p^{q-1}a^q, \qquad \frac{x^p-1}{x-1} = pu^q, \qquad y = pau,$$

y simétricamente

$$y+1 = q^{p-1}b^p, \qquad \frac{y^q+1}{y+1} = qv^p, \qquad x = qbv.$$

Demostración: Supondremos que $p > q$ y que $p \nmid y$ por contradicción. Luego, $(x-1)$ y $\frac{x^p-1}{x-1}$ son coprimos y, en particular, $x-1 = a^q$. Por la cota de Hyyrö, tenemos que $|x| \geq q^{p-1}+q$, de modo que

$$|a|^q \geq q^{p-1}. \tag{14.5}$$

Considere $\alpha := p/q$ y $m := \lceil \alpha \rceil$, entonces

$$x^{p/q} = a^p(1+a^{-q})^\alpha = a^p\left(\sum_{n=0}^{m}\binom{\alpha}{n}a^{-qn}+r\right),$$

donde, por (14.2), tenemos que

$$|r| \leq (1-|a|^{-q})^{\alpha-m-1}\left|\binom{\alpha}{m+1}a^{-q(m+1)}\right|.$$

Podemos acotar

$$(1-|a|^{-q})^{\alpha-m-1} \leq (1-q^{-(p-1)})^{-2} < 1{,}1,$$

(donde probamos las combinaciones $(p,q)=(3,5)$ y $(p,q)=(5,3)$.) Además

$$\left|\binom{\alpha}{m+1}\right| = \frac{\alpha}{m}\frac{\alpha-1}{m-1}\cdots\frac{\alpha-m+1}{1}\frac{|\alpha-m|}{m+1} < 1\cdot 1\cdots 1\cdot\frac{1}{m+1}\leq\frac{1}{3},$$

Luego $|r|\leq 0{,}5|a|^{-q(m+1)}$ y, por tanto,

$$\left|x^{p/q}-\sum_{n=0}^{m}\binom{\alpha}{m}a^{p-qn}\right|\leq |a|^p\,|r|\leq 0{,}5|a|^{p-(m+1)q},$$

sea

$$\sum_{n=0}^{m}\binom{\alpha}{m}a^{p-qn}=:\frac{A}{B},$$

donde A, B son enteros coprimos. Por el lema 14.7, vemos que $B \mid q^{m+\nu_q(m!)}a^{qm-p}$. Como $\nu_q(m!)<m/(q-1)$, se concluye que

$$|B|\leq q^{m+\nu_q(m!)}a^{qm-p} < q^{\frac{mq}{q-1}}|a|^{mq-p}.$$

También por el mismo lema, recordamos que

$$\forall 0\leq j<m\quad \nu_q\left(\binom{\alpha}{m}a^{p-qm}\right)<\nu_q\left(\binom{\alpha}{j}a^{p-qj}\right),$$

por lo que $\nu_p(A/B)=\nu_p\left(\binom{\alpha}{m}a^{p-qm}\right)<0$ y, en consecuente, A/B no es entero.

Ahora bien, recordando que $p>q$ tenemos

$$|x|^{p-\frac{p}{q}}>|x|^{5-\frac{5}{3}}=|x|^{10/3}>(|x|+1)^2\geq|a|^{2q}\geq|a|^{(m+1)q-p}.$$

Luego, empleando (14.4) y la desigualdad triangular:

$$\left|y-\frac{A}{B}\right|\leq\frac{1{,}1}{q}|x|^{\frac{p}{q}-p}+0{,}5|a|^{p-(m+1)q}\leq|a|^{p-(m+1)q}.$$

Además,

$$pq+1\geq p(p-1)+1=p^2-p+1>4p>2(p+q),$$

luego $(p-1)(q-1)=pq-p-q+1>p+q$, con ello

$$p-1>\frac{p+q}{q-1}\geq\frac{mq}{q-1},$$

con lo que, empleando además que $|a|^q > q^{p-1} \geq q^{\frac{mq}{q-1}}$ por (14.5), vemos que

$$|a|^{p-(m+1)q} = |a|^{-q}|a|^{p-mq} < q^{\frac{mq}{q-1}}|a|^{p-mq} < |B|^{-1},$$

así que $|y - A/B| < |1/B|$ y, por ende, $y = A/B$ lo que es absurdo, pues A/B no es entero. □

Teorema 14.14 (cotas de Hyyrö): Sea (x, y, p, q) un contraejemplo de Catalan. Entonces

$$|x| \geq \text{máx}\{q^{p-1} + q, p^{q-1}(q-1)^q + 1\} \tag{14.6}$$

(y simétricamente, $|y| \geq \text{máx}\{p^{q-1} + p, q^{p-1}(p-1)^p + 1\}$).

Demostración: Las cotas involucran dos desigualdades. En ésta demostración, emplearemos el hecho de los números x, y, a, b de las relaciones de Cassels o bien son todos positivos, o bien son todos negativos.

- $\underline{|x| \geq p^{q-1}(q-1)^q + 1}$: Como $q \mid x$ tenemos que

  $$p^{q-1}a^q = x - 1 \equiv -1 \pmod{q},$$

  por el pequeño teorema de Fermat $p^{q-1} \equiv 1\ (q)$ y $a \equiv a^q \equiv -1\ (q)$. Análogamente, $b \equiv 1 \pmod{p}$.

  En el caso positivo, $a \geq q - 1$, por lo que, $x \geq p^{q-1}(q-1)^p + 1$ como se quería probar.

  En el caso negativo, o bien $a = -1$ o $a \leq -q - 1$, en cuyo caso

  $$|x| \geq p^{q-1}(q+1)^p - 1 \geq p^{q-1}(q-1)^p - 1.$$

  $\underline{\text{Basta mostrar que } a \neq -1}$: Por contradicción, se tendría que $1 - x = 1 + |x| = p^{q-1}$ y además $b \leq 1 - p$, por lo que

  $$\begin{aligned} |y| = (|x|^p + 1)^{1/q} &\leq (1 + |x|)^{p/q} < p^p < 2^{p-1}(p-1)^p \\ &< q^{p-1}|b|^p = |1 + y| < |y|, \end{aligned}$$

  lo cual es absurdo.

- $\underline{|x| \geq q^{p-1} + p}$: Supondremos que $p < q$ pues el otro caso ya está probado. Así:

  $$|x| \geq p^{q-1}(q-1)^q + 1 > 2(q-1)^q > 2p^q > 2q^p > q^{p-1} + p,$$

  como queríamos probar. □

14.3 Teoremas de divisibilidad superior

Lema 14.15 (principal): Sea (x, y, p, q) un contraejemplo de Catalan. Sea $\zeta := \zeta_p$. Entonces el número

$$\lambda := \frac{x - \zeta}{1 - \zeta} \in \mathbb{Z}[\zeta]$$

es un entero algebraico, y existe un ideal $\mathfrak{a} \lhd \mathbb{Z}[\zeta]$ tal que $(\lambda) = \mathfrak{a}^q$.

Demostración: Recuérdese (teorema 8.23) que $\pi := 1 - \lambda$ es un primo de $\mathbb{Z}[\zeta]$ y que $(p) = (\pi)^{p-1}$. Por las relaciones de Cassels, $p \mid x - 1$, de modo que $x \equiv 1 \equiv \zeta \pmod{\pi}$, pero $\pi^2 \nmid x - \zeta$ (¿por qué?), de modo que λ es un entero algebraico y $\pi \nmid \lambda$.

Definiendo $\lambda_j := x - \zeta^j/(1 - \zeta^j)$, entonces lo mismo se concluye para λ_j. Como

$$\zeta^n - \zeta^m = (x - \zeta^m) - (x - \zeta^n) = (1 - \zeta_p^m)\lambda_m - (1 - \zeta_p^n)\lambda_n,$$

de modo que para $1 \leq n < m < p$ tenemos que si $\gamma \mid \zeta^n$ y $\gamma \mid \zeta^m$, entonces $(\gamma) \supseteq (\zeta^n - \zeta^m) = (\pi)$; de modo que los números $\lambda_1, \ldots, \lambda_{p-1}$ son coprimos dos a dos.

Ahora, como

$$\Phi_p(t) := \frac{t^p - 1}{t - 1} = (t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{p-1})$$

se tiene que

$$\frac{x^p - 1}{x - 1} \cdot \frac{1}{p} = \frac{\Phi_p(x)}{\Phi_p(1)} = \lambda_1 \cdots \lambda_{p-1}.$$

Por las relaciones de Cassels, tenemos que $\lambda_1 \cdots \lambda_{p-1} = u^q$ para algún $u \in \mathbb{Z}$ y, como los λ_i's son coprimos dos a dos, entonces cada $(\lambda_i) = \mathfrak{a}^q$. □

Proposición 14.16: Sea (x, y, p, q) un contraejemplo de Catalan. Entonces $q^2 \mid x$ syss $p^{q-1} \equiv 1 \pmod{q^2}$.

Demostración: Como $q \mid x$ por las relaciones de Cassels, entonces $p^{q-1}a^q \equiv -1 \pmod{q}$. Como $p^{q-1} \equiv 1 \ (q)$ por el pequeño teorema de Fermat, entonces $a^q \equiv -1 \ (q)$ y $a \equiv -1 \ (q)$.

Por el lema 14.1, si $A^q \equiv B^q \ (q)$, entonces $A^q \equiv B^q \ (q^2)$ y, en particular, $a^q \equiv -1 \ (q)$. Así, que $p^{q-1} \equiv 1 \ (q^2)$ equivale a que $q^2 \mid x$. □

Proposición 14.17: Sea (x, y, p, q) un contraejemplo de Catalan tal que $q \nmid h_p$, donde h_p es el número de clases de $\mathbb{Q}(\zeta_p)$. Entonces

$$\mu := \frac{1-\zeta_p x}{1-\overline{\zeta}_p x} \in \mathbb{Q}(\zeta_p)$$

es una potencia q-ésima (en $\mathbb{Q}(\zeta_p)$).

Demostración: Denotemos $\zeta := \zeta_p$ y $K := \mathbb{Q}(\zeta)$. Sea $\lambda := (x-\zeta)/(1-\zeta)$, ya sabemos que $(\lambda) = \mathfrak{a}^q$ en $\mathbb{Z}[\zeta]$. Sea $G := \operatorname{Cl} K$ el grupo de clases, entonces como $\mathfrak{a}^q \equiv 1 \pmod{G}$ tenemos que $\operatorname{ord}_G \mathfrak{a} \mid q$. Como $h := |G|$ es coprimo con q, entonces necesariamente $\operatorname{ord}_G \mathfrak{a} = 1$ y $\mathfrak{a} = \alpha\mathbb{Z}[\zeta]$. Por tanto, $\lambda = \alpha^q \eta$, donde $\eta \in \mathbb{Z}[\zeta]^\times$.

Ahora bien, por la proposición 8.33, existe $\epsilon \in \mathbb{Z}[\zeta + \zeta^{-1}]^\times \subseteq \mathbb{R}$ tal que $\eta = \zeta^r \epsilon$ para algún r. Redefiniendo α podemos suponer que η es una unidad ciclotómica real. Luego $\lambda/\overline{\lambda} = (\alpha/\overline{\alpha})^q$ es una potencia q-ésima en K, luego

$$\mu = \frac{1-\zeta x}{1-\overline{\zeta} x} = \frac{(1-\zeta)\lambda}{(1-\overline{\zeta})\overline{\lambda}} = \frac{\zeta}{\overline{\zeta}} \cdot \frac{1-\overline{\zeta}}{1-\zeta} \cdot \frac{\lambda}{\overline{\lambda}} = -\zeta \cdot \frac{\lambda}{\overline{\lambda}}$$

es una potencia q-ésima en K. □

Lema 14.18: Sea K un cuerpo numérico, sea $\mathfrak{q} \lhd \mathcal{O}_K$ un primo y sean

$$\alpha, \beta \in \mathfrak{o}_\mathfrak{q} := \{\gamma \in K : \nu_\mathfrak{q}(\gamma) \geq 0\}.$$

Sea $(q) = \mathfrak{q} \cap \mathbb{Z}$. Si $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}}$, entonces $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}^2}$.

Demostración: Como $0 \equiv \alpha^q - \beta^q \equiv (\alpha - \beta)^q \ (\mathfrak{q})$, entonces se sigue que $\alpha \equiv \beta \ (\mathfrak{q})$, vale decir, existe $\gamma \in \mathfrak{q}$ tal que $\alpha = \beta + \gamma$. Luego

$$\alpha^q = \beta^q + \gamma \sum_{j=1}^{q-1} \binom{q}{j} \gamma^{j-1} + \gamma^q.$$

Basta notar que $q \mid \gamma$ y $q \mid q = \binom{q}{1}$ para concluir. □

Lema 14.19: Sea K un cuerpo numérico y sea $\mathfrak{q} \lhd \mathcal{O}_K$ primo. Para todo $n \in \mathbb{Z}$ y todo $\alpha \in K$ con $\nu_\mathfrak{q}(\alpha) > 0$, se tiene que

$$(1+\alpha)^n \equiv 1 + n\alpha \pmod{\mathfrak{q}^2}.$$

Teorema 14.20 (de divisibilidad de Inkeri): Sea (x, y, p, q) un contraejemplo de Catalan. Si $q \nmid h_p$, entonces $q^2 \mid x$.

Demostración: Sean $\zeta := \zeta_p$ y $K := \mathbb{Q}(\zeta)$. Como q no se ramifica en K, basta probar que $\mathfrak{q}^2 \mid x$ para algún $\mathfrak{q} \mid q$ en $\mathcal{O}_K$. Como $q \mid x$ (por las relaciones de Cassels), entonces $\mu := (1-\zeta x)/(1-\overline{\zeta}x)$ satisface que $\mu \equiv 1 \pmod{\mathfrak{q}}$ y, como μ es una potencia q-ésima, entonces por el lema 14.18 tenemos que $\mu \equiv 1 \pmod{\mathfrak{q}^2}$.

Por otro lado, el lema anterior implica que $(1-\overline{\zeta}x)^{-1} \equiv 1+\overline{\zeta}x \pmod{\mathfrak{q}^2}$, de modo que

$$1 \equiv \mu \equiv (1-\zeta x)(1+\overline{\zeta}x) = 1 + (\overline{\zeta}-\zeta)x \pmod{\mathfrak{q}^2},$$

y como $\nu_{\mathfrak{q}}(\overline{\zeta}-\zeta) = 0$ (¿por qué?), concluimos que $\mathfrak{q}^2 \mid x$ como se quería probar. □

Corolario 14.20.1: Sea (x, y, p, q) un contraejemplo de Catalan. Entonces $q \mid h_p$ o $p^{q-1} \equiv 1 \pmod{q^2}$.

La segunda condición se llama *condición de Wieferich* y sus implicancias son enormes, reduciendo bastante la cantidad de primos.

Ahora veremos cómo emplear el teorema y el ideal de Stickelberger para agudizar la condición anterior.

Proposición 14.21: Sea (x, y, p, q) un contraejemplo de Catalan. Sean $\zeta := \zeta_p, K := \mathbb{Q}(\zeta), G := \mathrm{Gal}(K/\mathbb{Q})$ e $\iota \in G$ la conjugación compleja. Si $\theta \in \mathbb{Z}[G]$ aniquila el grupo de clases $\mathrm{Cl}(\mathbb{Z}[\zeta])$, vale decir, si para todo ideal $\mathfrak{a} \lhd \mathbb{Z}[\zeta]$ se cumple que $\mathfrak{a}^\theta$ es principal. Entonces $(1-\zeta x)^{(1-\iota)\theta}$ es una q-ésima potencia en K.

Demostración: Sea $\lambda := (x-\zeta)/(1-\zeta) \in \mathbb{Z}[\zeta]$ (por el lema principal) y sea $(\lambda) =: \mathfrak{a}^q$. Por hipótesis, $\mathfrak{a}^\theta = (\alpha)$, por lo que, $\lambda^\theta = \eta\alpha^q$ para algun $\eta \in \mathbb{Z}[\zeta]^\times$ y, quizá modificando α, podemos suponer que η es real. Luego $(\lambda/\overline{\lambda})^\theta = (\alpha/\overline{\alpha})^q$ es una potencia q-ésima, por lo que

$$(1-\zeta x)^{(1-\iota)\theta} = \left(\frac{1-\zeta x}{1-\overline{\zeta}x}\right)^\theta = \left(\frac{\zeta}{\overline{\zeta}} \cdot \frac{1-\overline{\zeta}}{1-\zeta}\right)^\theta \cdot \left(\frac{\overline{\lambda}}{\lambda}\right)^\theta = (-\zeta)^\theta \left(\frac{\overline{\alpha}}{\alpha}\right)^q,$$

la cual es una potencia q-ésima. □

Proposición 14.22: Sea (x, y, p, q) un contraejemplo de Catalan. Sean $\zeta := \zeta_p, K := \mathbb{Q}(\zeta), G := \mathrm{Gal}(K/\mathbb{Q})$ e $\iota \in G$ la conjugación compleja. Si $\theta \in \mathbb{Z}[G]$ satisface que $(1-\zeta x)^\theta$ sea una potencia q-ésima y tal que $q \nmid \theta$ (en $\mathbb{Z}[G]$). Entonces $q^2 \mid x$ (en $\mathbb{Z}$).

Demostración: Sea $\mathfrak{q} \lhd \mathbb{Z}[\zeta]$ un primo tal que $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$ (sin fijar). Basta probar que $\mathfrak{q}^2 \mid x$. Como $q \mid x$ por relaciones de Cassels, entonces $\mathfrak{q} \mid x$, de modo que $(1-\zeta x)^\theta \equiv 1 \pmod{\mathfrak{q}}$ y como $(1-\zeta x)^\theta$ es una potencia q-ésima, entonces por el lema 14.18, tenemos que

$$(1-\zeta x)^\theta \equiv 1 \pmod{\mathfrak{q}^2}.$$

Sea $\theta := \sum_{\sigma \in G} a_\sigma \sigma$, como $q \nmid \theta$, entonces $q \nmid a_\tau$ para un $\tau \in G$. Como $\{\sigma\zeta : \sigma \in G\}$ es una $\mathbb{Z}$-base de $\mathbb{Z}[\zeta]$, entonces $q \nmid \sum_{\sigma \in G} a_\sigma \zeta^\sigma =: \alpha$. Debido a que q no se ramifica en $\mathbb{Z}[\zeta]$, entonces sea $\mathfrak{q}$ un primo tal que $\mathfrak{q} \mid q$ y $\mathfrak{q} \nmid \alpha$.

Aplicando el lema 14.19 tenemos que

$$(1-\zeta x)^\theta = \prod_{\sigma \in G} (1-\zeta^\sigma x)^{a_\sigma} \equiv 1 - x \sum_{\sigma \in G} a_\sigma \zeta^\sigma = 1 - \alpha x \quad (\mathfrak{q}^2),$$

como $(1-\zeta x)^\theta \equiv 1$ $(\mathfrak{q}^2)$ concluimos que $\nu_\mathfrak{q}(\alpha x) \geq 2$, pero $\nu_\mathfrak{q}(\alpha) = 0$ por construcción, por lo que $\mathfrak{q}^2 \mid x$ como se quería probar. □

Teorema 14.23 – *Primer teorema de Mihăilescu*: Sea (x, y, p, q) un contraejemplo de Catalan, entonces $q^2 \mid x$, y simétricamente $p^2 \mid y$.

Demostración: Sean $\zeta := \zeta_p, K := \mathbb{Q}(\zeta), G := \mathrm{Gal}(K/\mathbb{Q})$ e $\iota \in G$ la conjugación compleja. Sea $\Theta := \sum_{j=1}^{p-1} j\sigma_j^{-1}$ el elemento de Stickelberger; por el teorema de Stickelberger tenemos que Θ aniquila el grupo de clases $\mathrm{Cl}(\mathbb{Z}[\zeta])$ por lo que una proposición anterior implica que $(1-\zeta x)^{(1-\iota)\Theta}$ es una potencia q-ésima en K y, como $q \nmid (1-\iota)\Theta$ en $\mathbb{Z}[G]$, concluimos que $q^2 \mid x$ por la proposición anterior. □

Corolario 14.23.1: Sea (x, y, p, q) un contraejemplo de Catalan, entonces $p^{q-1} \equiv 1 \pmod{q^2}$, y simétricamente $q^{p-1} \equiv 1 \pmod{p^2}$.

Definición 14.24: Un par de primos distintos $\{p, q\}$ tales que $p^{q-1} \equiv 1$ (q^2) y $q^{p-1} \equiv 1$ (p^2) se dice un ***par de Wieferich doble***.

Para dimensionar lo fuerte que es la condición de Wieferich doble, gracias a un computador podemos buscar ejemplos y todos los que existen con $\min\{p,q\} \leq 3{,}2 \times 10^8$ son (cfr. Keller y Richstein [**36**]):

$$(2,1093),\quad (3,1006003),\quad (5,1645333507),\quad (5,188748146801),$$
$$(83,4871),\quad (911,318917),\quad (2903,18787).$$

14.4 El ideal de Mihăilescu

Definición 14.25: Sea G un grupo. Sobre la álgebra $\mathbb{Z}[G]$ se define la ***función peso*** $w\colon A[G] \to A$:

$$w\left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} a_g.$$

El núcleo $\ker w = A[G]^{\mathrm{aug}}$ se llama el ***ideal de augmentación***. Dado un ideal $\mathfrak{a} \lhd \mathbb{Z}[G]$ se denomina su ***parte de augmentación***:

$$\mathfrak{a}^{\mathrm{aug}} := \{a \in \mathfrak{a} : w(a) = 0\} = \mathfrak{a} \cap A[G]^{\mathrm{aug}}.$$

También se define la ***función tamaño*** $\|\ \|\colon A[G] \to A$ para algún subanillo $A \subseteq \mathbb{C}$:

$$\left\|\sum_{g\in G} a_g g\right\| := \sum_{g\in G} |a_g|.$$

Definición 14.26: Sea G un grupo. Para un elemento $\theta := \sum_{g\in G} a_g g \in \mathbb{Z}[G]$ se denota $\theta \geq 0$ si cada $a_g \geq 0$. En cuyo caso, $w(\theta) = \|\theta\|$. Definimos $\theta_+ := \sum_{g\in G} \max\{0, a_g\} g$ y $\theta_- := (-\theta)_+$, de modo que $\theta = \theta_+ - \theta_-$ y $\|\theta\| = \|\theta_+\| + \|\theta_-\|$.

Lema 14.27: Sean $x \in \mathbb{Z}_{\neq 0}$, p un primo impar, $\zeta := \zeta_p$ y $G := \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Para todo $\theta \in \mathbb{Z}[G]^{\mathrm{aug}}$ se tiene

$$h\big((x-\zeta)^\theta\big) \leq \frac{\|\theta\|}{2} \log(|x|+1),$$

(donde h denota la altura logarítmica.)

Demostración: Sea $\theta = \theta_+ - \theta_-$. Es fácil notar que

$$m := \|\theta_+\| = \|\theta_-\| = \frac{\|\theta\|}{2}.$$

Ahora bien, sean $\alpha := (x-\zeta)^{\theta_+}$ y $\beta := (x-\zeta)^{\theta_-}$, de modo que $(x-\zeta)^\theta = \alpha/\beta$. Nótese que α es un entero algebraico y es el producto de m términos de la forma $(x-\zeta)^\sigma$, por lo que, $|\alpha| \leq (|x|+1)^m$ y, de manera análoga, se verifica que $|\alpha^\sigma| \leq (|x|+1)^m$ y lo mismo para β.

Ahora bien, empleando la proposición 9.3:

$$h\big((x-\zeta)^\theta\big) \leq \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma\in G} m \log(|x|+1) = m\log(|x|+1). \qquad \square$$

Lema 14.28: Sean p un primo impar, $\zeta := \zeta_p$, $K := \mathbb{Q}(\zeta)$ y $G := \mathrm{Gal}(K/\mathbb{Q})$. Para todo $|x| > 1$ entero y todo $\theta \in \mathbb{Z}[G]^{\mathrm{aug}}$ se tiene que

$$|\log(x-\zeta)^\theta| \leq \frac{\|\theta\|}{|x|-1},$$

donde aquí, log representa la rama principal del logaritmo (complejo).

Demostración: Por la expansión de Taylor de log, para $z \in \mathbb{C}$ con $|z| < 1$ se cumple que

$$|\log(1+z)| \leq \frac{|z|}{1-|z|},$$

en particular

$$\left|\log\left(1-\frac{\zeta^\sigma}{x}\right)\right| \leq \frac{1}{|x|-1}.$$

Finalmente, basta notar que cuando $w(\theta) = 0$ se tiene que $(x-\zeta)^\theta = (1-\zeta/x)^\theta$. $\square$

Lema 14.29: Sean p un primo impar, $\zeta := \zeta_p$, $K := \mathbb{Q}(\zeta)$ y $G := \mathrm{Gal}(K/\mathbb{Q})$. Para todo $|x| \geq 3$ entero y todo $\theta \in \mathbb{Z}[G]$ no nulo se tiene que $(x-\zeta)^\theta \neq 1$.

Demostración: Sea $\pi := 1-\zeta \in \mathbb{Z}[\zeta], \mathfrak{p} := \pi\mathbb{Z}[\zeta]$ y recuérdese que $(p) = \mathfrak{p}^{p-1}$ (teorema 8.23). Para todo par $\sigma, \tau \in G$ distintos se cumple que $\mathfrak{p} = (\zeta^\sigma - \zeta^\tau)$, por tanto

$$(x-\zeta^\sigma, x-\zeta^\tau) \mid \mathfrak{p}. \tag{14.7}$$

Si el único primo que divide a $x-\zeta$ fuera $\mathfrak{p}$, entonces tendríamos que $(x-\zeta) = \mathfrak{p}^j$ y, como $\mathfrak{p}$ es estable bajo G, entonces $(x-\zeta^\sigma) = \mathfrak{p}^j$. Por la fórmula (14.7) se cumple que $j \leq 1$, de modo que $\mathrm{Nm}_{K/\mathbb{Q}}(x-\zeta) \in \{\pm 1, \pm p\}$.

Finalmente, como $|x| \geq 3$ tenemos que

$$|\operatorname{Nm}_{K/\mathbb{Q}}(x-\zeta)| = \prod_{\sigma\in G} |x-\zeta^\sigma| \geq 2^{p-1} > p;$$

esta contradicción prueba que $x-\zeta$ contiene otro divisor primo $\mathfrak{q}$.

Sea $\ell := \nu_{\mathfrak{q}}(x-\zeta)$. Nuevamente, por (14.7) tenemos que

$$\nu_{\sigma\mathfrak{q}}(x-\zeta^\tau) = \begin{cases} \ell, & \sigma = \tau, \\ 0, & \sigma \neq \tau. \end{cases}$$

Expandiendo $\theta := \sum_{g\in G} a_g g$, se calcula que $\nu_{\sigma\mathfrak{q}}\big((x-\zeta)^\theta\big) = \ell a_\sigma$. Si $(x-\zeta)^\theta = 1$, entonces $\ell a_\sigma = 0$ para todo a_σ y, como $\ell \neq 0$, necesariamente $\theta = 0$. □

Definición 14.30: Sean $x \in \mathbb{Z}_{\neq 0}$ un entero no nulo y p, q primos impares distintos. Denotemos $\zeta := \zeta_p$, $K := \mathbb{Q}(\zeta)$ y $G := \operatorname{Gal}(K/\mathbb{Q})$. Se define el ***ideal de Mihăilescu*** como

$$\mathfrak{I}_M := \{\theta \in \mathbb{Z}[G] : (x-\zeta)^\theta \in (K^\times)^q\}$$

Proposición 14.31: Sean $x \in \mathbb{Z}_{\neq 0}$ un entero no nulo y p, q primos impares distintos. Denotemos $\zeta := \zeta_p$, $K := \mathbb{Q}(\zeta)$ y $G := \operatorname{Gal}(K/\mathbb{Q})$. Se cumplen:

1. Para todo $\theta \in \mathfrak{I}_M$ existe un único $\rho(\theta) \in K^\times$ tal que $\rho(\theta)^q = (x-\zeta)^\theta$.
2. Para todo par $\theta_1, \theta_2 \in \mathfrak{I}_M$ tenemos
$$\rho(\theta_1+\theta_2) = \rho(\theta_1)\rho(\theta_2).$$
Es decir, $\rho\colon (\mathfrak{I}_M, +) \to (K^\times, \cdot)$ es un homomorfismo de grupos.
3. Si $|x| \geq 3$, entonces ρ es inyectivo.
4. Para todo $\theta \in \mathfrak{I}_M^{\text{aug}}$ tenemos
$$h(\rho(\theta)) \leq \frac{\|\theta\|}{2q} \log(|x|+1).$$

Demostración: Para la primera basta notar que si $\rho_1, \rho_2 \in K^\times$ satisfacen que $\rho_1^q = (x-\zeta)^\theta = \rho^2$, entonces $(\rho_1/\rho_2)^q = 1$. Como $\mathbb{Q}(\zeta_p)$ es linealmente disjunto de $\mathbb{Q}(\zeta_q)$ esto implica que $\rho_1 = \rho_2$. La segunda es un ejercicio y el resto se sigue de los lemas anteriores. □

Definición 14.32: Sea q un primo impar. Dado un complejo $z \in \mathbb{C}^\times$, se llama la raíz q-ésima ***más cercana*** ξ como la que satisface que

$$-\pi/q < \arg(z\chi_z^{-1}) \leq \pi/q.$$

Proposición 14.33: Sea $z \in \mathbb{C}^\times$ y ξ su raíz q-ésima más cercana. Se cumplen:

1. $\log(z\xi^{-1}) = \dfrac{1}{q}\log(z^q)$.
2. Si $|\arg(z^q)| < \pi$ (o equivalentemente, si $z^q \notin \mathbb{R}_{<0}$), entonces ξ^{-1} es la raíz q-ésima más cercana a z^{-1}.
3. Dados $z_1, z_2 \in \mathbb{C}^\times$ cuyas raíces q-ésimas más cercanas son ξ_1, ξ_2 resp. Si $|\arg(z_1^q)|, |\arg(z_2^q)| < \pi/2$, entonces $\xi_1\xi_2$ es la raíz q-ésima más cercana a z_1z_2.

Definición 14.34: Denotamos por $\xi\colon \mathfrak{I}_M \to \boldsymbol{\mu}_q$ a la aplicación que a cada $\theta \in \mathfrak{I}_M$ le asocia la raíz q-ésima más cercana a $\rho(\theta)$.

A priori, ξ no determina un homomorfismo de grupos, pero como $\rho(\theta)^q = (x-\zeta)^q$ es «cercano» a 1 (lema 14.28), entonces se espera que $\xi(\theta)$ sea «cercano» a $\rho(\theta)$, de modo que ξ sea un «casi-homomorfismo».

Proposición 14.35: Sean $x \in \mathbb{Z}_{\neq 0}$ un entero no nulo y p, q primos impares distintos. Denotemos $\zeta := \zeta_p$, $K := \mathbb{Q}(\zeta)$ y $G := \mathrm{Gal}(K/\mathbb{Q})$. Se cumplen:

1. Para todo $\theta \in \mathfrak{I}_M^{\mathrm{aug}}$ se tiene que
$$\left|\log\left(\rho(\theta)\xi(\theta)^{-1}\right)\right| \leq \frac{1}{q}\,\frac{\|\theta\|}{|x|-1}. \tag{14.8}$$
2. Supongamos que $\theta \in \mathfrak{I}_M^{\mathrm{aug}}$ satisface que $\|\theta\| < \pi(|x|-1)$, entonces $\xi(-\theta) = \xi(\theta)^{-1}$.
3. Si $\theta_1, \theta_2 \in \mathfrak{I}_M^{\mathrm{aug}}$ satisfacen que
$$\|\theta_1\|, \|\theta_2\| < \frac{\pi}{2}(|x|-1),$$
entonces
$$\xi(\theta_1+\theta_2) = \xi(\theta_1)\xi(\theta_2).$$

Demostración: Es una aplicación de las dos últimas proposiciones. □

Definición 14.36: Sea $A \subseteq \mathbb{C}$ un subanillo y sea G un grupo. Para todo subconjunto $S \subseteq A[G]$ y todo $r > 0$ se denota

$$S(r) := \{a \in S : \|a\| \leq r\}.$$

Sean G, H un par de grupos y $f\colon G \to H$ una aplicación. Dado un subconjunto $S \subseteq G$ se dice que f es un ***cuasihomomorfismo*** sobre S si para todo $x, y \in S$ se cumplen que

$$f(x^{-1}) = f(x)^{-1}, \qquad f(xy) = f(x)\, f(y).$$

Así, la proposición anterior se reduce en que $\xi\colon \mathfrak{I}_M^{\text{aug}} \to \boldsymbol{\mu}_q$ es un cuasihomomorfismo sobre $\mathfrak{I}_M^{\text{aug}}(r)$ para todo $r < \frac{\pi}{2}(|x| - 1)$.

Lema 14.37: Sea $a \in \mathbb{R}_{>0}$, entonces para todo $w \in \mathbb{C}$ tal que $|w| \leq a$ se satisface que

$$|e^w - 1| \leq \frac{e^a - 1}{a}|w|.$$

Demostración: Para todo $|z| \leq 1$ se tiene que

$$|e^{az} - 1| = \left|az + \frac{(az)^2}{2!} + \frac{(az)^3}{3!} + \cdots\right| \leq a + \frac{a^2}{2!} + \frac{a^3}{3!} + \cdots = e^a - 1.$$

Definiendo $f(z) := (e^{az} - 1)/(e^a - 1)$, entonces $f(0) = 0$ y $|f(z)| \leq 1$ para todo $|z| \leq 1$, de modo que por el lema de Schwartz, $|f(z)| \leq |z|$ para todo $|z| \leq 1$. □

Proposición 14.38: Sean $x \in \mathbb{Z}_{\neq 0}$ un entero no nulo y p, q primos impares distintos. Fijemos la álgebra $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$. Sean $0 < \epsilon \leq 1$ y $r > 0$ tales que

$$|x| \geq \text{máx}\left\{\left(\frac{20 \cdot 2^{p-1}}{(p-1)^2}\right)^{1/\epsilon}, \frac{4}{\pi}\frac{q}{p-1} + 1\right\} \tag{14.9}$$

y

$$r = (2 - \epsilon)\frac{q}{p-1} < \frac{\pi}{2}(|x| - 1). \tag{14.10}$$

Entonces para todo $\theta \in \mathfrak{I}_M^{\text{aug}}(2r)$ tal que $\xi(\theta) = 1$ se tiene que $\theta = 0$.

Demostración: Sea $\theta \in \mathfrak{I}_M^{\mathrm{aug}}(2r)$ tal que $\xi(\theta) = 1$. Defínase $\alpha := \rho(\theta)$, entonces por (14.8) tenemos que

$$|\log \alpha| \leq \frac{1}{q} \frac{\|\theta\|}{|x|-1}.$$

Es fácil comprobar que $2^{p-1} \geq (p-1)^2$, de modo que $|x| \geq 20$ por (14.9). Como $\|\theta\| \leq 2r < 4q/(p-1)$, entonces

$$|\log \alpha| \leq \frac{1}{q} \frac{2r}{|x|-1} < \frac{4}{(p-1)(|x|-1)} \leq \frac{2}{19}.$$

Empleando $w = \log \alpha$ y $a = 2/19$, entonces el lema anterior nos da

$$|\alpha - 1| \leq \frac{e^{2/19}-1}{2/19} |\log \alpha| \leq \frac{1{,}06}{q} \frac{\|\theta\|}{|x|-1}.$$

Por otro lado, empleando que $\alpha \neq 1$ pues $|x| > 3$, podemos aplicar la desigualdad fundamental (de alturas):

$$|\alpha - 1|^2 = \|\alpha - 1\|_\infty \geq H(\alpha - 1)^{-[K:\mathbb{Q}]} = e^{(p-1)h(\alpha-1)}.$$

Empleando la proposición 9.5 podemos acotar

$$h(\alpha - 1) \leq h(\alpha) + \log 2 \leq \frac{\|\theta\|}{2q} \log(|x|+1) + \log 2.$$

Ahora combinando ambas cotas tenemos

$$\begin{aligned} 2\left(\log(|x|-1) - \log\left(\frac{1{,}06\|\theta\|}{q}\right)\right) &\leq \log(|\alpha-1|^{-2}) \\ &\leq (p-1)\left(\frac{\|\theta\|}{2q}\log(|x|+1) + \log 2\right). \end{aligned}$$

Debido a que

$$\|\theta\| \leq 2r = 2(2-\epsilon)\frac{q}{p-1},$$

la desigualdad se preserva sustituyendo $\|\theta\|$ por $2(2-\epsilon)q/(p-1)$ en el lado derecho y por $4q/(p-1)$ en el izquierdo:

$$\begin{aligned} &2\log(|x|-1) - 2\log\left(\frac{4{,}24}{p-1}\right) \leq (2-\epsilon)\log(|x|+1) + (p-1)\log 2, \\ &\qquad \iff \epsilon \log(|x|+1) \leq 2\log(4{,}24) + 2\log\left(\frac{|x|+1}{|x|-1}\right) + \log\left(\frac{2^{p-1}}{(p-1)^2}\right). \end{aligned}$$

Finalmente, como $|x| \geq 20$, tenemos

$$\epsilon \log(|x|+1) \leq 2\log(4{,}24) + 2\log(21/19) + \log\left(\frac{2^{p-1}}{(p-1)^2}\right) < \log\left(\frac{20 \cdot 2^{p-1}}{(p-1)^2}\right)$$

lo que contradice la hipótesis (14.9). □

Teorema 14.39: Sean $x \in \mathbb{Z}_{\neq 0}$ un entero no nulo y p, q primos impares distintos. Fijemos la álgebra $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$. Sean $0 < \epsilon \leq 1$ y $r > 0$ tales que se satisfacen las (des)igualdades (14.9) y (14.10). Entonces $|\mathfrak{I}_M^{\mathrm{aug}}(r)| \leq q$.

Demostración: En efecto, supongamos que $\theta_1, \theta_2 \in \mathfrak{I}_M^{\mathrm{aug}}(r)$ satisfacen que $\xi(\theta_1) = \xi(\theta_2)$, entonces como ξ es un cuasihomomorfismo en $\mathfrak{I}_M^{\mathrm{aug}}(r)$ tenemos que $\xi(\theta_1 - \theta_2) = 1$ y, por la proposición anterior, se verifica que $\theta_1 = \theta_2$. Por tanto, ξ es inyectivo y se concluye lo pedido. □

Tomando $\epsilon = 1$ tenemos el siguiente corolario:

Teorema 14.40: Sean p, q primos impares distintos y $|x| \geq \mathrm{máx}\{2^{p+2}, q\}$ un entero. Fijemos la álgebra $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$. Con $r := q/(p-1)$ tenemos que $|\mathfrak{I}_M^{\mathrm{aug}}(r)| \leq q$.

Necesitaremos otro teorema más:

Lema 14.41: Sea $\alpha \in \mathbb{C}^\times$ un complejo y sea ξ su raíz q-ésima más cercana con $\xi \neq 1$. Si $|\log(\alpha\xi^{-1})| \leq 1/10q$, entonces $|\alpha - 1| \geq 5/q$.

Demostración: Como $\xi \neq 1$, entonces $\xi = \exp(2\pi \mathrm{i} j/q)$ con $1 \leq j < q$. Luego $|\xi - 1| = 2|\sin(\pi j/q)| \geq 2\sin(\pi/q)$. Ahora bien, la función $(\sin x)/x$ decrece en $[0, \pi/2]$, por lo que

$$\frac{\sin(\pi/q)}{\pi/q} \geq \frac{\sin(\pi/3)}{\pi/3},$$

de modo que

$$|\xi - 1| \geq 2\sin(\pi/q) \geq 2 \cdot \frac{\sin(\pi/3)}{\pi/3} \cdot \frac{\pi}{q} \geq \frac{5{,}19}{q}.$$

Finalmente, empleando el lema 14.37 tenemos

$$|\alpha - \xi| = |\alpha\xi^{-1} - 1| \leq \frac{e^{0{,}1} - 1}{0{,}1} \cdot \frac{0{,}1}{q} \leq \frac{0{,}11}{q},$$

y finalmente, por desigualdad triangular, $|\alpha - 1| \geq 5{,}19/q - 0{,}11/q > 5/q$ como se quería probar. □

Teorema 14.42: Sean $x \in \mathbb{Z}$ un entero, p, q primos impares distintos y $0 < \epsilon \leq 1$ un número real tales que $p \leq (2-\epsilon)q + 1$ y

$$|x| \geq \text{máx}\left\{\left(\frac{20 \cdot 2^{p-1}}{(p-1)^2}\right)^{1/\epsilon}, 8q^q\right\}. \tag{14.11}$$

Entonces $\mathfrak{I}_M^{\text{aug}}(2) = \{0\}$.

Demostración: Definiendo $r := (2-\epsilon)q/(p-1)$, tenemos que

$$r \leq \frac{\pi}{2}(|x| - 1).$$

De modo que la proposición 14.38 implica que si $\theta \in \mathfrak{I}_M^{\text{aug}}(2r)$ tiene $\xi(\theta) = 1$, entonces $\theta = 0$.

Claramente $r \geq 1$, por lo que la proposición aplica, así que, por contradicción supongamos que existe $\theta \in \mathfrak{I}_M^{\text{aug}}$ tal que $\xi := \xi(\theta) \neq 1$. Sea $\alpha := \rho(\theta)$ y, como $|x| \geq 8 \cdot 3^3 = 216$ por (14.11), tenemos que

$$|\log(\alpha\xi^{-1})| \leq \frac{1}{q} \cdot \frac{2}{|x| - 1} < \frac{0{,}1}{q}$$

por (14.8). Por el lema anterior, concluimos que $|\alpha - 1| \geq 5/q$.

Sea $\sigma \in G$, entonces como $\rho(\sigma\theta) = \sigma\alpha$, entonces un razonamiento análogo prueba que $|\sigma\alpha - 1| \geq 5/q$. Sea S_K^∞ el conjunto de lugares al infinito de K, entonces:

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S_K^\infty} \log \text{máx}\{1, |\alpha - 1|_v^{-1}\}$$
$$= \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma \in G} \log \text{máx}\{1, |\sigma\alpha - 1|^{-1}\} \leq \log(q/5).$$

Sean $\sigma_1, \sigma_2 \in G$ automorfismos distintos y definamos $\zeta_i := \sigma_i\zeta$. Si $|\alpha - 1|_v < 1$ para un lugar finito $v \in M_K$, entonces $|\alpha^q - 1|_v \leq |\alpha - 1|_v < 1$. Definiendo $\theta := \sigma_1 - \sigma_2$ tenemos que

$$\alpha^q - 1 = (x - \zeta)^\theta - 1 = \frac{\zeta_2 - \zeta_1}{x - \zeta_2}, \tag{14.12}$$

donde numerador y denominador son enteros algebraicos, por lo que, se sigue que

$$|\alpha - 1|_v \geq |\zeta_2 - \zeta_1|_v = \begin{cases} p^{-1}, & v \mid p, \\ 1, & v \nmid p. \end{cases}$$

Por lo tanto,

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \notin S_K^\infty} \log \text{máx}\{1, |\alpha - 1|_v^{-1}\} \leq \frac{\log p}{p-1} \leq \frac{\log 3}{2}.$$

Finalmente, agrupando todo tenemos que

$$h(\alpha - 1) = h\big((\alpha - 1)^{-1}\big) \leq \log q - \log\left(\frac{5}{\sqrt{3}}\right) < \log q - \log 2.$$

Por lo que $h(\alpha) \leq h(\alpha - 1) + \log 2 < \log q$.

Reescribiendo (14.12), tenemos que

$$x = \frac{\zeta_2 - \zeta_1}{\alpha^q - 1} + \zeta_2,$$

y luego podemos acotar

$$\begin{aligned} \log|x| = h(x) = h\left(\frac{\zeta_2 - \zeta_1}{\alpha^q - 1} + \zeta_2\right) &\leq h(\zeta_2 - \zeta_1) + h(\alpha^q - 1) + \log 2 \\ &\leq q h(\alpha) + 3\log 2 < \log(8q^q), \end{aligned}$$

lo cual es absurdo. □

Aplicando $\epsilon = 1$:

Teorema 14.43: Sean $x \in \mathbb{Z}$ un entero, $p < q$ primos impares distintos y $|x| \geq 8q^q$. Fijemos la álgebra $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$. Entonces $\mathfrak{I}_M^{\text{aug}}(2) = \{0\}$.

§14.4.1 ¡Regreso a Catalan!. Volvemos al contexto particular y veamos cómo los últimos teoremas de hecho acotan bastante el problema de Catalan.

Teorema 14.44 (Bugueaud-Hanrot): Sea (x, y, p, q) un contraejemplo de Catalan con $p < q$. Entonces $q \mid h_p$ y, mejor aún, $q \mid h_p^-$.

Demostración: Como $p \geq 3$ y $q \geq 5$, por las cotas de Hyyrö tenemos que

$$|x| \geq p^{q-1}(q-1)^q = \frac{q-1}{q}\left(\frac{p(q-1)}{q}\right)^{q-1} q^q \geq \frac{4}{5}\left(\frac{12}{5}\right)^4 q^q > 8q^q,$$

por lo que se satisfacen las hipótesis del teorema anterior.

La proposición 14.17 ahora dice que, si $q \nmid h_p$, entonces $\mu = (1-\zeta x)^\theta$ con $\theta = 1-\iota$ (donde ι es la conjugación compleja) es una potencia q-ésima, luego $\theta \in \mathfrak{I}_M^{\text{aug}}(2)$ lo cual es absurdo por el teorema anterior. Así que necesariamente $q \mid h_p$.

Para mejorar la condición en $q \mid h_p^-$ hay que notar que es necesaria una mejora de la proposición 14.17. Esto se deja de ejercicio para el lector: que revise las demostraciones previas y emplee la descomposición de unidades en una unidad real para poder agudizar los resultados. □

En la práctica, gracias al uso de computadores podemos calcular números de clases (relativos), así que, volvamos a la lista de candidatos que teníamos; veremos que nos reducimos a los pares[2] $\{(911, 318917), (2903, 18787)\}$.

Teorema 14.45 – *Segundo teorema de Mihăilescu*: Sea (x, y, p, q) un contraejemplo de Catalan, entonces $q < 3(p-1)^2$.

Corolario 14.45.1: Sea (x, y, p, q) un contraejemplo de Catalan. Entonces $q \not\equiv 1 \pmod{p}$ (y simétricamente, $p \not\equiv 1 \pmod{q}$).

Demostración: Supongamos que $q \equiv 1\ (p)$. Por el primer teorema de Mihăilescu, $q^{p-1} \equiv 1\ (p^2)$ y, por tanto, $q \equiv 1\ (q^2)$.

Ahora, nótese que $q \notin \{1+p^2, 1+3p^2\}$ puesto que q es impar. Nótese que $p \neq 3$, puesto que $\mathbb{Z}[\zeta_3]$ son los enteros de Eisenstein, que son un DFU, y por tanto $h_3^- = 1$, lo que contradice el teorema de Bugueaud-Hanrot. Así que $q \neq 1 + 2p^2$, puesto que $1 + 2p^2 \equiv 0\ (3)$. Por tanto, $q \geq 1 + 4p^2$ lo que es absurdo por el teorema anterior. □

Notas históricas

La conjetura de Catalan apareció en [**17**] (1844). El teorema de Ko Chao fue probado en [**18**] (1965); nosotros reproducimos la demostración de Mignotte [**42**] (2004) que emplea el teorema de Nagell [**45**] (1921).

La historia de la conjetura de Catalan da un primer giro tras el encuentro de las relaciones de Cassels [**16**] (1960). El matemático finlandés **Kutsaa Inkeri** y, su estudiante S. Hyyrö trabajaron en buscar cotas efectivas para

[2] «Nos reducimos», esencialmente porque existen tablas calculando números de clases. Para $h_3^- = h_5^- = 1$ y $h_{83}^- = 3 \cdot 279405653$ (cfr. Washington [**108,** pág. 353]).

contraejemplos a la conjetura de Catalan, resultando en las cotas de Hyyrö **[32]** (1964) y en el teorema de divisibilidad de Inkeri **[33]** (1990). De hecho, los primeros ejemplos de pares de Wieferich doble fueron hallados por K. Inkeri junto con M. Aaltonen.

Referencias

64. Alter, R. y Kubota, K. K. The Diophantine Equation $x^2 + 11 = 3^n$ and a Related Sequence. *J. Number Theory* **7,** 5-10. doi:10.1016/0022-314X(75)90003-7 (1975).

65. Andreescu, T., Andrica, D. y Feng, Z. *104 number theory problems: from the training of the USA IMO team* (Springer Science & Business Media, 2007).

66. Ankeny, N. C. Sums of three squares. *Proc. Amer. Math. Soc.* doi:10.1090/S0002-9939-1957-0085275-8 (1957).

67. Artin, E. y Whaples, G. Axiomatic Characterization of Fields by the Product Formula for Valuations. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1945-08383-9 (1945).

107. author. title. *Amer. Math. Monthly* **128,** 239-249. arXiv: 1909.07121 (2021).

68. Bilu, Y. F., Bugeaud, Y. y Mignotte, M. *The Problem of Catalan* (Springer International Publishing Switzerland, 2014).

69. Bombieri, E. y Gubler, W. *Heights in Diophantine Geometry* (Cambridge University Press, 2006).

6. Brieskorn, E. y Knorrer, H. *Plane Algebraic Curves* trad. por Stillwell, J. (Birkhäuser Verlag, 1981).

70. Cassels, J. W. S. *Global fields* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 42-84.

71. Cassels, J. W. S. *Local Fields* (Cambridge University Press, 1986).

72. (eds. Cassels, J. W. S. y Fröhlich, A.) *Algebraic Number Theory* (Academic Press, 1967).

73. Clark, P. L. *Geometry of numbers with applications to Number Theory* http://alpha.math.uga.edu/~pete/geometryofnumbers.pdf (2015).

74. Cohn, H. A Short Proof of the Simple Continued Fraction Expansion of e. *Amer. Math. Mon.* doi:10.2307/27641837 (2006).

75. Corvaja, P. Autour du Théorème de Roth. *Mh. Math.* **124,** 147-175. doi:10.1007/bf01300617 (1997).

76. Corvaja, P. *Integral Points on Algebraic Varieties. An Introduction to Diophantine Geometry* (Springer-Verlag, 2016).

77. CORVAJA, P. y ZANNIER, U. A subspace theorem approach to integral points on curves. *C. R. Acad. Sci. Paris, Ser. I* **334,** 267-271. doi:10.1016/S1631-073X(02)02240-9 (2002).

78. COX, D. A. *Primes of the form $x^2 + ny^2$* 3.ª ed. (American Mathematical Society, 2020).

1. CUEVAS, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).

2. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

79. DE SOUZA, A. N. *Where do odd perfect numbers live?* 2018. arXiv: 1801.06182 [math.NT].

7. DICKSON, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

80. EDWARDS, H. M. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory Graduate Texts in Mathematics* **50** (Springer-Verlag, 1977).

81. EGGLETON, R. B., LACAMPAGNE, C. B. y SELFRIDGE, J. L. Euclidean Quadratic Fields. *Amer. Math. Mon.* doi:10.2307/2324118 (1992).

82. ERDŐS, P. Representations of real numbers as sums and products of Liouville numbers. *Michigan Math. J.* **9,** 59-60. https://old.renyi.hu/~p_erdos/1962-18.pdf (1962).

83. GAUSS, C. F. *Disquisitiones Arithmeticae* trad. por RUIZ ZÚÑIGA, A. https://archive.org/details/disquisitiones-arithmeticae-carl-f.-gauss-espanol (Universidad de Costa Rica, 1801).

84. GRANVILLE, A. *Number Theory Revealed. A Masterclass* (American Mathematical Society, 2020).

85. HLAWKA, E., SCHOISSENGEIER, J. y TASCHNER, R. *Geometric and Analytic Number Theory* (Springer-Verlag, 1991).

86. HUA, L. K. *Introduction to Number Theory* (Springer-Verlag Berlin Heidelberg, 1982).

3. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).

87. JANUSZ, G. J. *Algebraic Number Fields* 2.ª ed. *Graduate Studies in Mathematics* **7** (American Mathematical Society, 1973).

88. JAVANPEYKAR, A. *The Lang-Vojta Conjectures on Projective Pseudo-Hyperbolic Varieties* en *Arithmetic Geometry of Logarithmic Pairs and Hyperbolicity of Moduli Spaces* (ed. NICOLE, M.-H.) (Springer, Cham, 2020), 135-196.

89. JAVANPEYKAR, A. y KAMENOVA, L. Demailly's notion of algebraic hyperbolicity: geometricity, boundedness, moduli of maps. *Math. Z.* **296,** 1645-1672. doi:10.1007/s00209-020-02489-6 (2020).

90. Khinchin, A. *Continued Fractions* (University of Chicago Press, 1964).

91. Lang, S. *Fundamentals of Diophantine Geometry* (Springer-Verlag, 1983).

92. Lang, S. Hyperbolic and Diophantine Analysis. *Bull. Amer. Math. Soc.* **14,** 159-205. doi:10.1090/S0273-0979-1986-15426-1 (1986).

93. Lang, S. *Number Theory.* III: *Diophantine Geometry Encyclopaedia of Mathematical Sciences* **60** (Springer-Verlag, 1991).

94. Lehmer, D. N. A Theorem in Continued Fractions. *Ann. Math.* **2,** 146-147. doi:10.2307/2007192 (1900).

4. Liu, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

95. McFeat, R. B. *Geometry of numbers in adèle spaces* PhD (University of Adelaide, 1969).

96. Milne, J. S. *Algebraic Number Theory* https://www.jmilne.org/math/CourseNotes/ant.html (19 de mayo de 2020).

97. Miyake, T. *Modular forms* trad. por Maeda, Y. (Springer-Verlag, 2006).

98. Mordell, L. J. *Diophantine Equations* (Academic Press, 1969).

99. Narkiewicz, W. Class number and factorization in quadratic number fields. *Colloquium Math.* doi:10.4064/CM-17-2-167-190 (1967).

100. Nathanson, M. B. *Elementary Methods in Number Theory* (Springer-Verlag New York, 2000).

8. Newton, I. *The Correspondence of Isaac Newton* (ed. Turnbull, H. W.) (Cambridge University Press, 1960).

101. Niven, I. *Irrational Numbers* (Mathematical Association of America, 1956).

102. Pollack, P. *Not Always Buried Deep* (American Mathematical Society, 2009).

103. Ribenboim, P. *Fermat's Last Theorem for Amateurs* (Springer-Verlag New York, 1999).

9. Roquette, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

104. Samuel, P. About Euclidean rings. *J. Algebra* **19,** 282-301. doi:10.1016/0021-8693(71)90110-4 (1971).

105. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

106. Soundararajan, K. *Bertrand's postulate and the existence of finite fields* 2020. arXiv: 2007.01389 [math.NT].

108. Washington, L. C. *Introduction to Cyclotomic Fields Graduate Texts in Mathematics* **83** (Springer-Verlag New York, 1982).

109. WEIL, A. *Basic Number Theory* (Springer-Verlag, 1967).

10. WILLIAMS, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. BENNETT, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

5. WILSON, J. S. *Profinite groups* (Oxford University Press, 1999).

110. ZHANG, Y. Congruence and uniqueness of certain Markoff numbers. *Acta Math.* **128,** 295-301. doi:10.4064/aa128-3-7 (2007).

Otros recursos.

1. CUEVAS, J. *Álgebra* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/algebra/algebra.pdf (2022).

2. CUEVAS, J. *Topología y Análisis* https://github.com/JoseCuevasBtos/apuntes-tex/raw/master/topologia-analisis/topologia-analisis.pdf (2022).

3. JACOBSON, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).

4. LIU, Q. *Algebraic Geometry and Arithmetic Curves* (Oxford University Press, 2002).

5. WILSON, J. S. *Profinite groups* (Oxford University Press, 1999).

Historia.

6. BRIESKORN, E. y KNORRER, H. *Plane Algebraic Curves* trad. por STILLWELL, J. (Birkhäuser Verlag, 1981).

7. DICKSON, L. E. *History of the Theory of Numbers* 3 vols. (Chelsea Publishing Company, 1923).

8. NEWTON, I. *The Correspondence of Isaac Newton* (ed. TURNBULL, H. W.) (Cambridge University Press, 1960).

9. ROQUETTE, P. *The Riemann Hypothesis in Characteristic p in Historical Perspective Lecture Notes in Mathematics* **2222** (Springer Nature Switzerland, 2018).

10. WILLIAMS, H. C. *Solving the Pell Equation* en *Number Theory for the Millennium* (eds. BENNETT, M. A. *et al.*) **3** (CRC Press, 2002), 397-436.

Documentos históricos.

11. ALFORD, W. R., GRANVILLE, A. y POMERANCE, C. There are Infinitely Many Carmichael Numbers. *Ann. Math.* **139,** 703-722. doi:10.2307/2118576 (1994).

12. APÉRY, R. en *Journées Arithmétiques de Luminy Astérisque* 61 (Société mathématique de France, 1979). http://www.numdam.org/item/AST_1979__61__11_0/.

13. Barnes, E. S. y Swinnerton-Dyer, H. P. F. The inhomogeneous minima of binary quadratic forms (I). *Acta Math.* **87,** 259-323. doi:10.1007/BF02392288 (1952).

14. Beukers, F. A Note on the Irrationality of $\zeta(2)$ and $\zeta(3)$. *Bull. London Math. Soc.* **11,** 268-272. doi:10.1112/blms/11.3.268 (1979).

15. Bombieri, E. y Vaaler, J. D. On Siegel's Lemma. *Invent. Math.* **73,** 11-32. doi:10.1007/BF01393823 (1983).

16. Cassels, J. W. S. On the equation $a^x - b^y = 1$ II. *Math. Proc. Cambridge Phil. Soc.* **56,** 97-103. doi:10.1017/S0305004100034332 (1960).

17. Catalan, E. C. Note extraite d'une lettre adressée à l'éditeur. *J. Reine Angew. Math.* **27,** 192 (1844).

18. Chao, K. On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. *Sci. Sinica* **14,** 457-460 (1965).

19. Chatland, H. y Davenport, H. Euclid's Algorithm in real Quadratic Fields. *Canadian Journal of Mathematics* **2,** 289-296. doi:10.4153/CJM-1950-026-7 (1950).

20. Clark, D. A. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.* doi:10.1007/BF02567617 (1994).

21. De Bessy, F. Traité des triangles rectangles en nombres. *Mémoires de l'Académie royale des sciences.* https://www.biodiversitylibrary.org/item/81352#page/29/mode/1up (1676).

22. Dedekind, R. *Was sind und was sollen die Zahlen?* (Braunschweig, 1888).

23. Dickson, L. E. *Algebren und ihre Zahlentheorie* (Zurich u. Leipzig, 1927).

24. Dirichlet, G. L. en *G. Lejeune Dirichlet's Werke* (ed. Kronecker, L.) 1-20 (Cambridge University Press, 1889). doi:10.1017/CBO9781139237338.003.

25. Euler, L. Theorematum quorundam arithmeticorum demonstrationes. *Commentarii academiae scientiarum Petropolitanae* **10,** 125-146. https://scholarlycommons.pacific.edu/euler-works/98/ (1747).

26. Euler, L. De numeris, qui sunt aggregata duorum quadratorum. *Novi Commentarii academiae scientiarum Petropolitanae* **5,** 3-40. https://scholarlycommons.pacific.edu/euler-works/228/ (1758).

27. Euler, L. *Vollständige Anleitung zur Algebra* 2 vols. https://scholarlycommons.pacific.edu/euler-works/387/ (St. Petersburg: Imperial Academy of Sciences, 1770).

28. Gauss, C. F. en *Werke* 387-398 (Cambridge University Press, 1863). doi:10.1017/CBO9781139058230.016.

29. Harper, M. $\mathbb{Z}[\sqrt{-14}]$ is Euclidean. *Canadian J. Math.* doi:10.4153/CJM-2004-003-9 (2004).

30. HENSEL, K. Über eine neue Begründung der Theorie der algebraischen Zahlen. *Jahresbericht der Deutschen Mathematiker-Vereinigung.* https://eudml.org/doc/144593 (1897).

31. HENSEL, K. Neue Grundlagen der Arithmetik. *J. Reine Angew. Math.* https://eudml.org/doc/149178 (1904).

32. HYYRÖ, S. Über das Catalan'sche problem. *Ann. Univ. Turku Ser. AI* **79,** 3-10 (1964).

33. INKERI, K. On Catalan's Conjecture. *J. Number Theory* **34,** 142-152. doi:10.1016/0022-314X(90)90145-H (1990).

34. INKERI, K. Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Scient. Fennicae* **41,** 1-35 (1947).

35. KAUSLER, C. F. Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse. *Novi Acta Acad. Petrop.* **13,** 245-253 (1802).

36. KELLER, W. y RICHSTEIN, J. Solutions of the congruence $a^{p-1} \equiv 1 \pmod{p^r}$. *Math. Comp.* **74,** 927-936. www.jstor.org/stable/4100096 (2005).

37. KÜRSCHÁK, J. Über Limesbildung und allgemeine Körpertheorie. *J. Reine Angew. Math.* doi:10.1515/crll.1913.142.211 (1913).

38. LANG, S. Integral points on curves. *Publ. Math. de l'IHES* **6,** 27-43. doi:10.1007/BF02698777 (1960).

39. LEGENDRE, A.-M. *Théorie des nombres* 3.ª ed. (Firmin Didot Fréres, 1830).

40. LEHMER, D. H. Factorization of Certain Cyclotomic Functions. *Ann. Math.* **34,** 461-479. doi:10.2307/1968172 (1933).

41. MAHLER, K. On Some Inequalities for Polynomials in Several Variables. *J. London Math. Soc.* **37,** 341-344. doi:10.1112/jlms/s1-37.1.341 (1962).

42. MIGNOTTE, M. A New Proof of Ko Chao's Theorem. *Math. Notes* **76,** 358-367. doi:10.1023/B:MATN.0000043463.77207.2a (2004).

43. MINKOWSKI, H. *Geometrie der Zahlen* (Leipzig und Berlin, 1896).

44. MOTZKIN, T. The Euclidean algorithm. *Bull. Amer. Math. Soc.* doi:10.1090/S0002-9904-1949-09344-8 (1949).

45. NAGELL, T. Sur l'impossibilité de l'équation indéterminée $z^p+1 = y^2$. *Norsk Mat. Forenings Skrifter.* **4,** 14 (1921).

46. NORTHCOTT, D. G. An inequality in the theory of arithmetic on algebraic varieties. *Math. Proc. Cambridge Phil. Soc.* **45,** 502-509. doi:10.1017/S0305004100025202 (1949).

47. OCHEM, P. y RAO, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.* **81,** 1869-1877. doi:10.1090/S0025-5718-2012-02563-4 (2012).

48. OPPENHEIM, A. Quadratic fields with and without Euclid's algorithm. *Math. Ann.* **109,** 349-352. doi:10.1007/BF01449143 (1934).

49. Ostrowski, A. Über einige Fragen der allgemeinen Körpertheorie. *J. Reine Angew. Math.* **143,** 255-284 (1913).

50. Ostrowski, A. Über sogenannte perfekte Körper. *J. Reine Angew. Math.* **147,** 191-204 (1917).

51. Ostrowski, A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\cdot\varphi(y) = \varphi(xy)$. *Acta Math.* **41,** 271-284. doi:10.1007/BF02422947 (1918).

52. Ostrowski, A. Über algebraische Funktionen von Dirichletschen Reihen. *Mathematische Zeitschrift* **37,** 98-133. doi:10.1007/BF01474566 (1933).

53. Ostrowski, A. Untersuchungen zur arthmetischen Theorie der Körper. Die Theorie der Teilbarkeit in allgemeinen Körpern. *Mathematische Zeitschrift* **39,** 269-320. doi:10.1007/BF01201361 (1935).

54. Perron, O. Quadratische Zahlkörper mit Euklidischem Algorithmus. *Math. Ann.* **107,** 489-495. doi:10.1007/BF01448906 (1933).

55. Rédei, L. Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.* **118,** 588-608. doi:10.1007/BF01487388 (1941).

56. Rella, T. Ordnungsbestimmungen in Polynombereichen. *J. Reine Angew. Math.* **158,** 33-48 (1927).

57. Remak, R. Über den Euklidischen Algorithmus in reellquadratischen Zahlkörpern. *Jahresbericht der Deutschen Mathematiker-Vereinigung* **44,** 238-250. https://eudml.org/doc/146043 (1934).

58. Roth, K. F. Rational approximations to algebraic numbers. *Mathematika* **2,** 1-20. doi:10.1112/S0025579300000644 (1955).

59. Rychlík, K. Beitrag zur Körpertheorie. *Časopis* **48,** 145-165 (1919).

60. Rychlík, K. Zur Bewertungstheorie der algebraischen Körper. *J. Reine Angew. Math.* **153,** 94-107 (1924).

61. Siegel, C. L. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuß. Akad. Wissen. Phys.-math. Klasse,* 209-266 (1929).

62. Tate, J. *Fourier analysis in number fields, and Hecke's zeta-functions* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 305-347.

63. Verger-Gaugry, J.-L. *A Proof of the Conjecture of Lehmer and of the Conjecture of Schinzel-Zassenhaus* 2017. arXiv: 1709.03771 [math.NT].

15

Algunas conjeturas diofánticas

15.1 La conjetura *abc*

Definición 15.1: El ***radical*** de un entero no nulo N es el producto de sus factores primos:

$$\mathrm{Rad}(N) := \prod_{p|N} p.$$

Equivalentemente, $\mathrm{Rad}(N)$ es el mayor entero libre de cuadrados tal que $\mathrm{Rad}(N) \mid N$.

Comencemos por el siguiente ejemplo:

Ejemplo. Sea p un número primo. Por el teorema de Euler-Fermat, sabemos que $2^{\phi(p^2)} \equiv 1 \pmod{p^2}$ de modo que definiendo

$$a := 1, \qquad b := 2^{p^2-p} - 1, \qquad c := 2^{p^2-p}$$

vemos que son coprimos, que $a + b = c$ y que

$$\mathrm{Rad}(abc) = \mathrm{Rad}(2b) \leq \frac{2}{p} b < \frac{2}{p} c \iff c > \frac{p}{2} \mathrm{Rad}(abc),$$

pues $p^2 \mid b$.

Conjetura *abc* de Masser-Oesterlé, 1985 15.2: Para todo $\epsilon > 0$ existe una constante $\kappa_\epsilon > 0$ con la siguiente propiedad: dados enteros positivos coprimos a, b, c tales que $a + b = c$ se cumple que

$$c \leq \kappa_\epsilon \operatorname{Rad}(abc)^{1+\epsilon}.$$

El enunciado es equivalente a que la cota $c < \operatorname{Rad}(abc)^{1+\epsilon}$ se satisface para todas salvo finitas ternas (a, b, c). Nótese que el ejemplo anterior verifica que el ϵ es necesario.

También hay ocasiones en que el siguiente enunciado es útil:

Conjetura *abc* débil para $M > 1$ 15.3: Para todos salvo finitas ternas de naturales coprimos a, b, c tales que $a + b = c$ se cumple que

$$c < \operatorname{Rad}(abc)^{M}.$$

Al decir conjetura *abc* siempre nos referiremos a la *versión fuerte*.

El interés tras esta conjetura radica en su fuerte potencial en aplicaciones. Veamos un ejemplo:

Ejercicio 15.4: La conjetura *abc* débil implica que el Último Teorema de Fermat es cierto para exponentes $n \gg 0$.

Demostración: Sean X, Y, Z enteros positivos tales que $X^n + Y^n = Z^n$. Denotando $d := \operatorname{mcd}(X, Y, Z)$ definamos $(x, y, z) := (X/d, Y/d, Z/d)$, de modo que x, y, z son coprimos y satisfacen que $x^n + y^n = z^n$. Sea $M > 1$ tal que la conjetura *abc* débil fuese cierta para M, entonces aplicándola con $a = x^n, b = y^n, c = z^n$ se verifica que

$$z^n < \operatorname{Rad}(x^n y^n z^n)^M = \operatorname{Rad}(xyz)^M \leq (xyz)^M \leq z^{3M}.$$

De modo que el Último Teorema de Fermat sería válido para $n \geq 3M$ (quizá salvo finitas excepciones primitivas). □

Teorema 15.5: Son equivalentes:

1. La conjetura *abc* (fuerte).
2. **La conjetura de Hall fuerte:** Toda solución primitiva de $x^3 - y^2 = z \neq 0$ satisface que

$$|x| \ll_\epsilon \operatorname{Rad}(z)^{2+\epsilon}, \qquad |y| \ll_\epsilon \operatorname{Rad}(z)^{3+\epsilon}.$$

3. **La conjetura de Szpiro generalizada:** Para todo $\epsilon > 0$ existe una constante $\kappa_\epsilon > 0$ con la siguiente propiedad: sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass

$$E\colon \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

que es minimal respecto a $\mathbb{Z}$. Entonces

$$\text{máx}\{|D_{E/\mathbb{Q}}|, |c_4|^3\} \leq \kappa_E \cdot N_E^{6+\epsilon}.$$

§15.1.1 El caso de cuerpos de funciones.

Teorema 15.6 (Stothers-Mason, 1981): Sea K un cuerpo de $\operatorname{car} K = 0$. Dados polinomios $a(t), b(t), c(t) \in K[t]$ no constantes coprimos tales que $a + b + c = 0$, se cumple que

$$\text{máx}\{\deg a, \deg b, \deg c\} \leq \deg \text{Rad}(abc) - 1,$$

donde $\text{Rad}(f)$ es el producto de sus factores irreducibles mónicos (sin repetición).

15.2 Las conjeturas de Green-Griffiths-Lang

Está sección está principalmente inspirada en Lang **[93],** Javanpeykar **[88],** y Javanpeykar y Kamenova **[89].**

Unas consecuencias de las conjeturas de Vojta, ya antes conjeturados por Lang, es que existe una caracterización de los esquemas con pocos puntos racionales. Procedemos a introducir la terminología fundamental:

Definición 15.7 (Lang): Un esquema algebraico X sobre un cuerpo K se dice ***mordélico*** si para toda extensión finita $L \supseteq K$ se cumple que $X(L)$ es finito.

Corolario 15.7.1: Sea $f\colon X \to Y$ un morfismo étale finito entre esquemas proyectivos sobre un cuerpo K. Entonces X es mordélico (sobre K) syss Y lo es.

Pista: Esto es una aplicación del teorema de Chevalley-Weil. □

Otra manera de expresar el corolario anterior es que la propiedad de «ser un esquema mordélico sobre K» es étale-local.

Definición 15.8: Una variedad analítica X sobre $\mathbb{C}$ se dice ***Brody-hiperbólica*** si toda función holomorfa $\mathbb{C} \to X$ es constante.

Sea K un cuerpo algebraicamente cerrado de $\operatorname{car} K = 0$ y sea X una variedad suave sobre K. Se dice que X es ***fuertemente Brody-hiperbólica*** sobre K si para todo subcuerpo $K_0 \subseteq K$, todo modelo $\mathcal{X}$ de X en K_0 y todo monomorfismo $K_0 \hookrightarrow \mathbb{C}$ se cumpla que $\mathcal{X}_{\mathbb{C}}$ es hiperbólica.

Corolario 15.8.1: Sea $f\colon X \to Y$ un morfismo étale propio entre variedades analíticas sobre $\mathbb{C}$. Entonces X es (fuertemente) Brody-hiperbólica syss Y lo es.

Teorema 15.9 (Bloch-Ochiai-Kawamata): Sea X una subvariedad analítica de una variedad abeliana A sobre $\mathbb{C}$. Entonces X es hiperbólica syss no contiene una traslación de una subvariedad abeliana no nula de A.

Teorema 15.10 (Faltings): Sea X una subvariedad cerrada de una variedad abeliana A sobre un cuerpo K de $\operatorname{car} K = 0$. Entonces X es mordélica syss no contiene una traslación de una subvariedad abeliana no nula de A.

Recuérdese que un grupo algebraico T sobre un cuerpo K se dice un ***toro*** si existe una extensión L/K tal que $T_L \cong \mathbb{G}_{m,L}^n$ para algún n. Los toros de la forma $\mathbb{G}_{m,K}^n$ se dicen ***escindidos***.

Lema 15.11.A: Sea X un esquema algebraico separado sobre un cuerpo K de $\operatorname{car} K = 0$. Son equivalentes:

1. Todo K-morfismo $G \to X$, donde G es un grupo algebraico conexo sobre K, es constante.

2. Todo K-morfismo $G \to X$, donde G es una variedad abeliana sobre K o un toro, es constante.

Demostración: $1 \implies 2$. Trivial.

$2 \implies 1$. Por el teorema de estructura de Barsotti-Chevalley existe un grupo algebraico afín G_{aff} y una sucesión exacta $0 \to G_{\text{aff}} \to G \to A \to 0$ y, por la estructura de grupos algebraicos conmutativos afines, se cumple que $G_{\text{aff}} \cong T \times_K U$, donde T es un toro y U es unipotente. Así, el morfismo $G \to X$ es constante en T y en A, basta ver que también lo es en U. Ahora bien, un grupo algebraico es unipotente syss posee una serie normal con cocientes que son subgrupos de $\mathbb{G}_{a,k}$; y si todo morfismo $\mathbb{G}_{m,k} \to X$ es

constante, entonces todo morfismo $\mathbb{G}_{a,k} \to X$ también. □

Definición 15.11: Se dice que un esquema algebraico separado X sobre un cuerpo k de $\operatorname{car} k = 0$ es ***Lang-hiperbólico***[1] si el cambio de base $X_{k^{\mathrm{alg}}}$ en su clausura algebraica k^{alg} satisface las condiciones del lema anterior.

Observación 15.11.1: En la definición exigimos pasar a la clausura algebraica porque un esquema X podría no tener morfismos no constantes en k y ganarlos en la clausura algebraica. Una manera fácil de ver este desastre es que todo morfismo determina una función a nivel de puntos racionales, y un grupo algebraico siempre tiene el punto racional $e \in G(k)$ que juega el rol del neutro, mientras que $X(k)$ puede ser vacío, como cuando X es una variedad de Brauer-Severi.

Corolario 15.11.2: Sea X un esquema completo sobre un cuerpo K algebraicamente cerrado de $\operatorname{car} K = 0$. Entonces X es Lang-hiperbólico syss todo K-morfismo $A \to X$, desde una variedad abeliana A sobre K, es constante.

Demostración: Basta notar que todo K-morfismo $\mathbb{G}_{m,K} \to X$ se extiende a un morfismo $\mathbb{P}^1_K \to X$, pues $\mathbb{G}_{m,K}$ es un subesquema separado denso en $\mathbb{P}^1_K$ y éste último es completo. Pero siempre existe un morfismo sobreyectivo $E \to \mathbb{P}^1_K$, donde E es una curva elíptica sobre K, de modo que como la composición $E \to X$ es constante, también ha de serlo el morfismo original $\mathbb{G}_{m,K} \to X$. □

Proposición 15.12: Sea S una variedad íntegra sobre un cuerpo k y sea $X \to S$ un k-morfismo de tipo finito. Supongamos que el conjunto de puntos racionales $s \in S(k)$ cuya fibra X_s es Lang-hiperbólica sobre k es Zariski-denso en S. Entonces para toda extensión algebraicamente cerrada $L \supseteq K(S)$ del cuerpo de funciones, el cambio de base X_L es Lang-hiperbólico sobre L.

Lema 15.13.A: Sea X un esquema completo sobre un cuerpo k de $\operatorname{car} k = 0$. Si X es Lang-hiperbólico entonces $\mathbf{Aut}^0_{X/k}$ es el grupo algebraico

[1] No hay consenso sobre la terminología, otros autores le llaman *algebraicamente hiperbólico*, pero nosotros reservamos ese término para otras nociones. Javanpeykar [**88**] les llama *groupless*.

trivial. En particular, $\mathrm{Aut}_k(X)$ es un grupo numerable discreto.

Demostración: Sea $G := \mathbf{Aut}^0_{X/k}$, el cual es la componente conexa de la identidad dentro del grupo localmente algebraico $\mathbf{Aut}_{X/k}$, que representa el funtor $S \mapsto \mathrm{Aut}_S(X_S)$ y que es un subesquema de $\mathbf{Hom}_{X/k}(X, X)$. Así G es un grupo algebraico conexo y, pasando a $K := k^{\mathrm{alg}}$, vemos que cada $x \in X(K)$ determina un K-morfismo $G_K \to X_K$ dado por $\sigma \mapsto \sigma(x)$, por lo que ha de ser constante. Así cada punto de $G(K)$ estabiliza a cada punto geométrico de $X(K)$, luego $G_K = 1$.

El «en particular» se sigue de que $\mathbf{Aut}_{X/k}$ es una unión disjunta numerable de copias de $\mathbf{Aut}^0_{X/k}$. □

Para el siguiente resultado denotaremos por $\mathbf{Sur}_S(Y, X)$ al esquema que representa al funtor de conjuntos que a un S-esquema T le asigna los T-morfismos sobreyectivos $Y_T \to X_T$. Cuando Y es un esquema proyectivo sobre S, entonces $\mathbf{Sur}_S(Y, X)$ existe y es un subesquema abierto de $\mathbf{Hom}_S(X, Y)$, por lo que es un S-esquema separado y localmente de tipo finito.

Teorema 15.13 (Hwang-Kebekus-Peternell): Sean X, Y un par de variedades proyectivas sobre un cuerpo K de $\operatorname{car} K = 0$. Supongamos que X es Lang-hiperbólica y que Y es normal, entonces $\mathbf{Sur}_k(Y, X)$ es un k-esquema discreto con numerables puntos (esquemáticos).

Definición 15.14: Un esquema algebraico X sobre un cuerpo algebraicamente cerrado K se dice *Javanpeykar-puro* o ***J-puro***[2] si para toda variedad suave Y sobre K y todo K-morfismo $U \to X$, definido en un abierto denso U de Y se extiende a un K-morfismo $Y \to X$.

En la definición anterior, como X es completo, en particular es separado y, por tanto, la extensión es única.

Corolario 15.14.1: Sea X un esquema completo J-puro sobre un cuerpo algebraicamente cerrado K. Toda aplicación racional $Y \dashrightarrow X$, donde Y es un esquema suave sobre K, se extiende únicamente a un K-morfismo $Y \to X$.

Lema 15.15: Sea $X \to Y$ un morfismo afín entre esquemas algebraicos

[2] Lang [**92**] les llama *absolutamente minimales*.

sobre un cuerpo algebraicamente cerrado K. Si Y es J-puro, entonces X también lo es.

Proposición 15.16: Un esquema completo X sobre un cuerpo algebraicamente cerrado K es J-puro syss todo morfismo $\mathbb{P}^1_K \to X$ es constante. En consecuencia, todo esquema completo Lang-hiperbólico es J-puro.

Demostración: Sea $\mathbb{P}^1_K \to X$ un morfismo no constante, entonces necesariamente debe ser un morfismo finito (pues es propio y cuasifinito), y por lo tanto, también es afín. Si X fuese J-puro, entonces $\mathbb{P}^1_K$ también lo sería, pero la proyección $\mathbb{P}^2_K \smallsetminus \{[0:0:1]\} \to \mathbb{P}^1_K$ con centro $[0:0:1]$ no posee extensión a todo $\mathbb{P}^2_K$. □

Conjetura de Green-Griffiths-Lang 15.17: Sea X una variedad proyectiva sobre $\mathbb{C}$, son equivalentes:

1. X es Lang-hiperbólica.
2. X es Brody-hiperbólica.
3. Toda subvariedad cerrada de X es de tipo general.

$3'$ X es de tipo general.

Así formulada, la conjetura solo daba las equivalencias $1-3$, pero es claro que basta probar $3'$ ya que ser la propiedad de «ser Lang-hiperbólico» es hereditaria a subesquemas cerrados.

Referencias

88. Javanpeykar, A. *The Lang-Vojta Conjectures on Projective Pseudo-Hyperbolic Varieties* en *Arithmetic Geometry of Logarithmic Pairs and Hyperbolicity of Moduli Spaces* (ed. Nicole, M.-H.) (Springer, Cham, 2020), 135-196.

89. Javanpeykar, A. y Kamenova, L. Demailly's notion of algebraic hyperbolicity: geometricity, boundedness, moduli of maps. *Math. Z.* **296,** 1645-1672. doi:10.1007/s00209-020-02489-6 (2020).

92. Lang, S. Hyperbolic and Diophantine Analysis. *Bull. Amer. Math. Soc.* **14,** 159-205. doi:10.1090/S0273-0979-1986-15426-1 (1986).

93. Lang, S. *Number Theory.* III: *Diophantine Geometry Encyclopaedia of Mathematical Sciences* **60** (Springer-Verlag, 1991).

Apéndice

Índice alfabético

Lista de tareas pendientes