Teoría de Números Algebraicos

Alexey Beshenov

CIMAT, Guanajuato

Otoño 2020

Índice general

Introducción

Esta es una versión preliminar de mis apuntes del curso.
Para la última versión, visite la página http://cadadr.org/cimat-tna/apuntes.html
Preguntas, comentarios y correcciones: alexey.beshenov@cimat.mx

> I attended a course in algebraic number theory from Artin which was extremely elegant, although perhaps too advanced for me. However, it wasn't until a few years later that I learned what an algebraic number was. The course was so streamlined that algebraic numbers were never actually mentioned.
>
> John Milnor, citado por Steven Krantz

La teoría de números algebraicos estudia... los **números algebraicos**, es decir, los números complejos $\alpha \in \mathbb{C}$ que satisfacen una relación algebraica no trivial

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in \mathbb{Q}$ y $a_n \neq 0$. Estos números viven en los **campos de números** que son extensiones finitas $K/\mathbb{Q}$. A saber, los campos de números son de la forma $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$, donde los α_i son números algebraicos.

Un ejemplo sencillo de campo de números es

$$\mathbb{Q}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\},$$

la extensión cuadrática de los números racionales que se obtiene añadiendo la raíz cuadrada $\sqrt{-5}$.

La teoría de números surge al considerar subanillos en los campos de números $R \subset K$, que sería lógico denominar los **anillos de números**. (No es un término muy común, pero lo adoptaremos en nuestro curso, siguiendo a [Ste2017].) Por ejemplo

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

es un anillo de números dentro del campo de números $\mathbb{Q}(\sqrt{-5})$.

Los anillos de números son objetos unidimensionales. Específicamente, a cualquier anillo conmutativo R se puede asociar su *dimensión de Krull* $\dim R$, y para cualquier anillo de números se cumple $\dim R = 1$. En este sentido la teoría de anillos de números se parece mucho a la teoría de curvas algebraicas.

Los anillos de números son generalizaciones bastante sencillas del anillo de los números enteros $\mathbb{Z}$, pero en los anillos de números, entre otras cosas, ya no necesariamente se cumple el *teorema fundamental de la aritmética* (que afirma que todo número se expresa esencialmente de manera única como un producto de números primos). Por ejemplo, en el anillo $\mathbb{Z}[\sqrt{-5}]$

$$2 \cdot 3 = (1 + \sqrt{-5})\,(1 - \sqrt{-5})$$

son dos factorizaciones distintas del número 6. La idea de Richard Dedekind consistía en remplazar las factorizaciones en números primos por factorizaciones de *ideales* en *ideales primos* del anillo. En el ejemplo de arriba,

$$(2) = \mathfrak{p}^2, \quad (3) = \mathfrak{q}_1\mathfrak{q}_2, \quad (1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q}_1, \quad (1-\sqrt{-5}) = \mathfrak{p}\mathfrak{q}_2,$$

donde

$$\mathfrak{p} = (2, 1+\sqrt{-5}); \quad \mathfrak{q}_1 = (3, 1+\sqrt{-5}); \quad \mathfrak{q}_2 = (3, 2+\sqrt{-5})$$

son ideales primos en $\mathbb{Z}[\sqrt{-5}]$. Los anillos de números donde los ideales se descomponen de manera única en ideales primos se conocen como los **anillos de Dedekind**. Todas estas nociones serán introducidas y consideradas en detalles en el curso.

El objetivo principal será definir algunos invariantes fundamentales de los campos de números: el **anillo de enteros** $\mathcal{O}_K \subset K$, **grupo de clases** $\mathrm{Cl}(K)$, y **grupo de unidades** $\mathcal{O}_K^\times$, demostrar sus propiedades básicas y aprender a calcularlos.

Todos los invariantes que serán considerados en el curso se pueden calcular algorítmicamente. En particular, veremos ejemplos de cálculos en el programa PARI/GP (https://pari.math.u-bordeaux.fr/) y la base de datos LMFDB (https://lmfdb.org/). Todo el material teórico será acompañado de problemas con pruebas y cálculos particulares.

0.1 Para qué sirve este curso

Este curso podría ser interesante para los que estudian álgebra conmutativa, ya que serán consideradas algunas nociones fundamentales de esta área (ideales primos, anillos de valuación discreta, anillos de Dedekind, el grupo de Picard de un anillo conmutativo, el grupo de unidades, etc.), basándose en ejemplos muy concretos y calculables. En cierto sentido, el álgebra conmutativa históricamente se originó en la teoría de números algebraicos. (El mismo término «anillo» fue introducido por Hilbert en un contexto de anillos de números, e «ideal» es la abreviación del «número ideal».)

Además, la similitud entre los anillos de números y curvas algebraicas que mencioné arriba, haría este material útil para los que están aprendiendo superficies de Riemann, singularidades de curvas, etc. y los interesados en la geometría algebraica moderna (la teoría de esquemas etc.).

Por último, y no menos importante, este curso es fundamental para los estudiantes con intención de aprender la teoría de números.

0.2 Conocimientos preliminares

Tendré que suponer que los oyentes conozcan las nociones como anillo (conmutativo), ideal (primo, maximal), anillo cociente, módulo sobre un anillo (módulo libre, rango), y campo (incluso la teoría de campos finitos). Tampoco estaría mal conocer la teoría de Galois básica, pero el lector puede consultar el apéndice A para un breve resumen.

De todas maneras, cuando sea necesario en el transcurso, trataremos las nociones poco conocidas. Uno de mis objetivos es presentar diferentes herramientas algebraicas, así como ejemplos muy concretos.

0.3 Referencias

Mi fuente principal de inspiración son los apuntes de Peter Stevenhagen [Ste2017] de un curso que se imparte en la universidad de Leiden (Países Bajos). Además, podrían ser útiles diferentes libros de texto sobre el tema; he aquí algunas fuentes que puedo recomendar.

Algunos apuntes en línea, a parte de [Ste2017], son los siguientes:

- el curso de Andrew Sutherland en MIT: https://dspace.mit.edu/handle/1721.1/124987

- J.S. Milne: https://www.jmilne.org/math/CourseNotes/ant.html
- Paul Garrett: http://www-users.math.umn.edu/~garrett/m/number_theory/
- varios apuntes de Keith Conrad: https://kconrad.math.uconn.edu/blurbs/
- un curso de Robert B. Ash: https://faculty.math.illinois.edu/~r-ash/ANT.html

Algunos libros introductorios son [IR1990, Chapters 12, 13, 17], [AW2004], [KKS2011], [FT1993], [Mar2018], [Sam1967], [BS1966, Chapters 4, 5], [Cox2013].

Para experimentos en PARI/GP, véase el libro [RV2007].

Lectura avanzada: [Neu1999], [Lan1994], [CF2010].

En fin, en este curso veremos varios cálculos específicos, pero no hablaremos de algoritmos serios. Las fuentes recomendadas sobre la teoría algorítmica son [PZ1997], [Len1992], [Coh1993].

0.4 Agradecimientos

Agradezco a CIMAT por la oportunidad de dar este curso, y en particular al Dr. Xavier Gómez Mont y Dr. Pedro Luis del Ángel.

Pavel Solomatin y Dmitry Shvetsov han hecho varias observaciones útiles acerca de una versión preliminar de mis notas, y hemos tenido muchas conversaciones sobre la teoría de números y pedagogía.

También agradezco a todos los participantes del curso, y sobre todo a Marvin Ferman Bell, José de Jesús García Ruvalcaba, William Eduardo Pena, Óscar Andrés Ramírez Ramírez, y Alexis Zamora.

Capítulo 1

Primer encuentro con anillos de números

En este capítulo introductorio vamos a definir los campos y anillos de números y para motivar su estudio, veremos varios ejemplos de sus aplicaciones a los problemas de la teoría de números clásica.

1.1 Campos de números

Clase 1
10/08/20

Como sugiere el nombre del curso, nuestro objeto de estudio son los **números algebraicos** que son elementos de $\overline{\mathbb{Q}}$, la cerradura algebraica del campo de números racionales $\mathbb{Q}$.

1.1.1. Definición. Un número $\alpha \in \mathbb{C}$ es **algebraico** si este satisface alguna relación algebraica

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ y $a_n \neq 0$.

Por supuesto, siempre se pueden normalizar los coeficientes para obtener un polinomio mónico con $a_n = 1$. Si además se puede escoger un polinomio mónico con *coeficientes enteros*, se dice que α es un **entero algebraico**.

1.1.2. Definición. Se dice que $\alpha \in \mathbb{C}$ es un **entero algebraico** si

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

para algunos $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$.

1.1.3. Ejemplo. El número $\alpha = \frac{1+\sqrt{5}}{2}$ es un entero algebraico, ya que cumple la relación

$$\alpha^2 - \alpha - 1 = 0.$$ ▲

Todos los enteros algebraicos forman un subanillo de $\overline{\mathbb{Q}}$ (no es algo inmediato; lo veremos más adelante en el curso).

Los números algebraicos viven en campos de números.

1.1.4. Definición. Un **campo de números** es una extensión finita $K/\mathbb{Q}$.

Recordemos que por una extensión **finita** se entiende una extensión de grado $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K$ finito.

1.1.5. Ejemplo. Sea d un entero **libre de cuadrados**[*] (posiblemente negativo). Entonces,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$

es una extensión de $\mathbb{Q}$ de grado 2. A saber, como una base sobre $\mathbb{Q}$ se puede tomar $\{1, \sqrt{d}\}$. ▲

1.1.6. Ejemplo. Sea $f \in \mathbb{Q}[x]$ un polinomio irreducible. En este caso el anillo cociente $\mathbb{Q}[x]/(f)$ es un campo y es una extensión de $\mathbb{Q}$ de grado $\deg f$. Si α es una raíz de f, entonces el homomorfismo de evaluación

$$\mathbb{Q}[x] \to \mathbb{C}, \quad g \mapsto g(\alpha)$$

induce un isomorfismo

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f).$$

Notamos que el objeto a la derecha es puramente algebraico.

De hecho, toda extensión finita de $\mathbb{Q}$ es isomorfa a una de la forma $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$; este es el contenido del **teorema del elemento primitivo** (véanse los ejercicios). ▲

1.1.7. Ejemplo. Sea $\zeta_n = \exp(2\pi i/n)$ una raíz n-ésima primitiva. El polinomio mínimo de ζ_n es el **n-ésimo polinomio ciclotómico**

$$\Phi_n = \prod_{\substack{1 \le k < n \\ \mathrm{mcd}(k,n)=1}} (x - \zeta_n^k) \in \mathbb{Z}[x].$$

El hecho de que el polinomio de arriba tiene coeficientes enteros y es irreducible no es tan inmediato. El lector que no conoce los polinomios ciclotómicos puede revisar el Apéndice B.

El **n-ésimo campo ciclotómico**

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n)$$

es una extensión de grado $\phi(n)$ de $\mathbb{Q}$.

Se tiene $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ para $m < n$ si y solamente si m es impar y $n = 2m$. Esto también se refleja en la identidad para los polinomios ciclotómicos $\Phi_{2m}(x) = \Phi_m(x)$. ▲

1.2 Anillos de números

La siguiente terminología es un poco menos común, pero será útil en nuestro curso.

1.2.1. Definición. Un **anillo de números** es un subanillo de un campo de números.

1.2.2. Ejemplo. Los anillos $\mathbb{Z}$,

$$\mathbb{Z}\left[\frac{1}{n}\right] = \left\{\frac{a}{n^k} \;\middle|\; a \in \mathbb{Z},\, k = 0, 1, 2, \ldots\right\},$$
$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \;\middle|\; p \nmid b\right\}$$

(para $n > 0$ y p primo fijos) son anillos de números, siendo subanillos de $\mathbb{Q}$. Los anillos $\mathbb{Z}\left[\frac{1}{n}\right]$ y $\mathbb{Z}_{(p)}$ son diferentes **localizaciones** de $\mathbb{Z}$. ▲

1.2.3. Ejemplo. Si d es un entero libre de cuadrados, entonces

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

es un anillo de números, siendo un subanillo de $\mathbb{Q}(\sqrt{d})$. Este es un $\mathbb{Z}$-módulo libre de rango 2.

[*] Es decir, tal que $n^2 \nmid d$ para ningún $n > 1$

Si $d \equiv 1 \pmod 4$, se puede considerar el anillo más grande

$$\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] = \Big\{a + b\,\frac{1+\sqrt{d}}{2} \;\Big|\; a, b \in \mathbb{Q}\Big\} \subset \mathbb{Q}(\sqrt{d}).$$

Notamos que el número $\alpha = \frac{1+\sqrt{d}}{2}$ es un entero algebraico, ya que este satisface la relación

$$\alpha^2 - \alpha - \frac{d-1}{4} = 0.$$

De nuevo, $\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big]$ es un $\mathbb{Z}$-módulo libre de rango 2. ▲

1.2.4. Ejemplo. El anillo

$$\mathbb{Z}[\zeta_n] = \Big\{\sum_k a_k\,\zeta_n^k \mid a_k \in \mathbb{Z}\Big\}$$

es un anillo de números, siendo un subanillo del campo ciclotómico $\mathbb{Q}(\zeta_n)$. ▲

Una clase importante de anillos de números son órdenes.

1.2.5. Definición. Un anillo de números $R \subset K$ que es finitamente generado como $\mathbb{Z}$-módulo se llama un **orden** en su campo de fracciones $\operatorname{Frac} R \subseteq K$.

Puesto que un campo de números K como un grupo aditivo no tiene elementos de torsión, notamos que un orden es un $\mathbb{Z}$-módulo *libre*.

1.2.6. Ejemplo. Los anillos de números $\mathbb{Z}[\sqrt{d}]$ y $\mathbb{Z}[\zeta_n]$ son órdenes. En general, si $f \in \mathbb{Z}[x]$ es un polinomio mónico irreducible, entonces $\mathbb{Z}[x]/(f)$ es un orden de rango $\deg f$. Este anillo es isomorfo a $\mathbb{Z}[\alpha]$ donde α es una raíz de f. Notamos que $\mathbb{Z}[x]/(f)$ naturalmente se identifica con un subanillo de $\mathbb{Q}[x]/(f)$:

$$\mathbb{Z}[\alpha] \subset \mathbb{Q}(\alpha).$$

Este es el candidato más obvio para un subanillo en un campo de números. Sin embargo, más adelante veremos que no es siempre la mejor opción.

Notamos que en este ejemplo f es un polinomio mónico con coeficientes enteros, así que α es un entero algebraico. En el caso contrario, si α no es un entero algebraico, $\mathbb{Z}[\alpha]$ no será finitamente generado como un $\mathbb{Z}$-módulo. ▲

1.2.7. Ejemplo. Por otra parte, los anillos como $\mathbb{Q}$, $\mathbb{Z}\Big[\frac{1}{n}\Big]$ y $\mathbb{Z}_{(p)}$ no son órdenes (ejercicio). ▲

1.3 Primeros cálculos en PARI/GP

Durante el curso trataremos de ver ejemplos de cálculos en el programa PARI/GP. Para descargarlo y consultar la documentación, consulte la página

`https://pari.math.u-bordeaux.fr/`

También recomiendo el libro [RV2007] enfocado en la exploración de la teoría de números a través de cálculos en PARI/GP.

Ya que estábamos hablando de números algebraicos, la función `algdep(x,d)` busca una relación algebraica para x de grado $\leq d$. Por ejemplo,

```
? algdep((sqrt(13)+1)/2, 2)
% = x^2 - x - 3
? algdep(fibonacci(101)/fibonacci(100)*1.0, 2)
% = x^2 - x - 1
? algdep (exp (2*Pi*I/7), 6)
% = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1
? algdep (sqrt(2) + sqrt(3), 4)
% = x^4 - 10*x^2 + 1
? algdep (Pi,5)
% = 37542*x^5 - 69665*x^4 - 134081*x^3 - 77323*x^2 + 40979*x + 89174
? subst(%,x,Pi)
% = -1.7092371337382136939 E-26
```

(El número π es trascendente, así que no hay que esperar una relación algebraica razonable.)

Dado que todos los campos de números son de la forma $\mathbb{Q}[x]/(f)$ para un polinomio irreducible f, para hacer cálculos en ellos basta saber trabajar con los polinomios módulo f. Esto se hace mediante la división con resto, pero en práctica se puede usar PARI/GP. Allí la expresión `Mod(`g`,`f`)` denota el polinomio g módulo f. Si queremos olvidar de que g se considera módulo f, se puede usar la función `lift(`x`)`

Por ejemplo, para calcular las potencias de $1+\sqrt{2}$, podemos hacer lo siguiente:

```
? u = Mod (1+x, x^2-2);
? vector (10,i,u^i)
% = [Mod(x + 1, x^2 - 2), Mod(2*x + 3, x^2 - 2), Mod(5*x + 7, x^2 - 2),
     Mod(12*x + 17, x^2 - 2), Mod(29*x + 41, x^2 - 2),
     Mod(70*x + 99, x^2 - 2), Mod(169*x + 239, x^2 - 2),
     Mod(408*x + 577, x^2 - 2), Mod(985*x + 1393, x^2 - 2),
     Mod(2378*x + 3363, x^2 - 2)]
? lift (%)
% = [x + 1, 2*x + 3, 5*x + 7, 12*x + 17, 29*x + 41, 70*x + 99,
     169*x + 239, 408*x + 577, 985*x + 1393, 2378*x + 3363]
```

Para verificar si un polinomio es irreducible, se puede usar `polisirreducible(`f`)`, mientras que `factor(`f`)` encuentra los factores irreducibles.

```
? f = polcyclo(12)
% = x^4 - x^2 + 1

? polisirreducible(f)
% = 1
? factor (f*Mod(1,2))
% =
[Mod(1, 2)*x^2 + Mod(1, 2)*x + Mod(1, 2) 2]

? factor (f*Mod(1,3))
```

```
% =
[Mod(1, 3)*x^2 + Mod(1, 3) 2]

? factor (f*Mod(1,5))
% =
[Mod(1, 5)*x^2 + Mod(2, 5)*x + Mod(4, 5) 1]
[Mod(1, 5)*x^2 + Mod(3, 5)*x + Mod(4, 5) 1]

? factor (x^6-1)
% =
[      x - 1 1]
[      x + 1 1]
[x^2 - x + 1 1]
[x^2 + x + 1 1]
```

El polinomio mínimo y el polinomio característico se encuentran mediante `minpoly(x)` y `charpoly(x)` respectivamente:

```
? charpoly (Mod (x + x^-1, polcyclo (5)))
% = x^4 + 2*x^3 - x^2 - 2*x + 1
? factor(%)
% =
[x^2 + x - 1 2]

? minpoly (Mod (x + x^-1, polcyclo (5)))
% = x^2 + x - 1
```

1.4 Reciprocidad cuadrática mediante sumas de Gauss en $\mathbb{Z}[\zeta_p]$

Lectura adicional

Existen muchísimas pruebas de la ley de reciprocidad cuadrática, y en esta seccón vamos a ver la prueba de Gauss basada en cálculos ingeniosos en el anillo ciclotómoco $\mathbb{Z}[\zeta_p]$. Este es un ejemplo curioso de cómo propiedades de los números enteros $\mathbb{Z}$ se establecen al pasar a un anillo más grande.

1.4.1. Definición. Sea p un número primo fijo. Para un número entero a tal que $p \nmid a$ el **símbolo de Legendre** se define mediante

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

Además, para $p \mid a$ se pone $\left(\frac{a}{p}\right) = 0$.

De la definición está claro que si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Recordemos que el grupo multiplicativo $\mathbb{F}_p^\times$ es cíclico (véase A.12.3), lo que significa que existe un generador $x \in \mathbb{F}_p^\times$ tal que

$$\mathbb{F}_p^\times = \{1, x, x^2, x^3, \ldots, x^{p-2}\}.$$

Entonces, x^k es un cuadrado si y solamente si k es par. De aquí se ve fácilmente que el símbolo de Legendre es multiplicativo:

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

Entonces, se trata de un homomorfismo

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}.$$

Para calcular el símbolo de Legendre, se usa el siguiente resultado, descubierto por Gauss.

1.4.2. Teorema (Reciprocidad cuadrática). *Sean p y q diferentes primos impares. Entonces,*

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

Además, se cumple

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

1.4.3. Ejemplo. Para $p \neq 3$ calculemos el símbolo de Legendre $\left(\frac{-3}{p}\right)$. Tenemos

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

El único cuadrado no nulo módulo 3 es 1, así que

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

Por ejemplo,

$$-3 \equiv 2^2\ (7), -3 \equiv 6^2\ (13), -3 \equiv 4^2\ (19), -3 \equiv 11^2\ (31), -3 \equiv 16^2\ (37).$$ ▲

1.4.1 Congruencia de Euler y leyes suplementarias

Primero, nos servirá la siguiente interpretación del símbolo de Legendre.

1.4.4. Lema (Congruencia Euler). *Para $p \neq 2$ y a tal que $p \nmid a$ se tiene*

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

Demostración. Sea x un generador de $\mathbb{F}_p^\times$. Tenemos $[a]_p = x^i$ para algún i, y este es un cuadrado en $\mathbb{F}_p^\times$ si y solamente si i es par. Luego,

$$[a]_p^{\frac{p-1}{2}} = x^{i\frac{p-1}{2}}.$$

Si i es par, entonces $i\frac{p-1}{2}$ es divisible por $p-1 = \#\mathbb{F}_p^\times$, así que

$$x^{i\frac{p-1}{2}} = 1$$

(usando que $|\mathbb{F}_p^\times| = p-1$). Si i es impar, entonces $i^{\frac{p-1}{2}}$ no es divisible por $p-1$, y por ende

$$x^{i\frac{p-1}{2}} \neq 1.$$

Sin embargo,

$$\left(x^{i\frac{p-1}{2}}\right)^2 = x^{i(p-1)} = 1,$$

lo que nos permite concluir que

$$x^{i\frac{p-1}{2}} = -1.$$ ■

1.4.5. Corolario (Primera ley suplementaria). *Para $p \neq 2$ se cumple*

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

Demostración. Basta sustituir $a = -1$ en el criterio de Euler. ■

1.4.6. Corolario (Segunda ley suplementaria). *Para $p \neq 2$ se cumple*

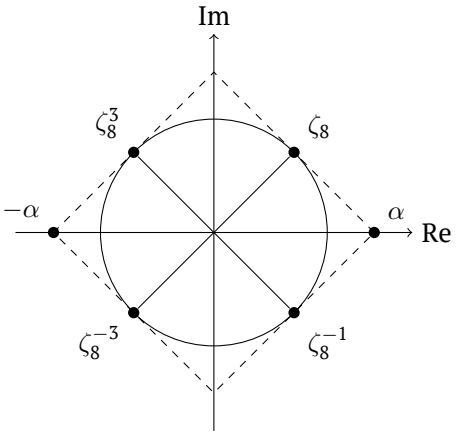
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p \equiv 1, 7 \pmod 8, \\ -1, & p \equiv 3, 5 \pmod 8. \end{cases}$$

Demostración. De nuevo, se puede aplicar el criterio de Euler

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

y hay que solo identificar el número a la derecha. Hay argumentos elementales, pero me gustaría presentar un cálculo con las raíces octavas de la unidad. Consideremos $\zeta_8 = \exp(2\pi i/8)$ y el número

$$\alpha = \zeta_8 + \zeta_8^{-1}.$$



Notamos que en el anillo $\mathbb{Z}[\zeta_8]$ se cumple

$$\alpha^p = (\zeta_8 + \zeta_8^{-1})^p \equiv \zeta_8^p + \zeta_8^{-p} \equiv \begin{cases} \zeta_8 + \zeta_8^{-1} = +\alpha, & p \equiv \pm 1 \pmod 8, \\ \zeta_8^3 + \zeta_8^{-3} = -\alpha, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p$$

(usando la identidad $(x+y)^p \equiv x^p + y^p \pmod p$). Puesto que $\alpha = \sqrt{2}$, calculamos

$$2^{\frac{p-1}{2}} = \alpha^{p-1} = \alpha^p\,\alpha^{-1} \equiv (\zeta_8 + \zeta_8^{-1})^p\,\alpha^{-1} \equiv \begin{cases} +1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases} \pmod p$$ ■

1.4.2 Sumas cuadráticas de Gauss

Vamos a trabajar en el anillo ciclotómico $\mathbb{Z}[\zeta_p]$, donde p es un primo impar fijo y $\zeta_p = \exp(2\pi i/p)$.

1.4.7. Definición. Para $a \in \mathbb{Z}$ la **suma cuadrática de Gauss** correspondiente viene dada

$$g_a = \sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) \zeta_p^{ai} \in \mathbb{Z}[\zeta_p].$$

Además, pongamos $g = g_1$.

A partir de ahora todas las sumas serán entre 0 y $p-1$, así que vamos a escribir «$\sum_i$» en lugar de «$\sum_{0 \le i \le p-1}$». Primero necesitamos algunos lemas.

1.4.8. Lema.

$$\sum_i \zeta_p^{ai} = \begin{cases} p, & si\ p \mid a, \\ 0, & si\ p \nmid a. \end{cases}$$

Demostración. Si $p \mid a$, entonces $\zeta_p^{ai} = 1$ y $\alpha^{ai} = 1$. Por otra parte, si $p \nmid a$, entonces $\zeta_p^a \neq 1$, $\zeta_p^p = 1$, y en $\mathbb{Q}(\zeta_p)$ se cumple

$$\sum_i \zeta_p^{ai} = \frac{\zeta_p^{ap} - 1}{\zeta_p^a - 1} = 0. \qquad \blacksquare$$

1.4.9. Lema. $g_a = \left(\frac{a}{p}\right) g$.

Demostración. Primero, si $p \mid a$, entonces $\left(\frac{a}{p}\right) = 0$ y

$$g_a = \sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) \underbrace{\zeta_p^{ai}}_{=1} = \sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) = 0.$$

Ahora supongamos que $p \nmid a$. En este caso calculamos

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_i \left(\frac{i}{p}\right) \zeta_p^{ai} = \sum_i \left(\frac{ai}{p}\right) \zeta_p^{ai} = \sum_j \left(\frac{j}{p}\right) \zeta_p^j = g.$$

Esto establece el resultado, dado que $\left(\frac{a}{p}\right) = \pm 1$. $\blacksquare$

Ahora consideremos el cuadrado de nuestra suma de Gauss:

$$g^2 = \left(\sum_i \left(\frac{i}{p}\right) \zeta_p^i\right)^2.$$

Se puede ver fácilmente que este es un entero (un elemento de $\mathbb{Z}$ y no solamente $\mathbb{Z}[\zeta_p]$) usando la teoría de Galois. A saber, el grupo $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ consiste en automorfismos $\sigma\colon \zeta_p \mapsto \zeta_p^a$ donde $1 \le a \le p-1$ (véase §B.3). Cada uno de ellos deja g^2 fijo:

$$\sigma(g^2) = \sigma(g)^2 = g_a^2 = \left(\frac{a}{p}\right)^2 \cdot g^2 = g^2.$$

Podemos concluir que $g^2 \in \mathbb{Z}[\zeta_p] \cap \mathbb{Q} = \mathbb{Z}$. Algunos cálculos suguieren cuál es el número entero en cuestión.

```
? test (p) = liftall (Mod(sum(i=1,p-1,kronecker(i,p)*x^i), polcyclo(p))^2);
? forprime (p=3,23, print ([p, test(p)]))
[3, -3]
[5, 5]
[7, -7]
[11, -11]
[13, 13]
[17, 17]
[19, -19]
[23, -23]
```

1.4.10. Lema. $g^2 = p^*$.

Demostración. El truco consiste en calcular la suma $\sum_a g_a g_{-a}$ de dos maneras diferentes. Primero, usando 1.4.9, calculamos que para $p \nmid a$ se tiene

$$g_a g_{-a} = \left(\frac{a}{p}\right) g \cdot \left(\frac{-a}{p}\right) g = \left(\frac{-1}{p}\right) \left(\frac{a}{p}\right)^2 g^2 = \left(\frac{-1}{p}\right) g^2.$$

Por otra parte, si $p \mid a$, entonces $g_a g_{-a} = 0$. Todo esto nos da la identidad

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right) (p-1)\, g^2. \tag{*}$$

Ahora el cálculo directo nos lleva a

$$\sum_a g_a g_{-a} = \sum_a \Big(\sum_i \left(\frac{i}{p}\right) \zeta_p^{ai}\Big) \cdot \Big(\sum_j \left(\frac{j}{p}\right) \zeta_p^{-aj}\Big) = \sum_i \sum_j \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \sum_a \zeta_p^{a\,(i-j)}.$$

Usando 1.4.8, calculamos

$$\sum_a \zeta_p^{a\,(i-j)} = \begin{cases} p, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Así se puede concluir que

$$\sum_a g_a g_{-a} = \sum_i \left(\frac{i}{p}\right)^2 p = (p-1)\, p,$$

y nos queda comparar el resultado con (*). ∎

De hecho, el signo fue calculado por Gauss:

$$g = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod 4, \\ i\sqrt{p}, & p \equiv 3 \pmod 4 \end{cases}$$

(véase [IR1990, Chapter 6]), pero esto no será relevante para nuestra prueba.

1.4.3 Demostración de la reciprocidad cuadrática

Sean p y q diferentes primos impares. Denotemos

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

Entonces, la reciprocidad cuadrática es equivalente a la fórmula

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

Vamos a trabajar con congruencias módulo q en el anillo $\mathbb{Z}[\zeta_p]$:

$$x \equiv y \pmod{q} \iff x - y = qz \text{ para algún } z \in \mathbb{Z}[\zeta_p],$$

o de manera equivalente, trabajar en el anillo cociente finito $\mathbb{Z}[\zeta_p]/(q)$. Por el momento no necesitamos saber mucho de su estructura, salvo las siguientes sencillas observaciones.

1. *Para cualesquiera $x, y \in \mathbb{Z}[\zeta_p]$ se tiene $(x+y)^q \equiv x^q + y^q \pmod{q}$.*

   Esto se sigue inmediatamente del teorema de binomio.

2. *Dos enteros $a, b \in \mathbb{Z}$ son congruentes módulo q en $\mathbb{Z}$ si y solamente si son congruentes módulo q en el anillo más grande $\mathbb{Z}[\zeta_p]$.*

   En efecto, para la implicación menos obvia, si $a - b = qx$ para algún $x \in \mathbb{Z}[\zeta_p]$, entonces $x = \frac{a-b}{q} \in \mathbb{Q}$, pero por otro lado, $\mathbb{Z}[\zeta_p] \cap \mathbb{Q} = \mathbb{Z}$.

Según 1.4.10, tenemos

$$g^2 = p^*.$$

Luego, en $\mathbb{Z}[\zeta_p]$ se cumple

$$g^{q-1} = (g^2)^{\frac{q-1}{2}} = (p^*)^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$$

(usando la congruencia de Euler). Ahora

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

Por otro lado,

$$g^q = \left(\sum_i \left(\frac{i}{p}\right) \zeta_p^i\right)^q \overset{\text{Obs. 1}}{\equiv} \sum_i \left(\frac{i}{p}\right)^q \zeta_p^{qi} = \sum_i \left(\frac{i}{p}\right) \zeta_p^{qi} = g_q \overset{1.4.9}{\equiv} \left(\frac{q}{p}\right) g \pmod{q}.$$

Combinando las dos congruencias,

$$\left(\frac{p^*}{q}\right) g \equiv \left(\frac{q}{p}\right) g \pmod{q}.$$

El anillo $\mathbb{Z}[\zeta_p]/(q)$ no tiene por qué ser un dominio, así que hay que tener cuidado antes de cancelar g. Sin embargo, multiplicando por g y usando otra vez más 1.4.10, se obtiene la congruencia en $\mathbb{Z}[\zeta_p]$

$$\left(\frac{p^*}{q}\right) p^* \equiv \left(\frac{q}{p}\right) p^* \pmod{q}.$$

Gracias a la segunda observación de arriba, esto es lo mismo que una congruencia módulo q en $\mathbb{Z}$, donde

$$\left(\frac{p^*}{q}\right) p^* \equiv \left(\frac{q}{p}\right) p^* \Longrightarrow \left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \Longrightarrow \left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right),$$

y hemos terminado la demostración. ■

La prueba de arriba ya demuestra el poder de los anillos de números. Además, a partir de ahora vamos a ocupar la reciprocidad cuadrática libremente en nuestras pruebas.

1.5 Divisibilidad y factorización en dominios

Clase 2
12/08/20

Nos interesan los anillos de números, y estos son dominios de integridad (no tienen divisores de cero), ya que por la definición están dentro de un campo. En la presente sección R siempre denotará un dominio.

1.5.1. Definición. Se dice que $\alpha \in R$ es una **unidad** si α es invertible; es decir, si existe $\beta \in R$ tal que $\alpha\beta = 1$. Las unidades forman un grupo multiplicativo que será denotado por $R^\times$.

En general no es fácil describir el grupo de unidades $R^\times$. Uno de los resultados principales del curso será la descripción de $R^\times$ en el caso cuando R es un orden en un campo de números.

1.5.2. Definición. Consideremos elementos $\alpha, \beta \in R$.

- Se dice que α **divide** a β (notación $\alpha \mid \beta$) si $\beta = \gamma\alpha$ para algún $\gamma \in R$.
- Se dice que α y β son **asociados** (notación $\alpha \sim \beta$) si $\alpha \mid \beta$ y $\beta \mid \alpha$.

Para un elemento $\alpha \in R$ vamos a denotar por

$$(\alpha) = \{\gamma\alpha \mid \gamma \in R\}$$

el **ideal principal** generado por α. La divisibilidad puede ser interpretada en términos de ideales principales:

$$\begin{aligned} \alpha \mid \beta &\iff (\alpha) \supseteq (\beta), \\ \alpha \sim \beta &\iff (\alpha) = (\beta), \\ \alpha \in R^\times &\iff (\alpha) = R. \end{aligned}$$

La relación de divisibilidad tiene todas las propiedades esperadas. La relación $\sim$ tiene el siguiente significado:

$$\alpha \sim \beta \iff \beta = u\alpha \text{ para } u \in R^\times.$$

Los elementos que no tienen divisores no triviales se llaman irreducibles, mientras que la noción de elementos primos es diferente y hay que hacer la distinción.

1.5.3. Definición. Sea $\pi \in R$ un elemento no nulo y no invertible.

1) Se dice que π es **irreducible** si se cumple

$$\alpha \mid \pi \Longrightarrow \alpha \in R^\times \text{ o } \alpha \sim \pi.$$

2) Se dice que π es **primo** si se cumple

$$\pi \mid \alpha\beta \Longrightarrow \pi \mid \alpha \text{ o } \pi \mid \beta.$$

1.5.4. Proposición. *Todo elemento primo es irreducible.*

Demostración. Ejercicio. ■

En general, un elemento irreducible no tiene por qué ser primo; vamos a ver ejemplos particulares en los ejercicios. Esto tiene que ver con falla de factorización única.

1.5.1 Dominios de factorización única

Se dice que R es un dominio de factorización única si en R se cumple el teorema fundamental de la aritmética en el siguiente sentido.

1.5.5. Definición. R es un **dominio de factorización única** si se cumplen las siguientes dos propiedades:

1) todo elemento no nulo y no invertible $\alpha \in R$ puede ser expresado como

$$\alpha = \pi_1 \cdots \pi_s,$$

donde $\pi_1, \ldots, \pi_s \in R$ son irreducibles;

2) estas expresiones son únicas salvo el orden de los múltiplos y la relación de equivalencia $\sim$: si

$$\alpha = \pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t$$

donde π_i, ρ_j son irreducibles, se tiene necesariamente $s = t$, y después de una permutación de los múltiplos, se cumple $\pi_i \sim \rho_i$ para todo $1 \leq i \leq s$.

El concepto de factorización única fue explorado sistemáticamente por primera vez por Gauss. Los anillos de números no suelen tener factorización única. Este es uno de los temas principales de nuestro curso. Los primeros ejemplos particulares se encuentran en los ejercicios.

1.5.6. Teorema. *Las siguientes condiciones son equivalentes.*

1) R es un dominio de factorización única;

2) R satisface las siguientes dos propiedades:

a) toda cadena ascendente de ideales principales se estabiliza: dada una cadena de ideales principales

$$(\alpha_1) \subseteq (\alpha_2) \subseteq (\alpha_3) \subseteq \cdots \subseteq R$$

existe n tal que $(\alpha_n) = (\alpha_{n+1}) = \cdots$

b) todo elemento irreducible es primo.

Demostración. Supongamos que R es un dominio de factorizacioń única. Ahora si

$$(\alpha) \subsetneq (\beta), \quad \alpha = \pi_1 \cdots \pi_s, \quad \beta = \rho_1 \cdots \rho_t$$

son factorizaciones en elementos irreducibles, entonces $s > t$. No podemos tener una cadena infinita

$$(\alpha) \subsetneq (\alpha_1) \subsetneq (\alpha_2) \subsetneq \cdots,$$

porque a cada paso el número de factores irreducibles disminuye. Esto establece la propiedad a).

Para la propiedad b), si π es un elemento irreducible y $\pi \mid \alpha\beta$, basta considerar las factorizaciones de α y β en irreducibles para concluir que $\pi \mid \alpha$ o $\pi \mid \beta$.

La implicación un poco más trabajosa es $2) \Rightarrow 1)$.

Primero, usando la propiedad a) se puede ver que en R todo elemento no nulo y no invertible $\alpha \in R$ es divisible por algún elemento irreducible. A saber, si el mismo α no es irreducible, entonces podemos escribir $\alpha = \alpha_1\beta$, donde $\alpha_1 \notin R^\times$ y $\alpha_1 \not\sim \alpha$. Si α_1 tampoco es irreducible, podemos repetir el proceso. La condición a) implica que en algún momento se encuentra un factor irreducible de α.

Ahora aplicando la existencia de factor irreducible y la condición a), se puede obtener una expresión

$$\alpha = \pi_1 \cdots \pi_s,$$

donde $\pi_1, \ldots, \pi_s \in R$ son irreducibles. (Dejo todos los detalles como un ejercicio.)

Esto establece la existencia de factorizaciones, falta probar su unicidad. Consideremos entonces dos expresiones

$$\pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t$$

Sin pérdida de generalidad, asumamos que $s \leq t$ y procedamos por inducción sobre s. Dado que π_s es primo, después de una renumeración de los ρ_j, podemos asumir que $\pi_s \mid \rho_t$. Pero ρ_t es irreducible, así que $\pi_s \sim \rho_t$. Los podemos cancelar y obtener un número menor de factores irreducibles. Esto nos da el paso inductivo. ■

Para terminar nuestra breve discusión de dominios de factorización única, recordemos la noción de valuación.

1.5.7. Definición. Si R es un dominio de factorización única, para un primo fijo $\pi \in R$ y $\alpha \in R$ la **valuación π-ádica** viene dada por

$$v_\pi(\alpha) = \text{máx}\{n \mid \pi^n \mid \alpha\}.$$

Además, pongamos $v_\pi(0) = \infty$.

La factorización única en R significa que para todo $\alpha \neq 0$ se cumple

$$\alpha \sim \prod_\pi \pi^{v_\pi(\alpha)},$$

donde el producto es sobre las clases de equivalencia de los elementos primos módulo la relación $\sim$. Es fácil comprobar las siguientes propiedades básicas:

v1) $v_\pi(\alpha) = \infty$ si y solamente si $\alpha = 0$.

v2) $v_\pi(\alpha\beta) = v_\pi(\alpha) + v_\pi(\beta)$.

v3) $v_\pi(\alpha + \beta) \geq \text{mín}\{v_\pi(\alpha), v_\pi(\beta)\}$.

A partir de la definición, o tratando a v1), v2), v3) como axiomas, podemos también deducir que

a) $v_\pi(u) = 0$ para todo $u \in R^\times$. En particular, $v_\pi(u\alpha) = v_\pi(\alpha)$ y $v_\pi(-\alpha) = v_\pi(\alpha)$.

b) Si $v_\pi(\alpha) \neq v_\pi(\beta)$, entonces $v_\pi(\alpha + \beta) = \text{mín}\{v_\pi(\alpha), v_\pi(\beta)\}$.

1.5.2 Dominios de ideales principales

1.5.8. Proposición. *Supongamos que R es un dominio de ideales principales. Es decir, para cualquier ideal $I \subseteq R$ existe $\alpha \in R$ tal que $I = (\alpha)$. Entonces, R es un dominio de factorización única.*

Demostración. Necesitamos verificar las condiciones a) y b).

Primero, para una cadena de ideales

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq R$$

por nuestra hipótesis existe $x \in R$ que genera el ideal $I = \bigcup_{n \geq 1} I_n$. Pero $x \in I_n$ para algún n, y luego $I_n = I_{n+1} = \cdots = I$.

Para verificar la condición b), sea $\pi \in R$ un elemento irreducible. Asumamos que para algunos $\alpha, \beta \in R$ se tiene $\pi \mid \alpha\beta$. Hay que probar que $\pi \mid a$ o $\pi \mid \beta$. Consideremos el ideal generado por π y α:

$$(\pi, \alpha) = \{x\pi + y\alpha \mid x, y \in R\}.$$

Por nuestra hipótesis, se tiene $(\pi, \alpha) = (\gamma)$ para algún $\gamma \in R$. En particular, $\gamma \mid \pi$ y $\gamma \mid \alpha$. Ahora dado que π es irreducible, hay dos posibilidades:

1) $\gamma \sim \pi$, y en este caso $\pi \mid \alpha$;

2) $\gamma \in R^\times$, y en este caso se puede ver que $\pi \mid \beta$. ■

1.5.3 Dominios euclidianos

Ahora bien, ¿cómo probar que algo es un dominio de ideales principales? En algunos casos particulares sirve verificar que R admite la división con resto en cierto sentido.

1.5.9. Definición. Se dice que R es un **dominio euclidiano** si sobre R existe una función $\delta\colon R\setminus\{0\}\to\mathbb{N}$ que satisface la siguiente propiedad. Para cualesquiera $\alpha,\beta\in R$, $\beta\neq 0$ existen $q,r\in R$ tales que $\alpha=q\beta+r$, donde $r=0$ o $\delta(r)<\delta(\beta)$.

1.5.10. Ejemplo. La división con resto habitual nos dice que el anillo de los enteros $\mathbb{Z}$ es euclidiano respecto al valor absoluto $\delta(a)=|a|$. Este ejemplo fue explorado por Euclides en sus «Elementos», y de allí viene el término «anillo euclidiano».

Si k es un campo, entonces el anillo de polinomios $k[x]$ es euclidiano respecto al grado $\delta(f)=\deg f$. Esto establece la división con resto de polinomios. ▲

La razón de ser de la noción de dominio euclidiano es el siguiente resultado.

1.5.11. Teorema. *Todo dominio euclidiano es un dominio de ideales principales, y en particular de factorización única.*

Demostración. Sea R un dominio euclidiano y sea $I\subseteq R$ un ideal. Si $I=(0)$, entonces es trivialmente principal. Si $I\neq(0)$, sea $\beta\in I$ un elemento no nulo con la mínima posible norma euclidiana $\delta(\beta)$ (es decir, si $r\in I$ y $\delta(r)<\delta(\beta)$, entonces $r=0$). Por la elección de β, cualquier otro elemento $\alpha\in I$ se divide sin resto por β, y entonces $\alpha\in(\beta)$. ■

Para resumir, hemos establecido las implicaciones

$$\text{dominio euclidiano}\implies\text{dominio de ideales principales}\implies\text{dominio de factorización única}.$$

En general, un dominio de factorización única no tiene por qué ser un dominio de ideales principales, y de la misma manera, un dominio de ideales principales no tiene por qué ser euclidiano. Véanse los ejercicios para más detalles.

1.6 Enteros de Gauss $\mathbb{Z}[i]$

Consideremos el anillo de los **enteros de Gauss** $\mathbb{Z}[i]\subset\mathbb{Q}(i)$. La conjugación compleja

$$\sigma\colon \alpha=a+bi\mapsto\overline{\alpha}=a-bi$$

es un automorfismo no trivial de $\mathbb{Q}(i)$. Ahora para $\alpha=a+bi\in\mathbb{Q}(i)$ definamos

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

La aplicación $N\colon\mathbb{Q}(i)\to\mathbb{Q}$ se llama la **norma**. Se ve que es multiplicativa:

$$N(\alpha\beta)=N(\alpha)\,N(\beta).$$

Además, notamos que la norma se restringe a $\mathbb{Z}[i]$ e induce una aplicación $N\colon\mathbb{Z}[i]\mapsto\mathbb{N}$.

1.6.1. Comentario. Recordemos que en general la **norma** y **traza** de una extensión finita de campos L/K se definen mediante el álgebra lineal: si

$$\mu_\alpha\colon L\to L,\quad x\mapsto\alpha x$$

es la application K-lineal de multiplicación por $\alpha\in L$, entonces

$$N_{L/K}(\alpha)=\det\mu_\alpha,\quad T_{L/K}(\alpha)=\operatorname{tr}\mu_\alpha.$$

Ahora, *si L/K es una extensión de Galois*, entonces

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha), \quad T_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Más adelante en el curso vamos a definir otros tipos de normas y trazas, pero por el momento estos términos van a significar lo que conocemos de la teoría de campos básica.

Vamos a ver al instante que la norma ayuda a relacionar la aritmética en $\mathbb{Z}[i]$ con la aritmética de números enteros.

1.6.2. Lema. *1) Se tiene*

$$\mathbb{Z}[i]^\times = \{\alpha \mid N(\alpha) = 1\} = \{\pm 1, \pm i\} = \mu_4(\mathbb{C}) = \{\textit{las raíces cuartas de la unidad}\}.$$

2) Si para $\pi \in \mathbb{Z}[i]$ la norma $N(\pi) = p$ es un número primo, entonces π es irreducible.

3) En general, si para $\pi \in \mathbb{Z}[i]$ la norma $n = N(\pi)$ es un número compuesto, pero en $\mathbb{Z}[i]$ no hay elementos de norma $d \mid n$ para $d \neq 1, n$, entonces π es irreducible.

Demostración. Si u es invertible, entonces $u\,u^{-1} = 1$ nos da $N(u)\,N(u^{-1}) = 1$, y luego $N(u) = 1$. Viceversa, si $N(u) = 1$, entonces $\sigma(u) = u^{-1}$. Como consecuencia, para encontrar las unidades, hay que resolver en números enteros la ecuación

$$N(x + yi) = x^2 + y^2 = 1.$$

Las únicas soluciones son $(\pm 1, 0)$ y $(0, \pm 1)$, de donde se obtiene 1).

Ahora supongamos que $N(\pi) = p$ es primo. Si $\pi = \alpha\beta$, entonces $p = N(\pi) = N(\alpha)\,N(\beta)$. Tenemos $N(\alpha) = 1$ y luego $\pi \sim \beta$ o $N(\beta) = 1$ y luego $\pi \sim \alpha$. Esto establece la parte 2), y la parte 3) se demuestra de manera análoga. ■

1.6.3. Lema. *$\mathbb{Z}[i]$ es un dominio euclidiano respecto a la norma $N(a+bi) = a^2+b^2$. En particular, es un dominio de ideales principales y dominio de factorización única.*

Demostración. Dados dos elementos $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, podemos dividir α por β en el campo $\mathbb{Q}(i)$:

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

Se ve que existen $a, b \in \mathbb{Z}$ tales que

$$N((x-a) + (y-b)\,i) = (x-a)^2 + (y-b)^2 < 1.$$

Pongamos

$$q = a + bi \in \mathbb{Z}[i]$$

y

$$r = \alpha - q\beta = \beta\,(x - a + (y-b)\,i).$$

Por la multiplicatividad de la norma,

$$N(r) = N(\beta)\,N(x - a + (y-b)\,i) < N(\beta).$$ ■

Ahora sabiendo que $\mathbb{Z}[i]$ es un dominio de factorización única, ¿cómo se ven los elementos primos (= irreducibles) en este caso? Supongamos que $\pi \in \mathbb{Z}[i]$ es primo. Luego,

$$\pi\,\overline{\pi} = N(\pi) = p_1 \cdots p_s,$$

donde los p_i son los factores primos del número natural $N(\pi)$. Entonces, $\pi \mid p_i$. Todo esto significa que los primos da Gauss $\pi \in \mathbb{Z}[i]$ surgen como factores de los primos $p \in \mathbb{Z}$.

Para evitar cualquier confusión, a partir de ahora vamos a decir que $p \in \mathbb{Z}$ son los **primos racionales**. Al pasar a un anillo más grande como $\mathbb{Z}[i]$, muy a menudo estos dejan de ser primos.

1.6.4. Proposición. *Sea $p \in \mathbb{Z}$ un primo racional.*

1) Si $p = 2$, entonces $2 = -i\,(1+i)^2$, donde $1+i$ es primo en $\mathbb{Z}[i]$.

2) Si $p \equiv 3 \pmod 4$, entonces p es primo en $\mathbb{Z}[i]$.

3) Si $p \equiv 1 \pmod 4$, entonces $p = \pi\,\overline{\pi}$ en $\mathbb{Z}[i]$, donde π y $\overline{\pi}$ son primos no asociados en $\mathbb{Z}[i]$.

Además, todos los primos $\pi \in \mathbb{Z}[i]$ surgen de esta manera (salvo la relación $\sim$).

Se dice que 2 **se ramifica** porque es asociado con una potencia del primo $1+i \in \mathbb{Z}[i]$. Los primos racionales $p \equiv 1 \pmod 4$ **se escinden**, mientras que los primos $p \equiv 3 \pmod 4$ son **inertes**, ya que no dejan de ser primos en $\mathbb{Z}[i]$.

Según el **teorema de Dirichlet sobre primos en progresiones aritméticas** (véase el apéndice D), en cierto sentido técnico, la mitad de los primos racionales cumplen $p \equiv 1 \pmod 4$ y la otra mitad satisface $p \equiv 3 \pmod 4$. El primo 2 es excepcional.

Demostración. Primero notamos que $N(1+i) = 2$, así que $1+i$ debe ser irreducible (= primo).

Si $p \equiv 3 \pmod 4$, notamos que $a^2 + b^2 \not\equiv 3 \pmod 4$, así que en $\mathbb{Z}[i]$ no hay elementos de norma p. Dado que $N(p) = p^2$, esto implica que p es irreducible, y por lo tanto primo.

En fin, si $p \equiv 1 \pmod 4$, entonces $\left(\frac{-1}{p}\right) = +1$ (véase 1.4.5), lo que significa que existe un entero a tal que $a^2 \equiv -1 \pmod p$. Ahora $p \mid (a^2+1) = (a+i)\,(a-i)$. Dado que $p \nmid (a \pm i)$, esto implica que p no es primo en $\mathbb{Z}[i]$. Entonces, $p = \pi\rho$ para algunos elementos no-invertibles π y ρ. Ahora $p^2 = N(\pi)\,N(\rho)$ implica que $N(\pi) = \pi\,\overline{\pi} = p$. Por el lema de arriba π es primo, y es fácil ver que π y $\overline{\pi}$ no son asociados. ■

Nuestra descripción de los primos en $\mathbb{Z}[i]$ contiene el siguiente famoso resultado.

1.6.5. Proposición (Fermat). *Un primo impar p es una suma de dos cuadrados si y solamente si $p \equiv 1 \pmod 4$. Además, si $p = x^2 + y^2$, entonces x e y están bien definidos salvo permutación y signo ± 1.*

Demostración. Si $p = x^2 + y^2$, entonces $p \equiv 1 \pmod 4$, dado que los cuadrados módulo 4 son 0 y 1.

Viceversa, asumamos que $p \equiv 1 \pmod 4$. En este caso, como hemos visto, $p = \pi\overline{\pi}$ para algún primo $\pi = x + iy \in \mathbb{Z}[i]$ que satisface $N(\pi) = x^2 + y^2 = p$.

Ahora si $p \equiv 1 \pmod 4$, consideremos dos representaciones

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

Supongamos que $x, y, x', y' > 0$. Notamos que x e y deben tener diferente paridad; sin pérdida de generalidad, podemos asumir que

$$x, x' \equiv 1, \quad y, y' \equiv 0 \pmod 2.$$

Se obtiene

$$\pi\,\overline{\pi} = \pi'\,\overline{\pi'},$$

donde $\pi = x + iy$, $\pi' = x' + iy'$ son primos. Se sigue que $\pi = u\pi'$ o $\pi = u\overline{\pi'}$ para algún $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Dejo al lector analizar diferentes casos y concluir que necesariamente $a = a'$ y $b = b'$. ■

Para la generalización de este resultado a $n = x^2 + y^2$ para n compuesto, véase 6.1.1.

1.6.6. Ejemplo. Los primeros primos $p \equiv 1 \pmod 4$ son

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

▲

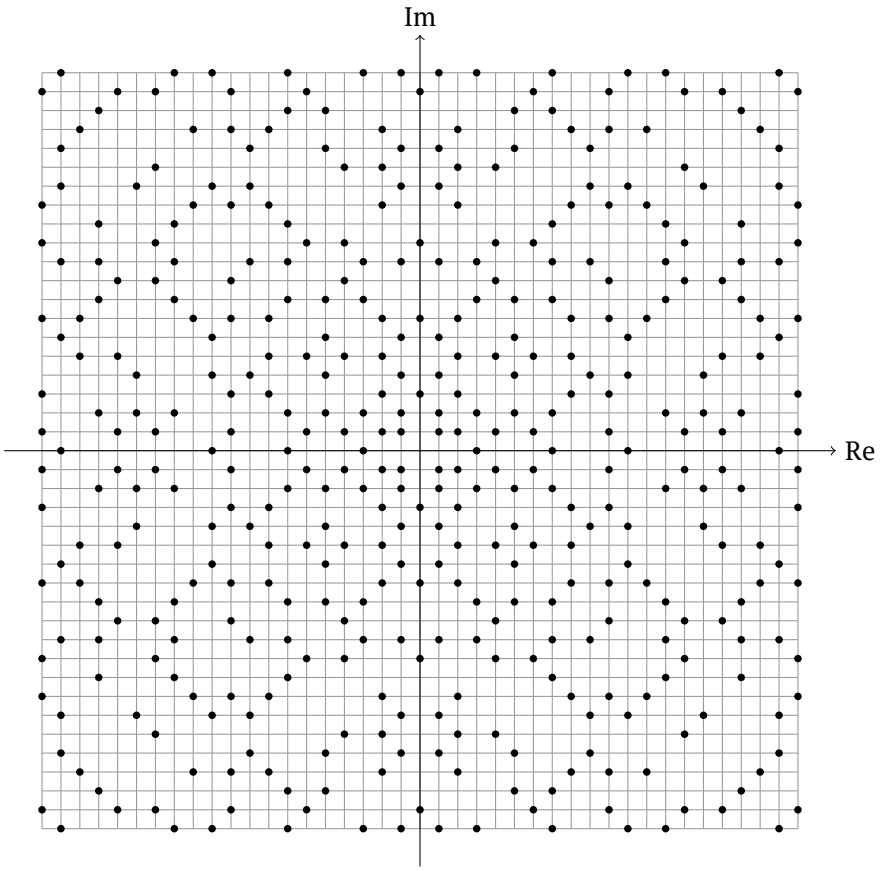


Figura 1.1: Los primos de Gauss $\pi \in \mathbb{Z}[i]$ en el plano complejo

Recordemos el siguiente resultado.

1.6.7. Proposición. *Si R es un dominio de ideales principales y $\pi \in R$ es un elemento primo, entonces $R/(\pi)$ es un campo.*

(De hecho, ya lo hemos usado de manera implícita cuando decíamos que $k[x]/(f)$ es un campo para un polinomio irreducible $f \in k[x]$.)

Demostración. El siguiente argumento es idéntico a la prueba de que $\mathbb{Z}/(p)$ es un campo para todo primo p.

Un elemento no nulo en $R/(\pi)$ será representado por $\alpha \in R$ tal que $\pi \nmid \alpha$. El ideal (π, α) es generado por algún $\gamma \in R$, ya que estamos en un dominio de ideales principales. Pero $\gamma \mid \pi$ y $\gamma \mid \alpha$ implica que $\gamma \in R^\times$, así que $(\pi, \alpha) = R$, y existen elementos $\beta, \alpha' \in R$ tales que

$$\pi\beta + \alpha\alpha' = 1.$$

Esto significa que α' es el inverso de α módulo π. ■

Volviendo al anillo $\mathbb{Z}[i]$, tenemos lo siguiente.

1.6.8. Proposición. *Para cualquier primo de Gauss $\pi \in \mathbb{Z}[i]$ el cociente $\mathbb{Z}[i]/(\pi)$ es un campo finito de $N(\pi)$ elementos:*

1) $\mathbb{Z}[i]/(1+i) \cong \mathbb{F}_2$*;*

2) si $p \equiv 3 \pmod 4$*, entonces* $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$*;*

3) si $p \equiv 1 \pmod 4$ *y* $p = \pi\overline{\pi}$*, entonces* $\mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p$*.*

Los campos finitos $\mathbb{Z}[i]/(\pi)$ se llaman los **campos residuales**.

Demostración. Para $\pi = 1 + i$ basta notar que

$$2 \equiv 0, \quad i \equiv 1 \pmod{1+i},$$

de donde se ve que cualquier entero de Gauss $a + bi$ es congruente a 0 o 1 módulo $1 + i$.

Luego, notamos que el ideal generado por un primo racional p viene dado como un $\mathbb{Z}$-submódulo por

$$(p) = p\mathbb{Z} \oplus pi\mathbb{Z} \subset \mathbb{Z} \oplus i\mathbb{Z}.$$

De aquí se ve que $\mathbb{Z}[i]/(p) \cong \mathbb{Z}/(p) \oplus i\mathbb{Z}/(p)$ como $\mathbb{Z}$-módulo, así que $\mathbb{Z}[i]/(p)$ tiene p^2 elementos. Si $p \equiv 3 \pmod 4$, entonces $\mathbb{Z}[i]/(p)$ es un campo. Por otra parte, si $p \equiv 1 \pmod 4$, el teorema chino del resto* nos da

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$$

(¡usando que π y $\overline{\pi}$ no son asociados!), de donde por el conteo de elementos $\mathbb{Z}[i]/(\pi) \cong \mathbb{F}_p$. ■

1.7 Enteros de Eisenstein $\mathbb{Z}[\zeta_3]$

Ahora consideremos el anillo de los **enteros de Eisenstein** $\mathbb{Z}[\zeta_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}(\zeta_3)$. El automorfismo no trivial de $\mathbb{Q}(\zeta_3)$ viene dado por

$$\sigma\colon a + b\zeta_3 \mapsto a + b\zeta_3^2 = (a - b) - b\zeta_3$$

(lo cual es lo mismo que la conjugación compleja). La **norma** de $\alpha = a + b\zeta_3$ se define como

$$N(\alpha) = \alpha\,\sigma(\alpha) = a^2 - ab + b^2.$$

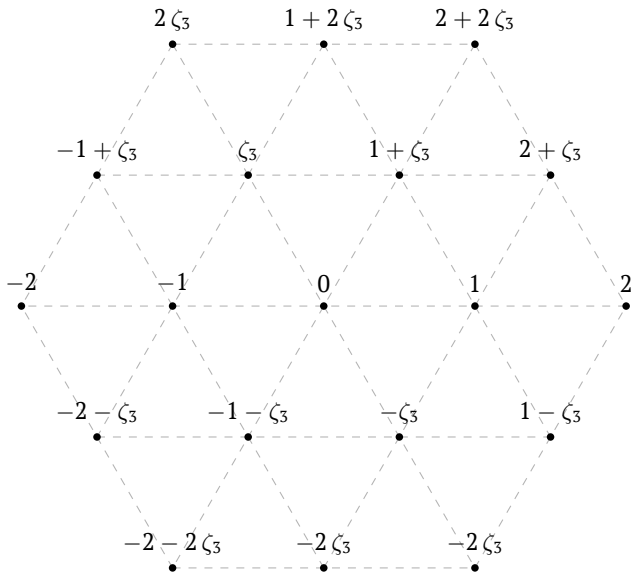


Figura 1.2: Los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$ en el plano complejo

La norma se restringe a $N\colon \mathbb{Z}[\zeta_3] \to \mathbb{N}$.

El siguiente lema se demuestra de manera parecida a lo que hicimos con $\mathbb{Z}[i]$ y se deja como un ejercicio.

1.7.1. Lema. *1) Se tiene*

$$\mathbb{Z}[\zeta_3]^\times = \{\alpha \mid N(\alpha) = 1\} = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} = \mu_6(\mathbb{C}) = \{\textit{las raíces sextas de la unidad}\}.$$

2) Si para $\pi \in \mathbb{Z}[\zeta_3]$ la norma $N(\pi) = p$ es un número primo, entonces π es irreducible.

En general, si para $\pi \in \mathbb{Z}[\zeta_3]$ la norma $n = N(\pi)$ es un número compuesto, pero en $\mathbb{Z}[\zeta_3]$ no hay elementos de norma $d \mid n$ para $d \neq 1, n$, entonces π es irreducible.

3) $\mathbb{Z}[\zeta_3]$ es un dominio euclidiano respecto a la norma $N(a+b\zeta_3) = a^2 - ab + b^2$. En particular, es un dominio de ideales principales y dominio de factorización única.

De nuevo, todos los primos de Eisenstein $\pi \in \mathbb{Z}[\zeta_3]$ aparecen en factorizaciones de los primos racionales $p \in \mathbb{Z}$.

1.7.2. Proposición. *Sea $p \in \mathbb{Z}$ un primo racional.*

1) Si $p = 3$, entonces $3 = -\zeta_3^2\,(1-\zeta_3)^2$, donde $1-\zeta_3$ es primo en $\mathbb{Z}[\zeta_3]$ y $\mathbb{Z}[\zeta_3]/(1-\zeta_3) \cong \mathbb{F}_3$.

2) Si $p \equiv 2 \pmod 3$, entonces p es primo en $\mathbb{Z}[\zeta_3]$ y $\mathbb{Z}[\zeta_3]/(p) \cong \mathbb{F}_{p^2}$.

3) Si $p \equiv 1 \pmod 3$, entonces $p = \pi\overline{\pi}$ en $\mathbb{Z}[\zeta_3]$, donde π y $\overline{\pi}$ son primos no asociados en $\mathbb{Z}[\zeta_3]$ y $\mathbb{Z}[\zeta_3]/(\pi) \cong \mathbb{F}_p$.

Además, todos los primos $\pi \in \mathbb{Z}[\zeta_3]$ surgen de esta manera (salvo la relación $\sim$).

[*] En cualquier dominio de ideales principales el teorema chino del resto puede ser probado de la misma manera que para $\mathbb{Z}$; más adelante vamos a recordar la versión general válida para cualquier anillo conmutativo.

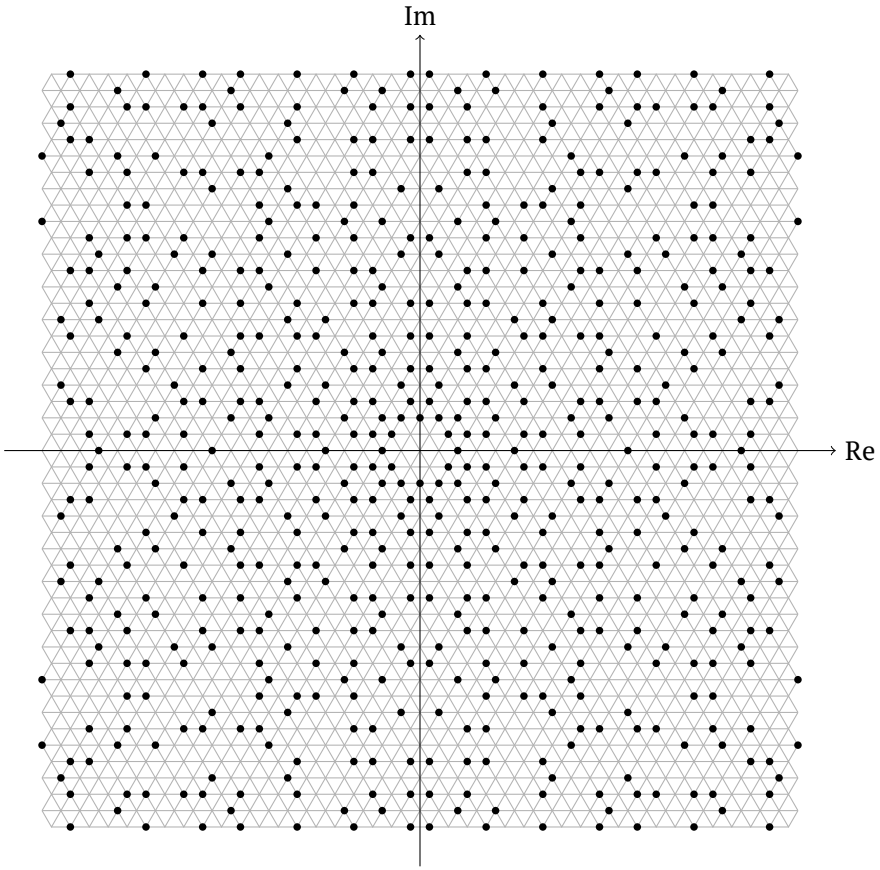


Figura 1.3: Los primos de Eisenstein $\pi \in \mathbb{Z}[\zeta_3]$ en el plano complejo

Demostración. Todo esto es muy parecido a lo que vimos para $\mathbb{Z}[i]$ en la sección anterior, así que dejaré los detalles al lector.

En 1), note que $N(1-\zeta_3) = 3$. Luego la observación clave en 2) es la siguiente: si $p \equiv 2 \pmod 3$, entonces $a^2 - ab + b^2 \not\equiv 2 \pmod 3$ y en $\mathbb{Z}[\zeta_3]$ no hay elementos de norma p.

En fin en 3), si $p \equiv 1 \pmod 3$, calculamos usando la reciprocidad cuadrática que $\left(\frac{-3}{p}\right) = +1$ (véase 1.4.3). Esto significa que existe un entero a tal que $a^2 \equiv -3 \pmod p$, y luego se tiene

$$p \mid (a^2+3) = (a+\sqrt{-3})\,(a-\sqrt{-3}) = (a+1+2\zeta_3)\,(a-1-2\zeta_3),$$

donde $p \nmid (a \pm (1+2\zeta_3))$, así que p no es primo. El resto del argumento es idéntico al caso de los enteros de Gauss $\mathbb{Z}[i]$. ■

Nuestra descripción de los primos en $\mathbb{Z}[\zeta_3]$ contiene el siguiente curioso resultado.

1.7.3. Proposición. *Si $p \equiv 1 \pmod 3$, entonces $4p = u^2 + 27v^2$ para algunos $u, v \in \mathbb{Z}$. Además, u y v están bien definidos salvo el signo.*

(Considerando $u^2 + 27v^2$ módulo 3, notamos que $p \equiv 1 \pmod 3$ es también una condición necesaria.)

Demostración. Como hemos visto, $p \equiv 1 \pmod 3$ implica que $p = \pi\overline{\pi}$ para algún primo $\pi = a + b\zeta_3$. Dejo como un ejercicio ver que precisamente para uno de los primos asociados con π se cumple

$$a \equiv 2, \quad b \equiv 0 \pmod 3.$$

Luego,

$$p = N(\pi) = a^2 - ab + b^2$$

y

$$4p = (2a - b)^2 + 3b^2.$$

Podemos entonces tomar $u = 2a - b$ y $v = b/3$. La unicidad de expresiones $4p = u^2 + 27v^2$ se deja como un ejercicio (use la factorización única en $\mathbb{Z}[\zeta_3]$). ■

1.7.4. Ejemplo. Tenemos

$$\begin{aligned} 4 \cdot 7 &= 1^2 + 27 \cdot 1^2, \\ 4 \cdot 13 &= 5^2 + 27 \cdot 1^2, \\ 4 \cdot 19 &= 7^2 + 27 \cdot 1^2, \\ 4 \cdot 31 &= 4^2 + 27 \cdot 2^2, \\ &\dots \end{aligned}$$

▲

1.8 Reciprocidad cúbica

Los anillos de números sirven para establecer varias leyes de reciprocidad parecidas a la reciprocidad cuadrática que revisamos en §1.4. Como un ejemplo particular, en la presente sección me gustaría presentar la ley de reciprocidad cúbica que se formula en términos de los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$.

1.8.1. Lema. *Sea $\pi \in \mathbb{Z}[\zeta_3]$ un primo de Eisenstein tal que $\pi \not\sim (1 - \zeta_3)$. Luego, para cualquier $\alpha \in \mathbb{Z}[\zeta_3]$ tal que $\pi \nmid \alpha$ se tiene*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv 1, \zeta_3, \zeta_3^2 \pmod{\pi},$$

donde $1, \zeta_3, \zeta_3^2$ no son congruentes módulo π.

Demostración. Primero notamos que se cumple $3 \mid (N(\pi) - 1)$. En efecto, hay dos casos posibles: $N(\pi) = p$, donde $p \equiv 1 \pmod 3$, o $N(\pi) = p^2$, donde $p \equiv 2 \pmod 3$. Ahora $\mathbb{Z}[\zeta_3]/(\pi)$ es un campo de $N(\pi)$ elementos, y por ende

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

Esto significa que $\alpha^{\frac{N(\pi)-1}{3}}$ es una raíz cúbica de la unidad en $\mathbb{Z}[\zeta_3]/(\pi)$, así que es congruente a $1, \zeta_3, \zeta_3^2$; dejo al lector comprobar que estos elementos no nos congruentes entre sí cuando $\pi \not\sim (1 - \zeta_3)$. ■

El lema que acabamos de establecer justifica la siguiente definición.

1.8.2. Definición. Para un primo de Eisenstein $\pi \in \mathbb{Z}[\zeta_3]$ tal que $\pi \not\sim (1 - \zeta_3)$ y $\alpha \in \mathbb{Z}[\zeta_3]$ tal que $\pi \nmid \alpha$ el **símbolo cúbico de Legendre** correspondiente $\left(\frac{\alpha}{\pi}\right)_3$ es la única raíz cúbica de la unidad tal que

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}.$$

Es fácil ver que

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$$

y

$$\alpha \equiv \beta \pmod{\pi} \Longrightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3.$$

Entonces, el símbolo cúbico de Legendre es un homomorfismo

$$\left(\frac{\cdot}{\pi}\right)_3 : (\mathbb{Z}[\zeta_3]/(\pi))^\times \to \mu_3(\mathbb{C}) = \{1, \zeta_3, \zeta_3^2\}.$$

1.8.3. Lema. *Se tiene* $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *si y solamente si la congruencia* $x^3 \equiv \alpha \pmod{\pi}$ *tiene solución en* $\mathbb{Z}[\zeta_3]$.

Demostración. Ejercicio para el lector. Use que el grupo $(\mathbb{Z}[\zeta_3]/(\pi))^\times$ es cíclico (como el grupo multiplicativo de cualquier campo finito; véase A.12.3). ■

Antes de formular la ley de reciprocidad para estos símbolos de Legendre, nos sirve una definición técnica.

1.8.4. Definición. Digamos que un primo de Eisenstein $\pi \in \mathbb{Z}[\zeta_3]$ es **primario** si $\pi \equiv 2 \pmod{3}$.

Esto tiene el siguiente significado: todo primo π viene con sus seis asociados $\zeta_6^n \pi$ para $n = 0, 1, \ldots, 5$. Resulta que si π es un primo tal que $N(\pi) = p \equiv 1 \pmod{3}$, entonces entre sus asociados precisamente uno es primario.

1.8.5. Teorema (Reciprocidad cúbica). *Sean* π_1 *y* π_2 *dos primos primarios tales que* $N(\pi_1) \neq N(\pi_2)$. *Entonces,*

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

Demostración. Para una prueba con sumas de Gauss (parecidas a las de §1.4) véase por ejemplo [IR1990, Chapter 9]. El argumento no es muy difícil, pero involucra varios cálculos y nos llevaría un poco lejos del tema principal del curso. ■

(También existe una ley suplementaria que calcula el símbolo $\left(\frac{1-\zeta_3}{\pi}\right)_3$, pero no la vamos a ocupar; véase por ejemplo [Wil1977].)

Como una aplicación de la reciprocidad cúbica, vamos a probar el siguiente resultado que fue conjeturado por Euler [E792, §407–408].

1.8.6. Teorema. *Un primo* p *tiene forma* $x^2 + 27y^2$ *si y solamente si* $p \equiv 1 \pmod{3}$ *y* 2 *es un cubo módulo* p *(es decir,* $x^3 \equiv 2 \pmod{p}$ *para algún* $x \in \mathbb{Z}$*).*

Por otra parte, notamos que 2 es un cubo módulo cualquier $p \equiv 2 \pmod{3}$. En efecto, si $p \equiv 2 \pmod{3}$, entonces $x \mapsto x^3$ define un automorfismo del grupo cíclico $\mathbb{F}_p^\times$, así que ¡todo resto módulo p es un cubo!

La observación clave es la siguiente.

1.8.7. Lema. *Para un primo primario* $\pi \in \mathbb{Z}[\zeta_3]$ *con* $N(\pi) = p \equiv 1 \pmod{3}$ *la congruencia* $x^3 \equiv 2 \pmod{\pi}$ *tiene solución en* $\mathbb{Z}[\zeta_3]$ *si y solamente si* $\pi \equiv 1 \pmod{2}$.

Demostración. Usando la reciprocidad cúbica,

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3 \equiv \pi^{\frac{N(\pi)-1}{3}} = \pi \pmod{2}.$$

Se sigue que la congruencia $x^3 \equiv 2 \pmod{\pi}$ tiene solución si y solamente si $\pi \equiv 1 \pmod{2}$. ■

Demostración del teorema. Ahora bien, supongamos que $p \equiv 1 \pmod{3}$ y 2 es un cubo módulo p. Esto significa que $x^3 \equiv 2 \pmod{p}$, y luego $x^3 \equiv 2 \pmod{\pi}$ tiene solución, donde $\pi \mid p$, y podemos asumir que π es primario. Por el lema de arriba, esto implica que $\pi \equiv 1 \pmod{2}$. Escribamos $\pi = a + b\zeta_3$. Las condiciones $\pi \equiv 1 \pmod{2}$ y $\pi \equiv 2 \pmod{3}$ se traducen en

$$\begin{aligned} a \equiv 1,\ b \equiv 0 \pmod{2}, \\ a \equiv 2,\ b \equiv 0 \pmod{3}. \end{aligned}$$

Ahora

$$N(\pi) = p = a^2 - ab + b^2,$$

y luego

$$4p = (2a - b)^2 + 3b^2.$$

Poniendo $x = \frac{2a-b}{2}$ e $y = \frac{b}{6}$, se obtiene

$$p = x^2 + 27y^2.$$

Viceversa, supongamos que $p = x^2 + 27y^2$. Esto claramente implica que $p \equiv 1 \pmod 3$. Además, cambiando el signo de x, podemos asegurarnos que $x \equiv 2 \pmod 3$. Tenemos

$$p = \pi\overline{\pi}, \text{donde } \pi = x + 3\sqrt{-3}y = x + 3y + 6y\zeta_3.$$

Tenemos $N(\pi) = N(\overline{\pi}) = p$ y $\pi \equiv 2 \pmod 3$, así que π es un primo primario. Notamos que $\pi \equiv x + y \pmod 2$, y x e y necesariamente tienen diferente paridad (puesto que $p = x^2 + 27y^2$), así que $\pi \equiv 1 \pmod 2$. Esto implica que la congruencia $x^3 \equiv 2 \pmod \pi$ tiene solución en $\mathbb{Z}[\zeta_3]$, pero $\mathbb{Z}[\zeta_3]/(\pi) \cong \mathbb{F}_p$, y entonces $x^3 \equiv 2 \pmod p$ tiene solución en $\mathbb{Z}$. ■

1.8.8. Ejemplo. Los primeros primos de la forma $x^2 + 27y^2$ son

$$\begin{aligned}
31 &= 2^2 + 27 \cdot 1^2, && (2 \equiv 4^3 \pmod{31}) \\
43 &= 4^2 + 27 \cdot 1^2, && (2 \equiv 20^3 \pmod{43}) \\
109 &= 1^2 + 27 \cdot 2^2, && (2 \equiv 57^3 \pmod{109}) \\
127 &= 10^2 + 27 \cdot 1^2, && (2 \equiv 32^3 \pmod{127}) \\
157 &= 7^2 + 27 \cdot 2^2. && (2 \equiv 62^3 \pmod{157})
\end{aligned}$$

▲

Para entender mejor el argumento de arriba, podemos reemplazar 2 por otro primo $p \equiv 2 \pmod 3$, por ejemplo 5.

1.8.9. Ejemplo. Investiguemos para cuáles primos de Eisenstein π la congruencia

$$x^3 \equiv 5 \pmod \pi$$

tiene solución. Notamos que si $\pi' \sim \pi$, entonces la respuesta no cambia al remplazar π por π', así que se puede asumir que π es primario. En este caso la reciprocidad cúbica nos da

$$\left(\frac{5}{\pi}\right)_3 = \left(\frac{\pi}{5}\right)_3.$$

El campo $\mathbb{Z}[\zeta_3]/(5) \cong \mathbb{F}_{25}$ tiene $\frac{25-1}{3} = 8$ cubos no nulos, y se puede ver que estos se representan por

$$1,\ 2,\ 3,\ 4,\ 1 + 2\zeta_3,\ 2 + 4\zeta_3,\ 3 + \zeta_3,\ 4 + 3\zeta_3.$$

```
? eisenstein_cubes_mod (p) = {
  local (cubes = List ([]));

  for (a=0,p-1,
    for (b=0,p-1,
      listput (cubes, Mod(Mod(a,p) + Mod(b,p)*x, polcyclo(3))^3)
    )
  );

  Set (cubes)
};

? liftall (eisenstein_cubes_mod(5))
% = [0, 1, 2, 3, 4, 2*x + 1, 4*x + 2, x + 3, 3*x + 4]
```

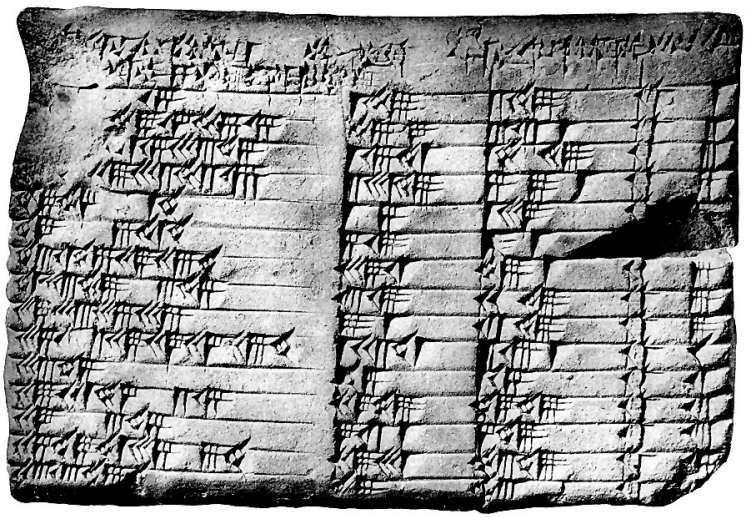


Figura 1.4: La tablilla babilónica Plimpton 322 (cerca de 1800 a. C.) que enumera algunas ternas pitagóricas. Véase [Wei2006, §I.V]

Entonces, para que 5 sea un cubo módulo π, el primo π debe ser congruente módulo 5 a uno de los números que acabamos de encontrar. En particular, cualquier primo $p \equiv 2 \pmod 3$ es un primo de Eisenstein y $x^3 \equiv 5 \pmod p$ tiene solución, ya que $1, 2, 3, 4$ son cubos módulo 5. Pero esta conclusión no es muy interesante: si $p \equiv 2 \pmod 3$, entonces cualquier resto módulo p es un cubo.

Por otra parte, para los primos racionales $p \equiv 1 \pmod 3$ la respuesta depende de p. Vamos a ver un par de casos particulares.

Si $p = 7$, entonces $p = \pi\overline{\pi}$, donde $\pi = -1 - 3\zeta_3$ es un primo primario. Su resto módulo 5 es $4 + 2\zeta_3$ y este no se encuentra en nuestra lista, así que la congruencia $x^3 \equiv 5$ no tiene solución módulo π, y por lo tanto módulo 7. De hecho, hay solo dos cubos módulo 7 y estos son claramente ± 1

Ahora si tomamos $p = 13$, entonces $p = \pi\overline{\pi}$, donde $\pi = -4 - 3\zeta_3$ es un primo primario. El resto $\pi \equiv 1 + 2\zeta_3 \pmod 5$ se encuentra en nuestra lista, así que $x^3 \equiv 5 \pmod \pi$ tiene solución. Pero $\mathbb{Z}[\zeta_3]/(\pi) \cong \mathbb{F}_{13}$, lo cual significa que $x^3 \equiv 5 \pmod{13}$ tiene solución en $\mathbb{Z}$. En efecto, $7^3 \equiv 5 \pmod{13}$. ▲

1.8.10. Comentario. El libro [Cox2013] está dedicado a los primos de la forma $p = x^2 + ny^2$. La respuesta involucra un montón de la teoría de números algebraicos (más allá de nuestro curso introductorio).

Clase 4
19/08/20

1.9 Ternas pitagóricas

A parte de las leyes de reciprocidad, otro tema importante en la teoría de números son los problemas **diofánticos** que se tratan de soluciones de ecuaciones polinomiales sobre $\mathbb{Z}$ o $\mathbb{Q}$. A continuación vamos a ver algunos ejemplos particulares; el principio general sugiere que muy a menudo para investigar problemas sobre los números enteros $\mathbb{Z}$, hay que considerar anillos de números más grandes (y otros objetos algebraicos y geométricos más sofisticados).

Las soluciones enteras de la ecuación $x^2 + y^2 = z^2$ se conocen como las **ternas pitagóricas**. Algunos ejemplos de estas son

$$(3, 4, 5),\ (5, 12, 13),\ (7, 24, 25).$$

A continuación vamos a olvidar de los signos y asumir que $x, y, z > 0$.

Las ternas pitagóricas corresponden a los enteros de Gauss cuya norma es un cuadrado: $N(x+yi) = z^2$. Puesto que $N(\alpha^2) = N(\alpha)^2$, podemos generar las ternas pitagóricas tomando cuadrados de los enteros de Gauss. Por ejemplo,

$$(2+i)^2 = 3+4i, \quad (3+2i)^2 = 5+12i, \quad (4+3i)^2 = 7+24i.$$

En general, tenemos $(a+bi)^2 = a^2 - b^2 + 2abi$, así que para cualesquiera $a, b \in \mathbb{Z}$ se obtiene una terna pitagórica

$$(a^2 - b^2,\ 2ab,\ a^2 + b^2). \tag{1.1}$$

Nuestro objetivo es probar que esencialmente todas las ternas pitagóricas surgen de esta manera.

Notamos que si (x, y, z) es una terna pitagórica, entonces (cx, cy, cz) también lo es para cualquier $c \in \mathbb{Z}$. Por este motivo será conveniente considerar solamente las ternas **primitivas** que satisfacen $\mathrm{mcd}(x, y, z) = 1$ (lo que también equivale a $\mathrm{mcd}(x, y) = 1$). Las ternas primitivas corresponden a los puntos *racionales* en el círculo unitario $x^2 + y^2 = 1$, como por ejemplo

$$\left(\frac{3}{5}, \frac{4}{5}\right),\ \left(\frac{5}{13}, \frac{12}{13}\right),\ \left(\frac{7}{25}, \frac{24}{25}\right).$$

Si (x, y, z) es una terna primitiva, se ve que x e y no pueden ser impares al mismo tiempo. Efectivamente, en el caso contrario $x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$, pero los cuadrados módulo 4 son 0 y 1. Entonces, sin pérdida de generalidad (intercambiando x e y si necesario), se puede suponer que x es impar e y es par, de acuerdo con la expresión (1.1).

1.9.1. Teorema. *Sea (x, y, z) una terna pitagórica primitiva, donde x es impar e y es par. Luego, existen enteros coprimos $a > b > 0$ tales que*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Demostración. Consideremos el entero de Gauss $x + yi$. Por nuestra hipótesis,

$$N(x+yi) = (x+yi)\,(x-yi) = z^2.$$

No es difícil ver que si x e y son coprimos y tienen diferente paridad, entonces $\mathrm{mcd}(x+yi,\ x-yi) = 1$ (ejercicio). Usando esto y el hecho de que su producto es un cuadrado, *gracias a la factorización única en $\mathbb{Z}[i]$* podemos concluir que $x \pm yi$ son también cuadrados; existen $\alpha = a + bi \in \mathbb{Z}[i]$ y $u \in \mathbb{Z}[i]^\times$ tales que

$$x + yi = u\alpha^2 = u\,(a^2 - b^2 + 2abi).$$

Dado que $-1 = i^2$, podemos asumir que $u \in \{+1, +i\}$. Nuestra hipótesis de que x es impar e y es par implica que $u = +1$. Además, $x, y > 0$, así que $a > b > 0$. En fin, $\mathrm{mcd}(x, y) = 1$ implica que $\mathrm{mcd}(a, b) = 1$. ■

Nuestra demostración usa de manera esencial la factorización única en $\mathbb{Z}[i]$. A saber, usamos que si $\alpha\beta = \gamma^2$ para $\mathrm{mcd}(\alpha, \beta) = 1$, entonces $\alpha \sim \alpha'^2$ y $\beta \sim \beta'^2$ para algunos α', β'. Sin factorización única no se puede llegar a esta conclusión.

1.9.2. Ejemplo. Consideremos el anillo $\mathbb{Z}[\sqrt{-5}]$. En este caso las unidades son $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Los números

$$\alpha = 2 + 3\sqrt{-5}, \quad \overline{\alpha} = 2 - 3\sqrt{-5}$$

tienen norma

$$N(\alpha) = \alpha\overline{\alpha} = 7^2.$$

Dado que $a^2 + 5b^2 \neq 7$ para ningún $a, b \in \mathbb{Z}$, se ve que α y $\overline{\alpha}$ son irreducibles, no asociados entre sí. Su producto es un cuadrado, pero no son asociados con cuadrados (¡son irreducibles!). Aquí no hay ninguna contradicción porque $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única. ▲

1.10 Ecuación de Fermat $x^3 + y^3 = z^3$

El lector probablemente ha escuchado del **último teorema de Fermat** que afirma que para $n \geq 3$ la ecuación $x^n + y^n = z^n$ no tiene soluciones enteras con $xyz \neq 0$. La prueba de este resultado (concluida por Andrew Wiles en 1995) fue uno de los logros más publicitados de las matemáticas del siglo pasado.

El caso particular de $n = 3$ fue resuelto por Euler. Aquí vamos a ver una demostración con los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$. Curiosamente, el mismo Euler trabajaba con el anillo más pequeño $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\zeta_3]$, suponiendo erróneamente que este tiene factorización única. (Véase [Edw1996, Chapter 2] para más detalles.)

Antes de lanzarnos en la prueba, notamos que con las terceras raíces de la unidad la ecuación de Fermat se factoriza como

$$x^3 + y^3 = (x + y)\,(x + \zeta_3 y)\,(x + \zeta_3^2 y) = z^3,$$

y esto explica la utilidad de los enteros de Eisenstein en nuestro problema.

Lectura adicional

Para el resto de esta sección fijemos el primo de Eisenstein $\pi = 1 - \zeta_3$. Recordemos que $\mathbb{Z}[\zeta_3]/(\pi) \cong \mathbb{F}_3$.

1.10.1. Lema. *La ecuación $x^3 + y^3 = uz^3$, donde $u \in \mathbb{Z}[\zeta_3]^\times$, no tiene soluciones $x, y, z \in \mathbb{Z}[\zeta_3]$ con $\pi \nmid xyz$.*

Demostración. Primero notamos que si $\pi \nmid x$, entonces $x \equiv \pm 1 \pmod{\pi}$, lo cual implica que $x^3 \equiv \pm 1 \pmod{\pi^4}$. Por ejemplo, si $x \equiv 1 \pmod{\pi}$, podemos escribir $x = 1 + \pi t$ para $t \in \mathbb{Z}[\zeta_3]$ y factorizar

$$x^3 - 1 = (x - 1)\,(x - \zeta_3)\,(x - \zeta_3^2) = \cdots = \pi^3\, t\,(t + 1)\,(t - \zeta_3^2).$$

Aquí $\zeta_3^2 \equiv 1 \pmod{\pi}$, y para cualquier residuo $t \equiv 0, +1, -1 \pmod{\pi}$ se ve que $x^3 - 1 \equiv 0 \pmod{\pi^4}$.

Ahora bien, si $x^3 + y^3 = uz^3$ y $\pi \nmid xyz$, entonces

$$\pm 1 \pm 1 \equiv \pm u \pmod{\pi^4}.$$

Es fácil verificar que todas las opciones para los signos $\pm$ y $u \in \mathbb{Z}[\zeta_3]^\times$ nos llevan a una contradicción (note que $\pi^4 \sim 9$, así que se trata de los restos módulo 9 en $\mathbb{Z}[\zeta_3]$). ∎

1.10.2. Lema. *Si $x^3 + y^3 = uz^3$ para $x, y, z \in \mathbb{Z}[\zeta_3]$ y $u \in \mathbb{Z}[\zeta_3]^\times$, y $\pi \nmid xy$, $\pi \mid z$, entonces $\pi^2 \mid z$.*

Demostración. Como en la prueba del lema anterior, se obtiene

$$\pm 1 \pm 1 \equiv uz^3 \pmod{\pi^4}.$$

Si $uz^3 \equiv \pm 2 \pmod{\pi^4}$, entonces $\pi \mid 2$, lo cual no es cierto. Por otra parte, si $uz^3 \equiv 0 \pmod{\pi^4}$, entonces

$$3v_\pi(z) = v_\pi(z^3) \geq 4,$$

lo que implica $v_\pi(z) \geq 2$. ∎

La idea clave, que el mismo Fermat aplicó al caso de $n = 4$ el método del descenso infinito, que en nuestro caso está contenido en el siguiente lema.

1.10.3. Lema (Descenso). *Supongamos que $x^3 + y^3 = uz^3$, para $x, y, z \in \mathbb{Z}[\zeta_3]$ y $u \in \mathbb{Z}[\zeta_3]^\times$, donde* $\operatorname{mcd}(x, y) = 1$, *$\pi \nmid xy$, $v_\pi(z) \geq 2$. Entonces, existen $x_1, y_1, z_1 \in \mathbb{Z}[\zeta_3]$ y $\epsilon \in \mathbb{Z}[\zeta_3]^\times$ tales que*

$$x_1^3 + y_1^3 = \epsilon z_1^3,$$

y $\pi \nmid x_1 y_1$, $v_\pi(z_1) = v_\pi(z) - 1$.

Demostración. Como hemos observado, la ecuación se factoriza como

$$(x+y)\,(x+\zeta_3 y)\,(x+\zeta_3^2 y) = uz^3.$$

Dado que por nuestra hipótesis

$$v_\pi(uz^3) = 3v_\pi(z) \geq 6,$$

por lo menos uno de los tres factores debe ser divisible por π^2. Remplazando y con $\zeta_3 y$ o $\zeta_3^2 y$, podemos asumir que $\pi^2 \mid (x+y)$. Ahora

$$v_\pi(x+\zeta_3 y) = v_\pi(x+y-(1-\zeta_3)y) = \text{mín}\{v_\pi(x+y), v_\pi(\pi y)\} = 1. \tag{1.2}$$

De la misma manera,

$$v_\pi(x+\zeta_3^2 y) = 1. \tag{1.3}$$

Entonces,

$$v_\pi(x+y) = 3v_\pi(z) - 2. \tag{1.4}$$

Tenemos

$$\text{mcd}(x+y, x+\zeta_3 y) = \text{mcd}(x+y, x+\zeta_3^2 y) = \text{mcd}(x+\zeta_3 y, x+\zeta_3^2 y) = \pi. \tag{1.5}$$

Por ejemplo, sea ρ un primo tal que $\rho \not\sim \pi$ y $\rho \mid (x+y)$ y $\rho \mid (x+\zeta_3 y)$. Entonces, $\rho \mid (1-\zeta_3)y = \pi y$ e $\rho \mid y$. Esto también implicaría que $\rho \mid x$, pero $\text{mcd}(x,y) = 1$ por nuestra hipótesis. Entonces, el único primo que divide a $x+y$ e $x+\zeta_3 y$ es π.

Usando (1.2), (1.3), (1.4), (1.5) podemos escribir

$$x+y = u_1\alpha^3\pi^{3v_\pi(z)-2}, \tag{a}$$

$$x+\zeta_3 y = u_2\beta^3\pi, \tag{b}$$

$$x+\zeta_3^2 y = u_2\beta^3\pi, \tag{c}$$

donde $\pi \nmid \alpha\beta\gamma$, $u_1, u_2, u_3 \in \mathbb{Z}[\zeta_3]^\times$ y

$$\text{mcd}(\alpha,\beta) = \text{mcd}(\alpha,\gamma) = \text{mcd}(\beta,\gamma) = 1.$$

La ecuación (a) + ζ_3(b) + ζ_3^2(c) nos da

$$(\underbrace{1+\zeta_3+\zeta_3^2}_{=0})\,(x+y) = u_1\alpha^3\pi^{3v_\pi(z)-2} + \zeta_3 u_2\beta^3\pi + \zeta_3^2 u_2\beta^3\pi.$$

Al cancelar π, nos queda

$$\zeta_3 u_2\beta^3 + \zeta_3^2 u_2\beta^3 = -u_1\alpha^3\pi^{3(v_\pi(z)-1)}.$$

Pongamos

$$x_1 = \beta, \quad y_1 = \gamma, \quad z_1 = \alpha\pi^{v_\pi(z)-1}.$$

Entonces, para ciertas unidades $\epsilon_1, \epsilon_2 \in \mathbb{Z}[\zeta_3]^\times$ se cumple

$$x_1^3 + \epsilon_1 y_1^3 = \epsilon_2 z_1^3.$$

Tenemos

$$v_\pi(z_1^3) = 3v_\pi(z) - 3 > 2,$$

así que la reducción módulo π^2 nos da

$$\pm 1 \pm \epsilon_1 \equiv 0 \pmod{\pi^2}.$$

Analizando todas las posibilidades para $\epsilon_1 \in \mathbb{Z}[\zeta_3]^\times$ notamos que la única posibilidad es $\epsilon_1 = \mp 1$. Remplazando y por $-y$ si necesario, llegamos a la ecuación de la forma

$$x_1^3 + y_1^3 = \epsilon z_1^3,$$

donde $\epsilon \in \mathbb{Z}[\zeta_3]^\times$, $\pi \nmid x_1 y_1$, $v_\pi(z_1) = v_\pi(z) - 1$. ■

Notamos que los argumentos de arriba usan la factorización única en $\mathbb{Z}[\zeta_3]$. Ahora estamos listos para probar el último teorema de Fermat para $n = 3$. Ya que hemos trabajado con el anillo $\mathbb{Z}[\zeta_3]$, el resultado será un poco más general.

1.10.4. Teorema. *La ecuación $x^3 + y^3 = uz^3$ para $u \in \mathbb{Z}[\zeta_3]^\times$ no tiene soluciones $x, y, z \in \mathbb{Z}[\zeta_3]$ con $xyz \neq 0$.*

Demostración. Asumamos que $x^3 + y^3 = uz^3$. El lema 1.10.1 dice que necesariamente $\pi \mid xyz$.

Supongamos que se cumple $\pi \nmid xy$ e $\pi \mid z$. Consideremos la solución con el valor de $v_\pi(z)$ más pequeño posible (entre todas las posibilidades para $u \in \mathbb{Z}[\zeta_3]^\times$). En este caso los lemas 1.10.2 y 1.10.3 nos llevan a una contradicción.

En fin, supongamos que $\pi \mid x$ y $\pi \nmid yz$. En este caso $u \equiv \pm 1 \pmod{\pi^3}$. Sin embargo, esto implica que $u = \pm 1$ y la ecuación puede ser escrita como $(\mp z)^3 + (-y)^3 = x^3$, lo cual corresponde al caso anterior. ■

1.10.5. Comentario. De manera parecida, el se puede probar que $x^4 + y^4 = z^4$ no tiene soluciones no triviales, usando los enteros de Gauss $\mathbb{Z}[i]$. De hecho, el argumento demostraría el resultado para $x, y, z \in \mathbb{Z}[i]$. En este caso hay que considerar el primo $\pi = 1 + i$ (note que $\pi^2 \sim 2$). Para los detalles, véase por ejemplo [Rib1999, §I.3].

Estas pruebas usan la factorización única en los anillos ciclotómicos $\mathbb{Z}[\zeta_3]$ y $\mathbb{Z}[i] = \mathbb{Z}[\zeta_4]$. En general, $\mathbb{Z}[\zeta_n]$ no tiene factorización única. Curiosamente, esto falla por primera vez para $n = 23$.

Los métodos mencionados establecen algunos casos particulares del último teorema de Fermat para anillos de números más grandes que $\mathbb{Z}$. Sin embargo, el caso general de $n \geq 3$ es un problema abierto: no se sabe si la ecuación de Fermat $x^n + y^n = z^n$ no tiene soluciones no triviales en $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_3]$, etc.[*]

1.11 Puntos enteros en curvas $y^2 = x^3 + t$

Consideremos la curva plana definida por la ecuación

$$E\colon y^2 = x^3 - 1.$$

Un famoso teorema de Siegel nos dice que el conjunto de los puntos enteros sobre cualquier curva elíptica

$$E\colon x^3 + ax + b, \quad a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0$$

es siempre finito [Sil2009, §X.3]. En este caso particular, una búsqueda sugiere que la única solución es $(1, 0)$, pero ¿cómo probarlo?

1.11.1. Proposición. *La ecuación $y^2 = x^3 - 1$ tiene única solución entera $(x, y) = (1, 0)$.*

Demostración. Supongamos que $x, y \in \mathbb{Z}$ cumplen $y^2 = x^3 - 1$. Primero notamos que $x^3 - 1 \not\equiv 1 \pmod 4$, así que y debe ser par. En el anillo $\mathbb{Z}[i]$ podemos factorizar nuestra expresión como

$$x^3 = (y + i)\,(y - i).$$

Dejo como un ejercicio comprobar que para y par se tiene $\operatorname{mcd}(y + i, y - i) = 1$. Luego, puesto que $y + i$ e $y - i$ son coprimos y su producto es un cubo, se cumple

$$y + i = u\,(a + bi)^3,$$

para algunos $u \in \mathbb{Z}[i]^\times$, $a, b \in \mathbb{Z}$. Todo elemento de $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ es un cubo, así que sin pérdida de generalidad $u = 1$. Tenemos

$$y + i = (a + bi)^3 = a\,(a^2 - 3b^2) + b\,(3a^2 - b^2)\,i.$$

De $1 = b\,(3a^2 - b^2)$ se ve que la única solución posible es $a = 0, b = -1$. Esto nos permite concluir que $y = 0$, y luego $x = 1$. ■

[*] Véase por ejemplo https://mathoverflow.net/questions/90972/ y [Ţ2018] para el reciente progreso.

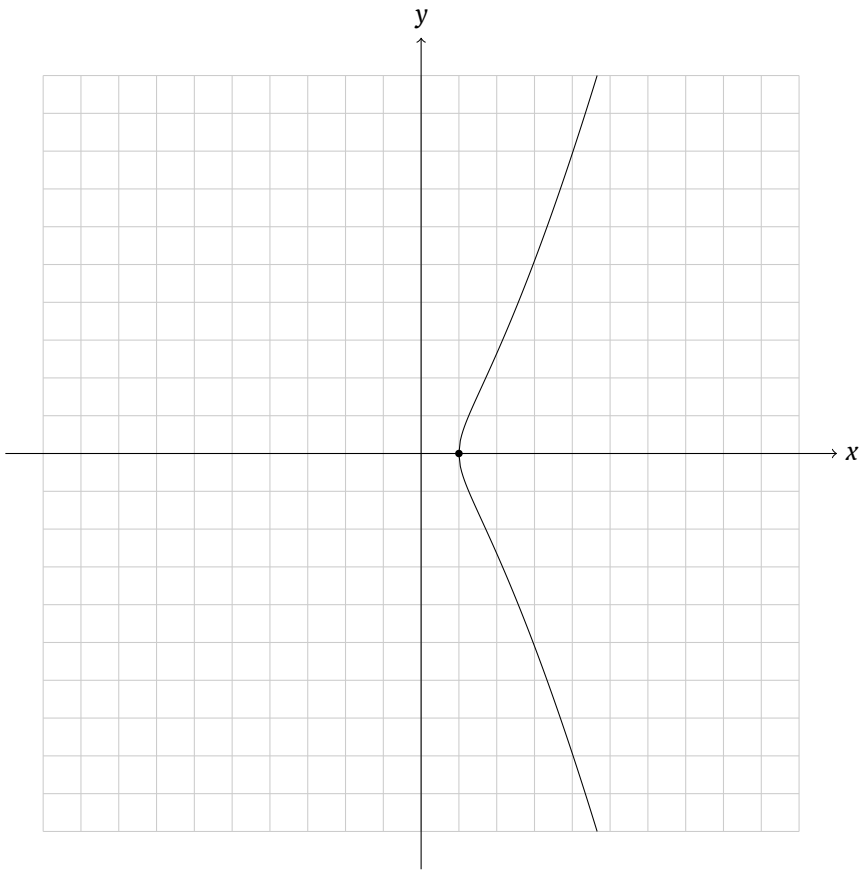


Figura 1.5: Curva elíptica $y^2 = x^3 - 1$

Ahora consideremos la ecuación parecida

$$y^2 = x^3 - 19.$$

Podemos tratar de aplicar el mismo truco y factorizar en el anillo $\mathbb{Z}[\sqrt{-19}]$

$$x^3 = (y + \sqrt{-19})\,(y - \sqrt{-19}).$$

Notamos que $x^3 - 19 \not\equiv 1 \pmod 8$, mientras que $y^2 \equiv 1 \pmod 8$ si y es impar. Entonces, y es necesariamente par, y además se ve que $y \neq 0$. En este caso $\operatorname{mcd}(y + \sqrt{-19}, y - \sqrt{-19}) = 1$, en el sentido que

$$(y + \sqrt{-19}, y - \sqrt{-19}) = \mathbb{Z}[\sqrt{-19}].$$

(¡Ejercicio!) Como antes, podemos escribir

$$y + \sqrt{-19} = (a + b\sqrt{-19})^3 = a\,(a^2 - 57b^2) + b\,(3a^2 - 19b^2)\,\sqrt{-19}.$$

(Note que $\mathbb{Z}[\sqrt{-19}]^\times = \{\pm 1\}$, así que podemos olvidar de la unidad.) En particular, $b\,(3a^2 - 19b^2) = 1$, pero esta ecuación no tiene soluciones enteras. Entonces, parece que la ecuación $y^2 = x^3 - 19$ no tiene soluciones enteras... Sin embargo, no es difícil verificar que

$$7^3 - 19 = 324 = 18^2,$$

así que $(7, \pm 18)$ es una solución entera. Entonces, nuestra lógica nos falló en algún momento.

El problema es que el anillo $\mathbb{Z}[\sqrt{-19}]$, a diferencia de $\mathbb{Z}[i]$, no tiene factorización única (véanse los ejercicios para una prueba). Con las herramientas que vamos a desarrollar en nuestro curso, veremos que el anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ sí tiene factorización única, así que hay que trabajar en este anillo.

1.11.2. Proposición. *Las únicas soluciones enteras de la ecuación* $y^2 = x^3 - 19$ *son* $(x, y) = (7, \pm 18)$.

Demostración. Denotemos $\alpha = \frac{1+\sqrt{-19}}{2}$. Notamos que $\alpha^2 - \alpha + 5 = 0$. Como mencionamos, $\mathbb{Z}[\alpha]$ tiene factorización única. Tenemos $\mathbb{Z}[\alpha]^\times = \{\pm 1\}$. El argumento de arriba nos da

$$(y - 1) + 2\alpha = y + \sqrt{-19} = (a + b\alpha)^3 = (a^3 - 15ab^2 - 5b^3) + (3a^2 + 3ab - 4b^2)\,b\alpha.$$

La ecuación $(3a^2 + 3ab - 4b^2)\,b = 2$ implica que $b = \pm 1, \pm 2$, y se ve que las únicas soluciones enteras son

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

Sustituyendo estos valores, llegamos precisamente a $y = \pm 18$, y luego $x^3 = 18^2 + 19 = 343$, así que $x = 7$. ■

1.11.3. Ejemplo. He aquí los puntos enteros sobre algunas curvas de la forma $y^2 = x^3 + t$. Para la teoría detrás de esta ecuación diofántica, véase por ejemplo [Coh2007].

$y^2 = x^2 + 1$:	$(-1, 0), (0, \pm 1), (2, \pm 3)$	$y^2 = x^3 - 1$:	$(1, 0)$
$y^2 = x^2 + 2$:	$(-1, \pm 1)$	$y^2 = x^3 - 2$:	$(3, \pm 5)$
$y^2 = x^2 + 3$:	$(1, \pm 2)$	$y^2 = x^2 - 3$:	—
$y^2 = x^2 + 4$:	$(0, \pm 2)$	$y^2 = x^2 - 4$:	$(2, \pm 2), (5, \pm 11)$
$y^2 = x^2 + 5$:	$(-1, \pm 2)$	$y^2 = x^2 - 5$:	—
$y^2 = x^2 + 6$:	—	$y^2 = x^2 - 6$:	—
$y^2 = x^2 + 7$:	—	$y^2 = x^2 - 7$:	$(2, \pm 1), (32, \pm 181)$
$y^2 = x^2 + 8$:	$(-2, 0), (1, \pm 3), (2, \pm 4), (46, \pm 312)$	$y^2 = x^2 - 8$:	$(2, 0)$
$y^2 = x^2 + 9$:	$(-2, \pm 1), (0, \pm 3), (3, \pm 6), (6, \pm 15), (40, \pm 253)$	$y^2 = x^2 - 9$:	—
$y^2 = x^2 + 10$:	$(-1, \pm 3)$	$y^2 = x^2 - 10$:	—

▲

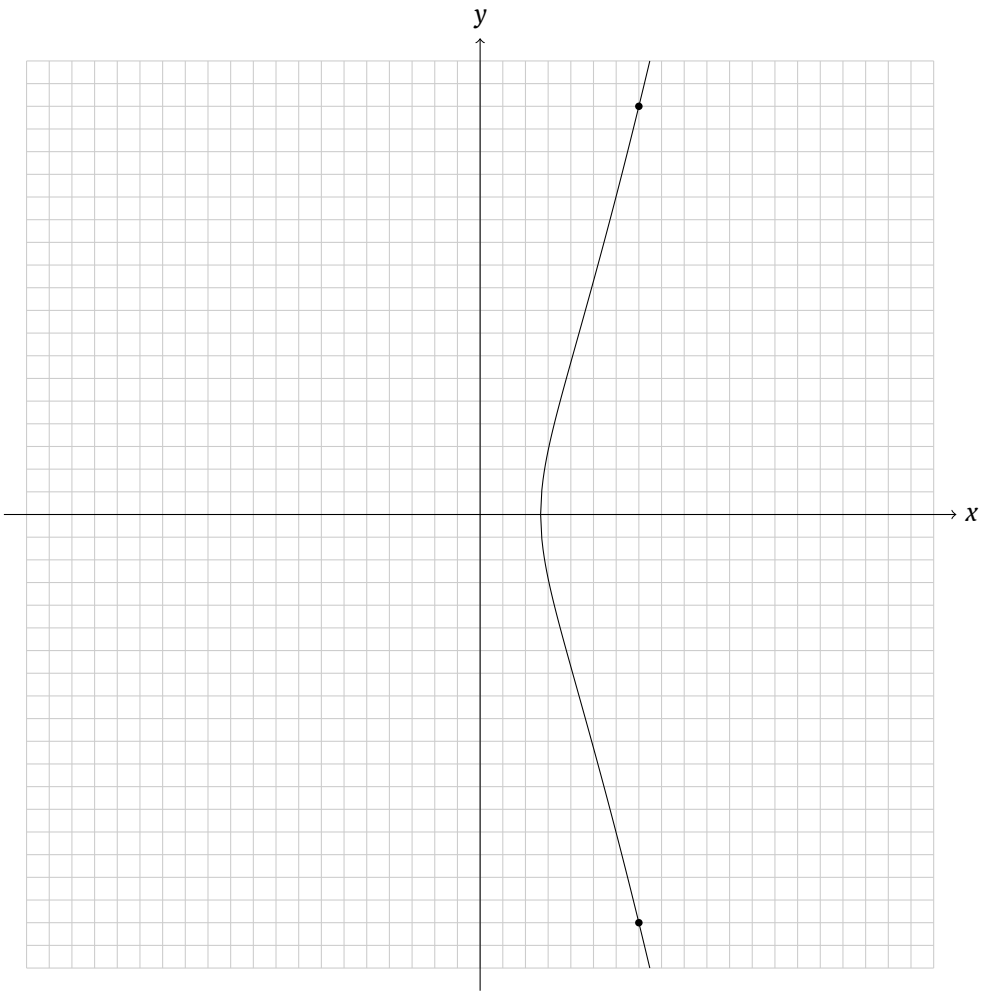


Figura 1.6: Curva elíptica $y^2 = x^3 - 19$

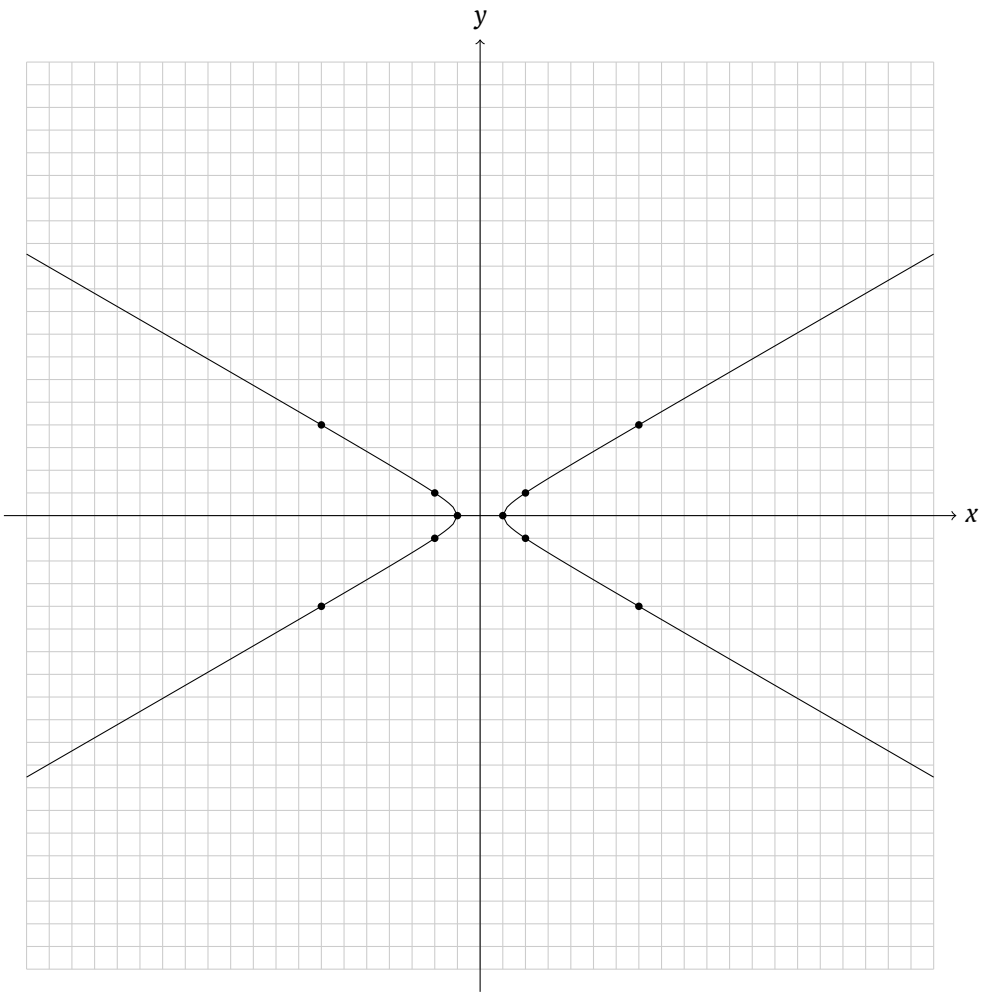


Figura 1.7: Algunos puntos enteros en la curva $x^2 - 3y^2 = 1$

1.12 Ecuación de Pell $x^2 - dy^2 = 1$

Sea $d > 0$ un entero libre de cuadrados. La ecuación diofántica

$$x^2 - dy^2 = 1$$

se conoce como la **ecuación de Pell**[*]. Nuestro objetivo es describir las soluciones enteras.

Por ejemplo, consideremos la ecuación $x^2 - 3y^2 = 1$ (véase la figura 1.7). Algunas soluciones evidentes son

$$(1,0),\ (2,1),\ (7,4).$$

Podemos usar PARI/GP para encontrar más soluciones. Basta fijarnos, por ejemplo, en los valores de y, y luego $x = \pm\sqrt{1 + 3y^2}$.

[*]John Pell (1611–1685), matemático inglés. No hay documentos que demuestren que Pell trabajó en algún momento de su vida en la «ecuación de Pell»; la atribución errónea del nombre se debe a Euler. Así que como matemático, Pell es conocido por una ecuación que nunca estudió.

```
? pell_sol_naive (d,n) = {
  for (y=0,n,
    if (issquare (1+d*y^2),
      print ([sqrtint (1+d*y^2), y])
    )
  )
};

? pell_sol_naive (3,10^6)
[1, 0]
[2, 1]
[7, 4]
[26, 15]
[97, 56]
[362, 209]
[1351, 780]
[5042, 2911]
[18817, 10864]
[70226, 40545]
[262087, 151316]
[978122, 564719]
```

Consideremos el anillo $\mathbb{Z}[\sqrt{3}]$. Este viene con la norma

$$N(x+y\sqrt{3}) = (x+y\sqrt{3})\,(x-y\sqrt{3}) = x^2 - 3y^2,$$

y el argumento que ya hemos visto arriba demuestra que

$$\mathbb{Z}[\sqrt{3}]^\times = \{\alpha \in \mathbb{Z}[\zeta_3] \mid N(\alpha) = \pm 1\}.$$

Considerando $x^2 - 3y^2$ módulo 4, notamos que la norma -1 nunca ocurre. Entonces, las soluciones de $x^2 - 3y^2 = 1$ corresponden exactamente a las unidades $u \in \mathbb{Z}[\sqrt{3}]^\times$. Por ejemplo, la solución $(2,1)$ corresponde a la unidad $u = 2+\sqrt{3}$, y nuestra sucesión de arriba nada más viene de las potencias u^n para $n = 0, 1, 2, 3, \ldots$ Por ejemplo,

$$(2+\sqrt{3})^2 = 7 + 4\sqrt{3},$$
$$(2+\sqrt{3})^3 = 26 + 15\sqrt{3}.$$

```
? K = nfinit(x^2-3);
? u = 2+x;
? for (n=1,10, u=nfeltmul(K,u,2+x); print(u));
[7, 4]~
[26, 15]~
[97, 56]~
[362, 209]~
[1351, 780]~
[5042, 2911]~
```

```
[18817, 10864]~
[70226, 40545]~
[262087, 151316]~
[978122, 564719]~
```

En particular, notamos que $u^m \neq u^n$ para $m \neq n$, así que la ecuación tiene un número infinito de soluciones. De hecho, en el caso contrario $u^{m-n} = 1$, pero los elementos de $\mathbb{Z}[\sqrt{3}]$ son números reales, y las únicas raíces de la unidad en $\mathbb{R}$ son ± 1.

El número $2 + \sqrt{3}$ se llama la **unidad fundamental** y surge de la siguiente manera.

1.12.1. Lema. *El número $2 + \sqrt{3}$ es la unidad más pequeña $u \in \mathbb{Z}[\sqrt{3}]^\times$ que cumple $u > 1$.*

Demostración. Supongamos que existe una unidad $u = a + b\sqrt{3}$ que cumple

$$1 \leq u \leq 2 + \sqrt{3}.$$

Luego, $u^{-1} = a - b\sqrt{3}$, y tomando los inversos se obtiene la desigualdad

$$2 - \sqrt{3} \leq u^{-1} \leq 1.$$

Sumando las dos desigualdades, llegamos a

$$1 < 3 - \sqrt{3} \leq u + u^{-1} \leq 3 + \sqrt{3} < 5.$$

El número $u + u^{-1} = 2a$ es par, así que hay solo dos posibilidades:

$$u + u^{-1} = 2 \quad \text{o} \quad u + u^{-1} = 4.$$

La primera ecuación implica que $u = 1$, mientras que la segunda implica que $u = 2 + \sqrt{3}$. ■

1.12.2. Teorema. *Toda unidad $u \in \mathbb{Z}[\sqrt{3}]^\times$ es de la forma $\pm(2 + \sqrt{3})^n$ para algún $n \in \mathbb{Z}$. En otras palabras, hay isomorfismo de grupos*

$$\mathbb{Z}[\sqrt{3}]^\times \cong \langle \pm 1 \rangle \times \langle 2 + \sqrt{3} \rangle \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

Este es un caso muy particular del **teorema de unidades de Dirichlet** que será uno de los resultados más importantes del curso.

Demostración. Está claro que $\pm(2 + \sqrt{3})^n$ son unidades, hay que probar que no hay otras. Sea $u \in \mathbb{Z}[\sqrt{3}]^\times$ una unidad. Pasando a u^{-1} y cambiando el signo, podemos asegurarnos de que $u \geq 1$. En este caso habrá algún $n = 0, 1, 2, 3, \ldots$ tal que

$$(2 + \sqrt{3})^n \leq u < (2 + \sqrt{3})^{n+1}.$$

Luego,

$$1 \leq u\,(2 + \sqrt{3})^{-n} < 2 + \sqrt{3},$$

y el lema de arriba implica que $u = (2 + \sqrt{3})^n$. ■

Ahora consideremos la ecuación $x^2 - 2011y^2 = 1$. Empleando la búsqueda tonta para todo $y \leq N$ (como por ejemplo al inicio de esta sección), no se encuentra ninguna solución no trivial.

```
? #
   timer = 1 (on)
? pell_sol_naive (2011,10^7)
[1, 0]
time = 5,093 ms.
? pell_sol_naive (2011,10^8)
[1, 0]
time = 50,371 ms.
```

¿Será que para $d = 2011$ la ecuación de Pell ya no tiene soluciones no triviales por alguna razón? De hecho no, 2011 no tiene nada de especial, solo que en este caso la unidad fundamental es

$$22903355954053525066202335319378237605968890 + 5107320211161387136750185662322016053209 97\sqrt{2011}.$$

Ninguna búsqueda razonable puede llegar a estos números.

Para calcular la unidad fundamental en un campo cuadrático real, podemos hacer lo siguiente.

```
? quadunit(4*3)
% = 2 + w
? quadunit(4*2011)
% = 22903355954053525066202335319378237605968890
      + 5107320211161387136750185662322016053209 97*w
? norm (%)
% = 1
```

Hemos escrito `quadunit(4*2011)` porque $d = 2011 \equiv 2, 3 \pmod 4$, y el campo $\mathbb{Q}(\sqrt{2011})$ tiene discriminante $4 \cdot 2011$; esto será explicado más adelante en el curso. Además, notamos que si $d \equiv 1 \pmod 4$, entonces `quadunit(`d`)` devuelve la unidad fundamental en el anillo $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Salvo algunos detalles, la ecuación de Pell siempre se resuelve encontrando la unidad fundamental correspondiente. Más adelante en el curso veremos un algoritmo para encontrarla.

1.12.3. Ejemplo. He aquí una breve lista de unidades fundamentales (es decir, las unidades más pequeñas tales que $u > 1$) en los anillos de la forma $\mathbb{Z}[\sqrt{d}]$ (y $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ para $d \equiv 1 \pmod 4$).

R:	$\mathbb{Z}[\sqrt{2}]$	$\mathbb{Z}[\sqrt{3}]$	$\mathbb{Z}[\sqrt{5}]$	$\mathbb{Z}[\sqrt{6}]$	$\mathbb{Z}[\sqrt{7}]$	$\mathbb{Z}[\sqrt{10}]$	$\mathbb{Z}[\sqrt{11}]$	$\mathbb{Z}[\sqrt{13}]$
u:	$1+\sqrt{2}$	$2+\sqrt{3}$	$2+\sqrt{5}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$18+5\sqrt{13}$
$N(u)$:	-1	$+1$	-1	$+1$	-1	-1	$+1$	-1
R:			$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$					$\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$
u:			$\frac{1+\sqrt{5}}{2}$					$1+\frac{1+\sqrt{13}}{2}$
$N(u)$:			-1					-1

Invito al lector a comprobar algunos casos (de la misma manera que hicimos con $\mathbb{Z}[\sqrt{3}]$ en 1.12.1). ▲

Para que el lector no piense que los anillos cuadráticos reales $\mathbb{Z}[\sqrt{d}]$ tienen algo especial, por ejemplo, tomemos el anillo ciclotómico

$$\mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p) = \mathbb{Z}[x]/(x^{p-1} + x^{p-2} + \cdots + x + 1).$$

Allí la división con resto de polinomios nos da

$$\Phi_p = (x+1)\,(x^{p-2} + x^{p-4} + \cdots + x^3 + x) + 1,$$

lo que demuestra que

$$(1+\zeta_p)^{-1} = -(\zeta_p + \zeta_p^3 + \cdots + \zeta_p^{p-4} + \zeta_p^{p-1}),$$

así que $1 + \zeta_p \in \mathbb{Z}[\zeta_p]^\times$. En general, en el anillo ciclotómico $\mathbb{Z}[\zeta_n]$ habrá muchas unidades, y el grupo $\mathbb{Z}[\zeta_n]^\times$ es finitamente generado de rango $\phi(n)/2 - 1$. Lo veremos más adelante en el curso.

Ejercicios

Campos y anillos de números

Ejercicio 1.1 (Campos cuadráticos)**.** Consideremos una extensión cuadrática $K/\mathbb{Q}$ (es decir, $[K:\mathbb{Q}]=2$).

a) Demuestre que $K \cong \mathbb{Q}(\sqrt{d})$ para algún entero libre de cuadrados d.

b) Demuestre que $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(\sqrt{d'})$ si y solamente si $d = d'$.

Advertencia: esto no funciona para el grado mayor que 2; por ejemplo, no todas las extensiones cúbicas son de la forma $\mathbb{Q}(\sqrt[3]{d})$. (¿Puede encontrar algún ejemplo?)

Ejercicio 1.2. El **teorema del elemento primitivo** afirma que para todo campo de números $K/\mathbb{Q}$ existe un elemento α tal que $K = \mathbb{Q}(\alpha)$.

a) Revise la prueba estándar en cualquier libro de texto [Lan2002, Chapter V, Theorem 4.6] o [Mor1996, Chapter I, Theorem 5.6].

b) Encuentre α para $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Exprese $\sqrt{2}, \sqrt{3}, \sqrt{5}$ en términos de la base estándar de $\mathbb{Q}(\alpha)$.

c*) Use la función `rnfequation(`K`,`f`)` de PARI/GP para obtener el polinomio mínimo de α.

Ejercicio 1.3. a) Demuestre que los anillos $\mathbb{Q}, \mathbb{Z}\left[\frac{1}{n}\right], \mathbb{Z}_{(p)}$ no son finitamente generados como $\mathbb{Z}$-módulos.

b) Demuestre que un grupo abeliano p-divisible para un primo p no puede ser finitamente generado.

Ejercicio 1.4. Sea $f \in \mathbb{Z}[x]$ un polinomio mónico irreducible con coeficientes enteros.

a) Demuestre que el anillo $\mathbb{Z}[x]/(f)$ es un $\mathbb{Z}$-módulo libre de rango $\deg f$ y el campo $\mathbb{Q}[x]/(f)$ es una extensión de $\mathbb{Q}$ de grado $\deg f$.

b) ¿Qué sucede si f no es mónico?

Factorización única

Ejercicio 1.5. Demuestre que los anillos $\mathbb{Z}[x]$ y $k[x,y]$ (donde k es un campo) no son dominios de ideales principales. (Son dominios de factorización única, ya que para cualquier DFU R, el anillo de polinomios $R[X]$ es también un DFU.)

Ejercicio 1.6. Demuestre que el anillo de polinomios con un número infinito de variables

$$k[x_1, x_2, x_3, \ldots] = \bigcup_{n \geq 0} k[x_1, \ldots, x_n]$$

(unión respecto a las inclusiones naturales) no es noetheriano, pero es un dominio de factorización única.

Este ejemplo explica la condición a) en 1.5.6 que es más débil que la condición noetheriana.

Ejercicio 1.7. Demuestre que los siguientes anillos son euclidianos respecto a su norma habitual:

$$\mathbb{Z}[\sqrt{-2}],\ \mathbb{Z}[\sqrt{2}],\ \mathbb{Z}[\zeta_3] = \mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big],\ \mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big],\ \mathbb{Z}\Big[\frac{1+\sqrt{-11}}{2}\Big].$$

Ejercicio 1.8. En este ejercicio vamos a probar que el anillo $R = \mathbb{Z}\Big[\frac{1+\sqrt{-19}}{2}\Big]$ no es euclidiano.

Supongamos que R es euclidiano (respecto a alguna función $\delta\colon R \setminus \{0\} \to \mathbb{N}$). Sea α un elemento no nulo y no invertible con el mínimo posible valor de $\delta(\alpha)$ (es decir, si $\delta(r) < \delta(\alpha)$, entonces $r = 0$ o $r \in R^\times$).

a) Demuestre que para cualquier $\beta \in R$ se tiene $\alpha \mid \beta$, o $\alpha \mid (\beta \pm 1)$.

b) Considere qué sucede con $\beta = 2$ y $\beta = \frac{1+\sqrt{-19}}{2}$ para concluir que tal α no existe.

Más adelante en el curso veremos que $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ es un dominio de ideales principales. De la misma manera, $\mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ son dominios de ideales principales, pero no son euclidianos. La moraleja de este ejercicio: la noción de dominio euclidiano no tiene ningún sentido profundo; es puramente utilitaria y se ocupa para probar que ciertos anillos son dominios de ideales principales. En práctica no es fácil demostrar que algo es un dominio euclidiano, ni que no lo es.

Enteros de Gauss $\mathbb{Z}[i]$

Ejercicio 1.9. Factorice el número 210 en $\mathbb{Z}[i]$.

Ejercicio 1.10. Sean a, b dos enteros coprimos de diferente paridad. Demuestre que $\mathrm{mcd}(a+bi, a-bi) = 1$ en $\mathbb{Z}[i]$. En particular, si a es par, entonces $\mathrm{mcd}(a+i, a-i) = 1$.

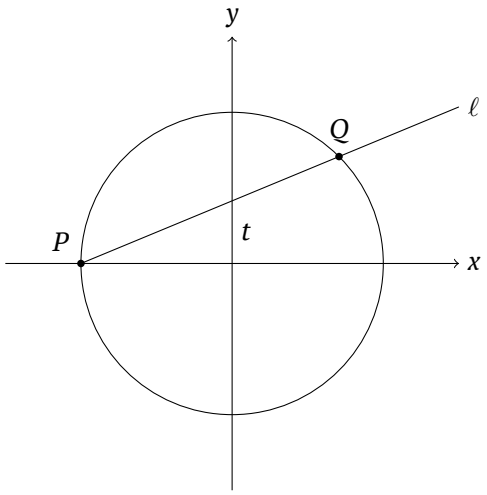
Ejercicio 1.11. Calcule $\mathrm{mcd}(a+i, a-i)$ y $\mathrm{mcd}(a+2i, a-2i)$ en el anillo $\mathbb{Z}[i]$.
Sugerencia: la respuesta depende de a módulo 2 *y* 4.

Ejercicio 1.12. Ya que nuestro curso está dedicado a números algebraicos, hemos usado el anillo $\mathbb{Z}[i]$ para describir las ternas pitagóricas. He aquí un modo más geométrico de hacerlo.

Notamos que una terna pitagórica primitiva (x, y, z) corresponde a un punto racional $(u, v) = \left(\frac{x}{y}, \frac{y}{z}\right)$ en el circulo unitario. Fijemos el punto $P = (-1, 0)$ y tracemos una recta que pasa por P y tiene otra intersección Q con el círculo. Esta recta tendrá la ecuación

$$\ell \colon y = tx + t$$

para algún t.



La intersección de esta recta con el círculo viene dada por

$$Q = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

Demuestre que de esta manera los puntos racionales en el círculo unitario salvo el punto P están en biyección con $t \in \mathbb{Q}$. Escribiendo $t = \frac{b}{a}$ con $\mathrm{mcd}(a, b) = 1$, recupere nuestra parametrización de las ternas pitagóricas primitivas.

Campos y anillos cuadráticos

Ejercicio 1.13. Sea $d < 0$ un entero *negativo* libre de cuadrados. Usando la norma correspondiente*, calcule los grupos de unidades

a) $\mathbb{Z}[\sqrt{d}]^\times$,

b) $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$ para $d \equiv 1 \pmod 4$.

Ejercicio 1.14. Sea $d \geq 3$ un entero libre de cuadrados.

a) Demuestre que en el anillo $\mathbb{Z}[\sqrt{-d}]$ el número 2 es irreducible pero no es primo.
Sugerencia: si d es par, $2 \mid (\sqrt{-d})^2$ *y si d es impar,* $2 \mid (1+\sqrt{-d})\,(1-\sqrt{-d})$.

b) La misma pregunta para $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 1 \pmod 4$.
Sugerencia: $2 \mid (\sqrt{d}+1)\,(\sqrt{d}-1)$.

Ejercicio 1.15. Consideremos el ideal $I = (2, 1+\sqrt{-3})$ en el anillo $\mathbb{Z}[\sqrt{-3}]$.

a) Demuestre que I no es principal.
Sugerencia: use la norma.

b) Demuestre que I es principal en el anillo más grande $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

Enteros de Eisenstein $\mathbb{Z}[\zeta_3]$

Ejercicio 1.16. Factorice el número 210 en $\mathbb{Z}[\zeta_3]$.

Ejercicio 1.17. Para un primo $p \equiv 1 \pmod 3$ demuestre que en la expresión $4p = u^2 + 27v^2$ los números u y v están bien definidos salvo signo.
Sugerencia: revise cómo estas expresiones surgen de los enteros de Eisenstein $\mathbb{Z}[\zeta_3]$ *y use la factorización única en* $\mathbb{Z}[\zeta_3]$.

Ejercicio 1.18. Demuestre que si $\pi \in \mathbb{Z}[\zeta_3]$ es un primo de Eisenstein tal que $\pi \not\sim 1-\zeta_3$, entonces $1, \zeta_3, \zeta_3^2$ no son congruentes módulo π.

Ejercicio 1.19. Sea $\pi \in \mathbb{Z}[\zeta_3]$ un primo de Eisenstein tal que $N(\pi) = p \equiv 1 \pmod 3$. Demuestre que entre sus asociados $\pi' \sim \pi$ precisamente uno cumple $\pi' \equiv 2 \pmod 3$.

Ejercicio 1.20. Demuestre que $\left(\frac{\alpha}{\pi}\right)_3 = 1$ si y solamente si α es un residuo cúbico en $\mathbb{Z}[\zeta_3]/(\pi)$ (es decir, si la congruencia $x^3 \equiv \alpha \pmod \pi$ tiene solución en $\mathbb{Z}[\zeta_3]$).

Ejercicio 1.21. Verifique sin computadora si la congruencia

$$x^3 \equiv 2 - 3\zeta_3 \pmod{23}$$

tiene solución en $\mathbb{Z}[\zeta_3]$.
Sugerencia: en total en $(\mathbb{Z}[\zeta_3]/(23))^\times$ *habrá* $\frac{23^2-1}{3} = 177$ *cubos y no es una buena idea enumerarlos uno por uno...*
En general, dado un primo racional $p \equiv 2 \pmod 3$, ¿cuándo $2+3\zeta_3$ es un cubo módulo p?

Ejercicio 1.22 ([Nag1964])**.** Demuestre que la ecuación $x^3 + y^3 = 3z^3$ no tiene soluciones $x, y, z \in \mathbb{Z}[\zeta_3]$ con $z \neq 0$.

*En este caso particular, $N_{K/\mathbb{Q}}(\alpha) = \alpha\,\sigma(\alpha)$, donde $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$.

Ecuación $y^2 = x^3 + t$

Ejercicio 1.23. Demuestre que si $a \neq 0$ es par, entonces en el anillo $\mathbb{Z}[\sqrt{-19}]$

$$(a + \sqrt{-19}, a - \sqrt{-19}) = \mathbb{Z}[\sqrt{-19}].$$

(Lo ocupamos en nuestro análisis de la ecuación $y^2 = x^3 - 19$.)

Ejercicio 1.24. Encuentre las soluciones enteras de $y^2 = x^3 - 4$.
Sugerencia: $y^2 + 4 = (y + 2i)(y - 2i)$.

Ecuación de Pell y grupos $\mathbb{Z}[\sqrt{d}]^\times$ y $\mathbb{Z}\left[\frac{\sqrt{d}}{2}\right]^\times$

Ejercicio 1.25. Sea $d > 1$ un entero libre de cuadrados. Demuestre que si la ecuación $x^2 - dy^2 = -1$ tiene soluciones enteras, entonces $x^2 - dy^2 = +1$ también tiene soluciones enteras.

Ejercicio 1.26. Consideremos la ecuación $x^2 - 3y^2 = n$ para

$$n = 2, 3, 4, 5, 6, 7, 8, 9, 10.$$

¿Para cuáles de estos n existen soluciones enteras? Demuestre que en este caso hay un número infinito de ellas.

Ejercicio 1.27. Demuestre que todas las soluciones de la ecuación $x^2 - 3y^2 = 1$ con $x, y \geq 0$ enteros vienen dadas por la recurrencia

$$(a_0, b_0) = (1, 0), \quad (a_1, b_1) = (2, 1),$$
$$(a_n, b_n) = 4(a_{n-1}, b_{n-1}) - (a_{n-2}, b_{n-2}) \text{ para } n \geq 2.$$

Ejercicio 1.28. Describa las soluciones enteras de las ecuaciones

$$x^2 - dy^2 = +1 \quad \text{y} \quad x^2 - dy^2 = -1,$$

donde $d = 2$ y 5.

Ejercicio 1.29. Consideremos el anillo $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

a) Encuentre la unidad más pequeña $u \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]^\times$ tal que $u > 1$.

b) Encuentre el índice de subgrupo $\left[\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]^\times : \mathbb{Z}[\sqrt{5}]^\times\right]$.

Ejercicio 1.30. Consideremos el anillo ciclotómico $\mathbb{Z}[\zeta_5]$.

a) Demuestre que $u = 1 + \zeta_5$ es una unidad en el anillo y el subgrupo de $\mathbb{Z}[\zeta_5]^\times$ generado por u es infinito. En realidad, $\mathbb{Z}[\zeta_5]^\times \cong \mu_{10}(\mathbb{C}) \times \langle u \rangle$, pero lo probaremos más adelante en el curso.

b) Demuestre que $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \subset \mathbb{Z}[\zeta_5]$ y calcule el índice $\left[\mathbb{Z}[\zeta_5]^\times : \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]^\times\right]$.

Capítulo 2

Aritmética de ideales

La idea de Richard Dedekind consistía en remplazar las operaciones aritméticas con elementos $\alpha \in R$ por las operaciones con ideales $I \subseteq R$. Los anillos de números donde este programa funciona sin obstáculos se conocen como **dominios de Dedekind**. Los vamos a definir en este capítulo. Una gran parte del material de abajo se encuentra en los libros de texto de álgebra conmutativa. Recomiendo consultar [AM1969] y [Rei1995].

2.1 Operaciones con ideales

Clase 5
24/08/20

Sea R un anillo conmutativo. Ya hemos hablado de ideales principales en el primer capítulo. En general, el ideal generado por elementos $\alpha_1, \ldots, \alpha_n \in R$ viene dado por

$$(\alpha_1, \ldots, \alpha_n) = \{c_1\alpha_1 + \cdots + c_n\alpha_n \mid c_1, \ldots, c_n \in R\}.$$

Los ideales de esta forma se llaman **finitamente generados**.

2.1.1. Definición. Para los ideales $I, J \subseteq R$ podemos considerar las siguientes operaciones.

- La **suma**
$$I + J = \{\alpha + \beta \mid \alpha \in I,\ \beta \in J\}$$
es el ideal generado por los elementos de I y J; en otras palabras, el ideal más pequeño que contiene a I e J.

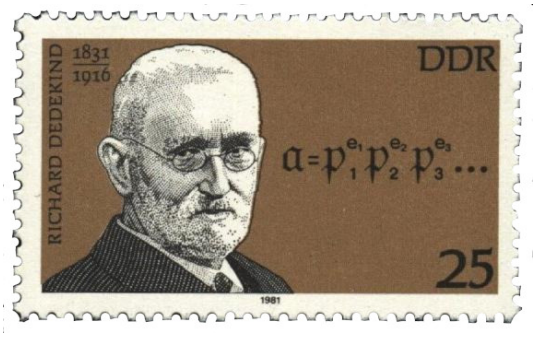


Figura 2.1: Estampilla de la República Democrática Alemana dedicada a Dedekind

En términos de generadores,

$$(\alpha_1, \ldots, \alpha_m) + (\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n).$$

- El **producto**

$$IJ = \Big\{ \sum_{1 \le i \le n} \alpha_i \beta_i \;\Big|\; n \ge 0,\ \alpha_i \in I,\ \beta_i \in J \Big\}$$

es el ideal generado por los productos $\alpha\beta$, donde $\alpha \in I$, $\beta \in J$. En términos de generadores,

$$(\alpha_1, \ldots, \alpha_m) \cdot (\beta_1, \ldots, \beta_n) = (\alpha_i \beta_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}.$$

Notamos que se cumple $IJ \subseteq I \cap J$.

Es fácil verificar que $+$ y $\cdot$ son operaciones asociativas y conmutativas sobre ideales. Tenemos

$$I + (0) = I,\ I + R = R,\ I \cdot (0) = (0),\ I \cdot R = I.$$

Además, se cumple la distributividad

$$(I + J)H = IH + JH$$

—dejo al lector verificar la doble inclusión.

Ya que hemos definido productos, podemos definir las potencias de la manera habitual:

$$I^0 = R, \quad I^1 = I, \quad I^2 = I \cdot I, \quad I^3 = I \cdot I \cdot I, \quad \ldots$$

Estas nos dan una cadena descendiente

$$R \supseteq I \supseteq I^2 \supseteq I^3 \supseteq \cdots$$

2.1.2. Comentario. Cuidado: los elementos de I^n no son productos de n elementos de I (y mucho menos potencias α^n para $\alpha \in I$), sino *sumas* de productos

$$\sum_{i_1, \ldots, i_n} \alpha_{i_1} \cdots \alpha_{i_n}.$$

Por ejemplo, en el anillo de polinomios $\mathbb{Z}[x]$, consideremos el ideal $I = (p, x)$. Entonces $p^2 + x^2 \in I$, pero este elemento no es de la forma fg con $f, g \in I$.

Notamos que si $J = IH$ para algún H, entonces se tiene $J \subseteq H$. Además, para los ideales principales se cumple

$$\alpha \mid \beta \iff (\alpha) \supseteq (\beta).$$

Esto justifica de alguna manera la siguiente definición.

2.1.3. Definición. Se dice que I divide a J (notación $I \mid J$) si $J \subseteq I$.

Sin embargo, hay que tener cuidado: en general no es cierto que $J \subseteq I$ siempre implica que $J = IH$ para algún ideal H. Vamos a ver un ejemplo particular un poco más adelante.

2.1.4. Definición. Se dice que dos ideales $I, J \subseteq R$ son **coprimos** si $I + J = R$.

2.1.5. Comentario. La motivación detrás del término «coprimo» es la siguiente: en un dominio de ideales principales (!) se tiene

$$(\alpha) + (\beta) = (\alpha, \beta) = (\gamma), \quad \text{donde } \gamma = \operatorname{mcd}(\alpha, \beta).$$

Entonces, $\operatorname{mcd}(\alpha, \beta) = 1$ implica que $(\alpha) + (\beta) = R$.

En general (si R no es un dominio de ideales principales), esto es falso. Por ejemplo, en el anillo de polinomios $k[x,y]$ se tiene $\text{mcd}(x,y)=1$: los polinomios x e y claramente no tienen divisor en común (excepto constantes $c\neq 0$). Por otra parte, $(x,y)\neq k[x,y]$; de hecho, $k[x,y]/(x,y)\cong k$.

Otro ejemplo, más relacionado con lo que estamos estudiando: en el anillo $\mathbb{Z}[\sqrt{-5}]$ consideremos el ideal $(2,1+\sqrt{-5})$. Sus dos generadores 2 y $1+\sqrt{-5}$ son elementos irreducibles no asociados entre sí, y por ende no tienen divisor en común. Sin embargo, no es difícil verificar que el ideal en cuestión es propio (y de hecho no es principal).

Ahora bien, ¿para qué sirven los ideales y operaciones aritméticas con ellos? En el capítulo anterior hemos usado en algunas ocasiones que en un dominio de factorización única, si $\text{mcd}(\alpha,\beta)=1$ y $\alpha\beta=\gamma^n$, entonces α y β (salvo un múltiplo invertible) son n-ésimas potencias: $\alpha\sim\alpha'^n$ y $\beta\sim\beta'^n$.

Si no hay factorización única, esta propiedad falla.

2.1.6. Ejemplo. Ya hemos notado que en el anillo $\mathbb{Z}[\sqrt{-5}]$ se tiene

$$(2+3\sqrt{-5})\,(2-3\sqrt{-5})=7^2,$$

donde $2\pm 3\sqrt{-5}$ no es un cuadrado. Para corregir este defecto, se puede pasar a los ideales. Pongamos

$$I=(2+3\sqrt{-5}),\quad J=(2-3\sqrt{-5}),\quad H=(7).$$

Tenemos

$$I+J=R,\quad IJ=H^2.$$

Ahora

$$(I+H)^2=I^2+IH+H^2=I\,(I+H+J)=I,$$

usando que $I+J=R$. De manera simétrica, $(J+H)^2=J$. Entonces, aunque los números $2\pm 3\sqrt{-5}$ no son cuadrados, los ideales principales generados por ellos sí lo son:

$$(7,2\pm 3\sqrt{-5})^2=(2\pm 3\sqrt{-5}).$$

El único detalle es que el ideal $(7,2\pm 3\sqrt{-5})$ no es principal; de manera contraria, tendríamos $2\pm 3\sqrt{-5}=\pm\alpha^2$ para algún α, pero no es el caso. ▲

El truco de arriba funciona en general.

2.1.7. Proposición. *Sean I,J dos ideales tales que $I+J=R$ e $IJ=H^n$. Entonces, $(I+H)^n=I$.*

Demostración. Primero una observación: si $I+J=R$, entonces $I^m+J=R$ para todo m. En efecto,

$$R=(I+J)^m=I^m+\underbrace{I^{m-1}J+\cdots+IJ^{m-1}+J^m}_{\subseteq J}\subseteq I^m+J.$$

Ahora

$$\begin{aligned}(I+H)^n&=I^n+I^{n-1}H+\cdots+IH^{n-1}+H^n\\&=I^n+I^{n-1}H+\cdots+IH^{n-1}+IJ\\&=I\,(I^{n-1}+I^{n-2}H+\cdots+H^{n-1}+J)\\&=I,\end{aligned}$$

usando que $I^{n-1}+J=R$. ■

Para terminar con la aritmética básica de ideales, revisemos el teorema chino del resto. En un dominio de ideales principales este nos dice que si $\text{mcd}(\alpha,\beta)=1$, entonces

$$R/(\alpha\beta)\cong R/(\alpha)\times R/(\beta).$$

En un anillo general, hay que considerar ideales coprimos. Primero hagamos una pequeña observación

2.1.8. Lema. *Si $I+J=R$, entonces $I\cap J=IJ$.*

Demostración. Tenemos $IJ\subseteq I\cap J$ en cualquier caso. Ahora si $I+J=R$, escribamos $1=\alpha+\beta$ para $\alpha\in I$, $\beta\in J$. Para todo $\gamma\in I\cap J$ se tiene entonces

$$\gamma=\gamma(\alpha+\beta)=\gamma\alpha+\gamma\beta\in IJ.$$

Esto demuestra la otra inclusión. ■

Ahora el teorema chino del resto para anillos conmutativos es el siguiente resultado.

2.1.9. Teorema (chino del resto). *Sean $I,J\subseteq R$ ideales tales que $I+J=R$. Luego, hay un isomorfismo natural*

$$\begin{aligned} R/(IJ) &\xrightarrow{\cong} R/I\times R/J,\\ \alpha+IJ &\mapsto (\alpha+I,\alpha+J).\end{aligned}$$

Demostración. Consideremos el homomorfismo

$$\phi\colon R\to R/I\times R/J,\quad x\mapsto(x+I,x+J).$$

Vamos a ver que es sobreyectivo y su núcleo es igual a IJ.

Para ver la sobreyectividad, necesitamos probar que para cualesquiera $\alpha,\beta\in R$ existe $x\in I$ tal que

$$x\equiv\alpha\pmod I,\quad x\equiv\beta\pmod J.$$

De nuevo, dado que $I+J=R$, escribamos $a+b=1$ para $a\in I$, $b\in J$. Notamos que

$$a\equiv 0\pmod I,\quad a\equiv 1\pmod J,\quad b\equiv 1\pmod I,\quad b\equiv 0\pmod J.$$

Se ve que funcionará el elemento

$$x=b\alpha+a\beta.$$

En fin, está claro que $\ker\phi=I\cap J$, y por el lema anterior $I\cap J=IJ$. ■

2.1.10. Comentario. La condición $I+J=R$ es necesaria para la prueba. Por ejemplo, si $I=J=2\mathbb{Z}$, entonces $\mathbb{Z}/4\mathbb{Z}\ncong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

De manera similar, se puede probar que para una familia de ideales $I_1,\dots,I_n$ tales que $I_i+I_j=R$ para $i\neq j$, se tiene un isomorfismo natural

$$R/(I_1\cdots I_n)\cong R/I_1\times\cdots\times R/I_n$$

(he tomado $n=2$ en la prueba se arriba solo para simplificar la notación).

2.1.11. Ejemplo. Para un primo racional $p\equiv 1\pmod 4$ se tiene $p=\pi\overline{\pi}$ en $\mathbb{Z}[i]$. Ya que se trata de un dominio de ideales principales, se tiene

$$(\pi)+(\overline{\pi})=(\operatorname{mcd}(\pi,\overline{\pi}))=\mathbb{Z}[i],$$

así que por el teorema chino del resto

$$\mathbb{Z}[i]/(p)\cong\mathbb{Z}[i]/(\pi)\times\mathbb{Z}[i]/(\overline{\pi})\cong\mathbb{F}_p\times\mathbb{F}_p.$$

Otro modo de ver qué está pasando: tenemos

$$\mathbb{Z}[i]\cong\mathbb{Z}[x]/(x^2+1),\quad \mathbb{Z}[i]/(p)\cong\mathbb{F}_p[x]/(x^2+1).$$

Ahora x^2+1 es irreducible o reducible en $\mathbb{F}_p[x]$ dependiendo del símbolo de Legendre $\left(\frac{-1}{p}\right)=\pm 1$. Cuando es reducible módulo p impar, salen dos diferentes factores lineales $x\pm a$, donde $a^2\equiv -1\pmod p$. ▲

2.2 Ideales primos y maximales

El concepto que remplaza la noción de elemento primo es el de *ideal* primo.

2.2.1. Definición. Se dice que un ideal $\mathfrak{p} \subset R$ es **primo** si este cumple una de las siguientes propiedades equivalentes:[*]

a) $\mathfrak{p} \neq R$ y si $\alpha\beta \in \mathfrak{p}$, entonces $\alpha \in \mathfrak{p}$ o $\beta \in \mathfrak{p}$;

a′) $\mathfrak{p} \neq R$ y si $IJ \subseteq \mathfrak{p}$, entonces $I \subseteq \mathfrak{p}$ o $J \subseteq \mathfrak{p}$;

b) el anillo cociente $R/\mathfrak{p}$ es un dominio.

El conjunto de los ideales primos en R se llama el **espectro** de R y se denota por

$$\operatorname{Spec} R = \{\mathfrak{p} \subset R \mid \text{ ideal primo}\}.$$

Se dice que un ideal $\mathfrak{m} \subset R$ es **maximal** si este cumple una de las siguientes propiedades equivalentes:[**]

a) $\mathfrak{m} \neq R$ y si $\mathfrak{m} \subseteq I \subseteq R$, entonces $I = \mathfrak{m}$ o $I = R$;

b) el anillo cociente $R/\mathfrak{m}$ es un campo.

(Por la definición, el anillo nulo $R = 0$ no se considera como un dominio, mucho menos como un campo.)

2.2.2. Proposición. *Todo ideal maximal es primo.*

Demostración. Está claro de la caracterización b). ■

2.2.3. Ejemplo. Si R es un dominio de ideales principales, entonces los ideales primos son

$$\operatorname{Spec} R = \{(0)\} \cup \{(\pi) \mid \pi \in R \text{ es primo}\}.$$

Los ideales de la forma (π) son maximales, dado que $R/(\pi)$ es un campo.

Para verlo, notamos que el ideal principal $(\pi) \subset R$ es primo si y solamente si $\pi \in R$ es un elemento primo en el sentido del capítulo anterior. En particular,

$$\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{(2), (3), (5), (7), (11), \ldots\}.$$ ▲

2.2.4. Ejemplo. En el anillo $\mathbb{Z}[\sqrt{-5}]$ consideremos los ideales

$$\mathfrak{p} = (7, 3 + \sqrt{-5}), \quad \overline{\mathfrak{p}} = (7, 3 - \sqrt{-5}).$$

Los ideales en cuestión no son principales: primero, analizando las normas se ve que 7 y $3 \pm \sqrt{-5}$ son elementos irreducibles no asociados (las unidades son ± 1). Luego, si $\mathfrak{p} = (\gamma)$, podemos considerar las expresiones

$$7 = \alpha\gamma, \quad 3 + \sqrt{-5} = \beta\gamma$$

para llegar a una contradicción. Dejo al lector los detalles.

Estos ideales son coprimos:

$$1 = 7 - (3 + \sqrt{-5}) - (3 - \sqrt{-5}) \in \mathfrak{p} + \overline{\mathfrak{p}}.$$

[*] Ejercicio: a) $\iff$ a′) $\iff$ b).

[**] Ejercicio: a) $\iff$ b).

Su producto viene dado por

$$\begin{aligned}\mathfrak{p}\overline{\mathfrak{p}} &= (7, 3+\sqrt{-5})\,(7, 3-\sqrt{-5}) \\ &= \left(7^2, 7\,(3+\sqrt{-5}), 7\,(3-\sqrt{-5}), 14\right) \\ &= (7)\,(\underbrace{7, 3+\sqrt{-5}, 3-\sqrt{-5}, 2}_{=R}) = (7).\end{aligned}$$

Los ideales $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son propios. Por ejemplo, si $\mathfrak{p} = \mathbb{Z}[\sqrt{-5}]$, entonces para algunos $a, b, c, d \in \mathbb{Z}$ se tiene

$$1 = (a+b\sqrt{-5})\cdot 7 + (c+d\sqrt{-5})\cdot(3+\sqrt{-5}) = (7a+3c+3d) + (7b+c+d)\sqrt{-5}.$$

De la ecuación $7b+c+d=0$ podemos expresar $d=-7b-c$, y luego al sustituirlo en $1 = 7a+3c+3d$ nos queda $1 = 7a-21b$, pero el número a la derecha es par.

Otra manera más lista es notar que el grupo

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q}) = \{1, \sigma\},$$

donde $\sigma\colon \sqrt{-5} \mapsto -\sqrt{-5}$, actúa sobre $\mathbb{Z}[\sqrt{-5}]$. Para un ideal $I \subset \mathbb{Z}[\sqrt{-5}]$ el conjunto $\sigma(I)$ es también un ideal, y además, en términos de generadores,

$$\sigma(\alpha_1, \ldots, \alpha_n) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n)).$$

En nuestro caso particular se tiene $\overline{\mathfrak{p}} = \sigma(\mathfrak{p})$. Ahora si $\mathfrak{p} = \mathbb{Z}[\sqrt{-5}]$, entonces también $\overline{\mathfrak{p}} = \mathbb{Z}[\sqrt{-5}]$, pero en este caso $\mathfrak{p}\,\overline{\mathfrak{p}} = \mathbb{Z}[\sqrt{-5}]$, lo que contradice nuestro cálculo de arriba.

Los ideales $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son maximales. Para verlo, podemos considerar el homomorfismo sobreyectivo

$$\phi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_7[x]/(3+x), \quad a+b\sqrt{-5} \mapsto a+b\overline{x}.$$

(Note que $3^2 \equiv -5 \pmod 7$.) Tenemos $\ker\phi = \mathfrak{p}$, y este ideal es maximal. De manera similar se define un homomorfismo sobreyectivo

$$\overline{\phi}\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_7[x]/(3-x),$$

donde $\ker\overline{\phi} = \overline{\mathfrak{p}}$.

Notamos que en general, un homomorfismo $\phi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_7$ está definido por la imagen de $\sqrt{-5}$ que debe cumplir $\phi(\sqrt{-5})^2 = -5$ en $\mathbb{F}_p$. Las únicas posibilidades son $\phi(\sqrt{-5}) = \pm 3$, así que hemos encontrado los únicos dos ideales maximales que cumplen $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{F}_7$.

El teorema chino del resto nos da en este caso

$$\begin{array}{ccccc}
\mathbb{Z}[\sqrt{-5}]/(7) & \cong & \mathbb{Z}[\sqrt{-5}]/\mathfrak{p} & \times & \mathbb{Z}[\sqrt{-5}]/\overline{\mathfrak{p}} \\
\downarrow\cong & & \downarrow\cong & & \downarrow\cong \\
\mathbb{F}_7[x]/(x^2+5) & \cong & \mathbb{F}_7[x]/(3+x) & \times & \mathbb{F}_7[x]/(3-x) \\
 & & \downarrow\cong & & \downarrow\cong \\
 & & \mathbb{F}_7 & \times & \mathbb{F}_7
\end{array}$$

▲

2.2.5. Proposición. *Un homomorfismo de anillos $\phi\colon S \to R$ induce una aplicación natural entre los espectros*

$$\phi^{-1}\colon \operatorname{Spec} R \to \operatorname{Spec} S, \quad \mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p}).$$

Demostración. Verifique si $\mathfrak{p} \subset R$ es un ideal primo, entonces $\phi^{-1}(\mathfrak{p})$ es un ideal primo en S. ■

2.2.6. Ejemplo. La inclusión natural $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-5}]$ induce una aplicación $\operatorname{Spec}\mathbb{Z}[\sqrt{-5}] \to \operatorname{Spec}\mathbb{Z}$ dada por $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathbb{Z}$. En el ejemplo de arriba,

$$(7, 3 \pm \sqrt{-5}) \cap \mathbb{Z} = 7\mathbb{Z}. \qquad \blacktriangle$$

También nos servirá la siguiente propiedad.

2.2.7. Proposición. *Dado un ideal propio $I \subsetneq R$, existe un ideal maximal $\mathfrak{m} \subset R$ tal que $I \subseteq \mathfrak{m}$.*

Demostración. Esta es una aplicación típica del lema de Zorn.

Sea $\mathcal{P}$ el conjunto de los ideales propios $I \subseteq J_\alpha \subsetneq R$ parcialmente ordenado respecto a la inclusión $J_\alpha \subseteq J_\beta$. Un elemento maximal en $\mathcal{P}$ sería precisamente un ideal maximal en R que contiene a I. Para deducir la existencia de un elemento maximal, tenemos que probar que toda cadena en $\mathcal{P}$ es acotada.

Una cadena en $\mathcal{P}$ es una colección de ideales propios $\mathcal{S} = \{J_\alpha \mid I \subseteq J_\alpha\}$ donde $J_\alpha \subseteq J_\beta$ o $J_\beta \subseteq J_\alpha$ para cualesquiera α y β. La unión $J = \bigcup_\alpha J_\alpha$ es también un ideal propio en R. Este ideal J nos da una cota superior para $\mathcal{S}$. ■

2.3 Ideales en anillos de números

Sea R un anillo de números.

2.3.1. Lema. *Para todo ideal no nulo $I \subseteq R$ se tiene $I \cap \mathbb{Z} \neq (0)$.*

Demostración. Si $\alpha \in I$ es un elemento no nulo, entonces α, siendo un número algebraico (!), satisface una relación algebraica no trivial

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in \mathbb{Z}$, y sin pérdida de generalidad, $a_0 \neq 0$. Entonces, $a_0 \in I$. ■

2.3.2. Corolario. *Para todo ideal primo no nulo $\mathfrak{p} \subset R$ se tiene $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para algún primo racional p.*

Demostración. La intersección $\mathfrak{p} \cap \mathbb{Z}$ debe ser un ideal primo no nulo en $\mathbb{Z}$. ■

2.3.3. Teorema. *Para todo ideal no nulo $I \subset R$ el cociente R/I es finito.*

Demostración. Consideremos R/I como un grupo abeliano ($\mathbb{Z}$-módulo). Un subgrupo finitamente generado de R/I corresponde a un subgrupo finitamente generado $M \subseteq R$ tal que $I \subseteq M$.

Dado que $M \subset K$, donde $K/\mathbb{Q}$ es un campo de números, M no tiene torsión y por ende es un $\mathbb{Z}$-módulo libre de rango r:

$$M \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r}.$$

Notamos que más de $[K : \mathbb{Q}]$ elementos de M tendrían una dependencia $\mathbb{Q}$-lineal (¡y luego $\mathbb{Z}$-lineal!) no trivial. Esto implica que $r \leq [K : \mathbb{Q}]$.

Denotemos por M/I la imagen de M en el cociente R/I. Como vimos arriba, $n \in I$ para algún entero $n > 0$, y luego

$$\#(M/I) \leq \#(M/(n)) \leq n^{[K:\mathbb{Q}]}.$$

Entonces, acabamos de probar que todo subgrupo finitamente generado $M/I \subset R/I$ es finito, y además $\#(M/I) \leq C$ para cierta constante C que no depende de M. Esto significa que R/I es finito. ■

2.3.4. Comentario. Los argumentos de arriba usan que R es un anillo de números. Sino, podemos tomar por ejemplo $R = \mathbb{Z}[x]$ y el ideal $\mathfrak{p} = (x)$. Se tiene entonces $R/\mathfrak{p} \cong \mathbb{Z}$ y $\mathfrak{p} \cap \mathbb{Z} = (0)$.

En este caso $R \subset K$, donde $K = \mathbb{Q}(x)$, pero la extensión $K/\mathbb{Q}$ es infinita de grado de trascendencia 1.

Clase 6
26/08/20

Después de definir el anillo de enteros $\mathcal{O}_K$, vamos a establecer algunas de sus propiedades básicas.

2.3.5. Corolario. *Todo anillo de números R es noetheriano.*

Demostración. Para dos ideales no nulos $I \subsetneq J \subseteq R$ tenemos un homomorfismo sobreyectivo natural $R/I \twoheadrightarrow R/J$, y luego $\#(R/J) < \#(R/I) < \infty$. Esto implica que no puede existir una cadena infinita ascendente

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$$

■

2.3.6. Corolario. *Todo ideal primo no nulo $\mathfrak{p} \subset R$ es maximal.*

Demostración. El anillo cociente $R/\mathfrak{p}$ es un dominio finito, pero recordemos que todo dominio finito es un campo.[*] ■

2.3.7. Corolario. *Si para dos ideales primos no nulos $\mathfrak{p}, \mathfrak{q} \subset R$ se tiene $\mathfrak{p} \subseteq \mathfrak{q}$, entonces $\mathfrak{p} = \mathfrak{q}$.*

2.3.8. Definición. Para un anillo conmutativo R la **dimensión de Krull** viene dada por

$$\dim R = \sup\{n \mid \text{existe una cadena de ideales primos } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq p_n \subset R\}.$$

Por ejemplo, todo campo k tiene el único ideal (0), así que $\dim k = 0$.

Si R es un anillo de números que no es un campo, entonces $\dim R = 1$ por lo que acabamos de probar: la cadena más larga de ideales primos tiene forma $(0) \subsetneq \mathfrak{p} \subset R$. Esto significa que R es un objeto unidimensional, y esto explica muchas buenas propiedades.

2.3.9. Ejemplo. En general, se puede probar que para los anillos de polinomios

$$\dim R[x_1, \ldots, x_n] = \dim R + n.$$

En particular, si k es un campo, $\dim k[x_1, \ldots, x_n] = n$. Esto corresponde al hecho geométrico de que el espacio afín $\mathbb{A}^n(k)$ tiene dimensión n.

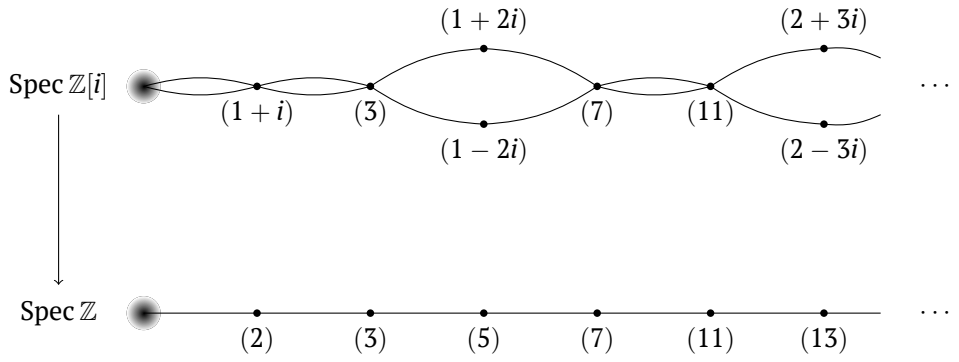
De la misma manera, $\dim \mathbb{Z}[x] = 2$, dado que $\dim \mathbb{Z} = 1$.

Para más información sobre la dimensión de Krull, véanse los libros de texto de álgebra conmutativa. ▲

Ahora bien, dado un anillo de números $R \subset K$ y un ideal primo no nulo (= maximal) $\mathfrak{p} \subset R$, tenemos $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$ para algún primo racional p, y el **campo residual** $R/\mathfrak{p}$ es una extensión de $\mathbb{F}_p$ de grado finito $f_\mathfrak{p} \leq [K : \mathbb{Q}]$.

$$\begin{array}{ccccc} \mathfrak{p} & \subset & R & \twoheadrightarrow & R/\mathfrak{p} \\ & & \big| & & \big| f_\mathfrak{p} \\ \mathfrak{p} \cap \mathbb{Z} = (p) & \subset & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \end{array}$$

2.3.10. Ejemplo. El siguiente dibujo representa los ideales primos en el anillo $R = \mathbb{Z}[i]$ a través de la aplicación $\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$. Aquí todo primo no nulo $\mathfrak{p} \subset R$ está sobre algún primo racional $p \in \mathbb{Z}$. Los «puntos gruesos» en el dibujo representan los ideales primos nulos (0).



[*] Si D es un dominio finito, entonces para todo elemento no nulo $a \in D$ la multiplicación por a

$$\mu_a : D \to D, \quad x \mapsto ax$$

es una aplicación inyectiva. Dado que D es finito, μ_a es también sobreyectiva y existe $a^{-1} \in D$ tal que $\mu_a(a^{-1}) = aa^{-1} = 1$.

Lo que vimos en el capitulo anterior puede ser resumido de la siguiente manera.

1) Se tiene $2\mathbb{Z}[i] = \mathfrak{p}^2$, donde $\mathfrak{p} = (1+i)$. En este caso $f = 1$.

2) Si $p \equiv 1 \pmod 4$, entonces $p\mathbb{Z}[i] = \mathfrak{p}\,\overline{\mathfrak{p}}$ para dos diferentes primos $\mathfrak{p}, \overline{\mathfrak{p}}$. Aquí $f_{\mathfrak{p}} = f_{\overline{\mathfrak{p}}} = 1$.

3) Si $p \equiv 3 \pmod 4$, entonces $p\mathbb{Z}[i]$ es primo, y en este caso $f = 2$. ▲

2.4 Ideales fraccionarios

Hemos visto cómo sumar y multiplicar los ideales. Estas operaciones cumplen varias propiedades parecidas a los axiomas de anillo conmutativo, pero para un ideal I no existe el ideal «$-I$» que cumpliría $I + (-I) = (0)$. De hecho, no hay manera razonable de añadirlo: en ese caso la identidad $I + I = I$ implicaría que $R = (0)$. Pero lo que sí se puede tratar de hacer es añadir los ideales inversos I^{-1} que cumplen $II^{-1} = R$.

Por ejemplo, el ideal inverso a $2\mathbb{Z} \subset \mathbb{Z}$ debería de ser algo como $\frac{1}{2}\mathbb{Z}$, pero $\frac{1}{2}$ no vive en $\mathbb{Z}$, sino en su campo de fracciones $\mathbb{Q}$. Esto nos lleva a la noción de ideales fraccionarios.

Aunque el material de la sección anterior es válido para cualquier anillo conmutativo, pero a partir de ahora tendremos que suponer que R es un dominio. Denotemos por K el campo de fracciones de R.

2.4.1. Definición. Un R-**ideal fraccionario** es un R-submódulo $I \subseteq K$ que cumple la siguiente propiedad: existe $\alpha \in K^\times$ tal que $\alpha I \subseteq R$.

Se dice que I es **principal** si $I = \alpha R$ para algún $\alpha \in K^\times$.

Si $I \subseteq R$, entonces I es un ideal en el sentido normal, y para subrayar este hecho se dice que I es un ideal **entero**.

La condición $\alpha I \subseteq R$ significa lo siguiente: aunque en I pueden estar fracciones, sus denominadores deben ser controlables y cancelarse al multiplicar I por un solo elemento.

2.4.2. Ejemplo. Consideremos $R = \mathbb{Z}$. En este caso $K = \mathbb{Q}$. Si αI es un subgrupo de $\mathbb{Z}$, entonces $\alpha I = n\mathbb{Z}$ para algún número natural n. Luego, $I = \alpha^{-1} n\mathbb{Z}$, donde $\alpha^{-1} n \in \mathbb{Q}$. Entonces, los ideales fraccionarios de $\mathbb{Z}$ son de la forma $\frac{a}{b}\mathbb{Z}$, donde $\frac{a}{b} \in \mathbb{Q}$. Todos son principales.

Hay muchos más $\mathbb{Z}$-submódulos $I \subseteq \mathbb{Q}$, como por ejemplo $\mathbb{Z}\left[\frac{1}{2}\right]$, pero estos no cumplen la condición $\alpha I \subseteq \mathbb{Z}$. ▲

El ejemplo de arriba funciona de manera similar en cualquier dominio de ideales principales.

Las operaciones $I + J$, $I \cap J$, IJ definidas para los ideales enteros en la sección anterior se definen de la misma manera para los ideales fraccionarios (se deja como un ejercicio verificar que el resultado es también un ideal fraccionario).

2.4.3. Definición. Se dice que un R-ideal fraccionario I es **invertible** si existe otro ideal fraccionario J tal que $IJ = R$.

2.4.4. Proposición. *Si I es invertible, entonces su inverso es igual a*

$$I^{-1} = \{\alpha \in K \mid \alpha I \subseteq R\}.$$

Entonces, I es invertible si y solamente si $II^{-1} = R$.

Demostración. Notamos que $II^{-1} \subseteq R$. Ahora si $IJ = R$, entonces se ve que $J \subseteq I^{-1}$. Por otra parte, $I^{-1} = I^{-1} \cdot IJ = (I^{-1}I) \cdot J \subseteq RJ = J$. ■

2.4.5. Ejemplo. Todo ideal fraccionario principal es invertible: para $\alpha \in K^\times$ se tiene $(\alpha R)^{-1} = \alpha^{-1} R$. ▲

No todos los ideales en un anillo de números es invertible. He aquí un ejemplo particular.

2.4.6. Ejemplo. Consideremos el ideal $\mathfrak{p} = (2, 1+\sqrt{-3})$ en el anillo $R = \mathbb{Z}[\sqrt{-3}]$. Se tiene $R/\mathfrak{p} \cong \mathbb{F}_2$, así que se trata de un ideal maximal. Su inverso tendría que ser

$$\mathfrak{p}^{-1} = \{\alpha \in \mathbb{Q}(\sqrt{-3}) \mid 2\alpha \in \mathbb{Z}[\sqrt{-3}], (1+\sqrt{-3})\,\alpha \in \mathbb{Z}[\sqrt{-3}]\}.$$

Escribiendo $\alpha = a + b\sqrt{-3}$, notamos que la primera condición significa que $a = a'/2$, $b = b'/2$ para $a', b' \in \mathbb{Z}$. Para la segunda condición, calculamos que

$$(1+\sqrt{-3})\left(\frac{a'}{2} + \frac{b'}{2}\sqrt{-3}\right) = \frac{a'-3b'}{2} + \frac{a'+b'}{2}\sqrt{-3}.$$

Este elemento está en $\mathbb{Z}[\sqrt{-3}]$ si y solamente si $a' \equiv b' \pmod 2$. Podemos concluir que

$$\mathfrak{p}^{-1} = \left\{\frac{a'}{2} + \frac{b'}{2}\sqrt{-3} \;\middle|\; a', b' \in \mathbb{Z}, a' \equiv b'(2)\right\} \overset{\text{Ejercicio}}{=} \mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big].$$

Ahora, usando $\frac{(1+\sqrt{-3})^2}{2} = -1+\sqrt{-3}$, tenemos

$$\mathfrak{p}\mathfrak{p}^{-1} = (2, 1+\sqrt{-3})\left(1, \frac{1+\sqrt{-3}}{2}\right) = (2, 1+\sqrt{-3}, -1+\sqrt{-3}) = \mathfrak{p} \neq R.$$

Por otra parte, en el anillo más grande $\mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big] = \mathbb{Z}[\zeta_3]$ (que es un dominio de ideales principales, como ya sabemos) tenemos $\mathfrak{p} = (2)$. ▲

2.4.7. Definición. Denotemos por $\mathcal{I}(R)$ el grupo de R-ideales fraccionarios invertibles y por $\mathcal{P}(R)$ el subgrupo de R-ideales fraccionarios principales. Luego, el **grupo de Picard** de R es el cociente

$$\mathrm{Pic}(R) = \mathcal{I}(R)/\mathcal{P}(R).$$

Aunque los ideales invertibles forman un grupo abeliano respecto a *multiplicación*, muy a menudo $\mathrm{Pic}(R)$ se escribe en la notación aditiva. La definición puede ser resumida en la **sucesión exacta** de grupos abelianos.

$$1 \to R^\times \to K^\times \xrightarrow{\alpha \mapsto \alpha R} \mathcal{I}(R) \to \mathrm{Pic}(R) \to 0$$

2.4.8. Ejemplo. Para todo dominio de ideales principales se tiene $\mathrm{Pic}(R) = 0$. ▲

2.4.9. Ejemplo. Sea R un **anillo local**; es decir, un anillo con único ideal maximal $\mathfrak{m}$. Afirmamos que en este caso $\mathrm{Pic}(R) = 0$.

Sea I un R-ideal fraccionario invertible. En este caso la ecuación $II^{-1} = R$ significa que se puede escribir

$$\sum_i \alpha_i \beta_i = 1,$$

donde $\alpha_i \in I$ y $\beta_i \in I^{-1}$. Tenemos necesariamente $\alpha_i\beta_i \in R^\times$ para algún i; en el caso contrario $\sum_i \alpha_i\beta_i$ está en el ideal maximal $\mathfrak{m} = R \setminus R^\times$ (es aquí donde estamos usando que R es local). Ahora $\beta_i I = R$, así que $I = (\beta_i^{-1})$ es principal. ▲

Uno de los resultados principales del curso establece la finitud de $\mathrm{Pic}(R)$ para todo orden $R \subset K$. También veremos cómo hacer cálculos particulares.

2.4.10. Ejemplo. Consideremos el anillo $R = \mathbb{Z}[\sqrt{-5}]$. El ideal

$$\mathfrak{p} = (2, 1+\sqrt{-5})$$

no es principal. Por ejemplo, podemos calcular que

$$\mathfrak{p}^2 = (2^2, 2\,(1+\sqrt{-5}), (1+\sqrt{-5})^2) = (2)\,(\underbrace{2, 1+\sqrt{-5}, -2+\sqrt{-5}}_{=R}) = 2R.$$

Ahora si $\mathfrak{p}$ fuera principal, esto nos daría $2 \sim \alpha^2$ para algún α, pero 2 es irreducible en el anillo $\mathbb{Z}[\sqrt{-5}]$.

El ideal es maximal: tenemos $R/\mathfrak{p} \cong \mathbb{F}_2$. De una vez hemos calculado que $\mathfrak{p}$ es invertible: su inverso es

$$\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p} = \left(1, \frac{1+\sqrt{-5}}{2}\right).$$

Dado que $\mathfrak{p}^2 = 2R$ es principal, $[\mathfrak{p}]$ es un elemento de orden 2 en el grupo de Picard. De hecho, $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$, donde $\mathfrak{p}$ representa el generador. Para justificar este calculo necesitamos varias herramientas que veremos más adelante en el curso.

Solo para dar un ejemplo de cómo se comportan los ideales en este caso, $\mathfrak{q} = (3, 1+\sqrt{-5})$ es también un ideal que no es principal. El lector puede verificar que

$$\mathfrak{q}\,\overline{\mathfrak{q}} = 3R, \quad \mathbb{Z}[\sqrt{-5}]/\mathfrak{q} \cong \mathbb{F}_3.$$

Para $\alpha = \frac{1-\sqrt{-5}}{3}$ tenemos

$$(\alpha)\,\mathfrak{q} = \left(\frac{1-\sqrt{-5}}{3}\right)(3, 1+\sqrt{-5}) = (2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5}) = \mathfrak{p}.$$

Entonces, $[\mathfrak{q}] = [\mathfrak{p}]$ en $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}])$. ▲

El grupo de Picard puede ayudar a resolver ecuaciones diofánticas.

2.4.11. Ejemplo. Continuando con el ejemplo anterior, consideremos la curva elíptica

$$y^2 = x^3 - 5.$$

Afirmamos que esta no tiene putos enteros.

Primero, y tiene que ser par. Por ejemplo, reduciendo la ecuación módulo 4, notamos que $x^3 - 5 \not\equiv 1 \pmod 4$. Además, $y \neq 0$.

Como hacíamos antes, empezamos por escribir

$$x^3 = (y - \sqrt{-5})\,(y + \sqrt{-5}).$$

El anillo $\mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, pero vamos a trabajar con ideales en lugar de elementos.

Afirmamos que para $y \neq 0$ par se tiene

$$(y - \sqrt{-5}, y + \sqrt{-5}) = \mathbb{Z}[\sqrt{-5}].$$

Primero calculamos que

$$\left(\frac{y}{2} - \sqrt{-5}\right) \cdot (y + \sqrt{-5}) - \frac{y}{2} \cdot (y - \sqrt{-5}) = 5 \in (y - \sqrt{-5}, y + \sqrt{-5}).$$

Además, está claro que

$$2y \in (y - \sqrt{-5}, y + \sqrt{-5}).$$

Por otro lado, se ve que $5 \nmid y$: para esto considere la ecuación $y^2 = x^3 - 5$ y fíjese en la valuación $v_5(\cdot)$. Tenemos entonces $\mathrm{mcd}(2y, 5) = 1$, así que $(y - \sqrt{-5}, y + \sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$.

Ahora $(y + \sqrt{-5})$ e $(y - \sqrt{-5})$ son ideales coprimos y su producto es $(x)^3$, así que gracias a 2.1.7 debe existir un ideal $I \subset R$ tal que

$$(y + \sqrt{-5}) = I^3$$

Aquí el ideal a la izquierda es principal, así que $[I^3]$ es trivial en $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}])$. Pero sabiendo que el grupo de Picard tiene orden 2, esto nos permite concluir que $[I]$ es trivial; es decir, un ideal principal. Escribiendo $I = (a + b\sqrt{-5})$, se obtiene

$$y + \sqrt{-5} = (a + b\sqrt{-5})^3 = a\,(a^2 - 15\,b^2) + b\,(3a^2 - 5b^2)\,\sqrt{-5}.$$

Pero la ecuación $b\,(3a^2 - 5b^2) = 1$ no tiene soluciones enteras, así que podemos concluir que $y^2 = x^3 + 5$ tampoco tiene soluciones enteras. ▲

Cabe mencionar que en geometría algebraica también existe la noción del grupo de Picard de una curva que se define de manera parecida como el cociente del grupo de divisores por los divisores principales. Véase [Sil2009, Chapter II] o [Lor1996] para mayor información.

2.5 Anillo de enteros $\mathcal{O}_K$

Siguiendo con nuestro programa de llevar la aritmética de elementos $\alpha \in R$ a la aritmética de ideales $I \subset R$, una propiedad que nos gustaría tener es el teorema fundamental de la aritmética que para los ideales quiere decir que todo ideal propio no nulo $I \subset R$ se descompone en producto de ideales primos

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

donde los elementos e_i están definidos de modo único. Desgraciadamente, esto no es siempre posible en un anillo de números.

2.5.1. Ejemplo. Consideremos el anillo $R = \mathbb{Z}[\sqrt{-3}]$ y el ideal $\mathfrak{p} = (2, 1 + \sqrt{-3})$. Calculamos que

$$\mathfrak{p}^2 = (2^2, 2\,(1 + \sqrt{-3}), (1 + \sqrt{-3})^2) = 2R \cdot (2, 1 + \sqrt{-3}, -1 + \sqrt{-3}) = 2R \cdot \mathfrak{p}.$$

Si tuviéramos la factorización única, esto implicaría que $\mathfrak{p} = 2R$. Sin embargo,

$$R \supset \mathfrak{p} \supsetneq 2R \supsetneq \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \mathfrak{p}^4 \supset \cdots \tag{*}$$

Aún peor, el ideal $2R$ no puede ser escrito como un producto de ideales primos. Para verlo, supongamos que para algunos ideales primos $\mathfrak{p}_i$ se cumple

$$2R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Luego, tenemos

$$\mathfrak{p}^2 \subsetneq 2R \subseteq \mathfrak{p}_i.$$

Esto implica que $\mathfrak{p} \subseteq \mathfrak{p}_i$ por la primalidad de $\mathfrak{p}_i$, pero luego $\mathfrak{p}_i = \mathfrak{p}$, dado que $\mathfrak{p}$ es un ideal maximal. Esto significa que $2R = \mathfrak{p}^n$ para algún n, pero esto contradice (*). Entonces, ¡el ideal $2R$ no es un producto de ideales primos! ▲

El ideal $\mathfrak{p}$ de arriba no es invertible, como ya vimos en 2.4.6. Resulta que si queremos descomposiciones en productos de ideales primos, no pueden existir ideales no invertibles.

2.5.2. Proposición. *Sea R un anillo de números donde todo ideal propio no nulo $I \subset R$ puede ser escrito como producto de ideales primos*

$$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Entonces, todo R-ideal fraccionario es invertible.

Demostración. Bajo la hipótesis, bastaría verificar que todo ideal primo no nulo $\mathfrak{p} \subset R$ es invertible. Consideremos un elemento no nulo $\alpha \in \mathfrak{p}$ y la descomposición

$$\alpha R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Los ideales $\mathfrak{p}_i$ son primos no nulos, y entonces maximales. Aquí todos los ideales $\mathfrak{p}_i$ son invertibles:

$$\mathfrak{p}_i^{-1} = \frac{1}{\alpha} R \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_i^{e_i - 1} \cdots \mathfrak{p}_s^{e_s}.$$

Tenemos

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \subseteq \mathfrak{p},$$

pero por la primalidad de $\mathfrak{p}$ y maximalidad de los $\mathfrak{p}_i$, tenemos $\mathfrak{p} = \mathfrak{p}_i$, así que es invertible. ■

Ahora ¿qué defecto tiene el anillo $\mathbb{Z}[\sqrt{-3}]$ que nos da ideales no invertibles? En $\mathbb{Q}(\sqrt{-3}) = \operatorname{Frac} \mathbb{Z}[\sqrt{-3}]$ tenemos el entero algebraico $\alpha = \frac{1+\sqrt{-3}}{2}$: este cumple la relación mónica

$$\alpha^2 - \alpha + 1 = 0.$$

Ahora consideremos el ideal fraccionario

$$I = (1, \alpha).$$

Calculamos que

$$I^2 = (1, \alpha, \alpha^2) = (1, \alpha) = I.$$

Si I fuera invertible, multiplicando esta ecuación por I^{-1} tendríamos $I = R$, pero esto no es el caso. Este truco funciona en general. Será oportuno dar una definición.

2.5.3. Definición. Sea R un dominio. Se dice que $\alpha \in \operatorname{Frac}(R)$ es **entero** sobre R si existe una relación mónica

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in R$. Si todo elemento entero sobre R está en R, entonces se dice que R es **integralmente cerrado**.

Por ejemplo, el anillo $\mathbb{Z}[\sqrt{-3}]$ no es integralmente cerrado porque no contiene el elemento $\frac{1+\sqrt{-3}}{2}$. Resulta que esta es la raíz de los problemas.

2.5.4. Proposición. *Sea R un anillo de números donde todo R-ideal fraccionario es invertible. Entonces, R es integralmente cerrado en* $\operatorname{Frac}(R)$.

Demostración. Sea $\alpha \in \operatorname{Frac}(R)$ un elemento no nulo que satisface una relación mónica

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in R$. Consideremos el ideal fraccionario

$$I = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1}).$$

Gracias a la relación de arriba, toda potencia α^k para $k \geq n$ se expresa como una combinación $\mathbb{Z}$-lineal de $1, \alpha, \ldots, \alpha^n$, y se ve que

$$I^2 = I.$$

Ahora si I es invertible, entonces $I = R$, y en particular $\alpha \in R$. ■

Ahora sabiendo la importancia de anillos integralmente cerrados, vamos a investigar este concepto.

2.5.5. Lema (Caracterización de integralidad). *Sea K un campo y $R \subset K$ un subanillo. Para $\alpha \in K$ las siguientes condiciones son equivalentes.*

a) α *es entero sobre* R.

b) $R[\alpha] \subset K$ *es un* R*-módulo finitamente generado.*

c) Existe un R*-módulo finitamente generado no nulo* $M \subseteq K$ *tal que* $\alpha M \subseteq M$.

Demostración. a)⇒b). Si α es entero sobre R, entonces este cumple una relación mónica

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Gracias a esta relación, α^m para $m \geq n$ se expresa como una combinación R-lineal de $1, \alpha, \ldots, \alpha^{n-1}$ así que estas potencias generan a $R[\alpha]$ como un R-módulo.
b)⇒c). Basta tomar $M = R[\alpha]$.
c)⇒a). Escribamos

$$M = \alpha_1 R + \cdots + \alpha_n R.$$

Consideremos la matriz de multiplicación por α sobre M:

$$\alpha\alpha_i = \sum_{1 \leq j \leq n} a_{ij}\alpha_j.$$

Ahora por el teorema de Cayley–Hamilton,

$$\det(\alpha I_n - A) = 0,$$

pero ese determinante es un polinomio mónico en α con coeficientes en R. ■

2.5.6. Ejemplo. $\alpha = \sqrt{2}$ y $\beta = \frac{1+\sqrt{-5}}{2}$ son enteros algebraicos:

$$\alpha^2 - 2 = 0, \quad \beta^2 - \beta - 1 = 0.$$

El anillo $\mathbb{Z}[\alpha, \beta]$ está generado como $\mathbb{Z}$-módulo por

$$1, \alpha, \beta, \alpha\beta.$$

Calculamos en esta base

$$\begin{aligned}(\alpha+\beta)\cdot 1 &= \alpha + \beta,\\ (\alpha+\beta)\cdot \alpha &= 2 + \alpha\beta,\\ (\alpha+\beta)\cdot \beta &= 1 + \beta + \alpha\beta,\\ (\alpha+\beta)\cdot \alpha\beta &= \alpha + 2\beta + \alpha\beta\end{aligned}$$

Entonces, la multiplicación por $\alpha + \beta$ se representa por la matriz

$$A = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

Calculamos que su polinomio característico es

$$p_A(x) = x^4 - 2x^3 - 5x^2 + 6x - 1.$$

Esto nos da la relación mónica

$$(\alpha+\beta)^4 - 2(\alpha+\beta)^3 - 5(\alpha+\beta)^2 + 6(\alpha+\beta) - 1 = 0.$$

```
? charpoly ([0,2,1,0;1,0,0,1; 1,0,1,2; 0,1,1,1])
% = x^4 - 2*x^3 - 5*x^2 + 6*x - 1
? algdep (sqrt(2) + (1+sqrt(5))/2, 4)
% = x^4 - 2*x^3 - 5*x^2 + 6*x - 1

? K = nfinit(t^2-2);
? L = rnfinit(K, x^2-5);
? rnfeltreltoabs(L, t + (1+x)/2)
% = Mod(-1/4*x^3 + 13/4*x + 1/2, x^4 - 14*x^2 + 9)
? charpoly(%)
% = x^4 - 2*x^3 - 5*x^2 + 6*x - 1
? subst (%, x, sqrt(2) + (1+sqrt(5))/2)
% = -2.115889831480117514 E-37
```

Esta sesión de PARI/GP demuestra el uso de campos de números relativos: definimos $K = \mathbb{Q}(\sqrt{2})$ y luego $L = K(\sqrt{5})$.

Recordamos que el polinomio característico no siempre coincide con el polinomio mínimo. En PARI/GP estos se calculan mediante `charpoly` y `minpoly` respectivamente.

▲

2.5.7. Proposición-definición. *Dado un campo de números K, su* ***anillo de enteros*** *viene dado*

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \textit{ es entero sobre } \mathbb{Z}\}.$$

Este es un anillo. Se tiene

$$\mathcal{O}_K = \{\alpha \in K \mid f^\alpha_{\mathbb{Q}} \in \mathbb{Z}[x]\},$$

donde $f^\alpha_{\mathbb{Q}}$ denota el polinomio mínimo de α sobre $\mathbb{Q}$.

Demostración. Usando el lema de arriba, si $\alpha, \beta \in \mathcal{O}_K$, entonces $M = \mathbb{Z}[\alpha, \beta]$ es un $\mathbb{Z}$-módulo finitamente generado. Tenemos $\alpha \pm \beta \in M$ y $\alpha\beta \in M$.

Si α es entero sobre $\mathbb{Z}$, entonces existe un polinomio mónico $g \in \mathbb{Z}[x]$ tal que $g(\alpha) = 0$. Este polinomio debe ser divisible por el polinomio mínimo $f^\alpha_{\mathbb{Q}} \in \mathbb{Q}[x]$, pero luego $f^\alpha_{\mathbb{Q}}(x) \in \mathbb{Z}[x]$ gracias al lema de Gauss. ■

2.5.8. Comentario. Tal vez la prueba con $\mathbb{Z}$-módulos finitamente generados se ve demasiado abstracta, pero al final de cuentas esta se reduce a las siguientes consideraciones de álgebra lineal. Dados dos números α y β, escribamos sus polinomios mínimos sobre $\mathbb{Q}$:

$$f = (x - \alpha_1) \cdots (x - \alpha_m), \quad g = (x - \beta_1) \cdots (x - \beta_n).$$

Estos son precisamente los polinomios característicos de las aplicaciones $\mathbb{Q}$-lineales

$$\begin{aligned} \mu_\alpha \colon \mathbb{Q}(\alpha) &\to \mathbb{Q}(\alpha), \\ x &\mapsto \alpha x \end{aligned} \qquad \begin{aligned} \mu_\beta \colon \mathbb{Q}(\beta) &\to \mathbb{Q}(\beta), \\ x &\mapsto \beta x. \end{aligned}$$

Ahora la aplicación

$$\mu_\alpha \otimes \mu_\beta \colon \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta)$$

tendrá como sus valores propios $\alpha_i\beta_j$, así que su polinomio característico es

$$\prod_{i,j} (x - \alpha_i\beta_j),$$

mientras que el polinomio característico de la aplicación

$$\mu_\alpha \otimes id + id \otimes \mu_\beta \colon \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}(\beta).$$

será[*]

$$\prod_{i,j} (x - (\alpha_i + \beta_j)).$$

De manera más concreta, μ_α corresponde a alguna matriz $A \in M_{m\times m}(\mathbb{Q})$ y μ_β corresponde a otra matriz $B \in M_{n\times n}(\mathbb{Q})$. Escribiendo polinomios característicos de las matrices $A\otimes B$ y $(A\otimes I_n)+(I_m\otimes B)$ de $(mn\times mn)$, se obtienen relaciones algebraicas para $\alpha\beta$ y $\alpha+\beta$. En fin, si α y β son enteros algebraicos, entonces las matrices A y B tendrán coeficientes enteros, o mejor dicho, en el argumento de arriba se pueden reemplazar los espacios $\mathbb{Q}$-vectoriales $\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\alpha)\otimes_{\mathbb{Q}}\mathbb{Q}(\beta)$ por $\mathbb{Z}$-módulos $\mathbb{Z}[\alpha], \mathbb{Z}[\beta], \mathbb{Z}[\alpha]\otimes_{\mathbb{Z}}\mathbb{Z}[\beta]$. De esta manera saldrán relaciones mónicas con coeficientes enteros.

Por ejemplo, si $\alpha = \sqrt{2}$ y $\beta = \frac{1+\sqrt{-5}}{2}$, entonces

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Calculemos los polinomios característicos correspondientes en PARI/GP.

```
/* Producto de Kronecker de A y B */
? kronprod(A,B) = matconcat(matrix(#A[,1],#A,i,j,A[i,j]*B));

? A = [0,2;1,0];
? B = [0,1;1,1];
? charpoly (kronprod(A,B))
% = x^4 - 6*x^2 + 4
? charpoly (kronprod(A,matid(2)) + kronprod(matid(2),B))
% = x^4 - 2*x^3 - 5*x^2 + 6*x - 1
? algdep (sqrt(2)*(1+sqrt(5))/2,4)
% = x^4 - 6*x^2 + 4
? algdep (sqrt(2) + (1+sqrt(5))/2,4)
% = x^4 - 2*x^3 - 5*x^2 + 6*x - 1
```

Clase 7
31/08/20

2.5.9. Lema. *Sea K un campo de números. Dado $\alpha \in K$, existe $N \in \mathbb{Z}$ no nulo tal que $N\alpha \in \mathcal{O}_K$.*

Demostración. El elemento α satisface alguna relación algebraica

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in \mathbb{Q}$ y $a_n \neq 0$. Multiplicando los coeficientes por su mínimo común denominador, siempre podemos asumir que $a_n \in \mathbb{Z}$. Ahora al multiplicar la ecuación por a_n^{n-1} nos queda

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_1a_n^{n-2}(a_n\alpha) + a_0a_n^{n-1} = 0.$$

Esto quiere decir que $a_n\alpha \in \mathcal{O}_K$. ■

2.5.10. Proposición. *Se tiene* $\operatorname{Frac}\mathcal{O}_K = K$.

[*]He aquí una prueba. Si α y β son valores propios de aplicaciones lineales $\phi\colon U\to U$ y $\psi\colon V\to V$, esto significa que existen vectores no nulos $u\in U, v\in V$ tales que $\phi(u)=\alpha u$, $\psi(v)=\beta v$. Luego, $(\phi\otimes\psi)(u\otimes v)=\alpha\beta\, u\otimes v$ y $(\phi\otimes id + id\otimes\psi)(u\otimes v)=(\alpha+\beta)\,u\otimes v$. Entonces, $\alpha\beta$ es un valor propio de $\phi\otimes\psi$ y $\alpha+\beta$ es un valor propio de $\phi\otimes id + id\otimes\psi$.

Demostración. Por la definición tenemos $\mathcal{O}_K \subset K$, y luego la inclusión $\operatorname{Frac}\mathcal{O}_K \subseteq K$. Por otro lado, dado un elemento $\alpha \in K$, por el lema anterior tenemos $N\alpha \in \mathcal{O}_K$ para algún $N \in \mathbb{Z}$ no nulo. Esto implica que $\alpha = \frac{1}{N} N\alpha \in \operatorname{Frac}\mathcal{O}_K$. ■

2.5.11. Proposición. *$\mathcal{O}_K$ es un anillo integralmente cerrado; es decir, si $\alpha \in K = \operatorname{Frac}\mathcal{O}_K$ es entero sobre $\mathcal{O}_K$, entonces $\alpha \in \mathcal{O}_K$.*

Demostración. Tenemos una relación mónica

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

donde $a_i \in \mathcal{O}_K$. Esta relación implica que $R[\alpha]$ es un R-módulo finitamente generado, donde $R = \mathbb{Z}[a_0, \ldots, a_{n-1}]$. Pero los $a_i \in \mathcal{O}_K$ también cumplen algunas relaciones mónicas sobre $\mathbb{Z}$, así que R es finitamente generado como $\mathbb{Z}$-módulo. De aquí se sigue que $R[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo[*]. Pero luego por nuestra caracterización de integralidad 2.5.5, esto implica que α es entero sobre $\mathbb{Z}$. ■

Para los resultados generales acerca de elementos enteros en extensiones de anillos $R \subset S$, véase por ejemplo [AM1969, Chapter 5].

Otra propiedad importante del anillo de enteros: $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $[K : \mathbb{Q}]$.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \Big| {\scriptstyle \mathrm{rk}=n} & & \Big| {\scriptstyle \deg=n} \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Lo vamos a probar un poco más adelante cuando tengamos las herramientas adecuadas, pero me gustaría mencionarlo ahora. Procedamos con algunos ejemplos de anillos de números.

2.5.12. Ejemplo. Está claro que para $K = \mathbb{Q}$ se tiene $\mathcal{O}_K = \mathbb{Z}$. ▲

2.5.13. Ejemplo. Calculemos el anillo de enteros $\mathcal{O}_K$ para el campo cuadrático $K = \mathbb{Q}(\sqrt{d})$, donde d es un entero libre de cuadrados.

Consideremos un elemento $\alpha = a + b\sqrt{d} \in K$. Si $\alpha \in \mathbb{Q}$, entonces $\alpha \in \mathcal{O}_K$ si y solamente si $\alpha \in \mathbb{Z}$. Si $\alpha \notin \mathbb{Q}$, entonces el polinomio mínimo de α viene dado por

$$f = (x - (a + b\sqrt{d}))\,(x - (a - b\sqrt{d})) = x^2 - 2ax + a^2 - db^2.$$

Para que los coeficientes sean enteros, necesitamos que se cumpla

$$2a, \quad a^2 - db^2 \in \mathbb{Z}.$$

La primera condición implica que $a = a'/2$ para algún $a' \in \mathbb{Z}$. Para la segunda condición, dado que d es un entero libre de cuadrados, se ve que necesariamente $b = \frac{b'}{2}$ para algún $b' \in \mathbb{Z}$.

Analicemos entonces la condición

$$a^2 - db^2 \in \mathbb{Z} \iff a'^2 - db'^2 \equiv 0 \pmod 4.$$

Si $d \equiv 1 \pmod 4$, entonces nos queda $a'^2 \equiv b'^2 \pmod 4$, lo que sucede precisamente cuando $a' \equiv b' \pmod 2$. Entonces, en este caso

$$\mathcal{O}_K = \left\{ \frac{a'}{2} + \frac{b'}{2}\sqrt{d} \;\middle|\; a', b' \in \mathbb{Z},\ a' \equiv b' \pmod 2 \right\} = \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big].$$

Por otra parte, si $d \equiv 2, 3 \pmod 4$, se ve que la condición es equivalente a $a' \equiv b' \equiv 0 \pmod 2$, así que

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}].$$ ▲

[*] Estamos usando la siguiente observación: para una extensión de anillos $A \subseteq B \subseteq C$, si B es finitamente generado como un A-módulo y C es finitamente generado como B-módulo, entonces C es finitamente generado como un A-módulo. De hecho, si $B = A\langle b_1, \ldots, b_m\rangle$ y $C = B\langle c_1, \ldots, c_n\rangle$, entonces $C = A\langle b_i c_j\rangle$.

Este ejemplo demuestra que si $K = \mathbb{Q}(\alpha)$, donde α es un entero algebraico, entonces el anillo de enteros $\mathcal{O}_K$ puede ser más grande que $\mathbb{Z}[\alpha]$.

2.5.14. Ejemplo. Para el campo ciclotómico $K = \mathbb{Q}(\zeta_n)$ se tiene $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Todavía no tenemos las herramientas adecuadas para probarlo en toda generalidad, y por el momento sugiero considerar el caso de $n = p$ primo.

La extensión ciclotómica $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de Galois, y los automorfismos vienen dados por $\zeta_p \mapsto \zeta_p^k$, donde $k = 1, 2, 3, \ldots, p-1$ (véase §B.3). El grupo de Galois es cíclico, isomorfo a $(\mathbb{Z}/p\mathbb{Z})^\times$. Denotemos por σ su generador:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{1, \sigma, \ldots, \sigma^{p-2}\}.$$

Si $\alpha \in \mathcal{O}_K$, entonces $\sigma^i(\alpha) \in \mathcal{O}_K$: todos los conjugados de Galois son raíces del mismo polinomio mínimo. Para una extensión de Galois la norma es el producto de todos los conjugados:

$$N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \alpha\,\sigma(\alpha)\,\sigma^2(\alpha)\cdots\sigma^{p-2}(\alpha).$$

Además, la **traza** es la suma de todos los conjugados:

$$T(\alpha) = T_{K/\mathbb{Q}}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{p-2}(\alpha).$$

Las expresiones de arriba son invariantes respecto a la acción del grupo de Galois, así que para todo $\alpha \in \mathcal{O}_K$ se tiene

$$N(\alpha), T(\alpha) \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$

De estas definiciones está claro que la norma es multiplicativa y la traza es $\mathbb{Q}$-lineal: para $\alpha, \beta \in K$ y $a, b \in \mathbb{Q}$

$$N(\alpha\beta) = N(\alpha)\,N(\beta), \quad T(a\alpha + b\beta) = a\,T(\alpha) + b\,T(\beta).$$

Por ejemplo,

$$N(1-\zeta_p) = (1-\zeta_p)\,(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = \Phi_p(1) = p.$$

Esto implica que $1-\zeta_p \notin \mathcal{O}_K^\times$ (como siempre, por la multiplicatividad de la norma, las unidades deben tener norma ± 1). Además, este cálculo nos dice que

$$p\mathbb{Z} \subseteq (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z}.$$

Pero el ideal $(1-\zeta_p) \subset \mathcal{O}_K$ es propio y $p\mathbb{Z}$ es maximal en $\mathbb{Z}$, así que

$$(1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}.$$

Ahora consideremos un elemento $\alpha \in \mathcal{O}_K$ dado por

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2},$$

donde $a_i \in \mathbb{Q}$. Calculamos

$$T(\alpha\,(1-\zeta_p)) = \sigma(\alpha)\,(1-\zeta_p) + \sigma^2(\alpha)\,(1-\zeta_p^2) + \cdots + \sigma^{p-2}(\alpha)\,(1-\zeta_p^{p-2}).$$

Para todo $i = 1, 2, \ldots, p-1$ tenemos

$$1 - \zeta_p^i = (1-\zeta_p)\,(1 + \zeta_p + \cdots + \zeta_p^{i-1}),$$

así que

$$T(\alpha\,(1-\zeta_p)) \in (1-\zeta_p)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}.$$

Por otro lado, podemos calcular directamente que

$$T(\alpha\,(1-\zeta_p)) = a_0 p$$

(un pequeño ejercicio para el lector: calcule $T(\zeta_p^k)$ y use la linealidad de la traza). Esto implica que $a_0 \in \mathbb{Z}$. Luego podemos pasar al entero algebraico

$$(\alpha - a_0)/\zeta_p = a_1 + a_2\,\zeta_p + a_3\,\zeta_p^2 + \cdots,$$

y el mismo argumento nos dirá que $a_1 \in \mathbb{Z}$, etcétera. Al final vamos a concluir que $\alpha \in \mathbb{Z}[\zeta_p]$. ▲

2.5.15. Advertencia. Los ejemplos que vimos hasta el momento son algo peligrosos porque en estos el anillo de enteros tiene forma

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \cdots \oplus \alpha^{n-1}\mathbb{Z} \quad \text{para algún } \alpha \in \mathcal{O}_K;$$

en otras palabras, $\mathcal{O}_K$ tiene una base sobre $\mathbb{Z}$ que consiste en potencias del mismo elemento α. Dedekind observó por primera vez que esto no es siempre posible y dio el primer ejemplo particular

$$K = \mathbb{Q}[x]/(x^3 - x^2 - 2x - 8).$$

En este caso él anillo de enteros $\mathcal{O}_K$ no tiene forma $\mathbb{Z}[\alpha]$, pero lo vamos probar más adelante, en el momento adecuado.

Los campos de números cuyo anillo de enteros tiene forma $\mathbb{Z}[\alpha]$ se llaman **monogénicos** y de hecho son muy especiales. Vamos a volver a este asunto más adelante, pero lo menciono para que el lector no quede con la falsa impresión de que todos los campos de números son monogénicos. En realidad, pocos lo son.

2.6 Dominios de Dedekind

Para resumir la situación, dado un campo de números K, hemos definido *de manera canónica* un subanillo $\mathcal{O}_K \subset K$ que es integralmente cerrado. Este es un dominio de Dedekind.

2.6.1. Definición. Un **dominio de Dedekind** es un dominio R que cumple las siguientes condiciones:

a) R es noetheriano,

b) $\dim R = 1$[*] (es decir, todo ideal primo no nulo $\mathfrak{p} \subset R$ es maximal),

c) R es integralmente cerrado.

Como hemos visto, las condiciones a) y b) se cumplen para cualquier anillo de números $R \subset K$. Sin embargo, la condición c) no siempre se cumple, y por esto introducimos el anillo de enteros $\mathcal{O}_K$.

No todos los dominios de Dedekind son de la forma $\mathcal{O}_K$. Por ejemplo, el anillo de polinomios $k[x]$ (donde k es un campo) es un anillo de Dedekind.

2.6.2. Comentario. Tal vez cabe mencionar que un anillo puede ser integralmente cerrado y unidimensional, pero no ser noetheriano. Un ejemplo natural es el anillo de todos los enteros algebraicos (es decir, elementos de $\overline{\mathbb{Q}}$ enteros sobre $\mathbb{Z}$). Este es un anillo muy grande que contiene todos los anillos de enteros $\mathcal{O}_K$. (Haga el ejercicio 2.15.)

Nuestro próximo objetivo será probar que todo dominio de Dedekind admite factorización única de ideales en ideales primos. De hecho, también es cierta la otra implicación: un dominio donde todo ideal propio no nulo $I \subset R$ se expresa como un producto de ideales primos debe ser un dominio de Dedekind. El lector interesado puede consultar [Clark-CA, Chapter 20] para más detalles y otras caracterizaciones de dominios de Dedekind.

Hasta el final de esta sección, sea R un dominio de Dedekind y K su campo de fracciones. En particular, esto funciona para el anillo de enteros $R = \mathcal{O}_K$ de un campo de números K. El lector notará que los argumentos de abajo usan todas las condiciones sobre R (noetheriano, unidimensional, integralmente cerrado).

2.6.3. Lema. *Todo ideal entero no nulo $I \subset R$ contiene un producto de ideales primos no nulos.*

[*] Algunos autores piden $\dim R \leq 1$.

Demostración. Supongamos que esto es falso. Sea I un ideal no nulo que es maximal respecto a la propiedad que I no contiene un producto de ideales primos no nulos. Este I existe gracias a la condición noetheriana. El mismo I no es primo, así que existen $\alpha, \beta \in R$ tales que $\alpha\beta \in I$, pero $\alpha, \beta \notin I$. Ahora tenemos

$$I \subsetneq I + \alpha R, \quad I \subsetneq I + \beta R.$$

Por la maximalidad de I, tenemos

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq I + \alpha R, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq I + \beta R$$

para algunos ideales primos $\mathfrak{p}_i, \mathfrak{q}_j$. Pero ahora

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \, \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq (I + \alpha R)(I + \beta R) = I^2 + \alpha I + \beta I + \alpha\beta R \subseteq I.$$

Contradicción. ■

2.6.4. Lema. *a) Para todo R-ideal fraccionario no nulo I se tiene*

$$(I : I) \overset{def}{=} \{\alpha \in K \mid \alpha I \subseteq I\} = R.$$

b) Dado un ideal entero propio no nulo $I \subsetneq R$, se tiene $R \subsetneq I^{-1}$.

Demostración. En a), la inclusión $R \subseteq (I : I)$ está clara por la definición de $(I : I)$. Para la otra inclusión, si $\alpha I \subseteq I$, entonces, dado que I es un R-módulo finitamente generado (por la condición noetheriana), podemos concluir que α es entero sobre R (recuerde nuestra caracterización de integralidad de 2.5.5). Pero R es integralmente cerrado por nuestra hipótesis, y por lo tanto $\alpha \in R$.

En b), recordemos que por la definición,

$$I^{-1} = \{\alpha \in K \mid \alpha I \subseteq R\}.$$

Para un elemento no nulo $\alpha \in I$, por el lema anterior tenemos

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \alpha R \subseteq I \subsetneq R$$

para algunos ideales primos no nulos $\mathfrak{p}_i$. Sea s el mínimo posible tal que αR contiene un producto de s ideales primos no nulos. Sea $\mathfrak{p}$ un ideal maximal tal que $I \subseteq \mathfrak{p}$. Ahora $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{p}$, y por la primalidad de $\mathfrak{p}$ y maximalidad de $\mathfrak{p}_i$ (¡gracias a la hipótesis que $\dim R = 1$!), tenemos $\mathfrak{p} = \mathfrak{p}_i$ para algún i. Sin pérdida de generalidad, $i = 1$.

Si $s = 1$, entonces $\mathfrak{p}_1 \subseteq \alpha R \subseteq I \subseteq \mathfrak{p}$ implica que $I = \alpha R$. Tenemos $R \subsetneq I^{-1} = \alpha^{-1} R$ (note que I es un ideal propio, así que $\alpha^{-1} \notin R$).

Si $s > 1$, entonces por la minimalidad de s, tenemos $\mathfrak{p}_2 \cdots \mathfrak{p}_s \not\subseteq \alpha R$. Tomemos $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_s \setminus \alpha R$. Notamos que $\alpha^{-1}\beta \notin R$. Por otra parte,

$$\alpha^{-1}\beta I \subseteq \alpha^{-1}\beta\mathfrak{p} \subseteq \alpha^{-1}\mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_s \subseteq \alpha^{-1}(\alpha R) = R.$$

Entonces, $\alpha^{-1}\beta \in I^{-1}$. ■

2.6.5. Lema. *Todo R-ideal fraccionario no nulo es invertible.*

Demostración. Tenemos que probar que $II^{-1} = R$. La inclusión $II^{-1} \subseteq R$ se cumple en cualquier caso por la definición de I^{-1}. De modo similar,

$$(II^{-1})(II^{-1})^{-1} \subseteq R \Longrightarrow I^{-1}(II^{-1})^{-1} \subseteq I^{-1}.$$

Esto significa que

$$(II^{-1})^{-1} \subseteq (I^{-1} : I^{-1}) = R,$$

donde la última igualdad se cumple por la parte a) del lema anterior.

Ahora $II^{-1} \subseteq R$ es un ideal entero y podemos aplicar la parte b) del lema: si $II^{-1} \subsetneq R$, entonces $R \subsetneq (II^{-1})^{-1}$. Pero no es el caso, y por ende $II^{-1} = R$. ■

Ahora todo está listo para establecer la factorización única de ideales.

2.6.6. Teorema. *En un dominio de Dedekind R todo ideal entero propio, no nulo $I \subset R$ puede ser escrito como un producto de ideales primos $I = \mathfrak{p}_1 \cdots \mathfrak{p}_s$. Además, esta expresión es única salvo una permutación de los $\mathfrak{p}_i$.*

Demostración. Primero vamos a establecer existencia de factorizaciones, y luego su unicidad. Supongamos que existen ideales propios no nulos que no se expresan como un producto de ideales primos. Sea I un ideal maximal con esta propiedad (este existe gracias a la condición noetheriana). El mismo I no es primo, así que existe un ideal maximal $\mathfrak{p}$ tal que $I \subsetneq \mathfrak{p}$. Tenemos $I = \mathfrak{p}J$, donde $J = \mathfrak{p}^{-1}I$ (esto tiene sentido, ya que los ideales son invertibles). Notamos que $J \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$, así que J es un ideal entero. Ahora tenemos $I \subsetneq J$ (si $I = J = \mathfrak{p}^{-1}I$, entonces $\mathfrak{p} = R$ gracias a la invertibilidad de I, pero no es el caso). Por la elección de I, tenemos $J = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, pero luego $I = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_s$. Contradicción.

Ahora para probar que las factorizaciones son únicas, procedamos por inducción de la manera habitual. Si

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \mathfrak{q}_1 \cdots \mathfrak{q}_t,$$

entonces, usando que los ideales son maximales, tenemos sin pérdida de generalidad $\mathfrak{p}_s = \mathfrak{q}_t$. Gracias a la invertibilidad de ideales, los podemos cancelar y obtener de esta manera

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{s-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_{t-1}.$$

Esto nos da el paso inductivo. ■

Entonces, dado un ideal entero no nulo I en un dominio de Dedekind, se tiene

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)},$$

donde el producto es sobre todos los ideales primos no nulos y los números $v_{\mathfrak{p}}(I) \geq 0$ están bien definidos (y casi todos son nulos, salvo un número finito de ellos).

Usando la factorización única, no es difícil ver que

$$J = II' \iff I \mid J \iff J \subseteq I.$$

La función $v_{\mathfrak{p}}$ se comporta como las valuación:

$$v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J), \quad v_{\mathfrak{p}}(I+J) = \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}.$$

Además,

$$v_{\mathfrak{p}}(I \cap J) = \max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}.$$

Para los ideales tiene sentido poner

$$\operatorname{mcd}(I,J) = I + J = \prod_{\mathfrak{p}} \mathfrak{p}^{\min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}},$$
$$\operatorname{mcm}(I,J) = I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}}.$$

En particular, se tiene

$$(I+J)\,(I \cap J) = IJ.$$

Este es un análogo[*] de la fórmula

$$\operatorname{mcd}(\alpha,\beta)\,\operatorname{mcm}(\alpha,\beta) = \alpha\beta.$$

[*] Análogo ideal :-)

Si I es un R-ideal fraccionario, entonces existe $\alpha \in R$ no nulo tal que $\alpha I \subseteq R$ es un ideal entero, y luego

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)},$$

donde $v_{\mathfrak{p}}(I) = v_{\mathfrak{p}}(\alpha I) - v_{\mathfrak{p}}(\alpha R)$. De esta manera la factorización única se generaliza a ideales fraccionarios (permitiendo potencias negativas de ideales primos).

Otra manera de expresar el hecho de que los ideales fraccionarios se factorizan de manera única en ideales primos es decir que el grupo abeliano de ideales invertibles (en un dominio de Dedekind todo ideal es invertible) es libre, generado por los ideales primos: tenemos un isomorfismo

$$\mathcal{I}(R) \xrightarrow{\cong} \bigoplus_{\mathfrak{p}} \mathbb{Z}, \quad I \mapsto (v_{\mathfrak{p}}(I))_{\mathfrak{p}}.$$

2.6.7. Comentario. En anillos noetherianos de dimensión superior ya no existen descomposiciones de ideales en productos de ideales primos, pero existe una noción general de la **descomposición primaria**. Véase por ejemplo [AM1969, Chapter 4, 6].

Para un dominio de Dedekind R, el grupo de Picard $\mathrm{Pic}(R)$ en algún sentido mide qué tan lejos R está de ser un dominio de factorización única. Específicamente, tenemos el siguiente resultado.

2.6.8. Teorema. *Para un dominio de Dedekind R las siguientes condiciones son equivalentes:*

1) $\mathrm{Pic}(R) = 0$*,*

2) R es un dominio de ideales principales,

3) R es un dominio de factorización única.

Demostración. Los ideales fraccionarios son principales si y solamente si los ideales enteros son principales, así que las condiciones 1) y 2) son equivalentes.

En el capítulo anterior ya vimos la implicación 2)⇒3).

La implicación 3)⇒2) funciona gracias al hecho de que $\dim R = 1$. A saber, supongamos que R es un dominio de factorización única. Todos los ideales en un dominio de Dedekind se factorizan en productos de ideales primos, así que será suficiente probar que todo ideal primo es principal. Para esto, dado un ideal primo no nulo $\mathfrak{p}$, tomemos un elemento no nulo $\alpha \in \mathfrak{p}$. Por la hipótesis sobre R, tenemos una factorización en *elementos* primos

$$\alpha = \pi_1 \cdots \pi_s.$$

Ahora

$$\alpha R = \mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{p},$$

donde $\mathfrak{p}_i = \pi_i R$ son ideales primos principales, y son también maximales, ya que $\dim R = 1$. Como siempre, dado que $\mathfrak{p}$ es primo y los $\mathfrak{p}_i$ son maximales, podemos concluir que $\mathfrak{p} = \mathfrak{p}_i = \pi_i R$ es principal. ■

La factorización única nos permite demostrar que los dominios de Dedekind no están muy lejos de ser dominios de ideales principales: cada ideal puede ser generado por dos elementos.

2.6.9. Proposición. *Sea R un dominio de Dedekind. Dado un ideal no nulo $I \subset R$ y un elemento no nulo $\alpha \in I$ existe $\beta \in I$ tal que*

$$(\alpha, \beta) = \alpha R + \beta R = I.$$

Demostración. Consideremos la factorización de ideales primos

$$\alpha R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Ahora $I \mid \alpha R$, así que

$$I = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'},$$

donde $e_i \leq e_i'$.

Se puede escoger $\beta \in R$ tal que $\mathfrak{p}_i^{e_i'} \mid \beta R$, pero $\mathfrak{p}_i^{e_i'+1} \nmid \beta R$. A saber, esto se hace mediante el teorema chino del resto, escogiendo $\beta_i \in \mathfrak{p}_i^{e_i'+1} \setminus \mathfrak{p}_i^{e_i'}$:

$$\begin{array}{ccc} R/(\mathfrak{p}_1^{e_1'+1} \cdots \mathfrak{p}_s^{e_s'+1}) & \xrightarrow{\cong} & R/\mathfrak{p}_1^{e_1'+1} \times \cdots \times R/\mathfrak{p}_s^{e_s'+1} \\ \downarrow & \beta \longmapsto (\beta_1, \ldots, \beta_s) & \downarrow \\ R/(\mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_s'}) & \xrightarrow{\cong} & R/\mathfrak{p}_1^{e_1'} \times \cdots \times R/\mathfrak{p}_s^{e_s'} \end{array}$$

Ahora $\beta R = IJ$, donde $\mathfrak{p}_i \nmid J$ para ningún $i = 1, \ldots, s$, y por lo tanto

$$(\alpha, \beta) = \alpha R + \beta R = \prod_{\mathfrak{p}} \mathfrak{p}^{\min\{v_{\mathfrak{p}}(\alpha R), v_{\mathfrak{p}}(\beta R)\}} = I. \qquad \blacksquare$$

Terminamos por una definición.

2.6.10. Definición. Dado un campo de números K, su **grupo de clases** viene dado por

$$\mathrm{Cl}(K) = \mathrm{Pic}(\mathcal{O}_K).$$

El término «grupo de clases» es una abreviación de «grupo de clases de ideales» (*Idealklassengruppe* en alemán) y se refiere al hecho de que los elementos de $\mathrm{Pic}(\mathcal{O}_K)$ son *clases* de equivalencia de ideales modulo ideales principales.

Uno de los resultados importantes del curso será probar que el grupo $\mathrm{Cl}(K)$ es finito para cualquier campo de números K. También veremos cómo se pueden calcular $\mathcal{O}_K$ y $\mathrm{Cl}(K)$.

La evidencia numérica *sugiere que* todo grupo abeliano finito es isomorfo a $\mathrm{Cl}(K)$ para algún campo de números K, pero esta es una conjetura abierta. Sin embargo, si consideramos todos los dominios de Dedekind, un teorema de Claborn dice que cualquier grupo abeliano A es isomorfo a $\mathrm{Pic}(R)$ para algún dominio de Dedekind R. Véase [Cla1966].

Clase 8
02/09/20

2.7 Teorema de Kummer–Dedekind

Hasta el momento, hemos introducido el anillo de enteros $\mathcal{O}_K$ y probamos mediante argumentos muy generales que todo ideal no nulo en $\mathcal{O}_K$ se factoriza de manera única en ideales primos. Me gustaría presentar algunas técnicas que nos permiten factorizar ideales en práctica, y en particular un resultado conocido como el teorema de Kummer–Dedekind. Aunque todavía no sabemos bien cómo calcular $\mathcal{O}_K$ a partir de un campo de números específico K, este teorema no trabaja con el mismo $\mathcal{O}_K$, sino con un subanillo posiblemente más pequeño que no es necesariamente integralmente cerrado.

Empecemos entonces por el siguiente resultado auxiliar.

2.7.1. Lema. *Sean R un anillo de números (no necesariamente integralmente cerrado), $\mathfrak{p} \subset R$ un ideal invertible y $\kappa(\mathfrak{p}) = R/\mathfrak{p}$ el campo residual correspondiente. Entonces, para todo $e \geq 1$ se cumple lo siguiente:*

1) $\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}^e/\mathfrak{p}^{e+1}) = 1$*;*

2) $\dim_{\kappa(\mathfrak{p})}(R/\mathfrak{p}^e) = e$*, y en particular* $\#(R/\mathfrak{p}^e) = \#(R/\mathfrak{p})^e$.

Demostración. Consideremos la filtración de R por las potencias de $\mathfrak{p}$.

$$R \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \mathfrak{p}^3 \supsetneq \cdots$$

* cambié un poco el argumento (07/09/20)

Aquí $\mathfrak{p}^{e+1} \subsetneq \mathfrak{p}^e$ son inclusiones estrictas, por ejemplo, por la invertibilidad de $\mathfrak{p}$. Los cocientes $R/\mathfrak{p}$ y $\mathfrak{p}^e/\mathfrak{p}^{e+1}$ tienen estructura natural de R-módulos. Además, estos cocientes se aniquilan por $\mathfrak{p}$, así que se trata de $R/\mathfrak{p}$-módulos; es decir, espacios vectoriales sobre el campo residual $\kappa(\mathfrak{p})$.

Un subespacio vectorial no nulo $0 \subsetneq V \subseteq \mathfrak{p}^e/\mathfrak{p}^{e+1}$ corresponde a un ideal $I \subset R$ tal que $\mathfrak{p}^{e+1} \subsetneq I \subseteq \mathfrak{p}^e$. Pero $\mathfrak{p}$ es invertible por nuestra hipótesis, y multiplicando por $\mathfrak{p}^{-e}$ se obtiene $\mathfrak{p} \subsetneq I\mathfrak{p}^{-e} \subseteq R$, y luego $I = \mathfrak{p}^e$ por la maximalidad de $\mathfrak{p}$. Entonces, $V = \mathfrak{p}^e/\mathfrak{p}^{e+1}$, y por lo tanto $\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}^e/\mathfrak{p}^{e+1}) = 1$. Ahora

$$\frac{R/\mathfrak{p}^e}{\mathfrak{p}^{e-1}/\mathfrak{p}^e} \cong R/\mathfrak{p}^{e-1},$$

y en particular,

$$\dim_{\kappa(\mathfrak{p})}(R/\mathfrak{p}^e) = \dim_{\kappa(\mathfrak{p})}(R/\mathfrak{p}^{e-1}) + \dim_{\kappa(\mathfrak{p})}(\mathfrak{p}^{e-1}/\mathfrak{p}^e) = \dim_{\kappa(\mathfrak{p})}(R/\mathfrak{p}^{e-1}) + 1.$$

Esto implica por inducción que $\dim_{\kappa(\mathfrak{p})}(R/\mathfrak{p}^e) = e$. ■

2.7.2. Comentario. No estaría mal observar qué deja de funcionar en la prueba si $\mathfrak{p}$ no es invertible. Consideremos el anillo $R = \mathbb{Z}[\sqrt{-3}]$ y el ideal maximal $\mathfrak{p} = (2, 1 + \sqrt{-3})$. Tenemos inclusiones estrictas

$$\mathfrak{p}^2 \subsetneq 2R \subsetneq \mathfrak{p},$$

lo que no puede pasar cuando $\mathfrak{p}$ es invertible.

De hecho, tenemos $\mathfrak{p}^2 = 2R \cdot \mathfrak{p}$. No es difícil calcular que $R/\mathfrak{p} \cong \mathbb{F}_2$. Ahora si $\mathfrak{p}$ como $\mathbb{Z}$-submódulo de $R \cong \mathbb{Z} \oplus \sqrt{-3}\mathbb{Z}$ está generado por ω_1, ω_2, entonces $\mathfrak{p}^2$ está generado por $2\omega_1, 2\omega_2$, y se ve que $\#(\mathfrak{p}/\mathfrak{p}^2) = 4$ y no es 2, como nos diría el lema si $\mathfrak{p}$ fuera invertible.

El teorema de Kummer–Dedekind considera la siguiente situación: dado un anillo de números $R = \mathbb{Z}[\alpha]$ con α un entero algebraico y un primo racional $p \in \mathbb{Z}$, cómo el ideal pR se factoriza en ideales primos $\mathfrak{p} \subset R$.

2.7.3. Teorema (Kummer–Dedekind). *Sean α un entero algebraico y $f(x) \in \mathbb{Z}[x]$ el polinomio mínimo de α sobre $\mathbb{Q}$. Pongamos $n = \deg(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.*

Para un primo racional p, sean $g_i(x) \in \mathbb{Z}[x]$ polinomios mónicos tales que

$$\bar{f}(x) = \overline{g_1}^{e_1}(x) \cdots \overline{g_s}^{e_s}(x)$$

es la factorización de f en polinomios irreducibles en $\mathbb{F}_p[x]$.

1) *Los ideales primos en $\mathbb{Z}[\alpha]$ que contienen p son precisamente*

$$\mathfrak{p}_i = (p, g_i(\alpha)).$$

   Tenemos $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$.

2) *Se tiene*

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \subseteq p\mathbb{Z}[\alpha],$$

   y la igualdad se cumple si y solamente si cada $\mathfrak{p}_i$ es invertible.

   Además, si $\mathbb{Z}[\alpha]/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$, entonces $\sum_i e_i f_i = n$.

Demostración. La evaluación de polinomios en α induce un isomorfismo de anillos

$$\mathbb{Z}[x]/(f) \xrightarrow{\cong} \mathbb{Z}[\alpha], \quad g \bmod f \mapsto g(\alpha). \tag{*}$$

Tenemos una biyección

$$\{\text{primos } \mathfrak{p} \subset \mathbb{Z}[\alpha] \mid p \in \mathfrak{p}\} \longleftrightarrow \{\text{primos } \mathfrak{p} \subset \mathbb{Z}[\alpha]/(p)\}.$$

Ahora reduciendo el isomorfismo (*) módulo p,

$$\mathbb{Z}[\alpha]/(p) \cong \mathbb{Z}[x]/(p,f) \cong \mathbb{F}_p[x]/(\bar{f}),$$

así que

$$\{\text{primos } \mathfrak{p} \subset \mathbb{Z}[\alpha] \mid p \in \mathfrak{p}\} \longleftrightarrow \{\text{primos } \mathfrak{p} \subset \mathbb{F}_p[x]/(\bar{f})\}.$$

Dado que $\mathbb{F}_p[x]$ es un dominio de ideales principales, los primos no nulos $\mathfrak{p} \subset \mathbb{F}_p[x]/(\bar{f})$ son de la forma $\mathfrak{p} = (\overline{g})$, donde $\overline{g} \in \mathbb{F}_p[x]$ es un polinomio irreducible tal que $\overline{g} \mid \bar{f}$. Haciendo explícitas todas las biyecciones, se obtiene la parte 1).

Notamos que $\deg(g_i) = f_i$, donde $\mathbb{Z}[\alpha]/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$, así que

$$n = \deg(f) = \sum_i e_i \deg(g_i) = \sum_i e_i f_i.$$

Ahora en 2), si multiplicamos los ideales

$$(p, g_1(\alpha))^{e_1} \cdots (p, g_s(\alpha))^{e_s},$$

se ve que el resultado tiene sus generadores divisibles por p, con una posible excepción

$$g_1(\alpha)^{e_1} \cdots g_s(\alpha)^{e_s}.$$

Pero en este caso por nuestra elección de g_i y e_i se tiene

$$g_1(\alpha)^{e_1} \cdots g_s(\alpha)^{e_s} \equiv f(\alpha) = 0 \pmod{p}.$$

Esto establece la inclusión

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \subseteq p\mathbb{Z}[\alpha].$$

El ideal $p\mathbb{Z}[\alpha]$ es invertible, como todo ideal principal, así que la igualdad implicaría que los $\mathfrak{p}_i$ son invertibles.

Viceversa, supongamos que los $\mathfrak{p}_i$ son invertibles. Dado que $\mathfrak{p}_i \neq \mathfrak{p}_j$ para $i \neq j$ y los $\mathfrak{p}_i$ son maximales, tenemos $\mathfrak{p}_i + \mathfrak{p}_j = \mathbb{Z}[\alpha]$, y luego $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathbb{Z}[\alpha]$. Esto nos permite aplicar el teorema chino del resto:

$$\mathbb{Z}[\alpha]/(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}) \cong \mathbb{Z}[\alpha]/\mathfrak{p}_1^{e_1} \times \cdots \times \mathbb{Z}[\alpha]/\mathfrak{p}_s^{e_s}.$$

Por el lema de arriba, se tiene

$$\#(\mathbb{Z}[\alpha]/\mathfrak{p}_1^{e_1}) = \#(\mathbb{Z}[\alpha]/\mathfrak{p}_1)^{e_1} = p^{f_i e_i},$$

así que

$$\#(\mathbb{Z}[\alpha]/(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s})) = p^{\sum_i f_i e_i} = p^n.$$

Por otra parte, está claro que

$$\#(\mathbb{Z}[\alpha]/(p)) = p^n,$$

dado que cómo $\mathbb{Z}$-módulo, nuestro anillo tiene forma

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \cdots \oplus \alpha^{n-1}\mathbb{Z}$$

Entonces, hemos probado que

$$[\mathbb{Z}[\alpha] : \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}] = [\mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]],$$

y luego

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} = p\mathbb{Z}[\alpha].$$

■

2.7.4. Comentario. Recomiendo que el lector consulte §§2–3 de los apuntes de Stevenhagen [Ste2017], donde los argumentos parecidos a los de arriba usan la siguiente caracterización:

$$\mathfrak{p} \text{ es invertible } \iff R_{\mathfrak{p}} \text{ es un anillo de valuación discreta.}$$

Aquí $R_{\mathfrak{p}}$ es el **anillo local** en $\mathfrak{p}$. La presentación de Stevenhagen es mejor conceptualmente, pero decidí omitir por el momento las localizaciones.

2.7.5. Comentario. Se puede probar que $\mathfrak{p}_i$ *no será* invertible precisamente cuando $e_i > 1$ y la división con resto de f por g_i en $\mathbb{Z}[x]$ nos da

$$f(x) = g_i(x)\, q_i(x) + r_i(x),$$

donde $p^2 \mid r_i(x)$. Para esto refiero de nuevo a [Ste2017].

Procedamos con algunos ejemplos de uso de Kummer–Dedekind.

2.7.6. Ejemplo. Consideremos el anillo $R = \mathbb{Z}[\sqrt{-3}]$. En este caso $f = x^2 + 3$.
Módulo 2 tenemos

$$x^2 + 3 \equiv (x+1)^2 \pmod 2, \quad g = x + 1,\ e = 2.$$

Podemos concluir que

$$\mathfrak{p}^2 \subset 2R, \quad \mathfrak{p} = (2, 1 + \sqrt{-3}).$$

La igualdad no se cumple, pero es algo esperado, dado que $\mathfrak{p}$ no es invertible.
Por otra parte, módulo 3 se tiene

$$x^2 + 3 \equiv x^2 \pmod 3, \quad g = x,\ e = 2,$$

y esto nos da la factorización obvia

$$(\sqrt{-3}R)^2 = 3R.$$

Módulo 5 el polinomio $x^2 + 3$ es irreducible y se obtiene un ideal primo $5R$. En fin, módulo 7 se tiene $(\pm 2)^2 \equiv -3 \pmod 7$, así que

$$f \equiv (x+2)\,(x-2) \pmod 7.$$

Tenemos entonces

$$\mathfrak{p}\,\overline{\mathfrak{p}} \subseteq 7R,$$

donde

$$\mathfrak{p} = (7, 2 + \sqrt{-3}), \quad \overline{\mathfrak{p}} = (7, 2 - \sqrt{-3}).$$

De hecho es fácil ver que se cumple la igualdad; esto sucede gracias a la invertibilidad de los ideales $\mathfrak{p}$ y $\overline{\mathfrak{p}}$. ▲

En los siguientes ejemplos vamos a tener $\mathcal{O}_K = \mathbb{Z}[\alpha]$, así que todos los ideales son invertibles.

2.7.1 Ejemplo: campos cuadráticos

Consideremos el campo cuadrático $K = \mathbb{Q}(\sqrt{d})$, donde d es libre de cuadrados y $d \equiv 2, 3 \pmod 4$. En este caso $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Entonces, el teorema de arriba nos dice que para factorizar los ideales $p\mathcal{O}_K$, hay que ver cómo se factoriza el polinomio $f = x^2 - d$ módulo p. Esto depende del símbolo de Legendre $\left(\frac{d}{p}\right)$.

El siguiente resultado es una aplicación inmediata de Kummer–Dedekind.

2.7.7. Proposición. *Sea $d \equiv 2, 3 \pmod 4$ libre de cuadrados y $K = \mathbb{Q}(\sqrt{d})$.*
Consideremos un primo impar p.

- *Si $p \mid d$, entonces*
$$p\mathcal{O}_K = \mathfrak{p}^2, \quad \mathfrak{p} = (p, \sqrt{d}).$$
*(En este caso se dice que p **se ramifica** en K.)*

- *Si $\left(\frac{d}{p}\right) = +1$, entonces $d \equiv a^2 \pmod{p}$ para algún $a \in \mathbb{Z}$, y se tiene*
$$p\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},$$
donde
$$\mathfrak{p} = (p, a + \sqrt{d}), \quad \overline{\mathfrak{p}} = (p, a - \sqrt{d}).$$
*(Se dice que p **se escinde** en K.)*

- *En fin, si $\left(\frac{d}{p}\right) = -1$, entonces*
$$\mathfrak{p} = p\mathcal{O}_K$$
*es un ideal primo. (Se dice que p es **inerte** en K.)*

El primo $p = 2$ siempre se ramifica: tenemos
$$2\mathcal{O}_K = \mathfrak{p}^2,$$
donde
$$\mathfrak{p} = \begin{cases} (2, \sqrt{d}), & \text{si } d \equiv 2 \pmod 4, \\ (2, 1 + \sqrt{d}), & \text{si } d \equiv 3 \pmod 4. \end{cases}$$

De la misma manera podemos analizar el caso de $K = \mathbb{Q}(\sqrt{d})$, donde $d \equiv 1 \pmod 4$, solo que en este caso $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, así que nos interesa el polinomio
$$f = x^2 - x - \frac{d-1}{4}.$$
En este caso no cambiará mucho; la descripción para los primos impares será la misma. Por otra parte, el primo $p = 2$ se comporta de manera más interesante: se ve que la factorización de f módulo 2 depende de $d \pmod 8$.

2.7.8. Proposición. *Sea $d \equiv 1 \pmod 4$ libre de cuadrados y $K = \mathbb{Q}(\sqrt{d})$.*

- *Si $d \equiv 1 \pmod 8$, entonces*
$$2\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},$$
donde
$$\mathfrak{p} = \left(2, \frac{1+\sqrt{d}}{2}\right), \quad \overline{\mathfrak{p}} = \left(2, \frac{1-\sqrt{d}}{2}\right).$$

- *Si $d \equiv 5 \pmod 8$, entonces 2 es inerte; es decir,*
$$\mathfrak{p} = 2\mathcal{O}_K$$
es un ideal primo.

2.7.2 Ejemplo: campos ciclotómicos $\mathbb{Q}(\zeta_p)$

Ahora me gustaría considerar el caso de campos ciclotómicos $K = \mathbb{Q}(\zeta_p)$, donde para simplificar la vida, p es primo. Recordemos que $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ (véase 2.5.14). El polinomio mínimo de ζ_p es el polinomio ciclotómico

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Kummer–Dedekind nos dice que para saber factorizar $q\mathcal{O}_K$, hay que factorizar $\Phi_p(x)$ módulo q.

Primero, si $q = p$, entonces

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} \equiv \frac{(x-1)^p}{x-1} = (x-1)^{p-1} \pmod{p}.$$

Ahora supongamos que $q \neq p$. En este caso se ve que $\Phi_p(x)$ es un polinomio separable en $\mathbb{F}_q[x]$. Para verlo, podemos considerar $f = x^p - 1 = (x-1)\,\Phi_p(x)$ y calcular que

$$\operatorname{mcd}(f, f') = \operatorname{mcd}(x^p - 1, p\,x^{p-1}) = 1, \quad \text{en } \mathbb{F}_q[x]$$

dado que p es invertible en $\mathbb{F}_q[x]$ y se tiene $\frac{x}{p} \cdot (px^{p-1}) - (x^p - 1) = 1$. Esto quiere decir que $\overline{\Phi_p}(x)$ no tendrá factores irreducibles $\overline{g}^e$ con $e > 1$, y también que los primos $q \neq p$ no se ramifican en $\mathcal{O}_K$.

Pero no cualquier factorización es posible.

2.7.9. Ejemplo. Aquí están las factorizaciones de $\Phi_7(x)$ módulo algunos q (calculadas en PARI/GP):

$q = 2$: $(x^3 + x + 1)\,(x^3 + x^2 + 1)$	
$q = 3$: irreducible	
$q = 5$: irreducible	
$q = 7$: $(x-1)^6$	
$q = 11$: $(x^3 + 5x^2 + 4x + 10)\,(x^3 + 7x^2 + 6x + 10)$	$(q \equiv 4 \pmod 7)$
$q = 13$: $(x^2 + 3x + 1)\,(x^2 + 5x + 1)\,(x^2 + 6x + 1)$	$(q \equiv 6 \pmod 7)$
$q = 17$: irreducible	$(q \equiv 3 \pmod 7)$
$q = 19$: irreducible	$(q \equiv 5 \pmod 7)$
$q = 23$: $(x^3 + 10x^2 + 9x + 22)\,(x^3 + 14x^2 + 13x + 22)$	$(q \equiv 2 \pmod 7)$
$q = 29$: $(x-7)\,(x-16)\,(x-20)\,(x-23)\,(x-24)\,(x-29)$	$(q \equiv 1 \pmod 7)$
$q = 31$: irreducible	$(q \equiv 3 \pmod 7)$
$q = 37$: $(x^3 + 9x^2 + 8x + 36)\,(x^3 + 29x^2 + 28x + 36)$	$(q \equiv 2 \pmod 7)$
$\cdots$	

El patrón es el siguiente.

- Si $q \equiv 1 \pmod 7$, entonces $\Phi_7(x)$ es un producto de seis polinomios lineales.
- Si $q \equiv 2, 4 \pmod 7$, entonces $\Phi_7(x)$ es un producto de dos polinomios cúbicos. Notamos que 2 y 4 tienen orden 3 módulo 7:

$$2^2 = 4,\ 2^3 \equiv 1 \pmod 7, \quad 4^2 \equiv 2,\ 4^3 \equiv 1 \pmod 7.$$

- Si $q \equiv 3, 5 \pmod 7$, entonces $\Phi_7(x)$ es irreducible mód q. Notamos que 3 y 5 son generadores de $\mathbb{F}_7^\times$.
- si $q \equiv 6 \pmod 7$, entonces $\Phi_7(x)$ es un producto de tres polinomios cuadráticos. Notamos que 6 tiene orden 2 módulo 7:

$$6^2 \equiv (-1)^2 \equiv 1 \pmod 7.$$

▲

2.7.10. Lema. *Sea f el orden de q módulo p; es decir, el mínimo posible f tal que $q^f \equiv 1 \pmod{p}$. En este caso todos los factores irreducibles en la factorización*

$$\overline{\Phi_p}(x) = \overline{g_1}(x) \cdots \overline{g_s}(x) \quad \text{en } \mathbb{F}_q[x]$$

tienen el mismo grado f. El número de factores irreducibles es $s = (p-1)/f$.

Demostración. Consideremos el campo finito $\mathbb{F}_{q^f}$. Dado que $p \mid (q^f - 1)$, las raíces p-ésimas primitivas

$$\zeta, \zeta^2, \ldots, \zeta^{p-1}$$

están en $\mathbb{F}_{q^f}^\times$, y allí el polinomio se factoriza como

$$\overline{\Phi_p}(x) = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}).$$

El grupo de Galois $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ es cíclico, generado por el automorfismo de Frobenius $\sigma\colon x \mapsto x^q$ (véase A.12.4), y luego la teoría de Galois nos dice que

$$\mathbb{F}_q = \{a \in \mathbb{F}_{q^f} \mid \sigma(a) = a\}.$$

Ahora $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ permuta las raíces de $\overline{\Phi_p}$. Notamos que $\sigma^i(\zeta) = \zeta^{q^i}$, y entonces $\zeta, \zeta^q, \ldots, \zeta^{q^f}$ es una órbita de la acción. Tomando en lugar de ζ cualquier otra raíz primitiva, se obtiene una órbita de f elementos. De esta manera las raíces p-ésimas primitivas se descomponen en $(p-1)/f$ órbitas.

Ahora si $\alpha_1, \ldots, \alpha_f$ es una órbita de la acción del Frobenius, entonces todos los polinomios simétricos elementales en α_i:

$$\sum_i \alpha_i, \quad \sum_{i<j} \alpha_i\alpha_j, \quad \sum_{i<j<k} \alpha_i\alpha_j\alpha_j, \quad \ldots$$

están fijos por el Frobenius, y por lo tanto están en $\mathbb{F}_q$. Esto significa que al desarrollar el producto

$$(x-\alpha_1)\cdots(x-\alpha_f),$$

el polinomio correspondiente está en $\mathbb{F}_q[x]$. De esta manera surge la factorización en $\mathbb{F}_q[x]$

$$\overline{\Phi_p}(x) = \overline{g_1}(x)\cdots\overline{g_s}(x),$$

donde cada polinomio $\overline{g_i}(x)$ viene de una órbita del Frobenius y tiene grado f. Por otra parte, cada $\overline{g_i}(x)$ es el polinomio mínimo de cada una de sus raíces α: se tiene $\mathbb{F}_{q^f} = \mathbb{F}_q(\alpha)$, así que los factores son irreducibles. ■

Aplicando el Kummer–Dedekind, tenemos el siguiente resultado.

2.7.11. Proposición. *Para un primo $p \neq 2$ consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_p)$.*
El mismo p se ramifica en K: tenemos

$$p\mathcal{O}_K = \mathfrak{p}^{p-1}, \quad \mathfrak{p} = (p, 1-\zeta_p).$$

Para $q \neq p$ se tiene

$$q\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s,$$

donde $\mathfrak{p}_i$ son diferentes primos y $s = (p-1)/f$, donde f es el orden de q módulo p. Además, $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_{p^f}$ para todo i.

2.7.12. Ejemplo. La figura 2.2 representa la acción de $x \mapsto x^p$ sobre las séptimas raíces de la unidad y 2.3 representa las factorizaciones correspondientes de $p\mathbb{Z}[\zeta_7]$ para diferentes primos p. ▲

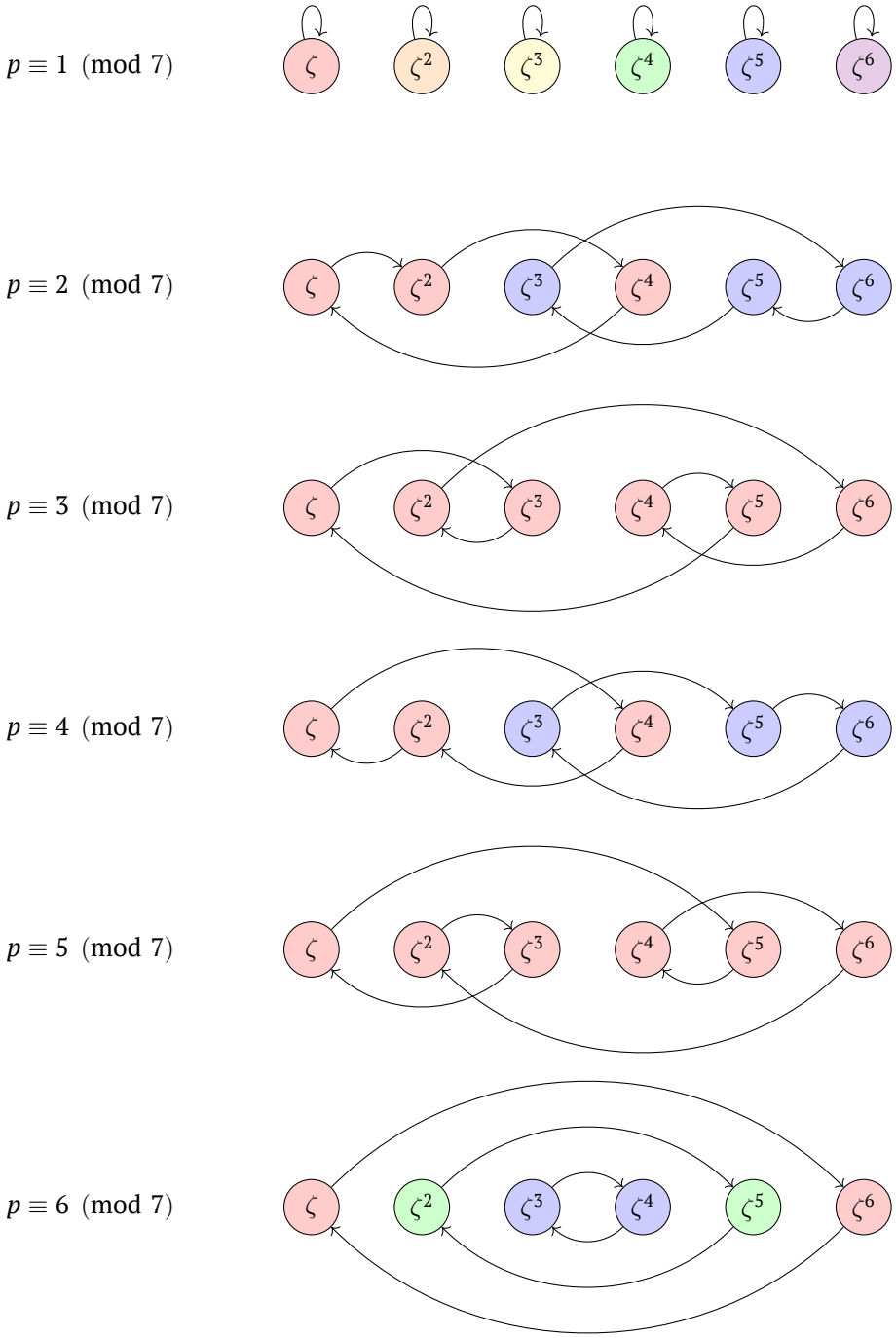


Figura 2.2: Frobenius $x \mapsto x^p$ actuando sobre las raíces séptimas primitivas en $\overline{\mathbb{F}}_p$

p	$p\mathcal{O}_K$	f	p (7)	p	$p\mathcal{O}_K$	f	p (7)
2	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2	127	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1
3	$\mathfrak{p}$	6	3	131	$\mathfrak{p}$	6	5
5	$\mathfrak{p}$	6	5	137	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
7	$\mathfrak{p}^6$	1	0	139	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6
11	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4	149	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2
13	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6	151	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
17	$\mathfrak{p}$	6	3	157	$\mathfrak{p}$	6	3
19	$\mathfrak{p}$	6	5	163	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2
23	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2	167	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6
29	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1	173	$\mathfrak{p}$	6	5
31	$\mathfrak{p}$	6	3	179	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
37	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2	181	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6
41	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6	191	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2
43	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1	193	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
47	$\mathfrak{p}$	6	5	197	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1
53	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4	199	$\mathfrak{p}$	6	3
59	$\mathfrak{p}$	6	3	211	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1
61	$\mathfrak{p}$	6	5	223	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6
67	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4	227	$\mathfrak{p}$	6	3
71	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1	229	$\mathfrak{p}$	6	5
73	$\mathfrak{p}$	6	3	233	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2
79	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2	239	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1
83	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6	241	$\mathfrak{p}$	6	3
89	$\mathfrak{p}$	6	5	251	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6
97	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2	6	257	$\mathfrak{p}$	6	5
101	$\mathfrak{p}$	6	3	263	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
103	$\mathfrak{p}$	6	5	269	$\mathfrak{p}$	6	3
107	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	2	271	$\mathfrak{p}$	6	5
109	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4	277	$\mathfrak{p}_1\,\mathfrak{p}_2$	3	4
113	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1	281	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1	1

Figura 2.3: Factorización de $p\mathcal{O}_K$ para $K = \mathbb{Q}(\zeta_7)$

2.7.13. Ejemplo. Tenemos $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, así que podemos comparar nuestras dos descripciones para la factorización de primos racionales en campos cuadráticos y ciclotómicos.

Para un primo $q \neq 2, 3$ se tiene

$$q\mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big] = \mathfrak{p}\,\mathfrak{p}' \iff \left(\frac{-3}{q}\right) = +1.$$

Por otra parte, en los campos ciclotómicos la condición es

$$q\mathbb{Z}[\zeta_3] = \mathfrak{p}\,\mathfrak{p}' \iff q \equiv 1 \pmod 3 = +1.$$

Entonces,

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

Este es un caso particular de la reciprocidad cuadrática. ▲

2.7.14. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_5)$ y su anillo de enteros $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$. La extensión $K/\mathbb{Q}$ es Galois, con el grupo de Galois cíclico

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times = \{1, \sigma, \sigma^2, \sigma^3\}.$$

Primero, tenemos la ramificación

$$5\mathcal{O}_K = \mathfrak{p}^4, \quad \mathfrak{p} = (5, 1-\zeta_5).$$

De hecho, en este caso se puede ver que $5/(1-\zeta_5) \in \mathbb{Z}[\zeta_5]$, así que $\mathfrak{p} = (1-\zeta_5)$.

Ahora para un primo $q \neq 5$ hay tres diferentes casos que corresponden al orden de q módulo 5.

- Si $q \equiv 1 \pmod 5$, entonces q se escinde en cuatro ideales primos
$$q\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4.$$
- Si $q \equiv 2, 3 \pmod 5$, entonces el ideal $q\mathcal{O}_K$ es primo.
- Si $q \equiv 4 \pmod 5$, entonces
$$q\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2.$$

Ahora empiezan las cosas interesantes. La teoría de Galois implica que K contiene único subcampo cuadrático F. Gracias a la identidad

$$\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5},$$

se ve que $F = \mathbb{Q}(\sqrt{5})$.

$$\begin{array}{ccccc} \mathcal{O}_K = & \mathbb{Z}[\zeta_5] & \subset & K = & \mathbb{Q}(\zeta_5) \\ & \Big| & & & \Big|{\scriptstyle 2} \\ \mathcal{O}_F = & \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big] & \subset & F = & \mathbb{Q}(\sqrt{5}) \\ & \Big| & & & \Big|{\scriptstyle 2} \\ & \mathbb{Z} & \subset & & \mathbb{Q} \end{array}$$

Consideremos un primo racional $q \neq 2, 5$. Como ya vimos,

$$q \text{ se escinde en } \mathcal{O}_F \iff \left(\frac{5}{q}\right) = +1.$$

Ahora si

$$q\,\mathcal{O}_F = \mathfrak{p}\overline{\mathfrak{p}},$$

donde $\mathfrak{p}$ y $\overline{\mathfrak{p}}$ son diferentes ideales primos, entonces en $\mathcal{O}_K$ estos ideales pueden dejar de ser primos y factorizarse aún más (cada uno en dos primos), pero de todos modos, q se escinde en $\mathcal{O}_K$.

Curiosamente, con un poco de trabajo y teoría de Galois, también se puede establecer la otra implicación: si q se escinde en $\mathcal{O}_K$, entonces este ya se escinde en $\mathcal{O}_F$. Nuestra descripción nos dice que los q que se escinden en $\mathcal{O}_K$ son $q \equiv 1, 4 \pmod 5$.

Tenemos entonces

$$\left(\frac{5}{q}\right) = +1 \iff q \equiv 1, 4 \pmod 5.$$

Esto demuestra un caso particular de la reciprocidad cuadrática para $p = 5$:

$$\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right).$$

Más adelante, en un momento adecuado, volveremos a este tema y veremos con todos los detalles cómo la reciprocidad cuadrática se sigue de la factorización de primos racionales en anillos cuadráticos y ciclotómicos. ▲

p	$p\mathcal{O}_F$	$p\mathcal{O}_K$	$p\ (5)$	p	$p\mathcal{O}_F$	$p\mathcal{O}_K$	$p\ (5)$
2	$\mathfrak{p}$	$\mathfrak{q}$	2	127	$\mathfrak{p}$	$\mathfrak{q}$	2
3	$\mathfrak{p}$	$\mathfrak{q}$	3	131	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
5	$\mathfrak{p}^2$	$\mathfrak{q}^4$	0	137	$\mathfrak{p}$	$\mathfrak{q}$	2
7	$\mathfrak{p}$	$\mathfrak{q}$	2	139	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
11	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	149	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
13	$\mathfrak{p}$	$\mathfrak{q}$	3	151	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
17	$\mathfrak{p}$	$\mathfrak{q}$	2	157	$\mathfrak{p}$	$\mathfrak{q}$	2
19	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	163	$\mathfrak{p}$	$\mathfrak{q}$	3
23	$\mathfrak{p}$	$\mathfrak{q}$	3	167	$\mathfrak{p}$	$\mathfrak{q}$	2
29	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	173	$\mathfrak{p}$	$\mathfrak{q}$	3
31	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	179	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
37	$\mathfrak{p}$	$\mathfrak{q}$	2	181	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
41	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	191	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
43	$\mathfrak{p}$	$\mathfrak{q}$	3	193	$\mathfrak{p}$	$\mathfrak{q}$	3
47	$\mathfrak{p}$	$\mathfrak{q}$	2	197	$\mathfrak{p}$	$\mathfrak{q}$	2
53	$\mathfrak{p}$	$\mathfrak{q}$	3	199	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
59	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	211	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
61	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	223	$\mathfrak{p}$	$\mathfrak{q}$	3
67	$\mathfrak{p}$	$\mathfrak{q}$	2	227	$\mathfrak{p}$	$\mathfrak{q}$	2
71	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	229	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
73	$\mathfrak{p}$	$\mathfrak{q}$	3	233	$\mathfrak{p}$	$\mathfrak{q}$	3
79	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	239	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
83	$\mathfrak{p}$	$\mathfrak{q}$	3	241	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
89	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	251	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
97	$\mathfrak{p}$	$\mathfrak{q}$	2	257	$\mathfrak{p}$	$\mathfrak{q}$	2
101	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1	263	$\mathfrak{p}$	$\mathfrak{q}$	3
103	$\mathfrak{p}$	$\mathfrak{q}$	3	269	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4
107	$\mathfrak{p}$	$\mathfrak{q}$	2	271	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
109	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	4	277	$\mathfrak{p}$	$\mathfrak{q}$	2
113	$\mathfrak{p}$	$\mathfrak{q}$	3	281	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1

Figura 2.4: Factorización de $p\mathcal{O}_F$ y $p\mathcal{O}_K$ en $F = \mathbb{Q}(\sqrt{5})$ y $K = \mathbb{Q}(\zeta_5)$

Ejercicios

Ejercicio 2.1. Verifique que para los ideales $I, J, H \subseteq R$ se tiene $(I+J)H = IH + JH$.

Ejercicio 2.2. Encuentre los ideales maximales $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-5}]$ tales que $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{F}_{23}$. Demuestre que no son principales.

Ejercicio 2.3. Demuestre que para todo $\alpha \in \mathbb{Z}[i]$ no nulo se tiene

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \#(R/(\alpha)).$$

Más adelante veremos un resultado más general.

Ejercicio 2.4. Consideremos el anillo $R = \mathbb{Z}[\sqrt{13}]$. ¿Cuáles de los siguientes ideales son maximales?

$$(2, 1+\sqrt{13}), \quad (3, 1+\sqrt{13}), \quad (5, 1+\sqrt{13}), \quad (7, 1+\sqrt{13}).$$

Ejercicio 2.5. Demuestre que los ideales primos en $\mathbb{Z}[x]$ son los siguientes.

- El ideal nulo (0).
- Ideales principales (f) para un polinomio irreducible $f \in \mathbb{Z}[x]$.
- Ideales maximales $\mathfrak{m} = (p, f)$, donde p es un primo racional y $f \in \mathbb{Z}[x]$ un polinomio irreducible módulo p.

Concluya que $\dim \mathbb{Z}[x] = 2$. Describa $\mathbb{Z}[x]/\mathfrak{m}$ para los ideales maximales.

Ejercicio 2.6. Describa $\operatorname{Spec} k[x, y]$ para un campo k y verifique que $\dim k[x, y] = 2$.

Ejercicio 2.7. Describa $\operatorname{Spec}(R \times S)$ en términos de $\operatorname{Spec} R$ y $\operatorname{Spec} S$.

Ejercicio 2.8. Demuestre que el ideal $(23, x)$ no es invertible en el anillo $R = \mathbb{Z}[x]$.

Ejercicio 2.9. Consideremos el anillo $\mathbb{Z}[\sqrt{5}]$ y los ideales

$$\mathfrak{p}_2 = (2, 1+\sqrt{5}), \quad \mathfrak{p}_{11} = (11, 4+\sqrt{5}).$$

Determine si son invertibles y encuentre I^{-1} en cada caso.

Ejercicio 2.10. Asumiendo que $\operatorname{Pic}(\mathbb{Z}[\sqrt{-37}]) \cong \mathbb{Z}/2\mathbb{Z}$, demuestre que la curva elíptica $y^2 = x^3 - 37$ no tiene puntos enteros.

Ejercicio 2.11. Encuentre el anillo de enteros $\mathcal{O}_K$ para $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(Hay modos listos de hacerlo, pero también se pueden ocupar cálculos directos como en el caso de campos cuadráticos; véase [Wil1970].)

Ejercicio 2.12. Demuestre que si R es un anillo con un número finito de ideales maximales (en este caso se dice que R es **semilocal**), entonces $\operatorname{Pic}(R) = 0$.

Ejercicio 2.13. Si R es un anillo finito, demuestre que

$$\#R^\times = \#R \cdot \prod_{\mathfrak{p} \in \operatorname{Spec} R} \left(1 - \frac{1}{\#(R/\mathfrak{p})}\right).$$

Ejercicio 2.14. Demuestre que todo dominio de factorización única es integralmente cerrado.

Ejercicio 2.15. Consideremos el anillo R que consiste en *todos* los enteros algebraicos; es decir, los elementos de $\overline{\mathbb{Q}}$ que son enteros sobre $\mathbb{Z}$.

1) Verifique que R es un anillo.

2) Demuestre que $\dim R = \dim \mathbb{Z} = 1$ usando [AM1969, Theorem 5.11].

3) Encuentre una sucesión infinita de enteros algebraicos $\alpha_1, \alpha_2, \alpha_3, \ldots$ tal que $\alpha_{i+1} \mid \alpha_i$, pero $\alpha_i \nmid \alpha_{i+1}$.

4) Concluya que R no es noetheriano y no es un dominio de factorización única.

Ejercicio 2.16. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_{11})$. Describa la factorización de $p\mathcal{O}_K$ para diferentes primos racionales $p \in \mathbb{Z}$. (La respuesta depende de $p \pmod{11}$.)

Ejercicio 2.17. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_8)$.

Más adelante veremos un modo adecuado para probar que $\mathcal{O}_K = \mathbb{Z}[\zeta_8]$, pero por el momento se puede aceptar este resultado.

1) Describa las factorizaciones de $p\mathcal{O}_K$ en ideales primos para diferentes primos racionales p. (La respuesta depende de $p \pmod 8$.)

2) Encuentre las subextensiones $\mathbb{Q} \subset F \subset K$ y encuentre las factorizaciones de $p\mathcal{O}_K$.

Ejercicio 2.18. Considerando la descomposición de primos racionales en $\mathcal{O}_K$, demuestre que $\zeta_p \notin \mathbb{Q}(\zeta_q)$ para diferentes primos impares $p \neq q$.

Ejercicio 2.19. Para el campo ciclotómico $K = \mathbb{Q}(\zeta_p)$ el grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ es cíclico, así que la teoría de Galois implica que existe un subcampo cuadrático único $F \subset K$. Considerando la factorización de primos racionales en $\mathcal{O}_F$ y $\mathcal{O}_K$, demuestre que $F = \mathbb{Q}(\sqrt{p^*})$, donde $p^* = (-1)^{(p-1)/2}p$.
(Sugerencia: si q se ramifica en $\mathcal{O}_F$, entonces q se ramifica en $\mathcal{O}_K$.)

Capítulo 3

Álgebra $\mathbb{Z}$-lineal

Dedicamos el capítulo anterior al álgebra conmutativa, y ahora nos ocuparemos de... álgebra lineal. Recordemos que para una extensión finita de campos L/K, la norma y traza de un elemento $\alpha \in L$ se definen como el determinante y traza de la aplicación K-lineal $x \mapsto \alpha x$. Ahora vamos a explorar estas construcciones para extensiones de anillos.

3.1 Norma y traza

Clase 9
07/09/20

3.1.1. Definición. Sea $A \subset B$ una extensión de anillos tal que B es un A-módulo libre de rango n sobre A. Para $\beta \in B$ consideremos la aplicación A-lineal de multiplicación por β:

$$\mu_\beta \colon B \to B, \quad x \mapsto \beta x.$$

La **norma** y **traza** de β se definen como el determinante y traza de μ_β respectivamente:

$$N_{B/A}(\beta) = \det \mu_\beta, \quad T_{B/A}(\beta) = \operatorname{tr} \mu_\beta.$$

Esto nos da aplicaciones

$$N_{B/A}, T_{B/A} \colon B \to A.$$

Específicamente, si $e_1, \dots, e_n$ es una base de B sobre A y $\beta\, e_i = \sum_j m_{ij} e_j$, entonces

$$N(\beta) = \det(m_{ij})_{i,j}, \quad T(\beta) = \sum_i m_{ii}.$$

El argumento habitual demuestra que esto no depende de la elección de base: si T es una matriz de cambio de base, entonces es invertible, y luego

$$\det(TMT^{-1}) = \det(T)\ \det(M)\ \det(T)^{-1} = \det(M),$$
$$\operatorname{tr}(TMT^{-1}) = \operatorname{tr}(T^{-1}TM) = \operatorname{tr}(M).$$

Vamos a denotar el polinomio característico correspondiente por

$$f^\beta_{B/A} = \det(xI_n - M).$$

Este es un polinomio mónico de grado n:

$$f^\beta_{B/A} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x].$$

El argumento habitual demuestra que

$$a_0 = (-1)^n N_{B/A}(\beta), \quad a_{n-1} = -T_{B/A}(\beta). \tag{3.1}$$

La norma es multiplicativa:

$$N(\beta\beta') = N(\beta)\,N(\beta'),$$

mientras que la traza es A-lineal:

$$T(a\beta) = a\,T(\beta), \quad T(\beta+\beta') = T(\beta) + T(\beta').$$

Para $a \in A$ se tiene

$$N(a) = a^n, \quad T(a) = na.$$

3.1.2. Proposición. *Para un campo de números $K/\mathbb{Q}$ tenemos $n = [K:\mathbb{Q}]$ encajes*

$$\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C},$$

y la norma y traza vienen dadas por

$$N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha), \quad T_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha).$$

Aquí $\sigma_i(\alpha)$ son las raíces del polinomio característico de α respecto a la extensión $K/\mathbb{Q}$.

Demostración. Primero, si $K = \mathbb{Q}(\alpha)$, entonces un encaje $\sigma\colon K \hookrightarrow \mathbb{C}$ está definido por la imagen de α y tiene que enviarlo a una raíz compleja del polinomio mínimo $f^\alpha_{\mathbb{Q}}$. De esta manera surgen los $[K(\alpha):\mathbb{Q}]$ encajes. Tenemos

$$f^\alpha_{\mathbb{Q}} = \prod_{\sigma\colon K\hookrightarrow\mathbb{C}} (x - \sigma(\alpha)).$$

En general, tenemos $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset K$, y cada encaje $\sigma\colon \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ admite $[K:\mathbb{Q}(\alpha)]$ extensiones a un encaje $K \hookrightarrow \mathbb{C}$. Ahora

$$f^\alpha_{K/\mathbb{Q}} = (f^\alpha_{\mathbb{Q}})^{[K:\mathbb{Q}(\alpha)]} = \prod_{\sigma\colon K\hookrightarrow\mathbb{C}} (x - \sigma(\alpha)),$$

donde $f^\alpha_{K/\mathbb{Q}}$ es el polinomio característico, mientras que $f^\alpha_{\mathbb{Q}}$ es el polinomio mínimo. En fin, recordemos cómo la norma y traza están relacionadas con los coeficientes del polinomio característico (las fórmulas (3.1)). ■

3.1.3. Comentario. Dado que $K/\mathbb{Q}$ es una extensión algebraica, en realidad todo encaje $\sigma\colon K \hookrightarrow \mathbb{C}$ tiene su imagen en $\overline{\mathbb{Q}}$, la cerradura algebraica de $\mathbb{Q}$, así que los números complejos no son tan relevantes.

Si $K/\mathbb{Q}$ es una extensión de Galois, entonces los encajes $K \hookrightarrow \mathbb{C}$ corresponden a los elementos de $\mathrm{Gal}(K/\mathbb{Q})$. En general, puede haber más encajes que automorfismos de Galois.

Para más detalles sobre la norma y traza de una extensión finita de campos, el lector puede revisar, por ejemplo, [Mor1996, §II.8] o [Lan2002, §VI.5].

3.1.4. Proposición. *Si $\alpha \in \mathcal{O}_K$, entonces $N_{K/\mathbb{Q}}(\alpha), T_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Demostración. Si $\alpha_1, \ldots, \alpha_n$ son las raíces del polinomio característico de α sobre $\mathbb{Q}$, entonces estas son también enteros algebraicos, y por lo tanto $N(\alpha) = \alpha_1\cdots\alpha_n$ y $T(\alpha) = \alpha_1 + \cdots + \alpha_n$ son enteros algebraicos. Al mismo tiempo son números racionales, así que $N(\alpha), T(\alpha) \in \mathbb{Z}$. ■

3.1.5. Proposición. *Se tiene*

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N(\alpha) = \pm 1\}.$$

Demostración. Si $\alpha \in \mathcal{O}_K$ tiene inverso $\alpha^{-1} \in \mathcal{O}_K$, entonces

$$N(\alpha)\,N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = 1.$$

Pero $N(\alpha^{\pm 1}) \in \mathbb{Z}$, así que $N(\alpha) = \pm 1$. Viceversa, si $\alpha \in \mathcal{O}_K$ y $N(\alpha) = \pm 1$, sean $\alpha_1 = \alpha$, α_2, …, α_n las raíces del polinomio característico de α. Tenemos

$$\alpha\alpha_2 \cdots \alpha_n = \pm 1,$$

y luego

$$\alpha^{-1} = \pm(\alpha_2 \cdots \alpha_n),$$

donde α_i son enteros algebraicos, así que el producto a la derecha está en $\mathcal{O}_K$[*]. ■

3.1.6. Ejemplo. Consideremos el campo cuadrático $K = \mathbb{Q}(\sqrt{d})$, donde d es libre de cuadrados. La multiplicación por $a + b\sqrt{d}$ en la base $1, \sqrt{d}$ se representa por la matriz

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Entonces,

$$N(a + b\sqrt{d}) = a^2 - db^2, \quad T(a + b\sqrt{d}) = 2a.$$

También calculamos

$$(a + b\sqrt{d})\,(a - b\sqrt{d}) = a^2 - db^2, \quad (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a. \qquad ▲$$

3.2 Recordatorio de álgebra lineal

Sea V un espacio vectorial de dimensión finita sobre un campo k. Consideremos una forma bilineal simétrica

$$\langle \cdot, \cdot \rangle \colon V \times V \to k.$$

Sea $e_1, \ldots, e_n$ una base de V. El **discriminante** de $\langle \cdot, \cdot \rangle$ respecto a esta base se define como

$$\Delta(e_1, \ldots, e_n) = \det(\langle e_i, e_j \rangle)_{i,j}.$$

El discriminante depende de la base. En general, si $f_1, \ldots, f_n$ son algunos elementos de V y $f_i = \sum_j a_{ij} e_j$, entonces calculamos que

$$\langle f_k, f_\ell \rangle = \langle \sum_i a_{ki} e_i, \sum_j a_{\ell j} e_j \rangle = \sum_{i,j} a_{ki}\,\langle e_i, e_j \rangle\, a_{\ell j}.$$

En términos de matrices,

$$(\langle f_i, f_j \rangle)_{i,j} = (a_{ij}) \cdot (\langle e_i, e_j \rangle)_{i,j} \cdot (a_{ij})^t.$$

Luego,

$$\det(\langle f_i, f_j \rangle)_{i,j} = \det(a_{ij})^2_{i,j} \cdot \det(\langle e_i, e_j \rangle)_{i,j}.$$

También recordemos que $f_1, \ldots, f_n$ es otra base de V si y solamente si $\det(a_{ij})_{i,j} \neq 0$.

Se dice que la forma $\langle \cdot, \cdot \rangle$ es **no degenerada** si se cumple una de las siguientes condiciones equivalentes:

1) el discriminante de $\langle \cdot, \cdot \rangle$ respecto a alguna base de V no es nulo;

2) $\langle \cdot, \cdot \rangle$ induce un isomorfismo entre V y el espacio dual $V^\vee = \mathrm{Hom}_k(V, k)$ mediante

$$\phi \colon V \xrightarrow{\cong} V^\vee, \quad v \mapsto (x \mapsto \langle v, x \rangle).$$

[*] No estamos diciendo que cada α_i está en K; esto sucede cuando $K/\mathbb{Q}$ es una extensión de Galois.

Ahora supongamos que se cumplen estas condiciones. Recordemos que el espacio dual $V^\vee$ tiene base $e_1^*, \dots, e_n^*$ definida por

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Usando el isomorfismo $\phi\colon V \cong V^\vee$ de arriba, podemos tomar los vectores $e_i' = \phi^{-1}(e_i^*)$, y luego $e_1', \dots, e_n'$ cumplen

$$\langle e_i', e_j \rangle = \delta_{ij}.$$

Podemos decir que $e_1', \dots, e_n'$ es la base **dual** a $e_1, \dots, e_n$ respecto a la forma bilineal.

3.3 Apareamiento de traza y el discriminante

3.3.1. Definición. Para una extensión de anillos $A \subset B$ tal que B es un A-módulo libre de rango n, el **apareamiento de traza**[*] es la forma A-bilineal simétrica

$$\langle \cdot, \cdot \rangle\colon B \times B \to A, \quad (x, y) \mapsto T_{B/A}(xy).$$

Para una base $e_1, \dots, e_n$ de B sobre A, el **discriminante** viene dado por

$$\Delta(e_1, \dots, e_n) = \det(\langle e_i, e_j \rangle)_{i,j}.$$

Si $f_1, \dots, f_n$ son otros elementos que se expresan en términos de los e_i mediante $f_i = \sum_j a_{ij} e_j$, entonces los mismos cálculos que vimos arriba nos dan la relación

$$\Delta(f_1, \dots, f_n) = \det(a_{ij})_{i,j}^2 \cdot \Delta(e_1, \dots, e_n).$$

Ahora $f_1, \dots, f_n$ es una base si y solamente si $(a_{ij})_{i,j}$ es una matriz invertible, lo que equivale a $\det(a_{ij})_{i,j} \in A^\times$. Entonces, si no queremos fijar una base particular, el discriminante está bien definido solamente salvo un factor de $(A^\times)^2$, como un elemento de $A^\times/(A^\times)^2$.

Sin embargo, en el caso particular cuando $A = \mathbb{Z}$, tenemos $(A^\times)^2 = 1$, así que el discriminante es un número entero bien definido. Vale la pena recordar esto como una definición. Como siempre nos interesan anillos de números $R \subset K$.

3.3.2. Definición. Sea R un anillo de números que es finitamente generado (y luego libre) como $\mathbb{Z}$-módulo. Entonces, **el discriminante** de R viene dado por

$$\Delta(R) = \det(\langle \alpha_i, \alpha_j \rangle)_{i,j},$$

donde $\alpha_1, \dots, \alpha_n$ es alguna base de R sobre $\mathbb{Z}$. (Como acabamos de notar, el resultado no depende de la base.)

3.3.3. Lema. *Sea R un $\mathbb{Z}$-módulo libre de rango n con una base $\alpha_1, \dots, \alpha_n$. Para $\beta_1, \dots, \beta_n \in R$ consideremos el $\mathbb{Z}$-submódulo generado por $\beta_1, \dots, \beta_n$:*

$$M = \mathbb{Z}\langle \beta_1, \dots, \beta_n \rangle.$$

Tenemos $\beta_i = \sum_j a_{ij}\alpha_j$ para $a_{ij} \in \mathbb{Z}$. Entonces,

$$[R : M] = \begin{cases} \infty, & \text{si } \det(a_{ij})_{i,j} = 0, \\ |\det(a_{ij})_{i,j}|, & \text{si } \det(a_{ij})_{i,j} \neq 0. \end{cases}$$

[*] En la primera versión de estos apuntes decía «emparejamiento» y luego me di cuenta de que en México es más común el término «apareamiento».

Demostración. Podemos identificar R con $\mathbb{Z}^n$ y el submódulo $M \subset R$ con la imagen de una aplicación $\mathbb{Z}$-lineal $A\colon \mathbb{Z}^n \to \mathbb{Z}^n$ (multiplicación por la matriz A).

Primero, si $\det A = 0$, esto significa que hay una dependencia $\mathbb{Z}$-lineal entre los vectores de M, así que $\operatorname{rk} M < n$, y el índice de M es infinito.

Podemos poner A en la **forma normal de Smith** (véase por ejemplo [Coh1993, Chapter 2])

$$B = \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix} = UAV,$$

donde B es una matriz diagonal y $U, V \in \mathrm{GL}_n(\mathbb{Z})$. Las aplicaciones $\mathbb{Z}$-lineales $U, V\colon \mathbb{Z}^n \to \mathbb{Z}^n$ son isomorfismos, así que $[\mathbb{Z}^n : A(\mathbb{Z}^n)] = [\mathbb{Z}^n : B(\mathbb{Z}^n)]$. Tenemos

$$\det B = \det(UAV) = \pm \det(A),$$

y luego

$$[\mathbb{Z}^n : B(\mathbb{Z}^n)] = \#(\mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_n\mathbb{Z}) = |\det B|. \qquad \blacksquare$$

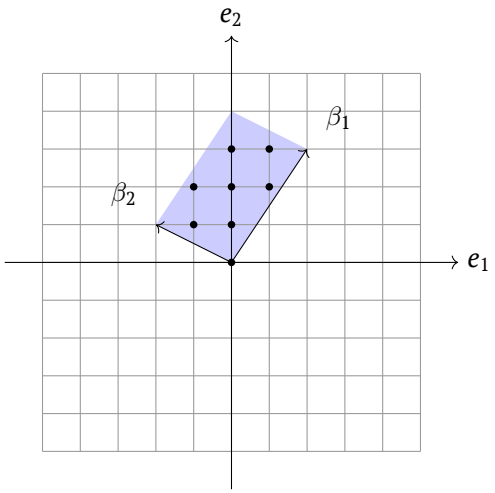
3.3.4. Ejemplo. Consideremos el subgrupo de $R = \mathbb{Z}^2$ generado por los vectores $\beta_1 = (2, 3)$ y $\beta_2 = (-2, 1)$. Estos corresponden a la matriz

$$A = \begin{pmatrix} 2 & -2 \\ 3 & 1 \end{pmatrix}.$$

La forma normal de Smith en este caso será

$$\begin{pmatrix} 1 & -6 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix} = \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}.$$

Entonces, el cociente de $\mathbb{Z}^2$ por $A(\mathbb{Z}^2)$ tiene 8 elementos. Aquí están dibujados los vectores β_1 y β_2 y ocho representantes del cociente $\mathbb{Z}^2/A(\mathbb{Z}^2)$.



▲

Esto nos lleva al siguiente resultado.

3.3.5. Proposición. *Sea R un anillo de números que es un $\mathbb{Z}$-módulo libre de rango n y $M \subseteq R$ un submódulo de rango n generado por algunos elementos $\beta_1, \ldots, \beta_n$. Luego,*

$$\Delta(M) = [R : M]^2 \cdot \Delta(R).$$

Demostración. $\Delta(M) = \Delta(\beta_1, \ldots, \beta_n) = \det(a_{ij})_{i,j}^2 \cdot \Delta(R)$, donde $|\det(a_{ij})| = [R : M]$. $\blacksquare$

3.4 Generación finita del anillo de enteros

Nuestro próximo objetivo es probar que para un campo de números el apareamiento de traza no es degenerado y sacar algunas consecuencias importantes de este resultado.

3.4.1. Lema. *Sea $K/\mathbb{Q}$ un campo de números y $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ sus diferentes encajes. Para una base $\alpha_1, \dots, \alpha_n \in K$, el discriminante correspondiente del apareamiento de traza viene dado por*

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))_{i,j}^2.$$

Demostración. Cálculo directo:

$$\langle \alpha_i, \alpha_j \rangle = T_{K/\mathbb{Q}}(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i)\, \sigma_k(\alpha_j).$$

Luego,

$$(\langle \alpha_i, \alpha_j \rangle)_{i,j} = (\sigma_i(\alpha_j))_{i,j}^t\, (\sigma_i(\alpha_j))_{i,j}.$$

Tomando los determinantes, se obtiene $\Delta(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))_{i,j}^2$. ■

3.4.2. Proposición. *Para un campo de números $K/\mathbb{Q}$ el apareamiento de traza*

$$\langle \cdot, \cdot \rangle \colon K \times K \to \mathbb{Q}, \quad (\alpha, \beta) \mapsto T_{K/\mathbb{Q}}(\alpha\beta)$$

es no degenerado.

Demostración. Si $\alpha_1, \dots, \alpha_n$ es alguna base de K sobre $\mathbb{Q}$, sería suficiente ver que

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))_{i,j}^2 \neq 0.$$

Esto es lo mismo que probar que los vectores de la matriz correspondiente son linealmente independientes. Lo último se sigue de la independencia lineal de los caracteres $\sigma_i \colon K^\times \to \mathbb{C}^\times$ (el lema de Dedekind; véase A.8.1).

A saber, una combinación lineal no trivial de las filas de $(\sigma_i(\alpha_j))_{i,j}$ sería

$$c_1\sigma_1(\alpha_j) + \cdots + c_n\sigma_n(\alpha_j) = 0$$

para todo $j = 1, \dots, n$. Por la linealidad, esto implica que

$$c_1\sigma_1(\alpha) + \cdots + c_n\sigma_n(\alpha) = 0$$

para todo $\alpha \in K^\times$, pero luego $c_1 = \cdots = c_n = 0$ según la independencia lineal de caracteres. ■

3.4.3. Teorema. *Sea $K/\mathbb{Q}$ un campo de números. Entonces, el anillo de enteros $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $n = [K : \mathbb{Q}]$.*

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \Big| n & & \Big| n \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Demostración. Sea $\alpha_1, \dots, \alpha_n \in K$ una base de K sobre $\mathbb{Q}$. Al multiplicar los α_i por un entero racional $N \in \mathbb{Z}$ suficientemente grande, podemos asumir que $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ (véase 2.5.9). Dado que el apareamiento de traza $\langle \cdot, \cdot \rangle$ es no degenerado, podemos tomar la base dual $\alpha_1', \dots, \alpha_n' \in K$ tal que

$$\langle \alpha_i, \alpha_j' \rangle = \delta_{ij}.$$

Todo $\alpha \in \mathcal{O}_K$ puede ser expresado como

$$\alpha = \sum_i a_i \alpha_i',$$

donde $a_i \in \mathbb{Q}$. En realidad, estos coeficientes son enteros:

$$a_i = \sum_j a_j \delta_{ij} = \sum_j a_j \langle \alpha_i, \alpha_j' \rangle = \langle \alpha_i, \sum_j a_j \alpha_j' \rangle = \langle \alpha_i, \alpha \rangle \in \mathbb{Z}$$

(usando que $\alpha, \alpha_i \in \mathcal{O}_K$. Entonces, tenemos

$$\alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z} \subseteq \mathcal{O}_K \subseteq \alpha_1' \mathbb{Z} \oplus \cdots \oplus \alpha_n' \mathbb{Z}.$$

Esto demuestra que $\mathcal{O}_K$ está entre dos $\mathbb{Z}$-módulos libres de rango n, y por lo tanto el mismo $\mathcal{O}_K$ es libre de rango n. ■

3.4.4. Comentario. El argumento de arriba usa de manera implícita la estructura de $\mathbb{Z}$-módulos finitamente generados. Si tenemos una extensión de campos de números L/K, entonces $\mathcal{O}_K \subset \mathcal{O}_L$, pero $\mathcal{O}_L$ no tiene por qué ser un $\mathcal{O}_K$-módulo libre: esto puede fallar si $\mathcal{O}_K$ no es un dominio de ideales principales. En general, un submódulo de un módulo libre no es necesariamente libre.

3.4.5. Corolario. *El anillo de enteros $\mathcal{O}_K$ es el subanillo más grande de K que es finitamente generado como $\mathbb{Z}$-módulo.*

Demostración. Ya vimos que el mismo $\mathcal{O}_K$ es finitamente generado. Por otra parte, si un subanillo $R \subset K$ es finitamente generado como $\mathbb{Z}$-módulo, entonces por nuestra caracterización de integridad (véase 2.5.5), todos elementos de R son enteros sobre $\mathbb{Z}$, y luego $R \subseteq \mathcal{O}_K$. ■

Un subanillo $R \subset K$ que es finitamente generado como $\mathbb{Z}$-módulo y tiene rango $n = [K : \mathbb{Q}]$ se llama un **orden**. El anillo de enteros $\mathcal{O}_K$ es entonces el **orden maximal**. La letra $\mathcal{O}$ viene del alemán *Ordnung*.

Ahora sabiendo que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre, tiene sentido dar la siguiente definición.

3.4.6. Definición. Dado un campo de números $K/\mathbb{Q}$, su **discriminante** es el discriminante del anillo de enteros $\mathcal{O}_K$:

$$\Delta_K = \Delta(\mathcal{O}_K).$$

3.4.7. Ejemplo. Consideremos un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$, donde como siempre d es un entero libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Tomemos $1, \sqrt{d}$ como su base sobre $\mathbb{Z}$ y calculamos

$$\Delta(\mathbb{Z}[\sqrt{d}]) = \det \begin{pmatrix} T(1) & T(\sqrt{d}) \\ T(\sqrt{d}) & T(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Si $d \equiv 1 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, y tomando como base 1, $\frac{1+\sqrt{d}}{2}$, calculamos

$$T\left(\left(\frac{1+\sqrt{d}}{2}\right)\right) = \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} = 1$$

y

$$T\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = T\left(\frac{1+2\sqrt{d}+d}{4}\right) = \frac{1+d}{2}.$$

Se obtiene

$$\Delta\left(\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

Entonces, para un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$ se tiene

$$\Delta_K = \begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2, 3 \pmod 4. \end{cases}$$

▲

3.5 Cálculos del discriminante y anillo de enteros

Clase 10
09/09/20

El discriminante puede ser calculado en términos de encajes $\sigma_i : K \hookrightarrow \mathbb{C}$. Ya hicimos este cálculo en 3.4.1: sustituyendo la fórmula

$$T_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

en la definición del discriminante, se obtiene lo siguiente.

3.5.1. Proposición. *Dado un anillo de números $R \subset K$ que es un $\mathbb{Z}$-módulo de rango $n = [K : \mathbb{Q}]$, sea $\alpha_1, \ldots, \alpha_n$ una base de R sobre $\mathbb{Z}$. Entonces, el discriminante viene dado por*

$$\Delta(R) = \det(\sigma_i(\alpha_j))_{i,j}^2.$$

Ahora consideremos la siguiente situación particular: dado un campo de números $K/\mathbb{Q}$, podemos escribir $K = \mathbb{Q}(\alpha)$, donde α es un entero algebraico (use el teorema del elemento primitivo y el hecho de que para un número algebraico α existe un entero racional no nulo $N \in \mathbb{Z}$ tal que $N\alpha$ es un entero algebraico). En este caso $R = \mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-submódulo de rango n con una base $1, \alpha, \ldots, \alpha^{n-1}$. Si $\alpha_1, \ldots, \alpha_n$ son diferentes raíces del polinomio mínimo de α sobre $\mathbb{Q}$, entonces $\sigma_i(\alpha) = \alpha_i$.

Tenemos

$$\Delta(\mathbb{Z}[\alpha]) = \det(\sigma_i(\alpha_j))_{i,j}^2 = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2.$$

Nos salió un determinante de Vandermonde:

$$\Delta(\mathbb{Z}[\alpha]) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Esta expresión es precisamente el discriminante del polinomio mínimo de α.

3.5.2. Definición. Para un polinomio mónico $f \in \mathbb{Q}[x]$ con raíces complejas $\alpha_1, \ldots, \alpha_n$ el **discriminante** viene dado por

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Entonces, hemos probado el siguiente resultado.

3.5.3. Proposición. *Dado un anillo de números $\mathbb{Z}[\alpha] \subset K$ que es un $\mathbb{Z}$-módulo de rango n, se tiene*

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f_{\mathbb{Q}}^{\alpha}).$$

Aunque el discriminante de polinomio está definido en términos de sus raíces complejas, la expresión

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

es invariante respecto a cualquier permutación de las raíces α_i, así que la teoría de Galois implica que $\Delta(f) \in \mathbb{Q}$. Además, los α_i son enteros algebraicos si f es mónico, así que $\Delta(f) \in \mathbb{Z}$. Hay una manera de calcular el discriminante usando álgebra lineal, sin calcular las raíces de f. Para esto se ocupa el resultante.

3.5.4. Definición. Dados dos polinomios

$$f = a\,(x - \alpha_1) \cdots (x - \alpha_m), \quad g = b\,(x - \beta_1) \cdots (x - \beta_n),$$

el **resultante** de f y g viene dado por una de las siguientes fórmulas equivalentes:

$$\operatorname{Res}(f,g) = a^n g(\alpha_1) \cdots g(\alpha_m) = (-1)^{mn} b^m f(\beta_1) \cdots f(\beta_n) = a^n b^m \prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} (\alpha_i - \beta_j).$$

3.5.5. Proposición. *Para un polinomio mónico*

$$f = (x - \alpha_1) \cdots (x - \alpha_n)$$

se tiene

$$\Delta(f) = (-1)^{\frac{n\,(n-1)}{2}}\ \mathrm{Res}(f, f').$$

Demostración. Si f tiene raíces múltiples, entonces $\Delta(f) = \mathrm{Res}(f, f') = 0$ (note que si α_i es una raíz múltiple, entonces esta es también una raíz de f'). Supongamos que las raíces de f son distintas. Tenemos

$$f'(x) = \sum_{1 \le i \le n} \prod_{j \ne i} (x - \alpha_j),$$

y luego

$$f'(\alpha_i) = \prod_{j \ne i} (\alpha_i - \alpha_j).$$

Ahora por la definición,

$$\mathrm{Res}(f, f') = f'(\alpha_1) \cdots f'(\alpha_n) = \prod_i \prod_{j \ne i} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n\,(n-1)}{2}} \Delta(f). \qquad \blacksquare$$

3.5.6. Corolario. *Para $K = \mathbb{Q}(\alpha)$, donde α es un entero algebraico y $f \in \mathbb{Z}[x]$ es el polinomio mínimo de α se tiene*

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f) = (-1)^{\frac{n\,(n-1)}{2}}\, N_{K/\mathbb{Q}}(f'(\alpha)).$$

Demostración. Tenemos

$$\mathrm{Res}(f, f') = f'(\alpha_1) \cdots f'(\alpha_n),$$

donde $\alpha_1, \ldots, \alpha_n$ son las raíces de f. En términos de encajes $\sigma_i \colon K \hookrightarrow \mathbb{C}$, tenemos $\alpha_i = \sigma_i(\alpha)$. Dado que $f \in \mathbb{Z}[x]$, tenemos $f' \in \mathbb{Z}[x]$, y luego $f'(\sigma_i(\alpha)) = \sigma_i(f'(\alpha))$. Entonces,

$$\mathrm{Res}(f, f') = \sigma_1(f'(\alpha)) \cdots \sigma_n(f'(\alpha)) = N_{K/\mathbb{Q}}(f'(\alpha)). \qquad \blacksquare$$

3.5.7. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_p)$, donde p es un primo impar. En este caso $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. El discriminante entonces viene dado por

$$\Delta_K = (-1)^{\binom{n}{2}}\, N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)).$$

Aquí $n = p - 1$, pero $\binom{n}{2} \equiv \frac{p-1}{2} \pmod 2$. Escribamos

$$x^p - 1 = (x - 1)\, \Phi_p(x),$$

y entonces

$$p\, x^{p-1} = \Phi_p(x) + (x - 1)\, \Phi_p'(x).$$

Sustituyendo $x = \zeta_p$, se obtiene

$$p\, \zeta_p^{p-1} = (\zeta_p - 1)\, \Phi_p'(\zeta_p).$$

Ahora

$$N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)) = \frac{p^{p-1}\, N_{K/\mathbb{Q}}(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(\zeta_p - 1)}.$$

Aquí $\zeta_p \in \mathcal{O}_K^\times$, y por lo tanto $N_{K/\mathbb{Q}}(\zeta_p)^{p-1} = (\pm 1)^{p-1} = 1$ (de hecho, la norma de ζ_p es igual a 1), y se ve que

$$N_{K/\mathbb{Q}}(\zeta_p - 1) = \Phi_p(1) = p.$$

Entonces,

$$\Delta_K = (-1)^{\frac{p-1}{2}}\, p^{p-2}. \qquad \blacktriangle$$

El resultante puede ser calculado de la siguiente manera.

3.5.8. Proposición. *Dados dos polinomios*

$$f = a_m x^m + \cdots + a_1 x + a_0, \quad g = b_n x^n + \cdots + b_1 x + b_0,$$

el resultante $\mathrm{Res}(f,g)$ *es igual al determinante de la siguiente matriz de* $(n+m)\times(n+m)$*:*

$$\begin{pmatrix}
a_m & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\
0 & a_m & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & 0 & a_m & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & a_m & a_{m-1} & a_{m-2} & \cdots & a_1 & a_0 \\
b_n & b_{n-1} & \cdots & b_2 & b_1 & b_0 & 0 & 0 & \cdots & 0 \\
0 & b_n & b_{n-1} & \cdots & b_2 & b_1 & b_0 & 0 & \cdots & 0 \\
0 & 0 & b_n & b_{n-1} & \cdots & b_2 & b_1 & b_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_2 & b_1 & b_0
\end{pmatrix}$$

(esta se conoce como la ***matriz de Sylvester****). Aquí los coeficientes de* f *se repiten en* $n = \deg(g)$ *filas y los coeficientes de* g *se repiten en* $m = \deg(f)$ *filas.*

A continuación no vamos a usar esta interpretación del resultante y la menciono solo para ser completo: a veces esto aparece como la definición del resultante. Para una prueba, véase por ejemplo [Coh1993, §3.3].

3.5.9. Ejemplo. Para el polinomio $f = x^2 + bx + c$ tenemos $f' = 2x + b$, y luego

$$\Delta(f) = -\det\begin{pmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{pmatrix} = b^2 - 4c.$$

Para el polinomio cúbico $f = x^3 + ax + b$ tenemos $f' = 3x^2 + a$ y

$$\Delta(f) = -\det\begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix} = \cdots = -(4a^3 + 27b^2). \qquad \blacktriangle$$

3.5.10. Ejemplo. Si d es un entero libre de cuadrados, entonces

$$\Delta(\mathbb{Z}[\sqrt{d}]) = \Delta(x^2 - d) = 4d.$$

Si $d \equiv 1 \pmod 4$, entonces

$$\Delta\Big(\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big]\Big) = \Delta\Big(x^2 - x - \frac{d-1}{4}\Big) = d. \qquad \blacktriangle$$

En PARI/GP, la función `poldisc(`f`)` calcula el discriminante de f, y `polresultant(`f`,`g`)` calcula el resultante.

Como un caso particular de 3.3.5 tenemos el siguiente resultado.

3.5.11. Proposición. *Sea* $K/\mathbb{Q}$ *un campo de números y* $\alpha \in \mathcal{O}_K$ *un entero algebraico de grado* $n = [K:\mathbb{Q}]$*. Entonces,*

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f_{\mathbb{Q}}^{\alpha}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K.$$

3.5.12. Ejemplo. Si d es un entero libre de cuadrados tal que $d \equiv 1 \pmod 4$, consideremos el campo cuadrático $K = \mathbb{Q}(\sqrt{d})$. En este caso

$$\mathcal{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big].$$

Notamos que

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus 2 \cdot \frac{1+\sqrt{d}}{2}\mathbb{Z},$$

así que

$$[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]] = 2.$$

Tenemos

$$\underbrace{\Delta(\mathbb{Z}[\sqrt{d}])}_{=4d} = \Big[\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big] : \mathbb{Z}[\sqrt{d}]\Big]^2 \cdot \underbrace{\Delta_K}_{=d}. \qquad \blacktriangle$$

La fórmula de 3.5.11 ayuda a calcular el anillo de enteros en ciertos casos.

3.5.13. Ejemplo. Consideremos el campo de números $K = \mathbb{Q}(\alpha)$, donde α es el entero algebraico tal que $\alpha^3 + \alpha - 1 = 0$. Calculamos

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(x^3 + x - 1) = -31.$$

Tenemos

$$\Delta(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]] \cdot \Delta_K,$$

pero -31 es libre de cuadrados, y entonces $\mathcal{O}_K = \mathbb{Z}[\alpha]$. $\blacktriangle$

3.5.14. Ejemplo. Calculamos que

$$\Delta(x^2 - x + 6) = \Delta(x^3 - x + 1) = -23.$$

Este número es libre de cuadrados, así que para los campos

$$K = \mathbb{Q}[\alpha]/(\alpha^2 - \alpha + 6) \cong \mathbb{Q}(\sqrt{-23})$$

y

$$K' = \mathbb{Q}[\beta]/(\beta^3 - \beta + 1)$$

tenemos

$$\mathcal{O}_K = \mathbb{Z}[\alpha], \quad \mathcal{O}_{K'} = \mathbb{Z}[\beta]. \qquad \blacktriangle$$

3.5.15. Comentario. El último ejemplo también demuestra que el discriminante de dos campos de números no isomorfos puede coincidir. Obviamente, si $K \cong K'$, entonces $\mathcal{O}_K \cong \mathcal{O}_{K'}$, y luego $\Delta_K = \Delta_{K'}$. Sin embargo, muy a menudo sucede que $\Delta_K = \Delta_{K'}$, pero $K \ncong K'$. El discriminante no es un invariante muy fino, pero este ayuda a enumerar los campos de números: más adelante veremos que hay solamente un número finito de campos de números (salvo isomorfismo) tales que $|\Delta_K| < C$ para alguna constante C.

3.5.16. Ejemplo (Dedekind). Consideremos el campo de números $K = \mathbb{Q}(\alpha)$, donde

$$\alpha^3 + \alpha^2 - 2\alpha + 8 = 0. \qquad (*)$$

Calculamos (con ayuda de computadora) que

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(x^3 + x^2 - 2x + 8) = -2^2 \cdot 503.$$

Aquí el número 503 es primo. Entonces, hay dos posibilidades: o tenemos $\mathcal{O}_K = \mathbb{Z}[\alpha]$, o $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 2$. En realidad, estamos en el segundo caso.

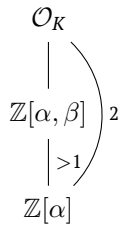
Primero, multiplicando (*) por $(2/\alpha)^3$, se obtiene

$$\frac{64}{\alpha^3} - \frac{16}{\alpha^2} + \frac{8}{\alpha} + 8 = 0.$$

Esto significa que

$$\beta = \frac{4}{\alpha} = -\frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + 1$$

es un entero algebraico. Sin embargo, $\beta \notin \mathbb{Z}[\alpha]$. Esto demuestra que $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$, pero luego tenemos



y entonces

$$\mathcal{O}_K = \mathbb{Z}[\alpha,\beta] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z}.$$

En efecto, $\alpha\beta = 4$, y se calcula que

$$\alpha^2 = 2 - \alpha - 2\beta, \quad \beta^2 = -2 - 2\alpha + \beta.$$

Dejo al lector confirmar que

$$\Delta(\mathbb{Z}[\alpha,\beta]) = -503.$$

De hecho, se puede ver que $\mathcal{O}_K$ no es de la forma $\mathbb{Z}[\gamma]$ para ningún entero algebraico γ. Primero, se puede ver (con ayuda de PARI/GP) que en $\mathcal{O}_K = \mathbb{Z}[\alpha,\beta]$ se tiene factorización en ideales primos

$$2\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3,$$

donde

$$\mathfrak{p}_1 = (2 - \alpha - \beta), \quad \mathfrak{p}_2 = (5 - 3\alpha - 2\beta), \quad \mathfrak{p}_3 = (7 - 4\alpha - 3\beta).$$

Ahora supongamos que $\mathcal{O}_K = \mathbb{Z}[\gamma] = \mathbb{Z}[x]/(f)$ para algún polinomio mónico irreducible f de grado 3. El teorema de Kummer–Dedekind (2.7.3) nos dice que para factorizar $2\mathcal{O}_K$ en ideales primos, hay que factorizar el polinomio f en $\mathbb{F}_2[x]$. Los polinomios irreducibles en $\mathbb{F}_2[x]$ son los siguientes:

$$\begin{aligned}
&\deg = 1\colon x,\ x+1,\\
&\deg = 2\colon x^2+x+1,\\
&\deg = 3\colon x^2+x+1,\ x^3+x^2+1.
\end{aligned}$$

Esto significa que f no puede ser expresado como producto de tres diferentes polinomios irreducibles. En términos de factorización del ideal $2\mathcal{O}_K$, esto excluye la factorización de la forma $2\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$. ▲

Clase 11
14/09/20

En general, para encontrar el anillo de enteros $\mathcal{O}_K$, puede servir la siguiente observación.

3.5.17. Proposición. *Para un campo de números $K/\mathbb{Q}$, sea $R \subset K$ un $\mathbb{Z}$-submódulo libre de rango $n = [K:\mathbb{Q}]$. Luego, se tiene*

$$R \subseteq \mathcal{O}_K \subseteq \frac{1}{d}R, \quad \textit{donde } d = \Delta(R).$$

Demostración. Sea $\beta_1, \ldots, \beta_n \in R$ una base de R sobre $\mathbb{Z}$. Expresamos un elemento arbitrario $\alpha \in \mathcal{O}_K$ como

$$\alpha = x_1\beta_1 + \cdots + x_n\beta_n,$$

donde $x_i \in \mathbb{Q}$. Aplicamos a esta expresión los encajes

$$\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}.$$

Se obtiene un sistema de ecuaciones lineales

$$\begin{aligned}\sigma_1(\alpha) &= x_1\sigma_1(\beta_1) + \cdots + x_n\sigma_1(\beta_n),\\ &\cdots\\ \sigma_n(\alpha) &= x_1\sigma_n(\beta_1) + \cdots + x_n\sigma_n(\beta_n).\end{aligned}$$

Podemos expresar los x_i usando la **regla de Cramer**:

$$x_i = \frac{\gamma_i}{\delta},$$

donde

$$\delta = \det \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix},$$

y γ_i es el determinante de la misma matriz, donde en lugar de la i-ésima columna está $(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))^t$.

Como ya sabemos, $d = \Delta(R) = \delta^2$. Entonces, podemos escribir $x_i = \frac{\gamma_i\delta}{d}$. Aquí $\gamma_i\delta = dx_i \in \mathbb{Q}$, pero al mismo tiempo $\gamma_i\delta$ es un entero algebraico, así que $\gamma_i\delta \in \mathbb{Z}$. Entonces, hemos probado que

$$\alpha \in \frac{\beta_1}{d}\mathbb{Z} \oplus \cdots \oplus \frac{\beta_n}{d}\mathbb{Z} = \frac{1}{d}R. \qquad \blacksquare$$

3.5.18. Comentario. He aquí algunas observaciones al respecto.

1. Dado que $R \subseteq \mathcal{O}_K$, toda clase lateral en $\frac{1}{d}R/R$ consiste en enteros algebraicos o no contiene ningún entero algebraico.
2. Tenemos $d = [\mathcal{O}_K : R]^2 \cdot \Delta_K$, así que para ver cuáles elementos de $\mathcal{O}_K$ no están en R, es suficiente considerar las clases laterales en $\frac{1}{m}R/R$, donde $m^2 \mid d$.
3. Se tiene $[\frac{1}{m}R : R] = m^n$, y por lo tanto este método es útil solo cuando el discriminante es relativamente pequeño.

La proposición de arriba solo nos dice que $\mathcal{O}_K$ es calculable; en realidad para calcular $\mathcal{O}_K$ se usan métodos más sofisticados. Véase por ejemplo [Coh1993, §6.1]. También recomiendo el artículo panorámico de Lenstra [Len1992].

3.5.19. Ejemplo. Consideremos el campo cúbico $K = \mathbb{Q}(\sqrt[3]{19})$. Primero para $\alpha = \sqrt[3]{19}$ calculamos

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(x^3 - 19) = -27 \cdot 19^2 = -3^3 \cdot 19^2.$$

Entonces,

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = m = 1, 3, 19, 3 \cdot 19.$$

Vamos a ver si algunos elementos de la forma

$$\frac{a}{m} + \frac{b}{m}\alpha + \frac{c}{m}\alpha^2,$$

donde $0 \leq a, b, c < m$ son enteros algebraicos.

```
polisintegral (f) = denominator(content(f)) == 1;

test (m) = {
  for (a=0,m-1,
    for (b=0,m-1,
      for (c=0,m-1,
        local (elt = (a + b*x + c*x^2)/m);
        if (polisintegral (minpoly (Mod(elt, x^3 - 19))),
          print (elt)
        )
      )
    )
  )
};

? test(3*19)
0
1/3*x^2 + 1/3*x + 1/3
2/3*x^2 + 2/3*x + 2/3
```

Los únicos elementos integrales que nos salieron son

$$\beta = \frac{1}{3}(1 + \alpha + \alpha^2), \quad 2\beta,$$

y luego $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$. Tenemos entonces

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3, \quad \Delta_K = -3 \cdot 19^2.$$ ▲

Este ejemplo solamente demuestra el procedimiento general. En realidad, si d es libre de cuadrados, no es difícil probar que para $K = \mathbb{Q}(\sqrt[3]{d})$ se tiene $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\sqrt[3]{d}]$. Véase el ejercicio 3.6.

3.6 Versión más general de Kummer–Dedekind

Hemos visto en §2.7 que para un anillo $R = \mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f)$, donde α es un entero algebraico, la factorización de un ideal pR en ideales primos corresponde a la factorización del polinomio f en $\mathbb{F}_p[x]$:

$$pR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} \longleftrightarrow \bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_s^{e_s} \text{ en } \mathbb{F}_p[x].$$

Pero esto funciona solamente cuando los ideales $\mathfrak{p}_i$ son invertibles. En particular, esto funciona si $\mathbb{Z}[\alpha] = \mathcal{O}_K$ es el anillo de enteros de $K = \mathbb{Q}(\alpha)$. ¿Qué hacer si $\mathcal{O}_K$ no es de la forma $\mathbb{Z}[\alpha]$?

Resulta que los primos problemáticos son solamente los que dividen al índice $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

3.6.1. Proposición. *Sea K un campo de números tal que $K = \mathbb{Q}(\alpha)$, donde α es un entero algebraico. Para un primo racional p tal que $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ el homomorfismo natural*

$$\mathbb{Z}[\alpha]/(p) \to \mathcal{O}_K/(p)$$

inducido por la inclusión $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ es un isomorfismo.

Demostración. Pongamos $m = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ y consideremos el siguiente diagrama:

$$\begin{array}{ccccc} m\mathcal{O}_K & \hookrightarrow & \mathbb{Z}[\alpha] & \hookrightarrow & \mathcal{O}_K \\ \downarrow & & \downarrow & & \downarrow \\ m\mathcal{O}_K/(p) & \longrightarrow & \mathbb{Z}[\alpha]/(p) & \longrightarrow & \mathcal{O}_K/(p) \end{array}$$

Aquí el homomorfismo $m\mathcal{O}_K/(p) \to \mathcal{O}_K/(p)$ es sobreyectivo: por nuestra hipótesis m es invertible módulo p: tenemos $mm' \equiv 1 \pmod{p}$ para algún m'. Luego, dado $x + (p) \in \mathcal{O}_K/(p)$, podemos escribirlo como

$$x + (p) = xmm' + (p) \in m\mathcal{O}_K/(p).$$

Entonces, $\mathbb{Z}[\alpha]/(p) \to \mathcal{O}_K/(p)$ es un homomorfismo sobreyectivo. Pero $\mathbb{Z}[\alpha]$ y $\mathcal{O}_K$ son $\mathbb{Z}$-módulos libres de rango $n = [K : \mathbb{Q}]$, así que

$$\#(\mathbb{Z}[\alpha]/(p)) = \#(\mathcal{O}_K/(p)) = p^n,$$

y se trata de un isomorfismo. ■

3.6.2. Ejemplo. Volvamos al ejemplo 3.5.19. Consideremos el campo $K = \mathbb{Q}(\sqrt[3]{19})$. Tenemos

$$\mathcal{O}_K = \mathbb{Z}[\alpha, \beta], \quad \alpha = \sqrt[3]{19}, \quad \beta = \frac{1}{3}(\alpha^2 + \alpha + 1).$$

Hemos calculado que

$$\Delta_K = -3 \cdot 19^2, \quad \Delta(\mathbb{Z}[\alpha]) = -3^3 \cdot 19^2.$$

El polinomio mínimo de β viene dado por

$$x^3 - x^2 - 6x - 12,$$

de donde se calcula

$$\Delta(\mathbb{Z}[\beta]) = -2^2 \cdot 3 \cdot 19^2.$$

```
? minpoly (Mod(1/3*(x^2+x+1), x^3-19))
% = x^3 - x^2 - 6*x - 12
? poldisc(%)
% = -4332
? factor(%)
% =
[-1 1]

[ 2 2]

[ 3 1]

[19 2]
```

Tenemos entonces

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3, \quad [\mathcal{O}_K : \mathbb{Z}[\beta]] = 2.$$

Esto significa que para factorizar $3\mathcal{O}_K$, podemos ocupar el anillo $\mathbb{Z}[\beta]$. Se tiene

$$x^3 - x^2 - 6x - 12 = x^2(x - 1) \quad \text{en } \mathbb{F}_3[x].$$

Para cualquier otro primo racional $p \neq 3$, podemos ocupar el anillo $\mathbb{Z}[\alpha]$; es decir, factorizar el polinomio $f = x^3 - 19$. Por ejemplo,

$$\bar{f} = (x+1)\,(x^2+x+1) \quad \text{en } \mathbb{F}_2[x].$$

He aquí algunas observaciones.

- Si $p = 19$, entonces $\bar{f} = x^3$. Supongamos ahora que $p \neq 19$.
- Si $p \equiv 2 \pmod 3$, entonces $x \mapsto x^3$ es un automorfismo de $\mathbb{F}_p^\times$, así que existe único $x \in \mathbb{F}_p$ tal que $x^3 = 19$. Esto significa que $\bar{f}$ tiene un factor lineal y otro cuadrático.
- Si $p \equiv 1 \pmod 3$, entonces $\mathbb{F}_p^\times$ contiene un elemento $\zeta \neq 1$ tal que $\zeta^3 = 1$. Hay dos posibilidades: o 19 no es un cubo módulo p, y en este caso f es irreducible, o $19 \equiv a^3 \pmod p$, y luego

$$\bar{f} = (x-a)\,(x-\zeta a)\,(x-\zeta^2 a).$$

Entonces, la factorización de primos racionales en $\mathcal{O}_K$ es la siguiente

- $3\mathcal{O}_K = \mathfrak{p}_1^2\,\mathfrak{p}_2$, donde $f_1 = f_2 = 1$.
- $19\mathcal{O}_K = \mathfrak{p}^3$, donde $\mathfrak{p} = \sqrt[3]{19}\mathcal{O}_K$ y $f = 1$.
- Si $p \equiv 2 \pmod 3$, entonces $p\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$, donde $f_1 = 1, f_2 = 2$.
- Si $p \neq 19$ y $p \equiv 1 \pmod 3$, entonces hay dos opciones.
  Si 19 no es un cubo módulo p, entonces $\mathfrak{p} = p\mathcal{O}_K$ es un ideal primo.
  Si 19 es un cubo módulo p, entonces $p\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$, donde $f_1 = f_2 = f_3 = 1$.

Para ver de manera eficaz si 19 es un cubo módulo $p \equiv 1 \pmod 3$, podemos factorizar $p = \pi\overline{\pi}$ en $\mathbb{Z}[\zeta_3]$. Aquí $\mathbb{Z}[\zeta_3]/(\pi) \cong \mathbb{F}_p$, así que la respuesta depende del símbolo de Legendre $\left(\frac{19}{\pi}\right)_3$ que puede ser calculado usando la reciprocidad cúbica. Notamos que $19 = \rho\,\overline{\rho}$ en $\mathbb{Z}[\zeta_3]$, donde $\rho = 3\zeta_3 + 5$ y $\overline{\rho} = -3\zeta_3 + 2$. ▲

3.7 Ramificación

3.7.1. Definición. Sea $K/\mathbb{Q}$ un campo de números. Para un primo racional $p \in \mathbb{Z}$ consideremos su factorización en ideales primos en $\mathcal{O}_K$:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

donde $e_i \geq 1$. En este caso $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_{p^{f_i}}$, y los números f_i se llaman los **grados de campos residuales**. Los números e_i se llaman los **índices de ramificación**. Si $e_i > 1$ para algún i, se dice que p **se ramifica** en K.

3.7.2. Teorema. *En la situación de arriba se tiene*

$$\sum_i e_i f_i = [K : \mathbb{Q}].$$

Antes de probar este resultado, sería oportuno introducir las normas de ideales.

3.7.3. Definición. Sea K un campo de números. Para un ideal no nulo $I \subset \mathcal{O}_K$ su **norma** se define mediante

$$N_{K/\mathbb{Q}}(I) = \#(\mathcal{O}_K/I).$$

Para el ideal nulo, se puede poner $N_{K/\mathbb{Q}}(I) = 0$.

p	$p\mathcal{O}_K$	f	$p\,(3)$	p	$p\mathcal{O}_K$	f	$p\,(3)$
2	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	127	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1
3	$\mathfrak{p}_1\,\mathfrak{p}_2^2$	$(1,1)$	0	131	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
5	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	137	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
7	$\mathfrak{p}$	3	1	139	$\mathfrak{p}$	3	1
11	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	149	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
13	$\mathfrak{p}$	3	1	151	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1
17	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	157	$\mathfrak{p}$	3	1
19	$\mathfrak{p}^3$	1	1	163	$\mathfrak{p}$	3	1
23	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	167	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
29	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	173	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
31	$\mathfrak{p}$	3	1	179	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
37	$\mathfrak{p}$	3	1	181	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1
41	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	191	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
43	$\mathfrak{p}$	3	1	193	$\mathfrak{p}$	3	1
47	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	197	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
53	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	199	$\mathfrak{p}$	3	1
59	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	211	$\mathfrak{p}$	3	1
61	$\mathfrak{p}$	3	1	223	$\mathfrak{p}$	3	1
67	$\mathfrak{p}$	3	1	227	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
71	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	229	$\mathfrak{p}$	3	1
73	$\mathfrak{p}$	3	1	233	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
79	$\mathfrak{p}$	3	1	239	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
83	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	241	$\mathfrak{p}$	3	1
89	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	251	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
97	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1	257	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
101	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	263	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
103	$\mathfrak{p}$	3	1	269	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2
107	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	271	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1
109	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1	277	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	$(1,1,1)$	1
113	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2	281	$\mathfrak{p}_1\,\mathfrak{p}_2$	$(1,2)$	2

Figura 3.1: Factorización de $p\mathcal{O}_K$ para $K = \mathbb{Q}(\sqrt[3]{19})$

3.7.4. Lema. *1) La norma es multiplicativa:*

$$N_{K/\mathbb{Q}}(IJ) = N_{K/\mathbb{Q}}(I)\, N_{K/\mathbb{Q}}(J).$$

2) La norma de un ideal principal es el valor absoluto de la norma habitual de su generador:

$$N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Demostración. Todo ideal no nulo en $\mathcal{O}_K$ se descompone de manera única en ideales primos, así que para la parte 1) basta ver que

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_s)^{e_s}.$$

Primero, por el teorema chino del resto se tiene

$$N(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}) = N(\mathfrak{p}_1^{e_1}) \cdots N(\mathfrak{p}_s^{e_s}).$$

Luego, hemos visto en 2.7.1 que para cualquier anillo de números R y un ideal primo invertible $\mathfrak{p} \subset R$ se cumple

$$N(\mathfrak{p}^e) = N(\mathfrak{p})^e,$$

y en $\mathcal{O}_K$ todo ideal no nulo es invertible. Esto establece la parte 1).

Para la parte 2), notamos que $\alpha\mathcal{O}_K$ es la imagen de la aplicación $\mathbb{Z}$-lineal de multiplicación por α:

$$\mu_\alpha \colon \mathcal{O}_K \to \mathcal{O}_K, \quad x \mapsto \alpha x.$$

Entonces, como fue observado en 3.3.3, se tiene

$$[\mathcal{O}_K : \alpha\mathcal{O}_K] = |\det(\mu_\alpha)|.$$

Por la definición,

$$\det(\mu_\alpha) = N_{\mathcal{O}_K/\mathbb{Z}}(\alpha) = N_{K/\mathbb{Q}}(\alpha).$$ ■

3.7.5. Ejemplo. Consideremos el anillo $\mathbb{Z}[i]$. Para $\alpha = a + bi \in \mathbb{Z}[i]$ no es difícil ver que el ideal generado por α está generado como $\mathbb{Z}$-módulo por $a + bi$ y $a - bi$:

$$\alpha\mathbb{Z}[i] = \{(c + di)\,(a + bi) \mid c, d \in \mathbb{Z}\} = \{c \cdot (a + bi) + d \cdot (-b + ai) \mid c, d \in \mathbb{Z}\}.$$

Ahora el número de elementos en el cociente de $\mathbb{Z}^2$ por el $\mathbb{Z}$-submódulo generado por (a, b) y $(-b, a)$ viene dado por

$$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 = N(a + bi).$$ ▲

Demostración de . Sacando las normas, tenemos

$$N(p\mathcal{O}_K) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_s)^{e_s},$$

donde $N(p\mathcal{O}_K) = |N_{K/\mathbb{Q}}(p)| = p^n$ y $N(\mathfrak{p}_i) = p^{f_i}$. ■

Más adelante veremos que si $K/\mathbb{Q}$ es una extensión de Galois, entonces $f_1 = \cdots = f_s$ y $e_1 = \cdots = e_s$.

3.7.1 Discriminante y ramificación

Ahora sea α un entero algebraico y $f \in \mathbb{Z}[x]$ su polinomio mínimo. Ahora si para un primo racional p se tiene

$$p \mid \Delta(f) = \prod_{1 \le i \le n} (\alpha_i - \alpha_j)^2,$$

esto significa que el polinomio $\bar{f} \in \mathbb{F}_p[x]$ tiene una raíz múltiple en $\overline{\mathbb{F}}_p$, y por lo tanto un factor múltiple módulo p:

$$\bar{f} = \overline{g}_1^{e_1} \cdots \overline{g}_s^{e_s} \quad \text{en } \mathbb{F}_p[x],$$

donde $e_i > 1$ para algún i. En vista del teorema de Kummer–Dedekind, estas consideraciones sugieren el siguiente resultado.

3.7.6. Teorema. *Para un campo de números $K/\mathbb{Q}$, un primo racional p se ramifica en K si solamente si $p \mid \Delta_K$.*

Sin embargo, no todos los anillos de enteros tienen forma $\mathbb{Z}[\alpha]$, así que necesitamos trabajar más para la prueba. Primero vamos a formular algunos lemas sobre discriminantes de álgebras sobre campos. En este caso el discriminante depende de una base particular, pero por abuso de lenguaje hablaremos *del* discriminante, porque al final nos interesará solo si este es nulo o no.

3.7.7. Lema. *Se tiene*

$$\Delta_K \bmod p = \Delta(\mathcal{O}_K/(p)/\mathbb{F}_p),$$

donde a la derecha está el discriminante de la $\mathbb{F}_p$-álgebra $\mathcal{O}_K/(p)$.

Demostración. La reducción módulo p nos da una $\mathbb{F}_p$-álgebra $\mathcal{O}_K/(p) \cong \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{F}_p$. Los determinantes y trazas conmutan con productos tensoriales, y en particular, el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/(p) \\ {\scriptstyle N}\downarrow\downarrow{\scriptstyle T} & & {\scriptstyle N}\downarrow\downarrow{\scriptstyle T} \\ \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \end{array}$$

Ahora si $\alpha_1, \ldots, \alpha_n$ es una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$, entonces $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ es una base de $\mathcal{O}_K/(p)$ sobre $\mathbb{F}_p$. Tenemos

$$\Delta_K = \det(T_{\mathcal{O}_K/\mathbb{Z}}(\alpha_i \alpha_j)),$$

y la reducción módulo p nos da

$$\overline{\Delta_K} = \det(T_{\mathcal{O}_K/(p)/\mathbb{F}_p}(\overline{\alpha_i}\overline{\alpha_j})).$$

Lo que está a la derecha, es el discriminante de $\mathcal{O}_K/(p)$ respecto a la base particular $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$. ∎

3.7.8. Lema. *Para un campo k, sean A y B dos k-álgebras de dimensión finita. Luego, para el producto de A y B se tiene*

$$\Delta(A \times B/k) = \Delta(A/k) \times \Delta(B/k).$$

Demostración. Si $a_1, \ldots, a_m$ es una base de A sobre k y $b_1, \ldots, b_n$ es una base de B sobre k, entonces

$$(a_1, 0), \ldots, (a_m, 0), \quad (0, b_1), \ldots, (0, b_n)$$

es una base de $A \times B$. Ahora el discriminante de $A \times B$ respecto a esta base es

$$\det \begin{pmatrix} (T(a_i a_j))_{i,j} & O \\ O & (T(b_k b_\ell))_{k,\ell} \end{pmatrix} = \Delta(A/k) \times \Delta(B/k).$$ ∎

3.7.9. Lema. *Para un ideal primo $\mathfrak{p} \subset \mathcal{O}_K$ se tiene $\Delta(\mathcal{O}_K/\mathfrak{p}^e/\mathbb{F}_p) = 0$ si y solamente si $e > 1$.*

Demostración. Denotemos $A = \mathcal{O}_K/\mathfrak{p}^e$. Si $e = 1$, entonces $A \cong \mathbb{F}_{p^f}$ es una extensión finita de $\mathbb{F}_p$. Estas extensiones son separables y tienen forma $\mathbb{F}_p[x]/(g)$, donde f es un polinomio irreducible, y sus raíces α_i en la cerradura algebraica $\overline{\mathbb{F}_p}$ son distintas:

$$g = (x - \alpha_1) \cdots (x - \alpha_f), \quad \alpha_i \neq \alpha_j.$$

Los cálculos parecidos a los que vimos arriba* nos dicen que

$$\Delta(A/\mathbb{F}_p) = \Delta(g) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \neq 0.$$

Supongamos ahora que $e > 1$. Podemos escoger una base de A que contiene un elemento representado por $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$. En este caso $\overline{\alpha} \neq 0$, pero $\overline{\alpha}^n = 0$, así que tenemos un nilpotente. Para cualquier otro elemento $\overline{\beta} \in A$, se obtiene un operador lineal nilpotente $\mu_{\overline{\alpha\beta}} \colon A \to A$, y su traza es nula**. Entonces, $T_{A/\mathbb{F}_p}(\overline{\alpha\beta}) = 0$ para todo $\overline{\beta} \in A$, así que $\Delta(A/\mathbb{F}_p) = 0$. ■

Demostración del teorema 3.7.6. Consideremos la factorización

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}.$$

Ocupando el teorema chino del resto, se obtiene un isomorfismo de $\mathbb{F}_p$-álgebras

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_s^{e_s}.$$

Gracias a los lemas de arriba,

$$\Delta_K \bmod p = \prod_i \Delta(\mathcal{O}_K/\mathfrak{p}_i^{e_i}/\mathbb{F}_p),$$

y el producto es nulo si y solamente si $e_i > 1$ para algún i. ■

3.7.10. Corolario. *Para un campo de números $K/\mathbb{Q}$ hay solamente un número finito de primos $p \in \mathbb{Z}$ que se ramifican en K.*

Más adelante también veremos que para toda extensión no trivial $K/\mathbb{Q}$ se tiene $|\Delta_K| > 1$, así que algún primo siempre se ramifica.

3.7.11. Ejemplo. Consideremos un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$, donde d es libre de cuadrados. Los primos impares que se ramifican en K son precisamente $p \mid d$. Además, si $d \equiv 2, 3 \pmod 4$, entonces 2 también se ramifica. Si $d \equiv 1 \pmod 4$, entonces 2 no se ramifica. Toda está información está contenida en el discriminante

$$\Delta_K = \begin{cases} d, & d \equiv 1 \pmod 4, \\ 4d, & d \equiv 2, 3 \pmod 4. \end{cases}$$ ▲

3.7.12. Ejemplo. Para el campo ciclotómico $K = \mathbb{Q}(\zeta_p)$ el único primo que se ramifica es el mismo p (véase 2.7.11). Por otra parte, calculamos en 3.5.7 que el discriminante es igual a

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

Este es un número bastante grande, pero su único divisor primo es p. ▲

3.7.13. Ejemplo. Como vimos en 3.6.2, para el campo $K = \mathbb{Q}(\sqrt[3]{19})$ tenemos $\Delta_K = -3 \cdot 19^2$, y los únicos primos que se ramifican en K son 3 y 19. ▲

3.8 Teoremas de Brill y Stickelberger

Clase 12
21/09/20

Hemos explicado el significado de los divisores primos del discriminante Δ_K. El discriminante también tiene signo, y no es difícil entender su significado. Será oportuno primero dar una definición.

3.8.1. Definición. Para un campo de números $K/\mathbb{Q}$, consideremos sus encajes

$$\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{Q}.$$

Si $\sigma_i(K) \subset \mathbb{R}$, se dice que σ_i es un encaje **real**. En el caso contrario, se dice que σ_i es un encaje **complejo**. Notamos que para cada encaje complejo σ_i su conjugado $\overline{\sigma_i} \neq \sigma_i$ es también un encaje. Entonces, tenemos

$$r_1 + 2r_2 = n = [K : \mathbb{Q}],$$

donde r_1 es el número de encajes reales y $2r_2$ es el número de encajes complejos. Se dice que (r_1, r_2) es la **signatura** de K.

En términos sencillos, si $K = \mathbb{Q}(\alpha)$ y $f = f_{\mathbb{Q}}^{\alpha}$ es el polinomio mínimo de α, entonces r_1 es el número de raíces reales de f, mientras que $2r_2$ es el número de sus raíces complejas.

3.8.2. Proposición (Brill[*]). *El signo de Δ_K es $(-1)^{r_2}$.*

Demostración. Escribamos $K = \mathbb{Q}(\alpha)$, donde α es un entero algebraico, $f \in \mathbb{Z}[x]$ su polinomio mínimo y α_i las raíces complejas de f. Tenemos

$$\Delta(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K,$$

así que el signo de Δ_K coincide con el signo de

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

Dejo como un ejercicio verificar que el signo de la última expresión será precisamente $(-1)^{r_2}$, donde $2r_2$ es el número de raíces complejas. ■

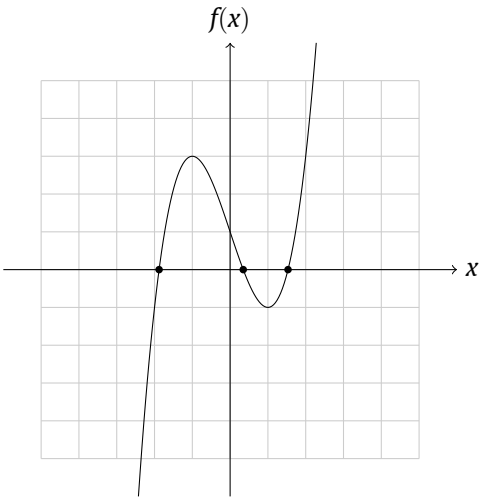
3.8.3. Ejemplo. He aquí una pequeña lista de campos con sus signaturas y discriminantes.

K	r_1	r_2	Δ_K
$\mathbb{Q}(\sqrt{d})$ donde $d > 1$	2	0	d o $4d$
$\mathbb{Q}(\sqrt{d})$ donde $d < 0$	0	1	d o $4d$
$\mathbb{Q}(\sqrt[3]{2})$	1	1	$-2^2 \cdot 3^3$
$\mathbb{Q}(\alpha)$ donde $\alpha^3 - 3\alpha + 1 = 0$	3	0	$+3^4$
$\mathbb{Q}(\zeta_p)$	0	$(p-1)/2$	$(-1)^{\frac{p-1}{2}} p^{p-2}$

En el caso de $f(x) = x^3 - 3x + 1$, notamos que el polinomio tiene tres raíces reales:

$$f(-2) = -1, \quad f(-1) = 3, \quad f(1) = -1, \quad f(2) = 3.$$

[*] Tal vez tenía que formular algunos lemas en la generalidad adecuada, para extensiones separables de campos...
[**] Ejercicio: para un operador lineal nilpotente $f\colon V \to V$ todos los valores propios en $\overline{\mathbb{F}_p}$ son nulos.
[*] Alexander von Brill (1842–1935)



Cabe mencionar que para encontrar el número de raíces reales de $f^{\alpha}_{\mathbb{Q}}$, y como consecuencia la signatura de $K = \mathbb{Q}(\alpha)$, no hay que calcular las mismas raíces; se puede usar algo como la **regla de los signos de Descartes**. ▲

El siguiente resultado también nos dice cuál es el resto de Δ_K módulo 4.

3.8.4. Proposición (Stickelberger[*]). *Se tiene* $\Delta_K \equiv 0$ *o* $1 \pmod 4$.

Demostración. Si $\alpha_1, \ldots, \alpha_n$ es una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$ y $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ son los encajes, entonces

$$\Delta_K = \det(\sigma_i(\alpha_j))^2.$$

Escribamos

$$\det(\sigma_i(\alpha_j)) = \sum_{\rho \in S_n} \operatorname{sgn}(\rho) \cdot \sigma_{\rho(1)}(\alpha_1) \cdots \sigma_{\rho(n)}(\alpha_n).$$

Denotemos por P los términos con $\operatorname{sgn}(\rho) = +1$ y por N los términos con $\operatorname{sgn}(\rho) = -1$. Ahora

$$\Delta_K = (P - N)^2 = (P + N)^2 - 4PN.$$

Notamos que las expresiones $P + N$ y PN son invariantes respecto a cualquier permutación de raíces, así que la teoría de Galois implica que son números racionales. Además, son enteros algebraicos, y por lo tanto $P + N, PN \in \mathbb{Z}$. Entonces, Δ_K es un cuadrado módulo 4. ■

3.8.5. Ejemplo. Consideremos un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$ donde d es libre de cuadrados. Tomamos $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \sqrt{d}\mathbb{Z}$ y calculamos

$$\Delta(\mathbb{Z}[\sqrt{d}]) = 4d = [\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]^2 \cdot \Delta_K.$$

Dado que d es libre de cuadrados, hay solo dos opciones: $\Delta_K = d$ o $4d$. Si $d \equiv 2, 3 \pmod 4$, entonces Stickelberger nos dice que necesariamente $\Delta_K = 4d$, y luego $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

Si $d \equiv 1 \pmod 4$, entonces Stickelberger no nos ayuda, pero basta calcular que $\frac{1+\sqrt{d}}{2}$ es entero y luego

$$\Delta(\mathbb{Z}\Big[\frac{1+\sqrt{d}}{2}\Big]) = d = [\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]^2 \cdot \Delta_K,$$

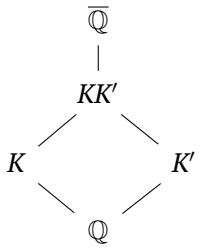
de donde $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, dado que d es libre de cuadrados. ▲

[*] Ludwig Stickelberger (1850–1936)

3.9 Campos linealmente disjuntos

Nuestro próximo objetivo será, como fue prometido, calcular que el anillo de enteros del n-ésimo campo ciclotómico $\mathbb{Q}(\zeta_n)$ es $\mathbb{Z}[\zeta_n]$. Primero, tenemos que hacer una digresión sobre campos linealmente disjuntos.

3.9.1. Definición. Para dos extensiones finitas $K/\mathbb{Q}$ y $K'/\mathbb{Q}$ adentro de un campo común (por ejemplo, adentro de una cerradura algebraica fija $\overline{\mathbb{Q}}$), el subcampo más pequeño que contiene a K y K' se llama el **compositum**[*] de K y K' y se denota por KK'.



Se dice que K y K' son **linealmente disjuntos** si se cumple una de las siguientes condiciones equivalentes:

a) el homomorfismo de $\mathbb{Q}$-álgebras

$$K \otimes_{\mathbb{Q}} K' \to KK', \quad x \otimes y \mapsto xy$$

es un isomorfismo;

a′) el mismo homomorfismo de $\mathbb{Q}$-álgebras es inyectivo;

b) si $\alpha_1, \ldots, \alpha_m$ es una base de K sobre $\mathbb{Q}$, esta es linealmente independiente sobre K';

b′) si $\beta_1, \ldots, \beta_n$ es una base de K' sobre $\mathbb{Q}$, esta es linealmente independiente sobre K;

c) si α_i y β_j son bases de K y K' respectivamente, entonces $\alpha_i\beta_j$ es una base de KK';

d) $[KK' : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [K' : \mathbb{Q}]$.

Para más detalles, véase §A.13.

3.9.2. Comentario. Un criterio útil para ver si dos campos son linealmente disjuntos es el siguiente: si $K/\mathbb{Q}$ y $K'/\mathbb{Q}$ son extensiones finitas de Galois y $K \cap K' = \mathbb{Q}$, entonces K y K' son linealmente disjuntos. Véase A.13.4 para la prueba.

Para calcular el anillo de enteros del compositum de campos, ocuparemos el siguiente resultado.

3.9.3. Proposición. *Sean K y K' dos campos de números linealmente disjuntos y sean*

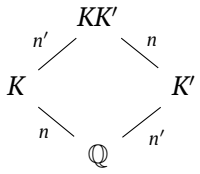
$$\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}, \quad \mathcal{O}_{K'} = \alpha'_1\mathbb{Z} \oplus \cdots \oplus \alpha'_{n'}\mathbb{Z}$$

bases de sus anillos de enteros. Supongamos que los discriminantes Δ_K y $\Delta_{K'}$ son coprimos. Entonces, $\alpha_i\alpha'_j$ es una $\mathbb{Z}$-base de KK' y

$$\Delta_{KK'} = \Delta_K^{[K':\mathbb{Q}]} \cdot \Delta_{K'}^{[K:\mathbb{Q}]}.$$

[*] En español a veces se usa el término **compuesto**, pero voy a decir «compositum»; estrictamente hablando, es una palabra latín.

Demostración. Pongamos $n = [K : \mathbb{Q}]$ y $n' = [K' : \mathbb{Q}]$. Bajo nuestra hipótesis, $[KK' : \mathbb{Q}] = nn'$, y los elementos $\alpha_i \alpha'_j$ forman una base del compositum KK' sobre $\mathbb{Q}$.



Dado un elemento $\alpha \in \mathcal{O}_{KK'}$, escribamos

$$\alpha = \sum_{i,j} a_{ij} \alpha_i \alpha'_j,$$

donde $a_{ij} \in \mathbb{Q}$. Vamos a ver que en realidad $a_{ij} \in \mathbb{Z}$. Pongamos

$$\beta_j = \sum_i a_{ij} \alpha_i.$$

Para calcular los discriminantes, consideremos los encajes

$$\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}, \quad \sigma'_1, \ldots, \sigma'_{n'} \colon K' \hookrightarrow \mathbb{C}.$$

Denotemos por brevedad $d = \Delta_K$ y $d' = \Delta_{K'}$. Recordemos que

$$d = \det(X)^2, \ d' = \det(Y)^2, \quad \text{donde } X = (\sigma_i(\alpha_j)), \ Y = (\sigma'_k(\alpha'_\ell)).$$

Escribamos

$$\vec{a} = (\sigma'_1(\alpha), \ldots, \sigma'_{n'})^t, \quad \vec{b} = (\beta_1, \ldots, \beta_{n'})^t.$$

Se tiene

$$\vec{a} = Y\vec{b}.$$

Ahora si Y^* es la matriz adjunta (compuesta por menores), entonces

$$Y Y^* = Y^* Y = \det(Y)\, I_{n'}.$$

Entonces,

$$\det(Y)\, \vec{b} = Y^* \vec{a}.$$

Dado que las matrices Y y Y^* y el vector $\vec{a}$ tienen entradas enteras sobre $\mathbb{Z}$, podemos concluir que

$$d' \beta_j = \sum_i d' a_{ij} \alpha_i \in \mathcal{O}_K,$$

y luego $d' a_{ij} \in \mathbb{Z}$. El argumento simétrico (intercambiando α_i con α'_j) demuestra que $d a_{ij} \in \mathbb{Z}$. Pero d y d' son coprimos, así que $a_{ij} \in \mathbb{Z}$. Esto demuestra que $\alpha_i \alpha'_j$ es una $\mathbb{Z}$-base de $\mathcal{O}_{KK'}$.

Bajo nuestra hipótesis de que los campos K y K' son linealmente disjuntos, los encajes del compositum KK' vienen dados por

$$\sigma_k \sigma'_\ell \colon KK' \hookrightarrow \mathbb{C}, \quad 1 \le k \le n, \ 1 \le \ell \le n',$$

y luego se puede ver que $\Delta_{KK'}$ es el discriminante de la matriz de $nn' \times nn'$ que consiste en bloques

$$\begin{pmatrix} \sigma_1(\alpha_1) Y & \cdots & \sigma_1(\alpha_n) Y \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) Y & \cdots & \sigma_n(\alpha_n) Y \end{pmatrix}, \quad Y = \begin{pmatrix} \sigma'_1(\alpha'_1) & \cdots & \sigma'_1(\alpha'_{n'}) \\ \vdots & \ddots & \vdots \\ \sigma'_{n'}(\alpha'_1) & \cdots & \sigma'_{n'}(\alpha'_{n'}) \end{pmatrix}.$$

Este es precisamente el **producto de Kronecker** $X \otimes Y$, y su determinante viene dado por

$$\det(X \otimes Y) = \det(X)^{n'} \cdot \det(Y)^{n}$$

(ejercicio 3.10). Entonces,

$$\Delta_{KK'} = \det(X \otimes Y)^2 = \det(X)^{2n'} \cdot \det(Y)^{2n} = d^{n'} \cdot d'^{n}. \qquad \blacksquare$$

3.9.4. Ejemplo. Los campos $K = \mathbb{Q}(\sqrt{3})$ y $K' = \mathbb{Q}(\sqrt{5})$ son linealmente disjuntos. Su compositum es $KK' = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Ahora $\Delta_K = 12$ y $\Delta_{K'} = 5$, así que la proposición de arriba nos dice que

$$\mathcal{O}_{KK'} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \frac{1+\sqrt{5}}{2}\mathbb{Z} \oplus \frac{\sqrt{3}+\sqrt{15}}{2}\mathbb{Z} = \mathbb{Z}\Big[\sqrt{3}, \frac{1+\sqrt{5}}{2}\Big]$$

y

$$\Delta_{KK'} = \Delta_K^2 \cdot \Delta_{K'}^2 = 2^4 \cdot 3^2 \cdot 5^2.$$

Solo para ilustrar la segunda parte del argumento de arriba, tenemos

$$\Delta_K = \det \begin{pmatrix} 1 & +\sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix}^2, \quad \Delta_{K'} = \det \begin{pmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{pmatrix}^2,$$

y luego

$$\Delta_{KK'} = \det \begin{pmatrix} 1 & +\sqrt{3} & (1+\sqrt{5})/2 & (+\sqrt{3}+\sqrt{15})/2 \\ 1 & -\sqrt{3} & (1+\sqrt{5})/2 & (-\sqrt{3}-\sqrt{15})/2 \\ 1 & +\sqrt{3} & (1-\sqrt{5})/2 & (+\sqrt{3}-\sqrt{15})/2 \\ 1 & -\sqrt{3} & (1-\sqrt{5})/2 & (-\sqrt{3}+\sqrt{15})/2 \end{pmatrix}^2 = \det \left(\begin{pmatrix} 1 & +\sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix} \otimes \begin{pmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{pmatrix} \right)^2. \qquad \blacktriangle$$

3.10 Anillo de enteros de $\mathbb{Q}(\zeta_n)$

Para el n-ésimo campo ciclotómico $\mathbb{Q}(\zeta_n)$ podemos factorizar $n = p_1^{e_1} \cdots p_s^{e_s}$, y en este caso $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{e_1}}) \cdots \mathbb{Q}(\zeta_{p_s^{e_s}})$, donde los campos $\mathbb{Q}(\zeta_{p_i^{e_i}})$ son linealmente disjuntos. De esta manera vamos a calcular el anillo de enteros de $\mathbb{Q}(\zeta_n)$ mediante la proposición , por inducción sobre el número de divisores primos de n. Primero necesitamos calcular el anillo de enteros de $\mathbb{Q}(\zeta_{p^e})$ y ver que los discriminantes son coprimos para diferentes p.

3.10.1. Lema. *Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_{p^e})$.*

1) Se tiene

$$\Delta(\mathbb{Z}[\zeta_{p^e}]) = \pm p^s, \quad \textit{donde } s = p^{e-1}(pe - e - 1).$$

2) El ideal principal $\mathfrak{p} = (1 - \zeta_{p^e})\mathcal{O}_K$ es primo y se tiene $p\mathcal{O}_K = \mathfrak{p}^{\phi(p^e)}$ y $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$.

Note que si $e = 1$, ya sabemos que $\Delta_K = \pm p^{p-2}$. El signo del discriminante no nos interesará porque este se determina fácilmente por el teorema de Brill.

Demostración. El cálculo del discriminante en la parte 1) es muy similar al que hicimos en 3.5.7 para el caso de $e = 1$, y lo dejo como un ejercicio para el lector.

Pongamos por brevedad $\zeta = \zeta_{p^e}$. Notamos que

$$\Phi_{p^e}(1) = \prod_{(k,p^e)=1} (1 - \zeta^k) = p.$$

Aquí $1-\zeta^k = \frac{1-\zeta^k}{1-\zeta}(1-\zeta)$, donde

$$N_{K/\mathbb{Q}}\left(\frac{1-\zeta^k}{1-\zeta}\right) = \frac{N_{K/\mathbb{Q}}(1-\zeta^k)}{N_{K/\mathbb{Q}}(1-\zeta)} = \pm 1,$$

así que $1-\zeta^k = \epsilon_k(1-\zeta)$, donde $\epsilon_k \in \mathcal{O}_K^\times$ es una unidad. Entonces, tenemos $(1-\zeta)^{\phi(p^e)} = \epsilon p$, donde $\epsilon \in \mathcal{O}_K^\times$. De aquí se sigue que $p\mathcal{O}_K = \mathfrak{p}^{\phi(p^e)}$, donde $\mathfrak{p} = (1-\zeta)\mathcal{O}_K$. Ahora tomando las normas de ideales,

$$N_{K/\mathbb{Q}}(\mathfrak{p})^{\phi(p^e)} = N_{K/\mathbb{Q}}(\mathfrak{p}^{\phi(p^e)}) = N_{K/\mathbb{Q}}(p\mathcal{O}_K) = p^{\phi(p^e)},$$

así que $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$, lo que implica que $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. ■

3.10.2. Proposición. *Para el campo ciclotómico $K = \mathbb{Q}(\zeta_{p^e})$ se tiene $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}]$.*

Demostración. Primero, si $d = \Delta(\mathbb{Z}[\zeta_{p^e}]) = \pm p^s$, entonces según 3.5.17 se tiene

$$\mathbb{Z}[\zeta_{p^e}] \subseteq \mathcal{O}_K \subseteq \frac{1}{d}\mathbb{Z}[\zeta_{p^e}],$$

lo que podemos escribir también como

$$p^s\mathcal{O}_K \subseteq \mathbb{Z}[\zeta_{p^e}] \subseteq \mathcal{O}_K.$$

Pongamos $\mathfrak{p} = (1-\zeta_{p^e})\mathcal{O}_K$. El lema anterior nos dice que $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$, así que $\mathcal{O}_K = \mathbb{Z} + \mathfrak{p}$, y luego

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}. \qquad (*)$$

Multiplicando esta identidad por $\mathfrak{p}$, se obtiene

$$\mathfrak{p} = \mathfrak{p}\mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^2.$$

Al sustituirlo a (*), tenemos

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^2.$$

Procediendo de esta manera, tenemos

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}] + \mathfrak{p}^t \quad \text{para todo } t \geq 1.$$

Ahora si $t = s\,\phi(p^e)$, entonces por el lema anterior,

$$\mathfrak{p}^t = (\mathfrak{p}^{\phi(p^e)})^s = p^s\mathcal{O}_K.$$

Pero $p^s\mathcal{O}_K \subseteq \mathbb{Z}[\zeta_{p^e}]$, así que podemos concluir que $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^e}]$. ■

3.10.3. Teorema. *Para el campo ciclotómico $K = \mathbb{Q}(\zeta_n)$ se tiene $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ y*

$$\Delta_K = (-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Demostración. Inducción sobre el número de divisores primos de n. Acabamos de probar el caso cuando $n = p^e$. La fórmula del discriminante es también correcta: calculamos que en este caso

$$\Delta = \pm p^s, \quad s = p^{e-1}(pe - e - 1).$$

Ahora para el paso inductivo, si $n = p_1^{e_1}\cdots p_s^{e_s}$, consideremos los campos

$$K_1 = \mathbb{Q}(\zeta_{p_1^{e_1}}),\ K_2 = \mathbb{Q}(\zeta_{p_2^{e_2}}), \ldots, K_s = \mathbb{Q}(\zeta_{p_s^{e_s}}).$$

Tenemos

$$\mathbb{Q}(\zeta_n) = K_1 \cdots K_s.$$

Los campos $K_1 \cdots K_{s-1}$ y K_s son linealmente disjuntos y tienen discriminantes coprimos, así que se aplica la proposición 3.10. Por la hipótesis de inducción, tenemos

$$\mathcal{O}_{K_1 \cdots K_{s-1}} = \mathbb{Z}[\zeta_{p_1^{e_1}} \cdots \zeta_{p_{s-1}^{e_{s-1}}}].$$

Luego, la proposición 3.10 nos dice que

$$\mathcal{O}_{K_1 \cdots K_s} = \mathbb{Z}[\zeta_{p_1^{e_1}} \cdots \zeta_{p_{s-1}^{e_{s-1}}}] \cdot \mathbb{Z}[\zeta_{p_s^{e_s}}] = \mathbb{Z}[\zeta_n].$$

El discriminante se calcula mediante

$$\Delta_{K_1 \cdots K_s} = \Delta_{K_1 \cdots K_{s-1}}^{[K_s:\mathbb{Q}]} \cdot \Delta_{K_s}^{[K_1 \cdots K_{s-1}:\mathbb{Q}]},$$

y se ve que se obtiene la fórmula enunciada. El signo del discriminante viene dado por el teorema de Brill. ■

3.10.4. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_{20})$. Tenemos $K = K_1 K_2$, donde $K_1 = \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ y $K_2 = \mathbb{Q}(\zeta_5)$. El teorema nos dice que $K = \mathbb{Z}[\zeta_{20}]$. Calculamos $\phi(20) = \phi(4)\,\phi(5) = 8$. Una posible base de $\mathcal{O}_K$ es

$$1, \zeta_{20}, \zeta_{20}^2, \zeta_{20}^3, \zeta_{20}^4, \zeta_{20}^5, \zeta_{20}^6, \zeta_{20}^7,$$

pero también podríamos tomar el producto de las bases $\{1, i\}$ y $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$. El discriminante viene dado por

$$\Delta_K = \Delta_{K_1}^4 \cdot \Delta_{K_2}^2 = 2^8 \cdot 5^6.$$ ▲

Clase 13
23/09/20

Ahora, dado que nos salió $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, no podemos resistir la tentación de aplicar el Kummer–Dedekind para factorizar $p\mathcal{O}_K$. Para esto tenemos que factorizar el n-ésimo polinomio ciclotómico $\Phi_n(x) \in \mathbb{Z}[x]$ módulo diferentes primos p.

3.10.5. Lema. *Factoricemos $n = \prod_p p^{v_p}$. Para un número primo p, sea f el orden de p módulo n/p^{v_p}, i.e. el número más pequeño tal que $p^f \equiv 1 \pmod{n/p^{v_p}}$. Luego, se tiene*

$$\overline{\Phi_n}(x) = (\overline{g_1} \cdots \overline{g_s})^{\phi(p^{v_p})} \quad \text{en } \mathbb{F}_p[x],$$

donde $\overline{g_1}, \ldots, \overline{g_s} \in \mathbb{F}_p[x]$ son distintos polinomios irreducibles de grado f.

Demostración. Ya hemos visto algo parecido para el caso de n primo (véase 2.7.10), y esta es una generalización.

Primero supongamos que $p \nmid n$, así que $v_p = 0$. En este caso $f = x^n - 1$ es un polinomio separable en $\mathbb{F}_p[x]$, como demuestra el cálculo de $\operatorname{mcd}(f, f') = 1$. Por nuestra elección, f es el número más pequeño tal que el grupo multiplicativo $\mathbb{F}_{p^f}^\times$ contiene elementos de orden n, así que $\mathbb{F}_{p^f}$ es precisamente el campo de descomposición del polinomio $\overline{\Phi_n} \in \mathbb{F}_p[x]$. La factorización en polinomios irreducibles será

$$\overline{\Phi_n} = \overline{g_1} \cdots \overline{g_s},$$

donde cada $\overline{g_i}$ es el polinomio mínimo sobre $\mathbb{F}_p$ de alguna raíz n-ésima $\zeta \in \mathbb{F}_{p^f}^\times$, y como consecuencia,

$$\deg \overline{g_i} = [\mathbb{F}_{p^f} : \mathbb{F}_p] = f.$$

(Como fue explicado en la prueba de 2.7.10, es instructivo ver cómo los factores $\overline{g_i}$ vienen de las órbitas del Frobenius.)

En el caso cuando $p \mid n$, escribamos $n = m\,p^e$, donde $e = v_p$ (y entonces $p \nmid m$). Este caso se reduce al anterior observando que

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^e)} \pmod{p}.$$

(¡Ejercicio!) ■

Ahora aplicando Kummer–Dedekind, se obtiene el siguiente resultado.

3.10.6. Teorema. *Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_n)$. Factoricemos $n = \prod_p p^{v_p}$. Para un número primo p, sea f el orden de p módulo n/p^{v_p}. Luego, se tiene factorización*

$$p\mathcal{O}_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_s^e,$$

donde los índices de ramificación son $e = \phi(p^{v_p})$, y los grados del campo residual son f.

En particular, los primos que se ramifican son los divisores de n, excepto el caso de $p = 2$ cuando $v_2(n) = 1$. Esto no es muy interesante, dado que en esta situación $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$. Notamos que la información sobre los primos que se ramifican también está en el discriminante que hemos calculado.

3.10.7. Ejemplo. En el campo ciclotómico $K = \mathbb{Q}(\zeta_{15})$ la factorización de $p\mathcal{O}_K$ depende de los restos de p módulo 3 y 5.

Para $p = 3$ hay ramificación con $e = \phi(3) = 2$ y para $p = 5$ hay ramificación con $e = \phi(5) = 4$. Para p distintos de 3 y 5, tenemos las siguientes posibilidades (véase también la figura 3.2).

p (3) \ p (5)	1	2	3	4
1	$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_8$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$
2	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$

Por ejemplo, si $p \equiv 2 \pmod 3$ y $p \equiv 2 \pmod 5$, entonces el orden de p módulo 3 es 2 y el orden de p módulo 5 es 4. Entonces, el orden de p módulo 15 es igual a 4. Esto nos da ideales $\mathfrak{p}_i$ con el grado del campo residual 4. Se cumple necesariamente $s \cdot 4 = \phi(15) = 8$, entonces hay $s = 2$ ideales primos en la factorización. Notamos que no hay primos inertes. ▲

3.10.8. Ejemplo (Kummer). Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_{23})$. El primer primo tal que $p \equiv 1 \pmod{23}$ es 47, lo que implica que

$$47\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{22},$$

donde $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = 47$. Los ideales primos $\mathfrak{p}_i$ no son principales. En efecto, si $\mathfrak{p}_i = \alpha\mathcal{O}_K$, entonces $|N_{K/\mathbb{Q}}(\alpha)| = 47$. Sin embargo, se puede ver que en $\mathcal{O}_K$ no hay elementos de norma 47[*].

A saber, para $\alpha \in \mathcal{O}_K$ se tiene

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha).$$

El grupo de Galois $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/23\mathbb{Z})^\times$ es cíclico de orden 22. Sea σ su generador. La teoría de Galois implica que en $\mathbb{Q}(\zeta_{23})$ hay único subcampo cuadrático, y este es el subcampo fijo por σ^2. Por razones de ramificación (véase ejercicio 2.19) se puede deducir que este subcampo cuadrático es $F = \mathbb{Q}(\sqrt{-23})$.

Escribamos

$$N_{K/\mathbb{Q}}(\alpha) = \Big(\alpha\,\sigma^2(\alpha)\,\sigma^4(\alpha)\cdots\sigma^{20}(\alpha)\Big)\,\Big(\sigma(\alpha)\,\sigma^3(\alpha)\,\sigma^5(\alpha)\cdots\sigma^{21}(\alpha)\Big).$$

Aquí cada uno de los dos múltiplos está en F, y además, se ve que uno es el conjugado complejo del otro: tenemos $\overline{\alpha} = \sigma^{11}(\alpha)$, y de esta manera,

$$\overline{\alpha\,\sigma^2(\alpha)\,\sigma^4(\alpha)\cdots\sigma^{20}(\alpha)} = \sigma^{11}(\alpha)\,\sigma^{2+11}(\alpha)\,\sigma^{4+11}(\alpha)\cdots\sigma^{20+11}(\alpha) = \sigma(\alpha)\,\sigma^3(\alpha)\,\sigma^5(\alpha)\cdots\sigma^{21}(\alpha).$$

[*] He aquí un cálculo en PARI/GP que lo confirma:

```
? K = bnfinit(polcyclo(23));
? bnfisintnorm(K,47)
% = []
```

Sin embargo, lo explicaré más tarde.

p	$p\mathcal{O}_K$	f	$p\,(15)$	p	$p\mathcal{O}_K$	f	$p\,(15)$	p	$p\mathcal{O}_K$	f	$p\,(15)$
2	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	127	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	283	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13
3	$\mathfrak{p}^2$	4	3	131	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	293	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8
5	$\mathfrak{p}^4$	2	5	137	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	307	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7
7	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	139	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	311	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11
11	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	149	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	313	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13
13	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	151	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	317	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2
17	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	157	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	331	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1
19	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	163	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	337	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7
23	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	167	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	347	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2
29	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	173	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	349	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4
31	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	179	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	353	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8
37	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	181	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	359	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14
41	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	191	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	367	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7
43	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	193	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	373	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13
47	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	197	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	379	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4
53	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	199	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	383	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8
59	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	211	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	389	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14
61	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	223	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	397	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7
67	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	227	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	401	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11
71	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	229	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	409	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4
73	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	233	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	419	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14
79	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	239	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	421	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1
83	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	241	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	431	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11
89	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	251	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	433	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13
97	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	257	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	439	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4
101	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	263	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	443	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8
103	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13	269	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14	449	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	14
107	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	2	271	$\mathfrak{p}_1\,\mathfrak{p}_2\cdots\mathfrak{p}_8$	1	1	457	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7
109	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	4	277	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	7	461	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11
113	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	8	281	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$	2	11	463	$\mathfrak{p}_1\,\mathfrak{p}_2$	4	13

Figura 3.2: Factorización de $p\mathcal{O}_K$ para $K = \mathbb{Q}(\zeta_{15})$

Podemos entonces escribir

$$N_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{-23})\,(a - b\sqrt{-23}) = a^2 + 23\,b^2$$

para algunos $a, b \in \mathbb{Q}$. Dado que α es un elemento entero, tenemos también $a + b\sqrt{-23} \in \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$, así que $a = \frac{a'}{2}$ y $b = \frac{b'}{2}$, donde $a', b' \in \mathbb{Z}$ y $a' \equiv b' \pmod 2$. Entonces,

$$N_{K/\mathbb{Q}}(\alpha) = \frac{a'^2 + 23\,b'^2}{4}.$$

Ahora si en $\mathbb{Z}[\zeta_{23}]$ hay un elemento de norma 47, esto implicaría que para algunos $a', b' \in \mathbb{Z}$ se cumple

$$a'^2 + 23b'^2 = 4 \cdot 47.$$

Sin embargo, no es difícil ver que esto es imposible[*].

Podemos concluir que los ideales primos $\mathfrak{p}_i$ que están sobre 47 en el campo ciclotómico $K = \mathbb{Q}(\zeta_{23})$ no son principales. Como consecuencia, el anillo $\mathcal{O}_K = \mathbb{Z}[\zeta_{23}]$ no es un dominio de factorización única.

Tenemos $\left(\frac{-23}{47}\right) = +1$, y entonces en el anillo $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ el ideal generado por $p = 47$ se factoriza como $\mathfrak{p}\,\overline{\mathfrak{p}}$, y lo que acabamos de ver demuestra que estos ideales primos tampoco son principales. (Al pasar a $\mathbb{Q}(\zeta_{23})$, cada uno de estos ideales se escinde en 11 ideales primos no principales.)

$$\begin{array}{ccccc}
\mathfrak{p}_1 \cdots \mathfrak{p}_{22} & \subset & \mathbb{Z}[\zeta_{23}] & \subset & \mathbb{Q}(\zeta_{23}) \\
\Big| & & \Big| & & \Big|{\scriptstyle 11} \\
\mathfrak{p}\overline{\mathfrak{p}} & \subset & \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right] & \subset & \mathbb{Q}(\sqrt{-23}) \\
\Big| & & \Big| & & \Big|{\scriptstyle 2} \\
47 & \subset & \mathbb{Z} & \subset & \mathbb{Q}
\end{array}$$

▲

De hecho, $K = \mathbb{Q}(\zeta_n)$ para $n = 23$ es el primer campo ciclotómico tal que $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ no tiene factorización única, o de manera equivalente, tal que el grupo de clases $\mathrm{Cl}(K)$ no es trivial. Esto fue descubierto por Kummer.

Hay una anécdota bien conocida relacionada con este resultado de Kummer. En 1847 el matemático francés Gabriel Lamé anunció ante la Academia de Ciencias de París una supuesta prueba del último teorema de Fermat basada en la factorización única en el anillo $\mathbb{Z}[\zeta_n]$. Liouville puso en duda esta afirmación y se comunicó con Kummer quien aparentemente ya tenía contraejemplos. Para los detalles históricos, véase por ejemplo [Edw1975] y [Edw1977]. El libro [Edw1996] también contiene detalles sobre los cálculos de Kummer.

Véase también https://en.wikipedia.org/wiki/23_enigma sobre la numerología detrás de 23.

[*] Tenemos necesariamente $23b'^2 \leq 4 \cdot 47$, y luego $|b'| \leq 2$. Basta entonces sustituir $b' = 1, 2$ y ver que la ecuación no tiene soluciones enteras.

3.11 Cálculos en PARI/GP

Ya he mencionado PARI/GP (https://pari.math.u-bordeaux.fr/) en varias ocasiones, y ahora veremos de manera un poco más sistemática cómo hacer cálculos con los campos de números en este programa. Si todavía no lo han descargado, es hora de hacerlo y probar los ejemplos de abajo.

He aquí algunos comandos útiles:

- `\l "log.txt"` — guardar toda la sesión en el archivo `log.txt` (otra vez `\l` deja de hacerlo),
- `?xxxxx` — ayuda sobre `xxxxx`, por ejemplo,

```
? ?idealprimedec
idealprimedec(nf,p,{f=0}): prime ideal decomposition of the prime number p
in the number field nf as a vector of prime ideals. If f is present and
non-zero, restrict the result to primes of residue degree <= f.
```

- `??xxxxx` — ayuda detallada sobre `xxxxx`,
- `%` — el resultado del cálculo anterior:

```
? 2^2
%1 = 4
? %^2
%2 = 16
? %^2
%3 = 256
? %1 + %2
%4 = 20
```

- `quit` o `\q` — salir del programa.

Cuando ocurre algún error, el programa entra en el «ciclo break» y nos recomienda escribir `break` para salir de allí. Esto sirve para encontrar errores en código más complejo y probablemente no será relevante para nuestros pequeños cálculos.

```
? mcd(2,3)
  ***   at top-level: mcd(2,3)
  ***                 ^--------
  ***   not a function in function call
  ***   Break loop: type 'break' to go back to GP prompt
break> break

? gcd(2,3)
% = 1
```

3.11.1 Polinomios

Un campo de números se especifica por un polinomio irreducible f tal que $K \cong \mathbb{Q}[x]/(f)$. Para ver si un polinomio es irreducible, sirve la función `polisirreducible(`f`)`.

```
? polisirreducible(x^3 - 3*x + 1)
% = 1
? polisirreducible(x^3-1)
% = 0
```

Si queremos factorizar un polinomio, podemos ocupar la función `factor(`f`)`.

```
? factor (x^8-1)
% =
[  x - 1 1]

[  x + 1 1]

[x^2 + 1 1]

[x^4 + 1 1]
```

El resultado es una matriz de $s \times 2$, donde en la primera columna se encuentran los factores irreducibles y en la segunda columna las potencias correspondientes:

$$f = g_1^{e_1} \cdots g_s^{e_s} \longleftrightarrow \begin{pmatrix} g_1 & e_1 \\ \vdots & \vdots \\ g_s & e_s \end{pmatrix}.$$

La factorización módulo p (que ocupamos para el Kummer–Dedekind) puede ser obtenida mediante `factor(`f`*Mod(1,`p`))`.

```
? factor (polcyclo(8)*Mod(1,2))
% =
[Mod(1, 2)*x + Mod(1, 2) 4]

? factor (polcyclo(8)*Mod(1,3))
% =
[Mod(1, 3)*x^2 + Mod(1, 3)*x + Mod(2, 3) 1]
[Mod(1, 3)*x^2 + Mod(2, 3)*x + Mod(2, 3) 1]

? factor (polcyclo(8)*Mod(1,5))
% =
[Mod(1, 5)*x^2 + Mod(2, 5) 1]
[Mod(1, 5)*x^2 + Mod(3, 5) 1]
```

El discriminante de un polinomio se calcula mediante `poldisc(`f`)`.

```
? poldisc (polcyclo(7))
% = -16807
? factor(%)
% =
[-1 1]
[ 7 5]
```

3.11.2 Campos de números

Para especificar un campo de números $K = \mathbb{Q}[x]/(f)$, hay que escribir K `= nfinit(`f`)`. Esta función calcula los invariantes básicos de K.

- K`.pol` — el polinomio usado para definir K,
- K`.zk` — el anillo de enteros $\mathcal{O}_K$,
- K`.disc` — el discriminante Δ_K,
- K`.sign` — la signatura $[r_1, r_2]$,
- ...

```
? K = nfinit(x^3-19);
? K.pol
% = x^3 - 19
? K.disc
% = -1083
? factor (%)
% =
[-1 1]
[ 3 1]
[19 2]

? K.zk
% = [1, 1/3*x^2 + 1/3*x + 1/3, x]
? K.r1
% = 1
? K.r2
% = 1
? K.sign
% = [1, 1]
```

Aquí escribí K `= nfinit(x^3-19);` con punto y coma para suprimir la salida. De todas maneras, el resultado será guardado en K. Pueden ejecutar el mismo comando sin punto y coma, y PARI/GP imprimirá toda la estructura de datos asociada con K.

Lo que se encuentra en `K.zk` es una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$ en términos de x mód f. En este caso particular el resultado significa que para $\mathbb{Q}[\alpha]/(\alpha^3 - 19)$ se tiene

$$\mathcal{O}_K = \mathbb{Z} \oplus \frac{1}{3}(\alpha^2 + \alpha + 1)\mathbb{Z} \oplus \alpha\mathbb{Z}.$$

Por supuesto, el mismo campo de números puede ser especificado por diferentes polinomios irreducibles. Para ver si dos campos de números son isomorfos, sirve la función `nfisisom(f,g)`. Como entrada podemos especificar polinomios irreducibles o las estructuras `nfinit`.

```
? nfisisom(x^4 + 2*x^2 + 4*x + 2, polcyclo(8))
% = [x^2 - x, x^2 + x, -x^3 - x^2, x^3 - x^2]

? nfisisom(x^4 + 2, polcyclo(8))
% = 0
```

Si la salida es `0`, esto significa que no hay isomorfismo; en el caso contrario, se devuelve una lista de posibles isomorfismos. En el ejemplo de arriba vimos entonces que

$$\mathbb{Q}[\alpha]/(\alpha^4 + 2\alpha^2 + 4\alpha + 2) \cong \mathbb{Q}(\zeta_8),$$

y además que uno de los isomorfismos viene dado por

$$\alpha \mapsto \zeta_8^2 - \zeta_8.$$

La función `nfisincl(f,g)` verifica si $\mathbb{Q}[x]/(f)$ es isomorfo a un subcampo de $\mathbb{Q}[x]/(g)$ y encuentra los isomorfismos. He aquí un ejemplo particular.

```
? nfisincl(x^2-7, polcyclo(7))
% = 0
? nfisincl(x^2+7, polcyclo(7))
% = [-2*x^4 - 2*x^2 - 2*x - 1, 2*x^4 + 2*x^2 + 2*x + 1]
```

Los resultados nos dicen que $\mathbb{Q}(\sqrt{7}) \not\subset \mathbb{Q}(\zeta_7)$ y $\mathbb{Q}(\sqrt{-7}) \subset \mathbb{Q}(\zeta_7)$. También hay modos de encontrar todos los posibles subcampos, pero los veremos cuando hablaremos de la teoría de Galois.

Una función muy útil es `polredbest(f)`. Esta a partir de un polinomio f nos da otro polinomio g tal que $\mathbb{Q}[x]/(f) \cong \mathbb{Q}[x]/(g)$, pero los coeficientes de g son relativamente pequeños. He aquí un ejemplo particular para qué sirve esta reducción.

Para ver un ejemplo particular, supongamos que nos interesa el campo bicuadrático $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Este se genera por $\alpha = \sqrt{2} + \sqrt{3}$, cuyo polinomio mínimo viene dado por $x^4 - 10x^2 + 1$. Ahora

$$\mathbb{Z}[\alpha] = 2^{14} \cdot 3^2, \quad \Delta_K = 2^8 \cdot 3^2,$$

lo que significa que

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 8.$$

```
? f = x^4 - 10*x^2 + 1;
? poldisc(f)
% = 147456
? factor(%)
% =
[2 14]

[3  2]

? K = nfinit(f);
? K.disc
% = 2304
? factor(%)
% =
[2 8]
[3 2]

? sqrtint(poldisc(f)/K.disc)
% = 8
```

¿Podemos encontrar un mejor subanillo cuyo índice en $\mathcal{O}_K$ sea menor? Con ayuda de PARI/GP encontramos $\mathbb{Z}[\beta]$, donde $\beta^4 - 4\beta^2 + 1 = 0$, y resulta que $\mathcal{O}_K = \mathbb{Z}[\beta]$. De hecho, $\beta = \sqrt{2 + \sqrt{3}}$.

```
? g = polredbest(f)
% = x^4 - 4*x^2 + 1
? poldisc(g)
% = 2304
? % == K.disc
% = 1
```

Otro ejemplo parecido: para $K = \mathbb{Q}(\alpha)$, donde $\alpha = \sqrt[3]{19}$ tenemos

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3.$$

Con ayuda de PARI/GP encontramos el subanillo $\mathbb{Z}[\beta]$, donde $\beta^3 - \beta^2 - 6\beta - 12 = 0$ y

$$[\mathcal{O}_K : \mathbb{Z}[\beta]] = 2.$$

```
? f = x^3-19;
? K = nfinit(f);
? sqrtint(poldisc(f)/K.disc)
% = 3
? g = polredbest(f)
% = x^3 - x^2 - 6*x - 12
? sqrtint(poldisc(g)/K.disc)
% = 2
```

Si queremos saber cómo α se expresa en términos de β (para trabajar en el nuevo anillo $\mathbb{Z}[\beta]$), hay que escribir `polredbest(`f`,1)`

```
? polredbest(f,1)
% = [x^3 - x^2 - 6*x - 12,
     Mod(1/2*x^2 - 1/2*x - 2, x^3 - x^2 - 6*x - 12)]
? %[2]^3
% = Mod(19, x^3 - x^2 - 6*x - 12)
```

La salida significa que

$$\alpha = \frac{1}{2}\beta^2 - \frac{1}{2}\beta - 2.$$

3.11.3 Operaciones con elementos de $K/\mathbb{Q}$

Hay varias maneras de especificar un elemento de un campo de números $\mathbb{Q}[x]/(f)$. Podemos trabajar con elementos módulo *f*.

```
? a = Mod(x^4 - x^3 - x^2 + x, polcyclo(5))
% = Mod(-2*x^3 - 2*x^2 - 1, x^4 + x^3 + x^2 + x + 1)
? a^2
% = Mod(5, x^4 + x^3 + x^2 + x + 1)
```

Otra opción es expresar los elementos en términos de la base de $\mathcal{O}_K$. La conversión se hace mediante `nfalgtobasis(`K`,`α`)` y `nfbasistoalg(`K`,[`a_1`, ..., `a_n`]~)`.

```
? K = nfinit(polcyclo(5));
? K.zk
% = [1, x, x^2, x^3]

? nfalgtobasis(K, -2*x^3 - 2*x^2 - 1)
% = [-1, 0, -2, -2]~
% = [-1, 0, -2, -2]~
? K.zk * %
% = -2*x^3 - 2*x^2 - 1

? nfbasistoalg(K,%)
% = Mod(-2*x^3 - 2*x^2 - 1, x^4 + x^3 + x^2 + x + 1)
```

Aquí `[-1, 0, -2, -2]~` representa el vector columna $(-1,0,-2,-2)^t$. Las funciones que trabajan con elementos de un campo de números empiezan por «`nfelt`». Por ejemplo,

`nfeltadd(`K,α,β`)`, `nfeltmul(`K,α,β`)`, `nfeltdiv(`K,α,β`)`.

Si los números algebraicos están especificados como polinomios módulo *f*, basta usar los operadores habituales `+`, `-`, `*`, `/`, etc. Otras funciones útiles son

- `nfeltnorm(`K`,`α`)` o `norm(Mod(`g`,`f`))` — norma;
- `nfelttrace(`K`,`α`)` o `trace(Mod(`g`,`f`))` — traza;
- `charpoly(Mod(`g`,`f`))` — polinomio característico;
- `minpoly(Mod(`g`,`f`))` — polinomio mínimo.

Trate de escribir `nfelt` y digitar $\boxed{\rightarrow}$ para ver la lista completa de funciones cuyo nombre empieza por `nfelt`.

```
? K = nfinit(polcyclo(7));
? nfelttrace(K,x)
% = -1
? trace(Mod(x,K.pol))
% = -1
? nfeltnorm(K, 1-x)
% = 7
? norm(Mod(1-x, K.pol))
% = 7

? charpoly(Mod(x + x^-1, K.pol))
% = x^6 + 2*x^5 - 3*x^4 - 6*x^3 + 2*x^2 + 4*x + 1
? minpoly(Mod(x + x^-1, K.pol))
% = x^3 + x^2 - 2*x - 1
```

3.11.4 Extensiones de campos de números

PARI/GP también trabaja con campos de números *relativos*, es decir, extensiones $\mathbb{Q} \subset K \subset L$. Las funciones correspondientes empiezan por «`rnf`» que es una abreviación de «relative number field». Para mayor información, les invito a consultar la documentación. He aquí un pequeño ejemplo donde calculamos el campo $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

```
? K = nfinit(t^3-2);
? L = rnfinit(K, polcyclo(3));
? L.polabs
% = x^6 + 3*x^5 + 6*x^4 + 11*x^3 + 12*x^2 - 3*x + 1
? rnfeltreltoabs(L,x+t)
% = Mod(-4/9*x^5 - 14/9*x^4 - 28/9*x^3 - 52/9*x^2 - 65/9*x - 4/9,
       x^6 + 3*x^5 + 6*x^4 + 11*x^3 + 12*x^2 - 3*x + 1)
? minpoly(%)
% = x^6 + 3*x^5 + 6*x^4 + 3*x^3 + 9*x + 9
? nfisisom(%, L.polabs)
% = [-x - 1, .....]
```

Es importante que las variables de los polinomios que definen K y L sean distintas, por esto pusimos $t^3 - 2$. El programa calculó que

$$L \cong \mathbb{Q}[x]/(x^6 + 3x^5 + 6x^4 + 11x^3 + 12x^2 - 3x + 1)$$

y que $\sqrt[3]{2}+\zeta_3$ tiene polinomio mínimo sobre $\mathbb{Q}$

$$x^6+3x^5+6x^4+3x^3+9x+9.$$

Aunque en este curso no vamos a hablar mucho de la situación relativa L/K[*], PARI/GP sabe calcular varios invariantes relativos, como el discriminante $\Delta_{L/K}$ que será un ideal en $\mathcal{O}_K$, los generadores de $\mathcal{O}_L$ como $\mathcal{O}_K$-módulo, etc. Para obtener un campo «absoluto», podemos escribir `nfinit(L)`.

```
? L.zk
% = [[1, x - 1], [1, [1, 0, 1/3; 0, 1, 2/3; 0, 0, 1/3]]]
? L.disc
% = [[3, 1, 2; 0, 1, 0; 0, 0, 1], -3]
? nfinit(L).disc
% = -34992

? factor(%)
% =
[-1 1]

[ 2 4]

[ 3 7]
```

3.11.5 Operaciones con ideales

Clase 14
28/09/20

Para un campo de números K el programa puede hacer cálculos con $\mathcal{O}_K$-ideales fraccionarios.

Un ideal principal $\alpha\mathcal{O}_K$ puede ser especificado por su generador α, que puede ser un polinomio en x (en la base $1, x, x^2, \ldots, x^{n-1}$ de $\mathbb{Q}[x]/(f)$) o vector `[`a_1`,...,`a_n`]~` (en la $\mathbb{Z}$-base de $\mathcal{O}_K$ calculada por el programa en `K.zk`).

En general, los ideales se representarán por matrices de $n\times n$. A saber, las columnas de dicha matriz forman una base de $I\subseteq\mathcal{O}_K$ como un $\mathbb{Z}$-submódulo de $\mathcal{O}_K$ (en términos de la base de $\mathcal{O}_K$). En la salida de PARI/GP la matriz estará en la **forma normal de Hermite**, que es una matriz triangular superior definida *de manera canónica* a partir de I (y la base fija de $\mathcal{O}_K$).

3.11.1. Proposición-definición. *Sea H una matriz de $n\times n$ con coeficientes en $\mathbb{Z}$. Digamos que el **coeficiente mayor** de cada fila es el primer coeficiente no nulo. Se dice que H está en la **forma normal de Hermite** si se cumplen las siguientes condiciones.*

1) *H es una matriz triangular superior con elementos ≥ 0.*
2) *El coeficiente mayor de cada fila está a la derecha del coeficiente mayor de la fila anterior.*
3) *Los elementos arriba del coeficiente mayor son estrictamente menor.*
4) *Los elementos abajo del coeficiente mayor son nulos.*

*Para toda matriz $A\in M_{n\times n}(\mathbb{Z})$ existe única $U\in \mathrm{GL}_n(\mathbb{Z})$ tal que $H=UA$ está en la forma normal de Hermite. En este caso se dice que H es la **forma normal de Hermite** de A.*

Demostración. [Coh1993, §2.4.2]. ■

[*] Los libros de texto avanzados empiezan en esta generalidad, pero no lo hago a propósito para simplificar la exposición.

3.11.2. Ejemplo. Tenemos

$$\underbrace{\begin{pmatrix} 0 & +1 & +1 \\ -1 & +1 & -1 \\ -1 & +1 & +2 \end{pmatrix}}_{U} \cdot \underbrace{\begin{pmatrix} +3 & -2 & 0 \\ +4 & +3 & -3 \\ 0 & -2 & +2 \end{pmatrix}}_{A} = \underbrace{\begin{pmatrix} 2 & 1 & 1 \\ 0 & 4 & 1 \\ 0 & 0 & 2 \end{pmatrix}}_{H}.$$

Aquí H es la forma normal de Hermite de A. ▲

Para convertir un ideal en la forma normal de Hermite se puede usar la función `idealhnf(`K`,`I`)`.

```
? K = nfinit(x^2-5);
? K.zk
% = [1, 1/2*x - 1/2]
? a = idealhnf(K, 4+x)
% =
[11 8]

[ 0 1]
```

(Notamos que la letra `I` en PARI/GP ya está reservada para la unidad imaginaria $\sqrt{-1}$, así que no hay que usarla para un ideal.) Interpretación de la salida: tenemos

$$\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z}, \quad \alpha_1 = 1, \quad \alpha_2 = \frac{\sqrt{5}-1}{2},$$

y luego

$$(4+\sqrt{5})\mathcal{O}_K = 11\alpha_1\mathbb{Z} \oplus (8\alpha_1 + \alpha_2)\mathbb{Z}.$$

Otro ejemplo más conocido: consideremos el campo $\mathbb{Q}(i)$.

```
? K = nfinit(x^2+1);
? K.zk
% = [1, x]
```

Allí todos los ideales son principales y tenemos

$$(m+ni) = \{(c+di)(m+ni) \mid c,d \in \mathbb{Z}\} = \{c\cdot(m+ni) + d\cdot(-n+mi) \mid c,d \in \mathbb{Z}\} = (m+ni)\mathbb{Z} \oplus (-n+mi)\mathbb{Z}.$$

Entonces, el ideal $(m+ni)$ se representa por la matriz

$$\begin{pmatrix} m & -n \\ n & m \end{pmatrix},$$

que luego puede ser reducida a la forma normal de Hermite.

```
? a = idealhnf(K, 2+3*x)
% =
[13 5]

[ 0 1]

? mathnf ([2, -3; 3, 2])
% =
[13 5]

[ 0 1]
```

Ya que la forma normal de Hermite es canónica, esta sirve para ver si dos ideales coinciden.

```
? a = idealhnf(K, 2+3*x)
% =
[13 5]

[ 0 1]

? b = idealhnf(K, -3+2*x)
% =
[11 8]

[ 0 1]

? Mod ((2+3*x)/(-3+2*x), K.pol)
% = Mod(-x, x^2 + 1)
```

La función `ideallist(`K`,`N`)` devuelve todos los ideales enteros $I \subseteq \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(I) \leq N$.

```
? K = nfinit(x^2+1);
? L = ideallist(K,10)
% = [[[1, 0; 0, 1]],  /* norma 1: I=O_K */
     [[2, 1; 0, 1]],
     [],              /* no hay de norma 3 */
     [[2, 0; 0, 2]],
     [[5, 3; 0, 1], [5, 2; 0, 1]],
     [],              /* no hay de norma 6 */
     [],              /* no hay de norma 7 */
     [[4, 2; 0, 2]],
     [[3, 0; 0, 3]],
     [[10, 3; 0, 1], [10, 7; 0, 1]]]
```

La salida es un vector

[ideales de norma 0, ideales de norma 1, . . ., ideales de norma N]

Por ejemplo, si queremos contar los ideales de cada norma, o ver cuántos son en total, podemos hacer lo siguiente:

```
? vector (#L,i,#L[i])
% = [1, 1, 0, 1, 2, 0, 0, 1, 1, 2, 0, 0, 2, 0, 0, 1, 2, 1, 0, 2]
? sum (i=1,#L,#L[i])
% = 17
```

Tenemos las siguientes operaciones básicas con ideales (todas las funciones relevantes empiezan por «`ideal`»):

- `idealadd`$(K,\mathfrak{a},\mathfrak{b})$ — suma $\mathfrak{a}+\mathfrak{b}$,
- `idealmul`$(K,\mathfrak{a},\mathfrak{b})$ — producto $\mathfrak{a}\mathfrak{b}$,
- `idealpow`$(K,\mathfrak{a},n)$ — $\mathfrak{a}^n$,
- `idealinv`$(K,\mathfrak{a})$ — $\mathfrak{a}^{-1}$,
- `idealintersect`$(K,\mathfrak{a},\mathfrak{b})$ — $\mathfrak{a}\cap\mathfrak{b}$.

Otras funciones útiles:

- `idealdown`$(K,\mathfrak{a})$ — el $\mathbb{Z}$-ideal $\mathfrak{a}\cap\mathbb{Q}$,
- `idealnorm`$(K,\mathfrak{a})$ — la norma $N_{K/\mathbb{Q}}(\mathfrak{a})$,
- `idealismaximal`$(K,\mathfrak{a})$ — verifica si el ideal es maximal.

```
? K = nfinit(x^2+1);
? idealdown(K,1+x)
% = 2
? idealdown(K,3+3*x)
% = 6

? idealnorm(K,1+x)
% = 2
? idealnorm(K,3)
% = 9
? idealnorm(K,3+3*x)
% = 18

? idealismaximal(K,1+x)
% = [2, [1, 1]~, 2, 1, [1, -1; 1, 1]]
? idealismaximal(K,3+3*x)
% = 0
```

Aquí `idealismaximal(`K`,`$\mathfrak{a}$`)` devuelve `0` si el ideal no es maximal, y en el caso contrario, devuelve varias cosas precalculadas, cuyo significado será explicado abajo.

Aunque la representación de ideales en PARI/GP es útil para cálculos, estamos más acostumbrados a representar los ideales por sus generadores. Como sabemos, dos generadores son siempre suficientes (véase 2.6.9). Para encontrar dos generadores, sirve la función `idealtwoelt(`K`,`$\mathfrak{a}$`)`.

```
? K = nfinit(x^3 - 2);
? a = [3,1,2; 0,1,0; 0,0,1]
% =
[3 1 2]

[0 1 0]

[0 0 1]

? idealtwoelt(K,a)
% = [3, [1, 1, 0]~]
? nfbasistoalg(K,%[2])
% = Mod(x + 1, x^3 - 2)
```

Interpretación de la salida: $\mathfrak{a} = (3, 1 + \sqrt[3]{2})$. Por supuesto, es muy interesante ver si algún ideal es principal y admite un solo generador. Esto equivale a ver si $\mathfrak{a}$ es trivial en el grupo de clases $\mathrm{Cl}(K)$, y es más complicado computacionalmente. Veremos cómo hacerlo en PARI/GP en otra ocasión, cuando hablaremos del grupo de clases.

3.11.6 Factorización de ideales en el anillo de enteros

Para factorizar un ideal $\mathfrak{a}$ en ideales primos, se usa `idealfactor(`K`,`$\mathfrak{a}$`)`. Nos va a interesar principalmente factorización de primos racionales $p \in \mathbb{Z}$ en $\mathcal{O}_K$, y para esto sirve la función `idealprimedec(`K`,`p`)`.

Antes de ver los cálculos en PARI/GP, hay que explicar el formato de la salida. Si la factorización tiene forma

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

entonces

$$\texttt{idealprimedec(}K\texttt{,}p\texttt{) = [}P_1\texttt{,...,}P_s\texttt{]},$$

donde P_i corresponde al múltiplo $\mathfrak{p}_i^{e_i}$. En particular, $P = P_i$ contiene los siguientes datos:

- P`.e` = el índice de ramificación e_i,
- P`.f` = el grado del campo residual $\mathcal{O}_K/\mathfrak{p}_i$,
- P`.gen = [`p`,` α`]`, donde $\mathfrak{p}_i = (p, \alpha)$.

He aquí un ejemplo particular: consideremos cómo los primos racionales se factorizan en el campo cuadrático $\mathbb{Q}(\sqrt{5})$ y el campo ciclotómico $\mathbb{Q}(\zeta_5)$.

```
? K = nfinit(x^2 - 5);

? decK = idealprimedec(K,11)
% = [[11, [-3, 2]~, 1, 1, [5, 2; 2, 3]],
     [11, [5, 2]~, 1, 1, [-3, 2; 2, -5]]]
? #decK
# 2               /* 2 factores */

? [decK[1].e, decK[1].f]
% = [1, 1]
? decK[1].gen
% = [11, [-3, 2]~]
? nfbasistoalg (K,%[2])
% = Mod(x - 4, x^2 - 5)

? [decK[2].e, decK[2].f]
% = [1, 1]
? decK[2].gen
% = [11, [5, 2]~]
? nfbasistoalg (K,%[2])
% = Mod(x + 4, x^2 - 5)
```

La interpretación de la salida:

$$11\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \quad \mathfrak{p}_1 = (11, \sqrt{5}-4),\ \mathfrak{p}_2 = (11, \sqrt{5}+4),\ f_1 = f_2 = 1.$$

Para el campo $L = \mathbb{Q}(\zeta_5)$ de la misma manera encontramos que

$$11\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4.$$

```
? L = nfinit(polcyclo(5));
? decL = idealprimedec(L,11);
? #decL
# 4               /* 4 factores */
? vector (#decL,i, [decL[i].e, decL[i].f])
% = [[1, 1], [1, 1], [1, 1], [1, 1]]
```

La única ramificación será en $p = 5$.

```
? idealprimedec(K,5)
% = [[5, [1, 2]~, 2, 1, [1, 2; 2, -1]]]
? %[1].e
% = 2
? idealprimedec(L,5)
% = [[5, [-1, 1, 0, 0]~, 4, 1, [.....]]]
? %[1].e
% = 4
```

Notamos que $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ para p impar, así que la factorización depende del resto de p módulo 5. Para ver diferentes casos, tomemos considerar $p = 2, 3, 5, 11, 19$. Invito al lector a hacerlo en PARI/GP.

Terminemos por el ejemplo de Kronecker con la factorización de $p = 47$ en $K = \mathbb{Q}(\zeta_{23})$.

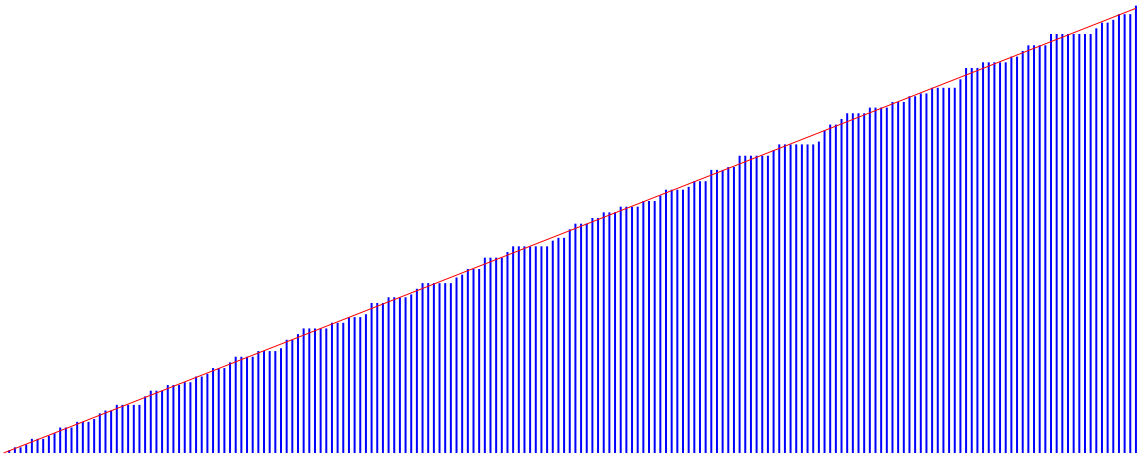
```
? K = nfinit(polcyclo(23));
? dec = idealprimedec(K,47);
? #dec
% = 22
```

3.12 Un par de experimentos numéricos

> The attitude adopted in this book is that while we expect to get numbers out of the machine, we also expect to take action based on them, and, therefore we need to understand thoroughly what numbers may, or may not, mean. To cite the author's favorite motto, "The purpose of computing is insight, not numbers," although some people claim, "The purpose of computing numbers is not yet in sight."
> There is an innate risk in computing because "to compute is to sample, and one then enters the domain of statistics with all its uncertainties."
>
> Richard W. Hamming, *Introduction to applied numerical analysis*, 1971

PARI/GP nos permite hacer varios experimentos numéricos. Me gustaría presentar un par de ejemplos curiosos, donde surgen ciertos fenómenos que serán explicados más adelante.

Usando la función `ideallist`, podemos contar los ideales enteros en $\mathcal{O}_K$ de norma $\leq N$ y ver cómo este número depende de N. Por ejemplo, para $K = \mathbb{Q}(i)$ el resultado se ve de la siguiente manera.



Aquí asintóticamente, la dependencia es lineal, pero ¿cómo explicarlo? Todos los ideales en $\mathcal{O}_K = \mathbb{Z}[i]$ son principales, y tenemos

$$N_{K/\mathbb{Q}}((a+bi)\mathbb{Z}[i]) = a^2 + b^2.$$

Además, para todo entero de Gauss no nulo $\alpha \in \mathbb{Z}[i]$ tenemos cuatro diferentes enteros de Gauss $u\alpha$, donde $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, que representan en mismo ideal. Entonces,

$$\#\{I \subseteq \mathbb{Z}[i] \mid N(I) \leq N\} = \frac{1}{4} \cdot \#\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 \leq N\}.$$

Entonces, el número que nos interesa es $\frac{1}{4}$ de los números enteros que están en el círculo de radio $\sqrt{N}$, así que asintóticamente,

$$\#\{I \subseteq \mathbb{Z}[i] \mid N_{K/\mathbb{Q}}(I) \leq N\} \sim \frac{\pi}{4} N.$$

```
? K = nfinit(x^2+1);
? L = ideallist(K,20);
? vector (#L,s, sum(i=1,s,#L[i]))
% = [1, 2, 2, 3, 5, 5, 5, 6, 7, 9, 9, 9, 11, 11, 11, 12, 14, 15, 15, 17]
? vector (20,i, ceil(Pi/4*i))
% = [1, 2, 3, 4, 4, 5, 6, 7, 8, 8, 9, 10, 11, 11, 12, 13, 14, 15, 15, 16]
```

Podemos tomar otros campos de números, por ejemplo $K_1 = \mathbb{Q}(\zeta_5)$, $K_2 = \mathbb{Q}(\sqrt{10})$, $K_3 = \mathbb{Q}(\sqrt[3]{19})$. De hecho, para K_2 y K_3 el anillo $\mathcal{O}_K$ no es un dominio de ideales principales (lo probaremos después), pero de la figura 3.3 se ve que la dependencia es siempre asintóticamente $\sim C \cdot N$. Más adelante explicaremos C de dónde sale la constante C en cada caso.

Otro fenómeno curioso que podemos investigar es la estadística de descomposiciones de primos racionales. Para ver un ejemplo concreto, consideremos el campo $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ y veremos cómo se factorizan diferentes primos racionales p en $\mathcal{O}_K$. Primero, calculamos que los primos que se ramifican son 2 y 3. Es fácil explicarlo: estos ya se ramifican en los subcampos $\mathbb{Q}(\sqrt[3]{2})$ y $\mathbb{Q}(\zeta_3)$.

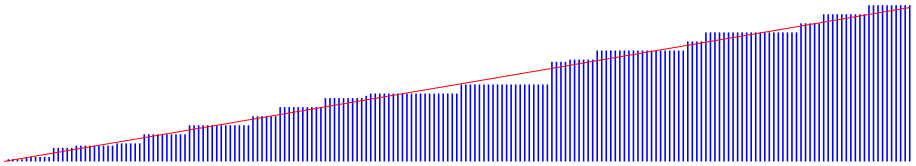
```
? F = nfinit(t^3-2);
? K = nfinit (rnfinit(F,polcyclo(3)));
? K.disc
% = -34992
? factor (%)
% =
[-1 1]

[ 2 4]

[ 3 7]
```

Ahora si p no se ramifica, tenemos descomposición

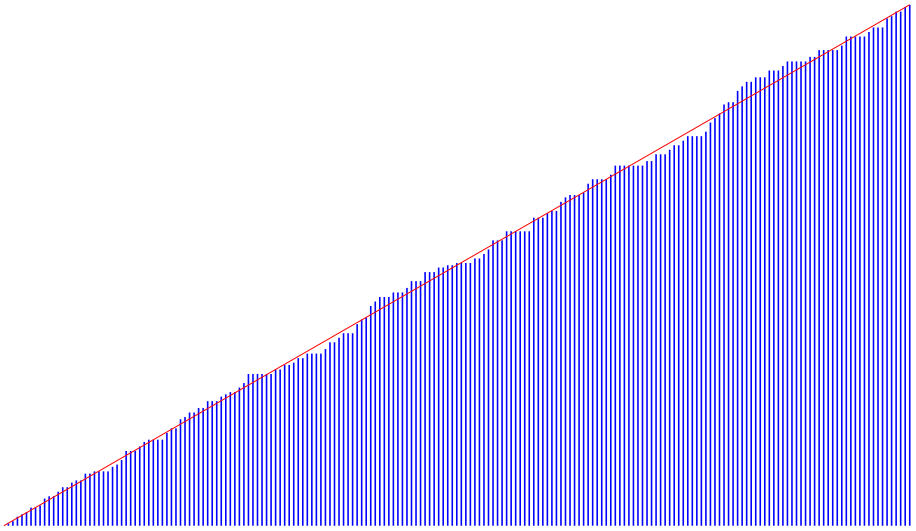
$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s, \quad \sum_i f_i = [K : \mathbb{Q}] = 6.$$

Entonces, diferentes factorizaciones corresponden a particiones de 6.

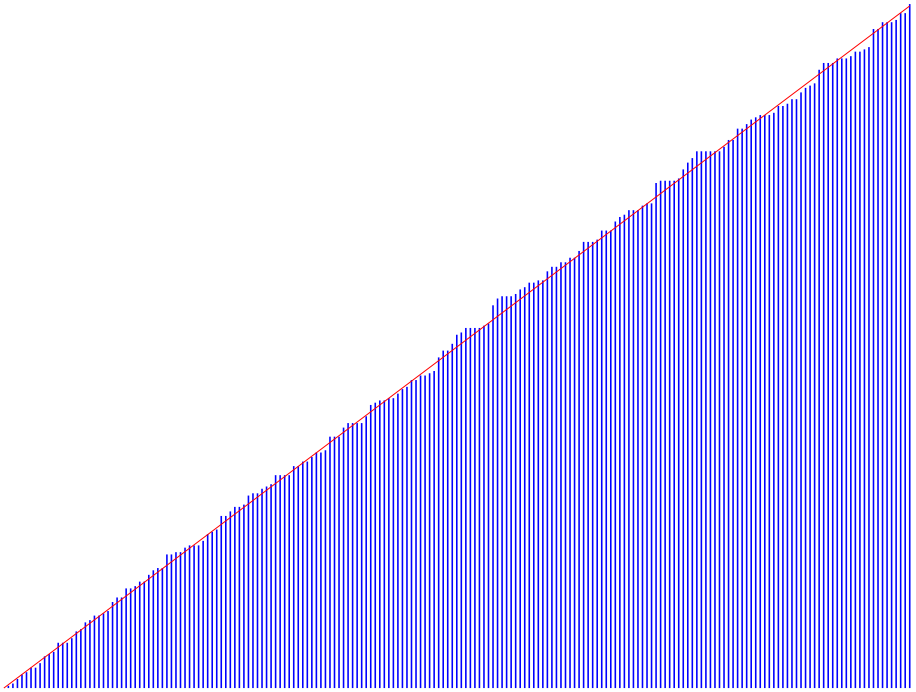
¿Será que cualquier partición puede ser realizada de esta manera? Al parecer, la respuesta es no: he aquí algunos ejemplos.



$K = \mathbb{Q}(\zeta_5)$



$K = \mathbb{Q}(\sqrt{10})$



$K = \mathbb{Q}(\sqrt[3]{19})$

Figura 3.3: El número de ideales en $\mathcal{O}_K$ de norma $\leq I$

p	partición	p	partición	p	partición
5	$2+2+2$	41	$2+2+2$	83	$2+2+2$
7	$3+3$	43	$1+1+1+1+1+1$	89	$2+2+2$
11	$2+2+2$	47	$2+2+2$	97	$3+3$
13	$3+3$	53	$2+2+2$	101	$2+2+2$
17	$2+2+2$	59	$2+2+2$	103	$3+3$
19	$3+3$	61	$3+3$	107	$2+2+2$
23	$2+2+2$	67	$3+3$	109	$1+1+1+1+1+1$
29	$2+2+2$	71	$2+2+2$	113	$2+2+2$
31	$1+1+1+1+1+1$	73	$3+3$	127	$1+1+1+1+1+1$
37	$3+3$	79	$3+3$	131	$2+2+2$

Se ve que los f_i deben ser iguales, pero esto no es muy sorprendente: ya vimos que lo mismo pasa con los campos ciclotómicos. En el siguiente capítulo veremos que esto sucede porque $K/\mathbb{Q}$ es una extensión de Galois. Además, parece que no hay primos inertes (dejo al lector pensar a qué se debe esto).

Las cosas sorprendentes aparecen si nos preguntamos cuál es la frecuencia de cada tipo de partición. A saber, podemos tomar N números primos, donde N es bastante grande, y ver cuántos de estos primos corresponden a cada una de las tres particiones. Aquí está una pequeña tabla de frecuencias de $1+\cdots+1$, $2+2+2$ y $3+3$ para diferentes N.

N	$1+\cdots+1$	$2+2+2$	$3+3$
10	0,1000	0,5000	0,4000
100	0,1500	0,5200	0,3300
1000	0,1570	0,5080	0,3350
10000	0,1635	0,5011	0,3354
100000	0,1659	0,5004	0,3337

Se ve que las frecuencias convergen lentamente a los números racionales $\frac{1}{6}$, $\frac{1}{2}$, $\frac{1}{3}$. Este fenómeno se explica por el **teorema de densidad de Chebotarëv** que será formulado en el siguiente capítulo. Para entender qué está pasando, tomemos otro campo $K=\mathbb{Q}(\zeta_7)$. Ya sabemos factorizar los primos racionales en los campos ciclotómicos. En este caso las factorizaciones son las siguientes.

p (7)	factorización	f
1	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4\,\mathfrak{p}_5\,\mathfrak{p}_6$	1
2	$\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3$	2
2, 4	$\mathfrak{p}_1\,\mathfrak{p}_2$	3
3, 5	$\mathfrak{p}$	6

Y aquí están las frecuencias.

N	$1+\cdots+1$	$2+2+2$	$3+3$	6
10	0,2000	0,1000	0,3000	0,4000
100	0,1700	0,1600	0,3200	0,3500
1000	0,1660	0,1660	0,3300	0,3380
10000	0,1662	0,1663	0,3324	0,3351
100000	0,1668	0,1669	0,3328	0,3336

Los números convergen a $\frac{1}{6}$, $\frac{1}{6}$, $\frac{1}{3}$, $\frac{1}{3}$, y es fácil explicarlo. En total tenemos 6 restos no nulos módulo 7. El primer caso, igual y como el segundo, corresponde a un resto. Por otra parte, el tercer y cuarto caso corresponden a dos restos cada uno. El hecho de que precisamente $\frac{1}{6}$ primos cumplen la condición $p \equiv a \pmod 7$ para $a = 1, 2, 3, 4, 5, 6$ es intuitivamente esperado, pero es el contenido del teorema de Dirichlet sobre primos en progresiones aritméticas (véase el apéndice D).

Ejercicios

Ejercicio 3.1. Encuentre la fórmula para el discriminante del polinomio $x^n + ax + b$.

Ejercicio 3.2. Para una extensión $K/\mathbb{Q}$, sea $e_1, \ldots, e_n$ una base de K sobre $\mathbb{Q}$ y $e'_1, \ldots, e'_n$ la base dual respecto al apareamiento de traza. Demuestre que

$$\Delta(e_1, \ldots, e_n) \cdot \Delta(e'_1, \ldots, e'_n) = 1.$$

Ejercicio 3.3. Encuentre el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K para el campo $K = \mathbb{Q}(\alpha)$ donde α cumple $\alpha^4 + \alpha + 1 = 0$.

Ejercicio 3.4. Sea $K/\mathbb{Q}$ un campo de números de grado $n = [K : \mathbb{Q}]$. Supongamos que para algún primo racional $p < n$ se tiene factorización en n diferentes primos $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Demuestre que en este caso $\mathcal{O}_K$ no es de la forma $\mathbb{Z}[\alpha]$.

Ejercicio 3.5. Sea $K/\mathbb{Q}$ un campo de números y $\alpha \in \mathcal{O}_K$ un elemento entero tal que $\alpha \notin m\mathcal{O}_K$ para $m > 1$. Demuestre que en este caso existe una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$ que contiene α. En particular, demuestre que $\mathcal{O}_K$ siempre admite una base que contiene 1.

Ejercicio 3.6. Sea d un entero libre de cuadrados. Consideremos el campo cúbico $K = \mathbb{Q}(\sqrt[3]{d})$. Denotemos $\alpha = \sqrt[3]{d}$ y consideremos un elemento

$$\beta = a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q}.$$

1) Calcule las trazas $T_{K/\mathbb{Q}}(\beta)$, $T_{K/\mathbb{Q}}(\alpha\beta)$, $T_{K/\mathbb{Q}}(\alpha^2\beta)$ y la norma $N_{K/\mathbb{Q}}(\beta)$.
2) Si $\beta \in \mathcal{O}_K$, entonces las trazas y normas de arriba son números enteros. Use esto para concluir que $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha]$.
3) Use estas consideraciones para calcular el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K.

Ejercicio 3.7. Encuentre el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K para los campos cúbicos $\mathbb{Q}(\sqrt[3]{6})$ y $\mathbb{Q}(\sqrt[3]{12})$.

Ejercicio 3.8. Sea $K/\mathbb{Q}$ un campo de números y N un número natural fijo.

1) Demuestre que hay un número finito de ideales $I \subseteq \mathcal{O}_K$ con la norma $N_{K/\mathbb{Q}}(I) \leq N$. (Indicación: use la factorización de ideales en ideales primos y multiplicatividad de la norma.)
2) Demuestre que módulo la relación $\sim$, hay un número finito de elementos $\alpha \in \mathcal{O}_K$, tales que $|N_{K/\mathbb{Q}}(\alpha)| \leq N$.

Ejercicio 3.9. Consideremos el campo cúbico $K = \mathbb{Q}(\sqrt[3]{17})$.

1) Calcule el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K.
2) Describa las factorizaciones de primos racionales $p \in \mathbb{Z}$ en $\mathcal{O}_K$.
3) Describa los ideales primos $\mathfrak{p} \subset \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq 10$.
4) Describa todos los ideales $I \subseteq \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(I) \leq 10$.

Ejercicio 3.10. Sea X una matriz de $n \times n$ e Y una matriz de $n' \times n'$. El **producto de Kronecker** $X \otimes Y$ es la matriz de $nn' \times nn'$ que consiste en bloques

$$\begin{pmatrix} x_{11}Y & \cdots & x_{1n}Y \\ \vdots & \ddots & \vdots \\ x_{n1}Y & \cdots & x_{nn}Y \end{pmatrix}.$$

(El significado de esta matriz: si X e Y corresponden a aplicaciones R-lineales $f\colon R^n \to R^n$ y $g\colon R^{n'} \to R^{n'}$, entonces $X \otimes Y$ corresponde a $f \otimes g\colon R^{nn'} \to R^{nn'}$ respecto a la base estándar $e_i \otimes e'_j$.)

Demuestre que

$$\det(X \otimes Y) = \det(X)^{n'} \cdot \det(Y)^n.$$

Ejercicio 3.11. Para el campo de números $K = \mathbb{Q}(\sqrt{3}, \zeta_5)$ calcule $\mathcal{O}_K$ y Δ_K. ¿Cuáles primos racionales se ramifican en K?

Ejercicio 3.12. Consideremos los campos cuadráticos $K = \mathbb{Q}(\sqrt{3})$ y $K' = \mathbb{Q}(\sqrt{-5})$ y su compositum $KK' = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$. Sea $\mathcal{O} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{-5}\mathbb{Z} \oplus \sqrt{-15}\mathbb{Z}$.

Calcule $\mathcal{O}_{KK'}$, $\Delta_{KK'}$ y el índice $[\mathcal{O}_{KK'} : \mathcal{O}]$.

Ejercicio 3.13. Calcule que

$$\Delta(\mathbb{Z}[\zeta_{p^e}]) = \Delta(\Phi_{p^e}) = \pm p^s, \quad \text{donde } s = p^{e-1}(pe - e - 1).$$

¿Cuál es el signo?
(Indicación: generalice el cálculo de 3.5.7.)

Ejercicio 3.14. Demuestre que si $n = mp^e$, donde $p \nmid m$, entonces se cumple la congruencia

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^e)} \pmod{p}.$$

Capítulo 4

Teoría de Galois

Ya hemos usado ciertos argumentos de la teoría de Galois, y en este capítulo veremos de manera más sistemática algunas propiedades de los campos de números $K/\mathbb{Q}$ que son extensiones de Galois.

4.1 Breve recordatorio sobre la teoría de Galois

Clase 15
05/10/20

En esta sección vamos a revisar rápidamente la teoría de Galois. El apéndice A contiene la mayoría de los resultados necesarios.

La teoría de Galois considera las extensiones de Galois que son extensiones separables y normales. En la característica nula cualquier extensión es separable, así que la condición que nos interesa para los campos de números es la normalidad.[*]

Dado un campo de números $K/\mathbb{Q}$, gracias al teorema del elemento primitivo, podemos escribirlo como $K = \mathbb{Q}(\alpha)$ para algún número algebraico α. Sea $f = f^{\alpha}_{\mathbb{Q}}$ el polinomio mínimo de α. Consideremos sus raíces complejas

$$f = (x - \alpha_1) \cdots (x - \alpha_n).$$

Por la separabilidad, se tiene $\alpha_i \neq \alpha_j$ para $i \neq j$. El campo de descomposición de f viene dado por $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, y esta es una extensión normal. El grupo

$$G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Aut}(L/\mathbb{Q})$$

se llama el **grupo de Galois**. Se tiene $|G| = [L : \mathbb{Q}]$. Hay una acción fiel y transitiva sobre las raíces

$$G \curvearrowright \{\alpha_1, \ldots, \alpha_n\}.$$

Fijando una numeración de las raíces (como ya hicimos implícitamente), se obtiene un homomorfismo inyectivo $G \hookrightarrow S_n$. Si $K = L$, entonces $K/\mathbb{Q}$ es una extensión de Galois. En el caso contrario, L es la **cerradura de Galois** de K.

4.1.1. Ejemplo. Ya hemos usado en varias ocasiones que las extensiones ciclotómicas $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ son de Galois: el polinomio mínimo de ζ_n es el polinomio ciclotómico Φ_n y sus raíces son las raíces n-ésimas primitivas que están en $\mathbb{Q}(\zeta_n)$.

Todo automorfismo $\sigma\colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ debe mandar ζ_n a otra raíz n-ésima primitiva, así que los automorfismos son

$$\sigma_a\colon \zeta_n \mapsto \zeta_n^a, \quad \mathrm{mcd}(a, n) = 1.$$

[*] También en este curso nos interesan extensiones finitas de campos finitos, pero estas son siempre extensiones de Galois.

Tenemos un isomorfismo

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma_a \mapsto \overline{a}.$$

Todo el trabajo duro consiste en probar que Φ_n es el polinomio mínimo de ζ_n; es decir, probar la irreducibilidad de Φ_n. Véase el apéndice B. ▲

4.1.2. Ejemplo. La extensión $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es de Galois. Tenemos

$$f = x^3 - 2 = (x - \sqrt[3]{2})\,(x - \zeta_3\sqrt[3]{2})\,(x - \zeta_3^2\sqrt[3]{2}).$$

El campo de descomposición de f es $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, y su grupo de Galois es el grupo simétrico S_3. Específicamente, hay dos automorfismos

$$\begin{aligned} \sigma\colon \sqrt[3]{2} &\mapsto \zeta_3\sqrt[3]{2}, \quad \zeta_3 \mapsto \zeta_3, \\ \tau\colon \sqrt[3]{2} &\mapsto \sqrt[3]{2}, \quad \zeta_3 \mapsto \zeta_3^2. \end{aligned}$$

Aquí el orden de σ es 3 y el orden de τ es 2. Tenemos $\sigma\tau = \tau\sigma^2 \neq \tau\sigma$. Estos dos elementos generan el grupo de Galois que es isomorfo al grupo simétrico S_3. ▲

El problema con el campo de números $K = \mathbb{Q}[\alpha]/(\alpha^3 - 2)$ es el siguiente: este tiene tres diferentes encajes $K \hookrightarrow \mathbb{C}$: un encaje real con imagen $\mathbb{Q}(\sqrt[3]{2})$ y dos encajes complejos con imagen $\mathbb{Q}(\zeta_3\sqrt[3]{2})$ y $\mathbb{Q}(\zeta_3^2\sqrt[3]{2})$. Esto no puede pasar con extensiones de Galois.

4.1.3. Proposición. *Sea $K/\mathbb{Q}$ una extensión de Galois. Entonces, todo encaje $\sigma\colon K \hookrightarrow \mathbb{C}$ tiene la misma imagen. Como consecuencia, todos los encajes son reales ($r_1 = [K:\mathbb{Q}]$) o todos los encajes son complejos ($r_2 = \frac{1}{2}[K:\mathbb{Q}]$).*

Demostración. En general, una extensión finita K/F es normal si y solamente si para todo F-homomorfismo $\sigma\colon K \to \overline{K}$ se cumple $\sigma(K) = K$ (véase A.5.1). ■

Este no es un curso de la teoría de Galois, pero nuestra discusión sería incompleta sin el siguiente resultado.

4.1.4. Teorema (Correspondencia de Galois). *Dada una extensión finita de Galois $K/\mathbb{Q}$, consideremos el grupo de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$. A una subextensión $\mathbb{Q} \subseteq F \subseteq K$ se puede asociar un subgrupo $H = \mathrm{Gal}(K/F) \subseteq G$. Viceversa, dado un subgrupo $H \subseteq G$, se obtiene una subextensión*

$$F = K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ para } \sigma \in H\}.$$

Esto nos da una biyección

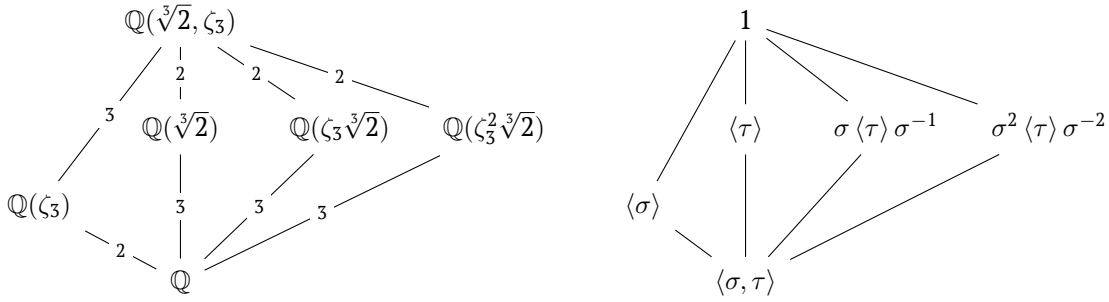
$$\{\text{ subcampos } F \subseteq K\} \underset{K^H \hookleftarrow H}{\overset{F \mapsto \mathrm{Gal}(K/F)}{\rightleftarrows}} \{\text{ subgrupos } H \subseteq G\}$$

Esta correspondencia satisface las siguientes propiedades.

- *La correspondencia invierte las inclusiones. Si $F \subseteq F'$, entonces $\mathrm{Gal}(K/F') \subseteq \mathrm{Gal}(K/F)$. Si $H \subseteq H' \subseteq G$, entonces $K^{H'} \subseteq K^H$.*
- $[K:F] = |H|$ y $[F:\mathbb{Q}] = [G:H]$.
- *La extensión $F/\mathbb{Q}$ es normal (y entonces Galois) si y solamente si el subgrupo $H \subseteq G$ es normal. En este caso la restricción de automorfismos $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(F/\mathbb{Q})$ es sobreyectiva y tiene H como su núcleo, así que $\mathrm{Gal}(F/\mathbb{Q}) \cong G/H$.*
- *Para dos subextensiones F y F' se tiene $F \cong F'$ si y solamente si los subgrupos correspondientes $H, H' \subseteq G$ son conjugados por un elemento de G.*

Demostración. Véase A.11.2. ■

4.1.5. Ejemplo. En $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ hay un subcampo cuadrático $\mathbb{Q}(\zeta_3)$ y tres subcampos cúbicos $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta_3\sqrt[3]{2})$, $\mathbb{Q}(\zeta_3^2\sqrt[3]{2})$ isomorfos entre sí. La correspondencia con los subgrupos de $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$ es la siguiente:



▲

Uno de los problemas abiertos más importantes de la aritmética es el **problema inverso de Galois** que pregunta si todo grupo finito es isomorfo a $\mathrm{Gal}(K/\mathbb{Q})$ para alguna extensión de Galois $K/\mathbb{Q}$.

4.1.6. Ejemplo. Según un teorema de Selmer [Sel1956], el polinomio $x^n - x - 1 \in \mathbb{Q}[x]$ es irreducible para todo n. Su campo de descomposición tiene S_n como su grupo de Galois; véase [Osa1987] o la exposición [KCd-Selmer]. ▲

Para los grupos abelianos, el problema se resuelve fácilmente de la siguiente manera.

4.1.7. Proposición. *Cualquier grupo abeliano finito puede ser realizado como un grupo de Galois.*

Demostración. Primero notamos que para todo primo p la extensión ciclotómica $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es una extensión de Galois, con el grupo de Galois cíclico

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/p\mathbb{Z})^\times$$

A saber, los automorfismos son

$$\sigma\colon \zeta_p \mapsto \zeta_p^a, \ \ \mathrm{mcd}(a,p) = 1.$$

Todo grupo abeliano finito se expresa como producto de grupos cíclicos

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}.$$

Ocupando el teorema de Dirichlet sobre primos en progresiones aritméticas (véase el apéndice D), podemos encontrar diferentes primos $p_1, \ldots, p_s$ tales que $p_i \equiv 1 \pmod{n_i}$. De hecho, el teorema afirma que para cada n_i existe un número infinito de primos p_i con esta propiedad.

Ahora consideremos el campo ciclotómico

$$K = \mathbb{Q}(\zeta_{p_1 \cdots p_s}).$$

Su grupo de Galois es un producto de grupos cíclicos

$$G \cong (\mathbb{Z}/p_1 \cdots p_s\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times.$$

Por nuestra elección de p_i, existe subgrupo $H_i \subset (\mathbb{Z}/p_i\mathbb{Z})^\times$ de índice n_i, y luego

$$G/(H_1 \times \cdots \times H_s) \cong C_{n_1} \times \cdots C_{n_s}.$$ ■

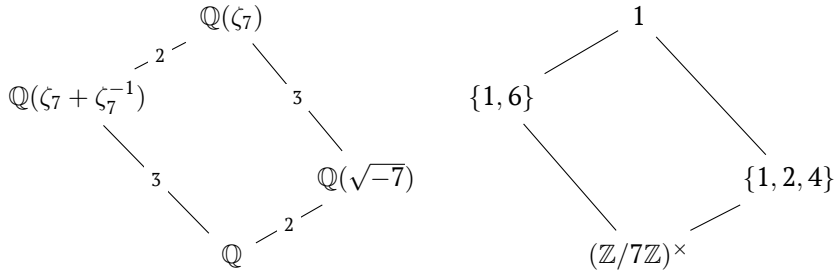
4.1.8. Ejemplo. Para hacerlo más específico, si buscamos una extensión con el grupo de Galois C_3, podemos tomar $p = 7$. Nos interesa entonces la extensión ciclotómica $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ y el grupo de Galois

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times.$$

La conjugación compleja $\zeta_7 \to \zeta_7^{-1}$ tiene orden 2. El subcampo cúbico real fijo por la conjugación compleja es $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. También hay automorfismo de orden 3 dado por $\zeta_7 \mapsto \zeta_7^2$. Este fija el subcampo cuadrático $\mathbb{Q}(\sqrt{-7})$, donde

$$\sqrt{-7} = 1 + 2\zeta_7 + 2\zeta_7^2 + 2\zeta_7^4.$$

Hemos descrito todas las posibles subextensiones:



▲

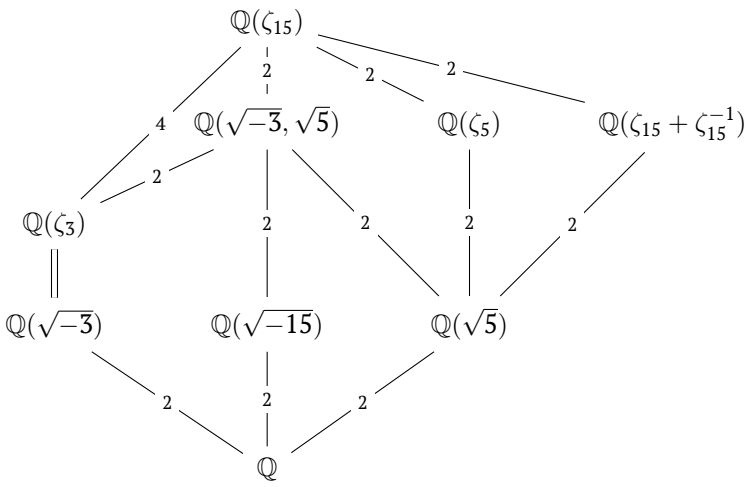
4.1.9. Ejemplo. Si queremos encontrar una extensión con el grupo abeliano $C_2 \times C_2$ usando este método, podemos tomar el campo ciclotómico $\mathbb{Q}(\zeta_{15})$ con el grupo de Galois

$$G \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times,$$

y tomar adentro el subgrupo

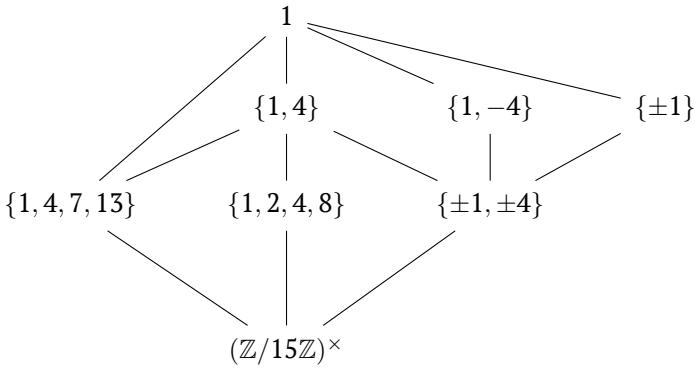
$$H = \{1, 4\} \subset (\mathbb{Z}/15\mathbb{Z})^\times.$$

Ahora el subcampo $\mathbb{Q}(\zeta_{15})^H$ es el campo bicuadrático $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$.



El diagrama de arriba contiene todos los subcampos de $\mathbb{Q}(\zeta_{15})$. Los subgrupos correspondientes $H \subseteq G$ son

los siguientes:



▲

Entonces, cualquier grupo de Galois abeliano se realiza mediante una subextensión de algún campo ciclotómico. Esta no es una coincidencia: se cumple el siguiente resultado mucho más fuerte.

4.1.10. Teorema (Kronecker–Weber). *Sea $K/\mathbb{Q}$ une extensión con el grupo* $\mathrm{Gal}(K/\mathbb{Q})$ *abeliano. Entonces, para algún n se tiene $K \subseteq \mathbb{Q}(\zeta_n)$.*

Demostración. La prueba requiere bastante trabajo y nos llevaría lejos de los objetivos de este curso... El lector interesado puede consultar [Was1997, Chapter 14]. ■

4.1.11. Ejemplo. Para un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$ es fácil encontrar n tal que $K \subset \mathbb{Q}(\zeta_n)$: use que para un primo impar p se tiene $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$, donde $p^* = (-1)^{\frac{p-1}{2}} p$ (véase ejercicio 2.19), y que $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ y $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8)$. Para el caso general, basta factorizar d en números primos. Dejo los detalles como un ejercicio. ▲

4.2 Acción del grupo de Galois sobre los ideales

A partir de ahora supongamos que $K/\mathbb{Q}$ es una extensión finita de Galois y denotemos $G = \mathrm{Gal}(K/\mathbb{Q})$. Primero notamos que la acción de G sobre K induce acción de G sobre $\mathcal{O}_K$ y los ideales en $\mathcal{O}_K$.

4.2.1. Proposición. *Consideremos un elemento $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.*

1) *Si $\alpha \in \mathcal{O}_K$, entonces $\sigma(\alpha) \in \mathcal{O}_K$.*
2) *Dado un ideal $I \subseteq \mathcal{O}_K$, el conjunto $\sigma(I) = \{\sigma(\alpha) \mid \alpha \in I\}$ es también un ideal en $\mathcal{O}_K$. En términos de generadores, si $I = (\alpha_1, \ldots, \alpha_n)$, entonces $\sigma(I) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$.*
3) *Hay isomorfismo natural $\mathcal{O}_K/I \cong \mathcal{O}_K/\sigma(I)$.*
4) *Si $\mathfrak{p} \subset \mathcal{O}_K$ es un ideal primo, entonces el ideal $\sigma(\mathfrak{p}) \subset \mathcal{O}_K$ es también primo. Además, si $\mathfrak{p} \mid p$ para un primo racional $p \in \mathbb{Z}$, entonces $\sigma(\mathfrak{p}) \mid p$, y los grados de campos residuales coinciden.*

Demostración. En la parte 1), si α es una raíz de un polinomio mónico $f \in \mathbb{Z}[x]$, entonces $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, así que $\sigma(\alpha) \in \mathcal{O}_K$. La parte 2) se verifica fácilmente usando el hecho de que σ preserva sumas y productos.

Para la parte 3), basta notar que el homomorfismo

$$\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\sigma(I), \quad \alpha \mapsto \sigma(\alpha) + \sigma(I)$$

tiene I como su núcleo y entonces induce el isomorfismo deseado.

En particular, $\mathcal{O}_K/\mathfrak{p}$ es un dominio si y solamente si $\mathcal{O}_K/\sigma(\mathfrak{p})$ es un dominio, y esto demuestra que para $\mathfrak{p}$ primo el ideal $\sigma(\mathfrak{p})$ es también primo. Ahora si $p \in \mathfrak{p}$, entonces $p = \sigma(p) \in \sigma(\mathfrak{p})$. En fin, el isomorfismo $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K/\sigma(\mathfrak{p})$ nos dice que los grados del campo residual son iguales. Esto establece la parte 4). ■

Entonces, si $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$, el grupo G actúa de alguna manera sobre el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Esta acción es el objeto principal de estudio del presente capítulo.

4.2.2. Ejemplo. Si $K = \mathbb{Q}(\sqrt{d})$ es una extensión cuadrática, entonces para $\left(\frac{d}{p}\right) = +1$ se obtiene

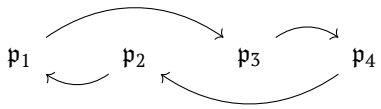
$$p\mathcal{O}_K = \mathfrak{p}\,\sigma(\mathfrak{p}),$$

donde $\sigma\colon \sqrt{d} \mapsto -\sqrt{d}$ es el automorfismo no trivial de $K/\mathbb{Q}$. ▲

Consideremos alguna extensión un poco más interesante que cuadrática.

4.2.3. Ejemplo. Consideremos algún campo ciclotómico, por ejemplo $K = \mathbb{Q}(\zeta_5)$. Tenemos $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$, donde como generador se puede tomar $\sigma\colon \zeta_5 \mapsto \zeta_5^2$. La descomposición de un primo racional p depende de su resto módulo 5.

- Si $p \equiv 1 \pmod 5$, entonces $p\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$, donde según Krull–Dedekind, $\mathfrak{p}_i = (p, \zeta_5 - a^i)$, y a es una quinta raíz primitiva de la unidad mód p. Se puede calcular que la acción de σ sobre los ideales primos viene dada por



  Nos conviene entonces escribir la factorización como $p\mathcal{O}_K = \mathfrak{p}\,\sigma(\mathfrak{p})\,\sigma^2(\mathfrak{p})\,\sigma^3(\mathfrak{p})$.
- Si $p \equiv 4 \pmod 5$, entonces la factorización tiene forma $p\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$. En este caso se puede calcular que $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$ y viceversa, $\sigma(\mathfrak{p}_2) = \mathfrak{p}_1$. Entonces, la factorización toma forma $p\mathcal{O}_K = \mathfrak{p}\,\sigma(\mathfrak{p})$.
- Si $p \equiv 2, 3 \pmod 5$, entonces p es inerte: el ideal $p\mathcal{O}_K$ es primo.
- Si $p = 5$, entonces tenemos ramificación $p\mathcal{O}_K = \mathfrak{p}^4$, donde $\mathfrak{p} = (1 - \zeta_5)$, y no es difícil comprobar a mano que $\sigma(\mathfrak{p}) = \mathfrak{p}$ (aunque ya lo sabemos: σ permuta los primos $\mathfrak{p} \mid p$, y en este caso hay un solo primo sobre p). ▲

Resulta que la acción de G sobre los primos $\mathfrak{p} \mid p$ es siempre transitiva. Esto puede ser probado usando el siguiente resultado general.

4.2.4. Lema (Tate). *Sean A un anillo conmutativo y G un grupo finito que actúa sobre A mediante automorfismos. Consideremos los elementos fijos respecto a esta acción:*

$$A^G = \{a \in A \mid \sigma(a) = a \text{ para todo } \sigma \in G\}.$$

Sean R un dominio y ϕ, ψ dos homomorfismos

$$A^G \subset A \underset{\psi}{\overset{\phi}{\rightrightarrows}} R$$

tales que $\phi|_{A^G} = \psi|_{A^G}$. Entonces, $\phi = \psi \circ \sigma$ para algún $\sigma \in G$.

Antes de probar el lema, vamos a sacar un corolario.

4.2.5. Corolario. *Para una extensión de Galois $K/\mathbb{Q}$, si $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_K$ son dos primos tales que $\mathfrak{p}_1, \mathfrak{p}_2 \mid p$, entonces existe $\sigma \in G$ tal que $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$.*

Demostración. Tenemos $K^G = \mathbb{Q}$, y luego $(\mathcal{O}_K)^G = \mathbb{Z}$. Cada $\mathfrak{p}_i$ es el núcleo de algún homomorfismo $\phi_i\colon \mathcal{O}_K \to \overline{\mathbb{F}_p}$. Estamos en la siguiente situación:

$$\mathbb{Z} \subset \mathcal{O}_K \underset{\phi_2}{\overset{\phi_1}{\rightrightarrows}} \overline{\mathbb{F}_p}$$

Aquí $\phi_1|_{\mathbb{Z}} = \phi_2|_{\mathbb{Z}}$, así que el lema de Tate implica que $\phi_1 = \phi_2 \circ \sigma$ para algún $\sigma \in G$. Ahora $\sigma(\ker(\phi_1)) = \ker(\phi_2)$. ■

Demostración del lema de Tate. Todo homomorfismo $\phi\colon A \to R$ se extiende a $\phi\colon A[x] \to R[x]$. Tenemos

$$A^G[x] \subset A[x] \underset{\psi}{\overset{\phi}{\rightrightarrows}} R[x] \tag{*}$$

Para un elemento $a \in A$ definamos un polinomio

$$f = \prod_{g\in G}(x - \sigma(a)).$$

Notamos que los coeficientes de este polinomio son invariantes respecto a la acción de G, así que $f \in A^G[x]$, y por nuestra hipótesis se tiene $\phi(f) = \psi(f)$ en $R[x]$. El elemento $\phi(a)$ es una raíz de $\phi(f) = \psi(f)$:

$$\phi(f) = \prod_{\sigma\in G} = (x - \phi\sigma(a)) = \psi(f) = \prod_{\sigma\in G} = (x - \psi\sigma(a)).$$

En particular, $\phi(a) = \psi\sigma(a)$ para algún $\sigma \in G$.

Ahora para cada $\sigma \in G$ consideremos

$$A_\sigma = \{a \in A \mid \phi(a) = \psi\sigma(a)\}.$$

Por lo que acabamos de probar,

$$A = \bigcup_{\sigma\in G} A_\sigma.$$

Afirmamos que se tiene $A = A_\sigma$ para algún $\sigma \in G$. Supongamos que esto no es cierto y para todo $\sigma \in G$ existe $a_\sigma \in A$ tal que $a_\sigma \notin A_\sigma$. Consideremos el polinomio

$$g = \sum_{\sigma\in G} a_\sigma x^{d_\sigma} \in A[x].$$

donde los d_σ son diferentes. El mismo argumento de arriba aplicado a (*) demuestra que

$$A[x] = \bigcup_{\sigma\in G} (A[x])_\sigma = \bigcup_{\sigma\in G} A_\sigma[x].$$

Tenemos $g \in A[x]$, pero $g \notin A_\sigma[x]$ para todo σ. Contradicción. ■

La transitividad de la acción del grupo de Galois sobre los primos $\mathfrak{p} \mid p$ tiene la siguiente consecuencia importante.

4.2.6. Proposición. *Sea $K/\mathbb{Q}$ una extensión finita de Galois. Para un primo racional p consideremos la factorización*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}. \tag{*}$$

Los grados de campos residuales e índices de ramificación coinciden:

$$f_1 = \cdots = f_s, \quad e_1 = \cdots = e_s.$$

Entonces, si f_p denota los grados de campos residuales, e_p denota los índices de ramificación y $g_p = s$ es el número de primos, se tiene

$$e_p f_p g_p = [K : \mathbb{Q}].$$

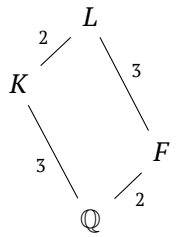
Demostración. Para la igualdad de los f_i, ya notamos que $\mathfrak{p}$ y $\sigma(\mathfrak{p})$ tienen el mismo grado del campo residual, y basta usar que la acción de G sobre los $\mathfrak{p}_i$ es transitiva. Para los índices de ramificación, aplicando σ a la expresión (*) se obtiene

$$p\mathcal{O}_K = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_s)^{e_s},$$

y luego si $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$, entonces $e_i = e_j$ por la unicidad de factorización en ideales primos. De nuevo, la transitividad de la acción de G sobre los $\mathfrak{p}_i$ implica que todos los e_i coinciden. ■

4.2.7. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_n)$, donde $n = \prod_p p^{v_p}$. Hemos visto que para un primo racional p se tiene $e_p = \phi(p^{v_p})$ y f_p es el orden de p módulo n/p^{v_p}. Notamos que estos números dependen solamente del resto de p módulo n. ▲

4.2.8. Ejemplo. Consideremos el campo de números $K = \mathbb{Q}(\sqrt[3]{19})$ y su cerradura de Galois $L = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$. También tenemos un subcampo cuadrático $F = \mathbb{Q}(\zeta_3)$.



Las siguientes consideraciones son útiles. Para un primo racional p y $\mathfrak{p} \mid p$ en $\mathcal{O}_K$, sea $\mathfrak{q}$ un primo en $\mathcal{O}_L$ tal que $\mathfrak{p} \subset \mathfrak{q}$. En este caso tenemos la siguiente situación:

$$\begin{array}{ccccc} \mathfrak{q} & \subset & \mathcal{O}_L & \twoheadrightarrow & \mathcal{O}_L/\mathfrak{q} \\ & & | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/\mathfrak{p} \\ & & | & & | f(\mathfrak{p}) \\ p & \subset & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p \end{array} \qquad f(\mathfrak{q})$$

En particular, $f(\mathfrak{p}) \mid f(\mathfrak{q})$.

Para analizar los primos ramificados, podemos calcular los discriminantes:

$$\Delta_F = -3, \quad \Delta_K = -3 \cdot 19^2, \quad \Delta_L = -3^3 \cdot 19^4.$$

En particular, los primos ramificados en $\mathcal{O}_L$ son los mismos que en $\mathcal{O}_K$.

- Para $p = 3$ se tiene $p\mathcal{O}_F = \mathfrak{r}^2$. El ideal $\mathfrak{r}\mathcal{O}_L$ se factoriza de alguna manera en ideales primos en $\mathcal{O}_L$ que tal vez pueden ramificarse más, pero de todos modos, tenemos $2 \mid e_3$. Por otra parte, $3\mathcal{O}_K = \mathfrak{p}^2\,\mathfrak{p}'$, así que $g_3 \geq 2$. Dado que $e_3 f_3 g_3 = 6$, esto nos deja la única posibilidad $(e_3, f_3, g_3) = (2, 1, 3)$. Entonces,
$$3\mathcal{O}_L = \mathfrak{q}^2\mathfrak{q}'^2\mathfrak{q}''^2,$$
donde $f_3 = 1$.
- Para $p = 19$ se tiene $19\mathcal{O}_K = \mathfrak{p}^3$. Por otra parte, $19\mathcal{O}_F = \mathfrak{p}'\mathfrak{p}''$. Entonces, $e_p \geq 3$ y $g_p \geq 2$. Pero esto nos deja con la única posibilidad $e_p = 3$, $g_p = 2$, $f_{19} = 1$:
$$19\mathcal{O}_L = \mathfrak{q}^3\mathfrak{q}'^3.$$

Ahora para los primos no ramificados, recordemos que p se escinde en F si y solamente si

$$\left(\frac{-3}{p}\right) = +1 \iff p \equiv 1 \pmod 3.$$

- Si $p \equiv 2 \pmod 3$, entonces
$$p\mathcal{O}_K = \mathfrak{p}\,\mathfrak{p}', \quad f(\mathfrak{p}) = 1,\ f(\mathfrak{p}') = 2.$$
Esto implica que $2 \mid f_p$ y $g_p > 1$, pero dado que $f_p g_p = 6$, la única posibilidad es $(f_p, g_p) = (2, 3)$.
$$p\mathcal{O}_L = \mathfrak{q}\,\mathfrak{q}'\,\mathfrak{q}''.$$

- Si $p \equiv 1 \pmod 3$ y 19 no es un cubo módulo p, entonces p es inerte en $\mathcal{O}_K$, lo cuál implica que $3 \mid f_p$. Por otra parte, p se escinde en F, y luego $g_p \geq 2$. Esto nos deja la única posibilidad $f_p = 3$ y $g_p = 2$:

$$p\mathcal{O}_L = \mathfrak{q}\,\mathfrak{q}'.$$

- Si $p \equiv 1 \pmod 3$ y 19 es un cubo módulo p, entonces $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$. Hay dos posibilidades: $p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, o $p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_6$.

  Pero sabemos que

$$p\mathcal{O}_L \cap \mathcal{O}_F = p\mathcal{O}_F = \mathfrak{r}\,\sigma(\mathfrak{r}),$$

  donde σ es la conjugación compleja. Entonces, $\mathfrak{r}\mathcal{O}_L$ y $\sigma(\mathfrak{r})\mathcal{O}_L$ se factorizan de la misma manera en ideales primos en $\mathcal{O}_L$, y la única posibilidad es

$$p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_6.$$

La figura 4.1 demuestra las factorizaciones en $\mathcal{O}_F$, $\mathcal{O}_K$ y $\mathcal{O}_K$. Los primeros primos $p \equiv 1 \pmod 3$ tales que 19 es un cubo mód p son

$$p = 97, 109, 127, 151, 181, 271, 277, 283, 307, 313, \ldots$$ ▲

Note que en el último ejemplo la factorización de p no depende del resto de p módulo algún N, sino de una condición misteriosa «19 es un cubo módulo p». Para las extensiones abelianas (con el grupo $\mathrm{Gal}(K/\mathbb{Q})$ abeliano), el comportamiento de primos sí depende del resto de p módulo algún N. La razón detrás de este fenómeno es el teorema de Kronecker–Weber.

4.3 Descomposición e inercia

Clase 17
12/10/20

El último ejemplo con la descomposición de primos en $\mathbb{Q}(\sqrt[3]{19})$ sugiere que es útil considerar extensiones de campos de números $L/K/\mathbb{Q}$. Vamos a resumir brevemente qué sucede en este caso. Dado un ideal primo $\mathfrak{p} \subset \mathcal{O}_K$, tenemos su factorización en ideales primos $\mathfrak{q} \subset \mathcal{O}_L$

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}.$$

Pongamos

$$f(\mathfrak{q}|\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})].$$

Se cumple entonces

$$\sum_{\mathfrak{q}\mid\mathfrak{p}} e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}) = [L : K].$$

Ahora si $\mathfrak{p} \mid p$ para un primo racional p, entonces se cumple

$$f(\mathfrak{q}|p) = f(\mathfrak{q}|\mathfrak{p}) \cdot f(\mathfrak{p}|p), \quad e(\mathfrak{q}|p) = e(\mathfrak{q}|\mathfrak{p}) \cdot e(\mathfrak{p}|p).$$

$$\begin{array}{ccccc}
\mathfrak{q} & \subset & \mathcal{O}_L & \twoheadrightarrow & \kappa(\mathfrak{q}) \\
\big| & & \big| & & \big| f(\mathfrak{q}|\mathfrak{p}) \\
\mathfrak{p} & \subset & \mathcal{O}_K & \twoheadrightarrow & \kappa(\mathfrak{p}) \\
\big| & & \big| & & \big| f(\mathfrak{p}|p) \\
(p) & \subset & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_p
\end{array} \qquad f(\mathfrak{q}|p)$$

p	$p\mathcal{O}_F$	$p\mathcal{O}_K$	$p\mathcal{O}_L$	$p\,(3)$	p	$p\mathcal{O}_F$	$p\mathcal{O}_K$	$p\mathcal{O}_L$	$p\,(3)$
2	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	127	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1
3	$\mathfrak{r}^2$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$\mathfrak{q}_1^2\mathfrak{q}_2^2\mathfrak{q}_3^2$	0	131	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
5	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	137	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
7	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	139	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
11	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	149	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
13	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	151	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1
17	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	157	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
19	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}^3$	$\mathfrak{q}_1^3\mathfrak{q}_2^3$	1	163	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
23	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	167	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
29	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	173	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
31	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	179	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
37	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	181	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1
41	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	191	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
43	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	193	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
47	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	197	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
53	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	199	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
59	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	211	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
61	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	223	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
67	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	227	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
71	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	229	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
73	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	233	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
79	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	239	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
83	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	241	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1
89	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	251	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
97	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1	257	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
101	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	263	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
103	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	1	269	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2
107	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	271	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1
109	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1	277	$\mathfrak{r}_1\mathfrak{r}_2$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$	1
113	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2	281	$\mathfrak{r}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$	2

Figura 4.1: Factorización de primos racionales en $F = \mathbb{Q}(\zeta_3)$, $K = \mathbb{Q}(\sqrt[3]{19})$ y $L = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$

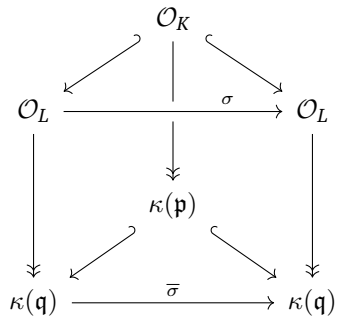
Si L/K es una extensión de Galois, el grupo $\mathrm{Gal}(L/K)$ induce una acción sobre $\mathcal{O}_L$, y luego para todo primo $\mathfrak{p} \subset \mathcal{O}_K$ una acción transitiva sobre los primos $\mathfrak{q} \mid \mathfrak{p}$ en $\mathcal{O}_L$. De la transitividad de esta acción se deduce que los números $f(\mathfrak{q}|\mathfrak{p})$ y $e(\mathfrak{q}|\mathfrak{p})$ coinciden para todo $\mathfrak{q} \mid \mathfrak{p}$, y entonces si $g_\mathfrak{p}$ es el número de ideales primos en $\mathcal{O}_L$ que están sobre $\mathfrak{p}$, se cumple

$$e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p})\, g_\mathfrak{p} = [L : K].$$

4.3.1. Definición. En la situación de arriba, para $\mathfrak{q} \mid \mathfrak{p}$ el **grupo de descomposición** es el estabilizador de $\mathfrak{q}$ respecto a la acción de $\mathrm{Gal}(L/K)$ sobre los primos sobre $\mathfrak{p}$:

$$D(\mathfrak{q}|\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

El grupo de descomposición tiene el siguiente significado: todo elemento $\sigma \in D(\mathfrak{q}|\mathfrak{p})$ induce un automorfismo $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$.



De esta manera se obtiene un homomorfismo de grupos

$$D(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})), \quad \sigma \mapsto \overline{\sigma}.$$

4.3.2. Definición. Para un primo $\mathfrak{q} \mid \mathfrak{p}$ el **grupo de inercia** viene dado por

$$I(\mathfrak{q}|\mathfrak{p}) = \ker\Big(D(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))\Big) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \text{para todo } \alpha \in \mathcal{O}_L\}.$$

(Note que $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ implica que $\sigma(\mathfrak{q}) = \mathfrak{q}$, así que $\sigma \in D(\mathfrak{q}|\mathfrak{p})$.)

4.3.3. Definición. Para los grupos $D = D(\mathfrak{q}|\mathfrak{p})$ e $I = I(\mathfrak{q}|\mathfrak{p})$ los campos fijos correspondientes L^D y L^I se llaman los **campos de descomposición e inercia** respectivamente.

Notamos que para $\sigma \in \mathrm{Gal}(L/K)$ se tiene

$$D(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, D(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}, \quad I(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, I(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}.$$

Esto implica que el campo de descomposición e inercia, salvo isomorfismo, depende solo de $\mathfrak{p}$.

En general, dado un subgrupo $H \subseteq \mathrm{Gal}(L/K)$, consideremos el subcampo fijo $K \subseteq L^H \subseteq L$ y el anillo

$$(\mathcal{O}_L)^H = L^H \cap \mathcal{O}_L.$$

Para un primo $\mathfrak{q} \subset \mathcal{O}_L$ consideremos el primo correspondiente en $(\mathcal{O}_K)^H$:

$$\mathfrak{q}^H = \mathfrak{q} \cap (\mathcal{O}_L)^H.$$

Tenemos entonces la siguiente situación para $\mathfrak{q} \mid \mathfrak{p}$:

$$\begin{array}{ccccc}
\mathfrak{q} & \subset & \mathcal{O}_L & \twoheadrightarrow & \kappa(\mathfrak{q}) \\
| & & | & & | \\
\mathfrak{q}^H & \subset & (\mathcal{O}_L)^H & \twoheadrightarrow & \kappa(\mathfrak{q}^H) \\
| & & | & & | \\
\mathfrak{p} & \subset & \mathcal{O}_K & \twoheadrightarrow & \kappa(\mathfrak{p})
\end{array}$$

4.3.4. Teorema. *Para una extensión de Galois de campos de números L/K, sean $\mathfrak{p} \subset \mathcal{O}_K$ y $\mathfrak{q} \subset \mathcal{O}_K$ primos tales que $\mathfrak{q} \mid \mathfrak{p}$ y $D = D(\mathfrak{q}|\mathfrak{p})$ e $I = I(\mathfrak{q}|\mathfrak{p})$ los grupos de descomposición e inercia correspondientes. Denotemos por $g_\mathfrak{p}$ el número de primos en $\mathcal{O}_L$ sobre $\mathfrak{p}$.*

1) Tenemos los siguientes grados de extensiones e índices de ramificación.

$$\begin{array}{lll}
L & \mathfrak{q} & e(\mathfrak{q}|\mathfrak{q}^I) = e(\mathfrak{q}|\mathfrak{p}) \qquad f(\mathfrak{q}|\mathfrak{q}^I) = 1 \\
\Big| e(\mathfrak{q}|\mathfrak{p}) & \Big| & \\
L^I & \mathfrak{q}^I & e(\mathfrak{q}^I|\mathfrak{q}^D) = 1 \qquad f(\mathfrak{q}^I|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p}) \\
\Big| f(\mathfrak{q}|\mathfrak{p}) & \Big| & \\
L^D & \mathfrak{q}^D & e(\mathfrak{q}^D|\mathfrak{p}) = 1 \qquad f(\mathfrak{q}^D|\mathfrak{p}) = 1 \\
\Big| g_\mathfrak{p} & \Big| & \\
K & \mathfrak{p} &
\end{array}$$

2) Se tiene $[G : D] = g_\mathfrak{p}$ e $|I| = e(\mathfrak{q}|\mathfrak{p})$.

3) Tenemos una sucesión exacta corta de grupos

$$1 \to I(\mathfrak{q}|\mathfrak{p}) \to D(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \to 1$$

En particular, si $\mathfrak{p}$ no se ramifica en L, entonces $I = 1$ y se tiene un isomorfismo

$$D(\mathfrak{q}|\mathfrak{p}) \cong \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})), \quad \sigma \mapsto \overline{\sigma}.$$

Demostración. Denotemos $G = \mathrm{Gal}(L/K)$.

- Primero vamos a probar que $[L^D : K] = g_\mathfrak{p}$. Por la teoría de Galois, se tiene $[L^D : K] = [G : D]$. Recordemos el teorema de órbitas y estabilizadores: si G actúa sobre un conjunto X, entonces para $x \in X$ hay una biyección entre la órbita Gx y las clases laterales del estabilizador G/G_x. En nuestro caso la acción es transitiva, así que $[G : D] = g_\mathfrak{p}$.
- Ahora veremos que $e(\mathfrak{q}^D|\mathfrak{p}) = f(\mathfrak{q}^D|\mathfrak{p}) = 1$. La acción de $\mathrm{Gal}(L/L^D)$ sobre los primos sobre $\mathfrak{q}^D$ es transitiva, pero $\mathrm{Gal}(L/L^D) \cong D$ deja $\mathfrak{q}$ fijo, así que podemos concluir que $\mathfrak{q}$ es el único primo que está sobre $\mathfrak{q}^D$. Como consecuencia, tenemos
$$[L : L^D] = e(\mathfrak{q}|\mathfrak{q}^D) f(\mathfrak{q}|\mathfrak{q}^D).$$
Ahora
$$[L : K] = e(\mathfrak{q}|\mathfrak{p}) f(\mathfrak{q}|\mathfrak{p}) g_\mathfrak{p}$$
junto con $[L^D : K] = g_\mathfrak{p}$ nos da
$$e(\mathfrak{q}|\mathfrak{q}^D) = e(\mathfrak{q}|\mathfrak{p}), \quad f(\mathfrak{q}|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p}),$$
y luego
$$e(\mathfrak{q}^D|\mathfrak{p}) = f(\mathfrak{q}^D|\mathfrak{p}) = 1.$$

- Vamos a ver que $f(\mathfrak{q}|\mathfrak{q}^I) = 1$. Esto equivale a probar que el grupo $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{q}^I))$ es trivial.

  Para $\alpha \in \mathcal{O}_K$ consideremos el polinomio

  $$f(x) = \prod_{\sigma \in I}(x - \sigma(\alpha)).$$

  Se ve que los coeficientes de $f(x)$ están en $(\mathcal{O}_L)^I$. Reduciendo módulo $\mathfrak{q}$, se obtiene un polinomio $\bar{f}(x) \in \kappa(\mathfrak{q})[x]$, y como acabamos de ver, sus coeficientes están en $\kappa(\mathfrak{q}^I)$.

  Para un elemento $\overline{\alpha} \in \kappa(\mathfrak{q})$, dado que $\sigma(\alpha) \equiv \overline{\alpha} \pmod{\mathfrak{q}}$ para todo $\sigma \in I$, tenemos $\bar{f}(x) = (x - \overline{\alpha})^n$, donde $n = |I|$, y el polinomio $\bar{f}(x)$ tiene coeficientes en $\kappa(\mathfrak{q}^I)$. Esto implica que cualquier automorfismo de $\kappa(\mathfrak{q})/\kappa(\mathfrak{q}^I)$ debe mandar $\overline{\alpha}$ a otra raíz de $\bar{f}(x)$, pero la única raíz de $\bar{f}(x)$ es $\overline{\alpha}$. Entonces, $\kappa(\mathfrak{q})/\kappa(\mathfrak{q}^I)$ no tiene automorfismos no triviales.

- De $f(\mathfrak{q}^D|\mathfrak{p}) = 1$ y $f(\mathfrak{q}|\mathfrak{q}^I) = 1$ se sigue que $f(\mathfrak{q}^I|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p})$.

- Tenemos $[L^I : L^D] = [D : I]$. Por una parte, $[L^I : L^D] \geq f(\mathfrak{q}^I|\mathfrak{q}^D) = f(\mathfrak{q}|\mathfrak{p})$. Además, tenemos una sucesión exacta

  $$1 \to I(\mathfrak{q}|\mathfrak{p}) \to D(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})),$$

  de donde $[D : I] \leq |\mathrm{Gal}(\mathfrak{q}/\mathfrak{p})| = f(\mathfrak{q}|\mathfrak{p})$. Entonces, podemos concluir que $[L^I : L^D] = [D : I] = f(\mathfrak{q}|\mathfrak{p})$, y además que el último homomorfismo en la sucesión exacta es sobreyectivo.

  Esto también implica que $e(\mathfrak{q}^I|\mathfrak{q}^D) = 1$.

- De lo que hemos calculado se sigue que $[L : L^I] = e(\mathfrak{q}|\mathfrak{p})$ y $e(\mathfrak{q}|\mathfrak{q}^I) = e(\mathfrak{q}|\mathfrak{p})$. ■

El resultado que acabamos de probar explica los términos «campo de descomposición» y «campo de inercia».

4.3.5. Corolario. *Si $D = D(\mathfrak{q}|\mathfrak{p})$ es un subgrupo normal en $G = \mathrm{Gal}(K/\mathbb{Q})$, entonces $\mathfrak{p}$ se descompone en $g_\mathfrak{p}$ diferentes primos en L^D. Además, si $I = I(\mathfrak{q}|\mathfrak{p})$ es también un subgrupo normal en G, entonces cada uno de esos primos es también primo en L^I (es decir, inerte). En fin, estos primos se ramifican en L, volviendo $e = e(\mathfrak{q}|\mathfrak{p})$-ésimas potencias.*

Demostración. Si $D \subseteq G$ es un subgrupo normal, entonces L^D/K es una extensión de Galois. En este caso todos los primos en L_D que están sobre $\mathfrak{p}$ tendrán $e = 1$ y $f = 1$, así que la factorización tiene forma $\mathfrak{p}\,(\mathcal{O}_L)^D = \mathfrak{p}'_1 \cdots \mathfrak{p}'_g$.

De la misma manera, si $I \subseteq G$ es un subgrupo normal, entonces L^I/K es una extensión de Galois y los índices de ramificación serán $e = 1$ y los grados de campos residual $f = f(\mathfrak{q}|\mathfrak{p})$, y habrá g primos. La factorización tiene forma $\mathfrak{p}\,(\mathcal{O}_L)^I = \mathfrak{p}''_1 \cdots \mathfrak{p}''_g$, lo que significa precisamente que los primos $\mathfrak{p}'_i$ son inertes en L^I. ■

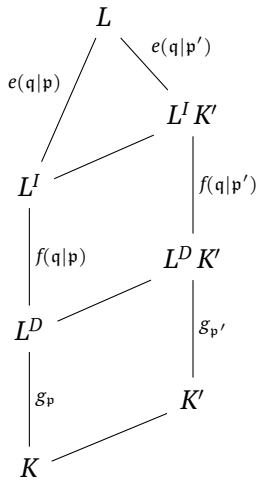
Los cálculos de 4.3.4 de hecho caracterizan el campo de descomposición e inercia. Usando la misma notación, consideremos un subcampo $K \subseteq K' \subseteq L$ y un primo $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_{K'}$. Tenemos $K' = L^H$ para algún subgrupo $H \subseteq \mathrm{Gal}(L/K)$, y la extensión L/K' es Galois. Notamos que $\mathfrak{p}' \mid \mathfrak{p}$. De las definiciones del grupo de descomposición e inercia se ve que

$$D(\mathfrak{q}|\mathfrak{p}') = D \cap H, \quad I(\mathfrak{q}|\mathfrak{p}') = I \cap H,$$

y los campos de descomposición e inercia correspondientes son los compositums

$$L^{D(\mathfrak{q}|\mathfrak{p}')} = L^D K', \quad L^{I(\mathfrak{q}|\mathfrak{p}')} = L^I K'.$$

El teorema 4.3.4 nos da el siguiente diagrama de extensiones



Añadí este resultado después

4.3.6. Proposición. *En la situación de 4.3.4, consideremos un subcampo $K \subseteq K' \subseteq L$. El campo de descomposición L^D e inercia L^I se caracterizan por las siguientes propiedades.*

a) L^D es el K' más grande tal que $e(\mathfrak{p}'|\mathfrak{p}) = f(\mathfrak{p}'|\mathfrak{p}) = 1$.

b) L^D es el K' más pequeño tal que $g_{\mathfrak{p}'} = 1$ (es decir, $\mathfrak{q}$ es el único primo en $\mathcal{O}_L$ tal que $\mathfrak{q} \mid \mathfrak{p}'$).

c) L^I es el K' más grande tal que $e(\mathfrak{p}'|\mathfrak{p}) = 1$.

d) L^I es el K' más pequeño tal que $e(\mathfrak{q}|\mathfrak{p}') = [L : K']$.

Demostración. Primero observamos que 4.3.4 nos dice que L^D y L^I cumplen las propiedades deseadas.

En a), si tenemos $e(\mathfrak{p}'|\mathfrak{p}) = f(\mathfrak{p}'|\mathfrak{p}) = 1$, entonces del diagrama de arriba se deduce que

$$[L : L^D K'] = e(\mathfrak{q}|\mathfrak{p}')\, f(\mathfrak{q}|\mathfrak{p}') = e(\mathfrak{q}|\mathfrak{p}')\, e(\mathfrak{p}'|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}')\, f(\mathfrak{p}'|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p})\, f(\mathfrak{q}|\mathfrak{p}) = [L : L^D].$$

Entonces, $L^D K' = L^D$, y por lo tanto $K' \subseteq L^D$.

En b), si $g_{\mathfrak{p}'} = [L^D K' : K'] = 1$, entonces $L^D K' = K'$, y por ende $L^D \subseteq K'$.

En c), si $e(\mathfrak{p}'|\mathfrak{p}) = 1$, entonces de la misma manera calculamos

$$[L : L^I K'] = e(\mathfrak{q}|\mathfrak{p}') = e(\mathfrak{q}|\mathfrak{p}')\, e(\mathfrak{p}'|\mathfrak{p}) = e(\mathfrak{q}|\mathfrak{p}) = [L : L^I],$$

y entonces $K' \subseteq L^I$.

En fin, en d), si $e(\mathfrak{q}|\mathfrak{p}') = [L : K']$, entonces del diagrama se ve que $L^I K' = K'$, y luego $L^I \subseteq K'$. ∎

4.3.7. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_{28})$. El primo $p = 2$ se ramifica. Tenemos

$$\Phi_{28} \equiv (x^3 + x + 1)^2\,(x^3 + x^2 + 1)^2 \pmod 2,$$

lo que nos da la factorización $p\mathcal{O}_K = \mathfrak{p}_1^2\,\mathfrak{p}_2^2$, donde $f_1 = f_2 = 3$, y

$$\mathfrak{p}_1 = (2, 1 + \zeta_{28} + \zeta_{28}^3), \quad \mathfrak{p}_2 = (2, 1 + \zeta_{28}^2 + \zeta_{28}^3).$$

Escribiendo $K = \mathbb{Q}(i, \zeta_7)$, se ve que $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times$. Como los generadores, podemos tomar

$$\sigma : i \mapsto -i,\ \zeta_7 \mapsto \zeta_7$$

de orden 2 y

$$\tau : i \mapsto i,\ \zeta_7 \mapsto \zeta_7^3$$

de orden 6. En términos de la raíz ζ_{28}, tenemos $\sigma\colon \zeta_{28} \mapsto \zeta_{28}^{15}$ y $\tau\colon \zeta_{28} \mapsto \zeta_{28}^{17}$. Calculamos que

$$\sigma(\mathfrak{p}_1) = \mathfrak{p}_1, \quad \tau(\mathfrak{p}_1) = \mathfrak{p}_2, \quad \sigma(\mathfrak{p}_2) = \mathfrak{p}_2, \quad \tau(\mathfrak{p}_2) = \mathfrak{p}_1.$$

De aquí se ve que el grupo de descomposición viene dado por $D(\mathfrak{p}_1|p) = \langle \sigma, \tau^2 \rangle$. Aquí σ y τ^2 inducen algunos automorfismos del campo finito

$$\mathbb{Z}[\zeta_{28}]/\mathfrak{p}_1 \cong \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_8.$$

Podemos notar, por ejemplo, que σ actúa de manera trivial, dado que $|\mathbb{F}_8^\times| = 7$ y $15 \equiv 1 \pmod 7$, y entonces $\overline{\sigma}\colon \overline{\zeta_{28}} \mapsto \overline{\zeta_{28}}$. Por otra parte, la acción de $\overline{\tau^2}$ no es trivial y viene dada por $\overline{\zeta_{28}} \mapsto \overline{\zeta_{28}}^2$. (En efecto, $17^2 \equiv 3^2 \equiv 2 \pmod 7$.) De estas consideraciones se sigue que $I(\mathfrak{p}_1|p) = \langle \sigma \rangle$.

Ahora el campo de inercia será $K^\sigma = \mathbb{Q}(\zeta_7)$, y el campo de descomposición es $K^{\langle \sigma, \tau^2 \rangle} = \mathbb{Q}(\sqrt{-7})$.

$$\begin{array}{c} \mathbb{Q}(\zeta_{28}) \\ \Big| e{=}2 \\ \mathbb{Q}(\zeta_7) \\ \Big| f{=}3 \\ \mathbb{Q}(\sqrt{-7}) \\ \Big| g{=}2 \\ \mathbb{Q} \end{array}$$

La factorización de $p = 2$ en $\mathbb{Q}(\sqrt{-7})$ toma forma $\mathfrak{r}_1\,\mathfrak{r}_2$, y la factorización en $\mathbb{Q}(\zeta_7)$ toma forma $\mathfrak{r}_1'\,\mathfrak{r}_2'$, donde $f_1 = f_2 = 3$: factorizando el polinomio ciclotómico correspondiente,

$$\Phi_7 \equiv (x^3 + x + 1)\,(x^3 + x^2 + 1) \pmod 2.$$

Ahora podemos considerar un primo no ramificado, por ejemplo $p = 3$. Tenemos entonces

$$\Phi_{28} \equiv (x^6 + x^5 + x^3 + x + 1)\,(x^6 - x^5 - x^3 - x + 1) \pmod 3,$$

lo que nos da factorización $p\mathcal{O}_K = \mathfrak{p}_1\,\mathfrak{p}_2$, donde

$$\mathfrak{p}_1 = (3, \zeta_{28}^6 + \zeta_{28}^5 + \zeta_{28}^3 + \zeta_{28} + 1), \quad \mathfrak{p}_2 = (3, \zeta_{28}^6 - \zeta_{28}^5 - \zeta_{28}^3 + \zeta_{28} + 1),$$

y $f_1 = f_2 = 3$. Podemos calcular el grupo de descomposición:

$$\sigma(\mathfrak{p}_1) = \mathfrak{p}_2, \quad \tau(\mathfrak{p}_1) = \mathfrak{p}_1, \quad \sigma(\mathfrak{p}_2) = \mathfrak{p}_1, \quad \tau(\mathfrak{p}_2) = \mathfrak{p}_1.$$

Se ve que $\sigma\tau$ y $\tau^2 = (\sigma\tau)^2$ están en el grupo de descomposición, y este será generado por

$$\sigma\tau\colon \zeta_{28} \mapsto \zeta_{28}^{15\cdot 17} = \zeta_{28}^3.$$

Al reducir $\sigma\tau$ módulo $\mathfrak{p}_1$, se obtiene el automorfismo de Frobenius $x \mapsto x^3$ sobre $\kappa(\mathfrak{p}_1) \cong \mathbb{F}_{3^3}$, y tenemos un isomorfismo

$$D(\mathfrak{p}_1|p) = \langle \sigma\tau \rangle \cong \mathrm{Gal}(\kappa(\mathfrak{p}_1)/\mathbb{F}_p).$$

El grupo de inercia $I(\mathfrak{p}_1|p)$ será trivial, y esto sucede precisamente porque $p = 3$ no se ramifica. ▲

4.3.1 Reciprocidad cuadrática

Como una aplicación de la teoría anterior, podemos dar otra prueba más de la ley de reciprocidad cuadrática. Dado un primo impar p, consideremos el campo ciclotómico $L = \mathbb{Q}(\zeta_p)$ y el subcampo cuadrático $K = \mathbb{Q}(\sqrt{p^*})$, donde $p^* = (-1)^{\frac{p-1}{2}} p$ (véase ejercicio 2.19). Primero notamos el siguiente resultado.

4.3.8. Lema. *Un primo impar $q \neq p$ se escinde en K si y solamente si q se factoriza en L en un número par de ideales primos.*

Demostración. Si q se escinde en K, entonces $q\mathcal{O}_K = \mathfrak{q}\,\sigma(\mathfrak{q})$ para algún $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{Gal}(L/\mathbb{Q})$. Luego, σ induce una biyección entre los primos $\mathfrak{Q} \subset \mathcal{O}_L$ tales que $\mathfrak{Q} \mid \mathfrak{q}$ y los primos $\mathfrak{Q} \mid \sigma(\mathfrak{q})$. Como consecuencia, el número $\#\{\mathfrak{Q} \mid q\} = 2 \cdot \#\{\mathfrak{Q} \mid \mathfrak{q}\}$ es par.

Viceversa, supongamos que el número g de primos $\mathfrak{Q} \subset \mathcal{O}_L$ tales que $\mathfrak{Q} \mid q$ es par. Para el grupo de descomposición $D = D(\mathfrak{Q}|q)$ se cumple $[\mathrm{Gal}(L/\mathbb{Q}) : D] = g$. El grupo $G = \mathrm{Gal}(L/\mathbb{Q})$ es cíclico de orden $p-1$. Para subgrupo H tal que $[G : H]$ se tiene $L^H = K$, pero luego, puesto que $[G : D]$ es par, se cumple $D \subset H$, y entonces $K \subset L^D$. Ahora $f(\mathfrak{Q}^D|q) = 1$, y luego $f(\mathfrak{Q} \cap K|q) = 1$. Esto significa que q se escinde en K. ■

Ahora sabemos que q se escinde en $K = \mathbb{Q}(\sqrt{p^*})$ si y solamente si $\left(\frac{p^*}{q}\right) = 1$.

Por otra parte, el número de ideales primos en $\mathcal{O}_L = \mathbb{Z}[\zeta_p]$ sobre q es igual a $g = \frac{p-1}{f}$, donde f es el orden de q módulo p (véase 2.7.11 y 3.10.6). Notamos que este número es par si y solamente si $f \mid \frac{p-1}{2}$; es decir, si y solamente si $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Recodando la congruencia de Euler $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$, estas consideraciones demuestran que

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

4.4 El Frobenius

Clase 18
14/10/20

> ...the Galois group $\mathrm{Gal}(L/K)$ contains an essential element called Frobenius substitution. This element <...> governs over the decomposition of $\mathfrak{p}$ in L: We might even claim that it has "the soul of $\mathfrak{p}$". It glimmers like a firefiy in $\mathrm{Gal}(L/K)$ for each and every prime ideal.
>
> [KKS2011, p. 18]

Como antes, consideremos una extensión de Galois de campos de números L/K y primos $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \subset \mathcal{O}_L$ tales que $\mathfrak{q} \mid \mathfrak{p}$. En este caso si $\mathfrak{p}$ no se ramifica en L, el grupo de inercia es trivial y tenemos un isomorfismo

$$D(\mathfrak{q}|\mathfrak{p}) \cong \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})), \quad \sigma \mapsto \overline{\sigma}.$$

El grupo $\mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ es cíclico, generado por el automorfismo de Frobenius $x \mapsto x^{\#\kappa(\mathfrak{p})}$. Gracias al isomorfismo de arriba, podemos considerar el elemento correspondiente en el grupo de descomposición.

4.4.1. Definición. En la situación de arriba, el elemento $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in D(\mathfrak{q}|\mathfrak{p})$ que se reduce mód $\mathfrak{q}$ a $x \mapsto x^{\#\kappa(\mathfrak{p})}$ se llama el **automorfismo de Frobenius**[*], o simplemente **el Frobenius**.

4.4.2. Comentario. Hagamos algunas observaciones básicas.

[*] Ferdinand Georg Frobenius (1849–1917), matemático alemán.

1) En otras palabras, $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ es el único elemento de $\mathrm{Gal}(L/K)$ que cumple

$$\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}(\alpha) \equiv \alpha^{\#\kappa(\mathfrak{p})} \pmod{\mathfrak{q}} \qquad (*)$$

para todo $\alpha \in \mathcal{O}_L$. (Esta condición implica que $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in D(\mathfrak{q}|\mathfrak{p})$.)

2) Al pasar de $\mathfrak{q} \mid \mathfrak{p}$ a otro primo $\sigma(\mathfrak{q}) \mid \mathfrak{p}$ se obtiene

$$\mathrm{Frob}_{\sigma(\mathfrak{q})|\mathfrak{p}} = \sigma \circ \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \circ \sigma^{-1}$$

(ejercicio para el lector). Entonces, la clase de conjugación del Frobenius depende solo de $\mathfrak{p}$.

3) En particular, para una extensión abeliana L/K, el Frobenius depende solo de $\mathfrak{p}$, y podemos denotarlo por $\mathrm{Frob}_{\mathfrak{p}}$. En este caso la condición (*) se cumple para todo $\mathfrak{q} \mid \mathfrak{p}$, y ocupando el teorema chino del resto (y que $e(\mathfrak{q}|\mathfrak{p}) = 1$ por nuestra hipótesis), podemos concluir que el Frobenius está definido por la condición

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^{\#\kappa(\mathfrak{p})} \pmod{\mathfrak{p}\mathcal{O}_L}.$$

4.4.3. Ejemplo. Consideremos un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$. Si p es un primo no ramificado, entonces hay dos posibilidades:

- p se escinde en dos ideales en K, y luego $D(\mathfrak{p}|p) = 1$, y Frob_p es el automorfismo trivial;
- p es inerte en K, y luego $D(\mathfrak{p}|p) = \mathrm{Gal}(K/\mathbb{Q})$, y $\mathrm{Frob}_p \colon \sqrt{d} \mapsto -\sqrt{d}$ es el automorfismo no trivial.

Para p impar tal que $p \nmid d$, podemos escribir entonces $\mathrm{Frob}_p \colon \sqrt{d} \mapsto \left(\frac{d}{p}\right)\sqrt{d}$. ▲

4.4.4. Ejemplo. Consideremos un campo ciclotómico $K = \mathbb{Q}(\zeta_n)$. Los primos $p \nmid n$ no se ramifican en K. En este caso $\mathrm{Frob}_p \colon \zeta_n \mapsto \zeta_n^p$. En efecto, para un elemento $\alpha \in \mathcal{O}_K = \mathbb{Z}[\zeta_n] = \sum_i a_i \zeta_n^i$, donde $a_i \in \mathbb{Z}$, calculamos que

$$\alpha^p \equiv \sum_i a_i^p \zeta_n^p \equiv \sum_i a_i \zeta_n^p \pmod{p}.$$ ▲

El orden de $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ es igual a $f(\mathfrak{q}|\mathfrak{p})$, y entonces determina el tipo de descomposición de $\mathfrak{p}$ en L: tenemos $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_g$, donde f es el orden de $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ y $g = [L : K]/f$. En particular, $\mathfrak{p}$ se descompone en $[L : K]$ ideales primos si y solamente si $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} = 1$. En este caso se dice que $\mathfrak{p}$ **se escinde completamente** en L.

El siguiente resultado forma una parte importante de la teoría de campos de clases y se conoce como el **teorema de densidad de Chebotarëv**. Solo para simplificar el enunciado, vamos a formular la versión para extensiones $K/\mathbb{Q}$ en lugar del caso general L/K[*].

4.4.5. Teorema. *Para una extensión de Galois $K/\mathbb{Q}$, sea C una clase de conjugación en el grupo $G = \mathrm{Gal}(K/\mathbb{Q})$. El conjunto de primos racionales $X = \{p \mid \mathrm{Frob}_p \in C\}$ tiene densidad $d(X) = \#C/\#G$.*

En particular, el teorema nos dice que salvo conjugación, cualquier elemento del grupo de Galois puede ser realizado como Frob_p para un número infinito de p.

Para más detalles (matemáticos e históricos), recomiendo el artículo [SL1996]. Para la definición de densidad $d(X)$, véase el apéndice D. El teorema es cierto para la densidad de Dirichlet (analítica) y también para la densidad natural[**].

4.4.6. Corolario. *Hay un número infinito de primos racionales p que se escinden completamente en K, y su densidad es igual a $1/\#G$.*

[*] Para las extensiones L/K hay que definir la noción de densidad para ideales primos en $\mathcal{O}_K$ que está relacionada con la **función zeta de Dedekind** $\zeta_K(s)$ de la misma manera que la densidad de primos racionales está relacionada con la función zeta de Riemann $\zeta(s)$.

[**] Véase https://mathoverflow.net/questions/302390/

4.4.7. Ejemplo. Para una extensión ciclotómica $K = \mathbb{Q}(\zeta_n)$ y un primo $p \nmid n$, el Frobenius Frob_p está determinado por el resto de p módulo n. En este caso el teorema de densidad de Chebotarëv se reduce al teorema de Dirichlet sobre los primos en progresiones aritméticas (véase el apéndice D). Se puede pensar en el teorema de Chebotarëv como una generalización del teorema de Dirichlet. ▲

4.4.8. Ejemplo. Consideremos el campo $K = \mathbb{Q}(\sqrt[3]{19}, \zeta_3)$. El grupo de Galois es isomorfo a S_3, donde hay tres clases de conjugación:

$$C = \{1\}, \quad C' = \{(1\ 2), (1\ 3), (2\ 3)\}, \quad C'' = \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

El teorema de Chebotarëv nos dice lo siguiente.

- Los primos con $\mathrm{Frob}_p \in C$ corresponden a las factorizaciones de la forma $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_6$. Su densidad es $\frac{1}{6}$. Estos son los primos $p \equiv 1 \pmod 3$ tales que 19 es un cubo mód p.
- Los primos con $\mathrm{Frob}_p \in C'$ corresponden a las factorizaciones de la forma $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_2$. Su densidad es $\frac{1}{2}$. Estos son los primos tales que $p \equiv 2 \pmod 3$.
- Los primos con $\mathrm{Frob}_p \in C''$ corresponden a las factorizaciones de la forma $\mathfrak{p}_1\mathfrak{p}_2$. Su densidad es $\frac{1}{3}$. Estos son los primos $p \equiv 1 \pmod 3$ tales que 19 no es un cubo mód p.

La densidad de los primos $p \equiv 2 \pmod 3$ viene dada por el teorema de Dirichlet sobre primos en progresiones aritméticas. Sin embargo, para $p \equiv 1 \pmod 3$ la condición «19 es un cubo mód p» es más sofisticada y no está claro por qué la densidad correspondiente debe ser $\frac{1}{6}$.

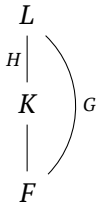
He aquí alguna estadística calculada con PARI/GP. En la primera columna está el número de primos y en la segunda la fracción de primos que cumplen la condición de que $p \equiv 1 \pmod 3$ y 19 es un cubo mód p.

$$\begin{aligned}
10^2&: 0{,}140000000\\
10^3&: 0{,}160000000\\
10^4&: 0{,}163500000\\
10^5&: 0{,}166410000\\
10^6&: 0{,}166575000\\
10^7&: 0{,}166609100\\
10^8&: 0{,}166655150\\
10^9&: 0{,}166663355
\end{aligned}$$ ▲

Notamos que el Frobenius contiene más información que el tipo de descomposición de $\mathfrak{p}$: dos elementos $\sigma, \tau \in \mathrm{Gal}(L/K)$ pueden tener el mismo orden pero estar en diferentes clases de conjugación. (Por ejemplo, en el grupo alternante A_4 los 3-ciclos $(1\ 2\ 3)$ y $(1\ 2\ 4)$ no son conjugados.)

4.5 Caso de extensiones no Galois

Aunque el Frobenius fue definido para extensiones de Galois L/K, en general es posible tomar la cerradura de Galois y determinar el tipo de descomposición mediante el Frobenius. Consideremos una torre de campos de números



donde L/F es una extensión de Galois con $\mathrm{Gal}(L/F) = G$ y $K = L^H$. Para un primo $\mathfrak{p} \subset \mathcal{O}_F$ que no se ramifica en L, sea $\mathfrak{Q} \subset \mathcal{O}_L$ un primo tal que $\mathfrak{Q} \mid \mathfrak{p}$. El grupo de descomposición $D(\mathfrak{Q}|\mathfrak{p})$ actúa sobre las clases laterales $H\sigma$ mediante la multiplicación por la derecha. Puesto que $D(\mathfrak{Q} \mid \mathfrak{p})$ está generado por el Frobenius $F = \mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}}$, las órbitas de esta acción vienen dadas por

$$\{H\sigma_1, H\sigma_1 F, H\sigma_1 F^2, \ldots, H\sigma_1 F^{n_1-1}\},$$
$$\ldots$$
$$\{H\sigma_s, H\sigma_s F, H\sigma_s F^2, \ldots, H\sigma_s F^{n_s-1}\},$$

donde n_i es el mínimo número tal que $H\sigma_i F^{n_i} = H\sigma_i$. Lo que tenemos es una partición de las clases laterales, así que $\sum_i n_i = [G : H] = [K : F]$.

4.5.1. Teorema. *En la situación de arriba se tiene* $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_s$*, donde* $\mathfrak{q}_i = \sigma_i(\mathfrak{Q}) \cap \mathcal{O}_K$ *y* $f(\mathfrak{q}_i|\mathfrak{p}) = n_i$*.*

Demostración. Está claro que $\mathfrak{q}_i \mid \mathfrak{p}$. Primero vamos a probar que $\mathfrak{q}_i \neq \mathfrak{q}_j$ para $i \neq j$. Supongamos que $\mathfrak{q}_i = \mathfrak{q}_j$. En este caso $\sigma_i(\mathfrak{Q})$ y $\sigma_j(\mathfrak{Q})$ son primos en $\mathcal{O}_L$ sobre el mismo primo en $\mathcal{O}_K$, y luego por la transitividad de la acción de Galois sobre ideales primos, existe $\sigma \in H$ tal que $\sigma_j(\mathfrak{Q}) = \tau\sigma_i(\mathfrak{Q})$. Luego tenemos $\sigma_j^{-1}\tau\sigma_i \in D(\mathfrak{Q}|\mathfrak{p})$. El grupo de descomposición es cíclico, generado por F, así que $\sigma_j^{-1}\tau\sigma_i = F^k$ para algún k. Esto implica que $H\sigma_i = H\sigma_j F^k$ están en la misma órbita, pero luego $i = j$.

Falta ver que los $\mathfrak{q}_i$ son todos los primos en $\mathcal{O}_K$ tales que $\mathfrak{q}_i \mid \mathfrak{p}$. Notamos que

$$\sum_i n_i = \sum_{\mathfrak{q}|\mathfrak{p}} f(\mathfrak{q}|\mathfrak{p}) = [K : F],$$

así que bastaría probar que para todo i se tiene $f(\mathfrak{q}_i|\mathfrak{p}) \geq n_i$. Estamos en la siguiente situación:

$$\begin{array}{ccc} \mathcal{O}_L & \twoheadrightarrow & \kappa(\sigma_i(\mathfrak{Q})) \\ \big| & & \big| \\ \mathcal{O}_K & \twoheadrightarrow & \kappa(\mathfrak{q}_i) \\ \big| & & \big| \\ \mathcal{O}_F & \twoheadrightarrow & \kappa(\mathfrak{p}) \end{array}$$

y se ve que (¡ejercicio!)

$$\mathrm{Frob}_{\sigma_i(\mathfrak{Q})|\mathfrak{q}_i} = (\mathrm{Frob}_{\sigma_i(\mathfrak{Q})|\mathfrak{p}})^{f(\mathfrak{q}_i|\mathfrak{p})} = (\sigma_i F \sigma_i^{-1})^{f(\mathfrak{q}_i|\mathfrak{p})} = \sigma_i F^{f(\mathfrak{q}_i|\mathfrak{p})} \sigma_i^{-1}.$$

Ahora $\mathrm{Frob}_{\sigma_i(\mathfrak{Q})|\mathfrak{q}_i} \in H$, y entonces $\sigma_i F^{f(\mathfrak{q}_i|\mathfrak{p})} \sigma_i^{-1} \in H$. Esto implica que $H\sigma_i = H\sigma_i F^{f(\mathfrak{q}_i|\mathfrak{p})}$, de donde $f(\mathfrak{q}_i|\mathfrak{p}) \geq n_i$. ■

Como mencionamos, el teorema de Kronecker–Weber nos dice que para toda extensión $K/\mathbb{Q}$ con el grupo $\mathrm{Gal}(K/\mathbb{Q})$ abeliano existe n tal que $K \subseteq \mathbb{Q}(\zeta_n)$. Entonces, la descomposición de primos en K depende solamente del resto de p módulo n. El caso de extensiones no abelianas es mucho más complicado.

4.5.2. Ejemplo. Consideremos el campo de números $K = \mathbb{Q}(\sqrt[4]{2})$. La extensión $K/\mathbb{Q}$ no es normal, y podemos pasar a la cerradura de Galois $L = \mathbb{Q}(\sqrt[4]{2}, i)$. Dejo al lector comprobar que el grupo de Galois de $L/\mathbb{Q}$ está generado por los automorfismos $\sigma\colon \sqrt[4]{2} \mapsto i\sqrt[4]{2}$ de orden 4 y $\tau\colon i \mapsto -i$ de orden 2. Se cumple $\sigma\tau = \tau\sigma^3 \neq \tau\sigma$. El grupo de Galois es isomorfo al grupo diédrico D_4 (también conocido como D_8):

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}.$$

Tenemos $K = L^{\langle\tau\rangle}$, y las clases laterales de $H = \langle\tau\rangle$ en G son

$$H, H\sigma, H\sigma^2, H\sigma^3.$$

En este caso el único primo que se ramifica en L es $p = 2$. (¡Ejercicio!) Par p impar sea $\mathfrak{p} \subset \mathcal{O}_L$ un primo tal que $\mathfrak{p} \mid p$, y consideremos el Frobenius correspondiente $F = \mathrm{Frob}_{\mathfrak{p}|p}$. Supongamos por ejemplo que $F = \tau$. En este caso calculamos que $HF = H$, $H\sigma F = H\sigma^3$, y $H\sigma^2 F = H\sigma^2$. Esto nos da tres órbitas

$$\{H\}, \quad \{H\sigma, H\sigma^3\}, \quad \{H\sigma^2\}.$$

Entonces, el teorema nos dice que $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, donde $f_1 = f_2 = 1$ y $f_3 = 2$.

Un ejercicio instructivo sería determinar el tipo de factorización para el resto de posibilidades para el Frobenius F. ▲

Con esto terminamos nuestra breve investigación de la teoría de Galois para los campos de números.

Ejercicios

Ejercicio 4.1. Para un campo cuadrático $\mathbb{Q}(\sqrt{d})$ encuentre n tal que $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$.

Ejercicio 4.2. Describa los subcampos de $\mathbb{Q}(\sqrt[4]{2}, i)$.

Ejercicio 4.3. Demuestre que para una extensión de Galois L/K, primos $\mathfrak{q} \subset \mathcal{O}_L$, $\mathfrak{p} \subset \mathcal{O}_K$, tales que $\mathfrak{q} \mid \mathfrak{p}$, y $\sigma \in \mathrm{Gal}(L/K)$ se tiene

$$D(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, D(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}, \quad I(\sigma(\mathfrak{q})|\mathfrak{p}) = \sigma\, I(\mathfrak{q}|\mathfrak{p})\, \sigma^{-1}.$$

Además, si $\mathfrak{p}$ no se ramifica, entonces el Frobenius cumple

$$\mathrm{Frob}_{\sigma(\mathfrak{q})|\mathfrak{p}} = \sigma\ \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}\ \sigma^{-1}.$$

Ejercicio 4.4. Sea F un campo de números, y $L/K/F$ una torre de extensiones tal que L/K es una extensión normal. Sean $\mathfrak{p} \subset \mathcal{O}_F$, $\mathfrak{q} \in \mathcal{O}_K$, $\mathfrak{Q} \subset \mathcal{O}_L$ ideales primos tales que $\mathfrak{Q} \mid \mathfrak{q}$ y $\mathfrak{q} \mid \mathfrak{p}$.

1) Demuestre que la restricción de automorfismos identifica $D(\mathfrak{Q}|\mathfrak{q})$ con un subgrupo de $D(\mathfrak{Q}|\mathfrak{p})$ e $I(\mathfrak{Q}|\mathfrak{q})$ con un subgrupo de $I(\mathfrak{Q}|\mathfrak{p})$.

2) Si $\mathfrak{p}$ no se ramifica en L, demuestre que

$$\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{q}} = (\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}})^{f(\mathfrak{q}|\mathfrak{p})}.$$

3) Si la extensión K/F es normal, demuestre que $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ es la restricción de $\mathrm{Frob}_{\mathfrak{Q}|\mathfrak{p}}$.

Ejercicio 4.5. Sea K el campo de descomposición del polinomio $f = x^4 + 8x + 12$. Calcule $\mathrm{Gal}(K/\mathbb{Q})$, las clases de conjugación, los tipos de descomposición que corresponden a cada $\mathrm{Frob}_{\mathfrak{p}|p}$, y las densidades que nos da el teorema de Chebotarëv.

Ejercicio 4.6. Para $K = \mathbb{Q}(\sqrt[4]{2})$ consideremos la cerradura de Galois $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

1) Demuestre que el único primo racional p que se ramifica en L es $p = 2$.

2) Para p impar sea $\mathfrak{p} \subset \mathcal{O}_L$ un primo tal que $\mathfrak{p} \mid p$. Determine cómo el tipo de factorización de p en $\mathcal{O}_K$ para toda posibilidad para $\mathrm{Frob}_{\mathfrak{p}|p}$.

Ejercicio 4.7. Para la extensión ciclotómica $L = \mathbb{Q}(\zeta_n)$ determine cómo los primos no ramificados $p \nmid n$ se descomponen en el subcampo $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Capítulo 5

Teoría de Minkowski

Clase 19
19/10/20

El objetivo de este capítulo es probar los siguientes teoremas.

1) Para una extensión no trivial $K/\mathbb{Q}$ se tiene $|\Delta_K| > 1$.
2) **Teorema de Hermite**: para C fijo, existe un número finito de campos de números $K/\mathbb{Q}$, salvo isomorfismo, con discriminante $|\Delta_K| < C$.
3) Dado un campo de números $K/\mathbb{Q}$, el grupo de clases $\mathrm{Cl}(K) = \mathrm{Pic}(\mathcal{O}_K)$ es finito.
   Este resultado es bastante sutil y no se sigue del álgebra conmutativa: si en lugar de $\mathcal{O}_K$ se toma otro dominio de Dedekind R, el grupo $\mathrm{Pic}(R)$ ya no tiene por qué ser finito.
4) **Teorema de unidades de Dirichlet**: el grupo $\mathcal{O}_K^\times$ es finitamente generado de rango $r_1 + r_2 - 1$, donde r_1 es el número de encajes reales $K \hookrightarrow \mathbb{R}$ y $2r_2$ es el número de encajes complejos $K \hookrightarrow \mathbb{C}$. En otras palabras, existen unidades $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1} \in \mathcal{O}_K^\times$, llamadas **unidades fundamentales**, tales que
   $$\mathcal{O}_K^\times \cong \mu_K \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_{r_1+r_2-1} \rangle.$$
   Aquí μ_K es el subgrupo de torsión que consiste en las raíces de unidad en K, mientras que ϵ_i son generadores de diferentes componentes cíclicas infinitas.

La herramienta principal en las pruebas será el teorema de Minkowski sobre puntos de retículos en conjuntos convexos simétricos. El término clásico para los resultados de Minkowski es «geometría de números» (*Geometrie der Zahlen*), pero hoy en día el punto de vista geométrico a la teoría de números está contenido más bien en la teoría de esquemas (véase por ejemplo [EH2000] y [GW2010]). Por esto un nombre más adecuado para este capítulo sería «teoría de Minkowski».

5.1 Retículos y el teorema de Minkowski

5.1.1. Definición. Sea V un espacio vectorial real. Un **retículo**[*] en V es un subgrupo aditivo $\Lambda \subset V$ de la forma
$$\Lambda = \mathbb{Z}\,\omega_1 + \cdots + \mathbb{Z}\,\omega_n,$$
donde $\omega_1, \ldots, \omega_n \in V$ son vectores linealmente independientes. En este caso se dice que $\omega_1, \ldots, \omega_n$ es una **base** de Λ. Si $n = \dim_{\mathbb{R}} V$, se dice que Λ **tiene rango completo** en V. El conjunto
$$\Pi = \Big\{ \sum_i \lambda_i\,\omega_i \;\Big|\; 0 \le \lambda_i < 1 \Big\}$$
se llama un **dominio fundamental** de Λ.

[*] *lattice* en inglés; no confundir con los retículos que estudian lógicos y «algebristas universales».

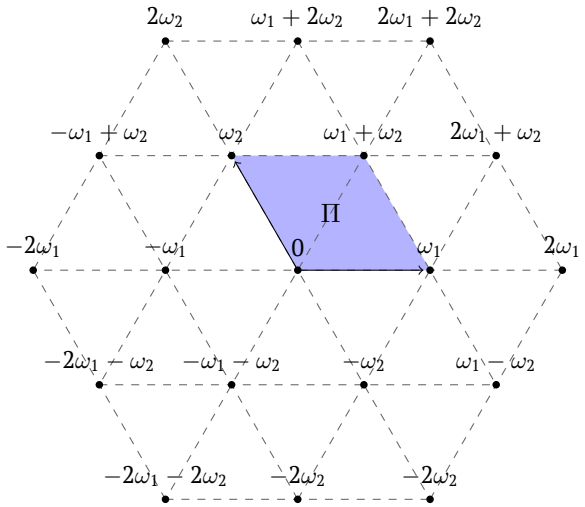
5.1.2. Comentario. Si Λ tiene rango completo, entonces V puede ser recubierto por el dominio fundamental Π trasladado por los elementos de Λ:

$$V = \bigsqcup_{\omega\in\Lambda} \Pi + \omega.$$

Esta unión es disjunta. El dominio fundamental se identifica con el cociente V/Λ.

5.1.3. Comentario. Vamos a considerar V como un espacio vectorial topológico, dotado de la topología real estándar. Para las aplicaciones que nos interesan, se puede pensar que $V = \mathbb{R}^n$.

5.1.4. Ejemplo. Consideremos los enteros de Eisenstein $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$. Identificando $\mathbb{C}$ con $\mathbb{R}^2$ de la manera habitual, podemos ver $\mathbb{Z}[\zeta_3]$ como un retículo generado por los vectores $\omega_1 = (1,0)$ y $\omega_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.



▲

5.1.5. Ejemplo. El subgrupo $\Lambda = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot\sqrt{2}$ no es un retículo en $\mathbb{R}$: los vectores 1 y $\sqrt{2}$ no son linealmente independientes. ▲

5.1.6. Lema. *Un retículo $\Lambda \subset V$ tiene rango completo si y solamente si existe un conjunto acotado $X \subseteq V$ tal que*

$$V = \bigcup_{\omega\in\Lambda} X + \omega. \qquad (*)$$

Demostración. Si $\Lambda = \mathbb{Z}\,\omega_1 + \cdots + \mathbb{Z}\,\omega_n$ tiene rango completo, entonces podemos tomar como X el dominio fundamental Π.

Viceversa, si existe un conjunto acotado X tal que se cumple (*), denotemos por V_0 el subespacio vectorial generado por los elementos de Λ. Nos gustaría ver que $V_0 = V$. Para todo $v \in V$ y $k \in \mathbb{N}$ podemos escribir $kv = x_k + \omega_k$ para algunos $x_k \in X$ y $\omega_k \in \Lambda$. Puesto que X es acotado,

$$\lim_{k\to\infty} \frac{1}{k}\, x_k = 0.$$

Ahora tenemos

$$v = \lim_{k\to\infty} \frac{1}{k}\, \omega_k \in V_0,$$

usando que V_0 es un subespacio cerrado de V. ■

Aunque nuestra definición de retículos menciona explícitamente una $\mathbb{Z}$-base de Λ, hay otra caracterización más canónica.

5.1.7. Lema. *Un subgrupo aditivo $\Lambda \subset V$ es un retículo si y solamente si Λ es discreto.*

Recordemos que $\Lambda \subset V$ es un subespacio **discreto** si para todo $\omega \in \Lambda$ existe un entorno abierto $U \ni \omega$ en V tal que $\Lambda \cap U = \{\omega\}$.

5.1.8. Ejemplo. Para $\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{2}$, usando la irracionalidad de $\sqrt{2}$, se puede ver que para cualquier $\epsilon > 0$ existe un número infinito de $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ tales que $|a + b\sqrt{2}| < \epsilon$. ▲

Demostración. Primero, si $\Lambda = \mathbb{Z}\,\omega_1 + \cdots + \mathbb{Z}\,\omega_n$ es un retículo en V, entonces para todo punto $\omega = \sum_i a_i\,\omega_i \in \Lambda$ podemos tomar el entorno abierto

$$U = \Big\{ \sum_i \lambda_i\,\omega_i \;\Big|\; |a_i - \lambda_i| < 1 \Big\},$$

y se cumple $\Lambda \cap U = \{\omega\}$.

Viceversa, supongamos que $\Lambda \subset V$ es un subgrupo discreto. En general, si G es un grupo topológico de Hausdorff, entonces cualquier subgrupo discreto $H \subset G$ es cerrado. En nuestro caso particular, Λ será cerrado. Sea V_0 el subespacio de V generado por los elementos de Λ. Podemos entonces escoger una base de V_0 que consiste en elementos $\omega_1, \ldots, \omega_n \in \Lambda$. Esta base nos da un subretículo

$$\Lambda_0 = \mathbb{Z}\,\omega_1 + \cdots + \mathbb{Z}\,\omega_n \subseteq \Lambda.$$

Dado que Λ_0 tiene rango completo en V_0, tenemos

$$V_0 = \bigcup_{\omega \in \Lambda_0} \Pi_0 + \omega,$$

donde Π_0 es el dominio fundamental que corresponde a la base $\omega_1, \ldots, \omega_n$. Vamos a probar que el cociente Λ/Λ_0 es finito. Sean $\omega_i \in \Lambda$ representantes de diferentes elementos en Λ/Λ_0. Escribamos

$$\omega_i = x_i + \omega_{0i},$$

donde $x_i \in \Pi_0$ y $\omega_{0i} \in \Lambda_0$. Aquí $x_i = \omega_i - \omega_{0i} \in \Lambda \cap \Pi_0$. El espacio $\Lambda \cap \Pi_0$ es discreto y acotado, así que es finito. Se sigue que el cociente Λ/Λ_0 es finito. Ahora

$$\Lambda_0 \subseteq \Lambda \subseteq \frac{1}{[\Lambda : \Lambda_0]}\,\Lambda_0,$$

y Λ es también un grupo abeliano de rango n, así que admite una $\mathbb{Z}$-base finita $\omega_1', \ldots, \omega_n'$. Estos vectores son linealmente independientes sobre $\mathbb{R}$ porque generan el espacio V_0 de dimensión n. ■

Ahora supongamos que V tiene estructura de espacio euclidiano; es decir, viene con una forma bilineal definida positiva

$$\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{R}.$$

5.1.9. Definición. Para un retículo $\Lambda = \mathbb{Z}\,\omega_1 + \cdots + \mathbb{Z}\,\omega_n$ el **covolumen** viene dado por

$$\operatorname{covol}(\Lambda) = \operatorname{vol}(\Pi) = |\det(\langle \omega_i, \omega_j \rangle)|^{1/2}.$$

Notamos que el covolumen no depende de una base particular: para otra base $\omega_1', \ldots, \omega_n'$ la matriz de cambio de base tiene determinante ± 1 (recuerde también nuestra discusión del discriminante en el capítulo 3).

5.1.10. Definición. Sea $X \subseteq V$ un subconjunto.

- Se dice que X es **simétrico** (respecto al origen) si para todo $x \in X$ se tiene $-x \in X$.

- Se dice que X es **convexo** si para cualesquiera $x, y \in X$ la recta entre x e y también está en X:

$$\{\lambda y + (1-\lambda)x \mid 0 \leq \lambda \leq 1\} \subseteq X.$$

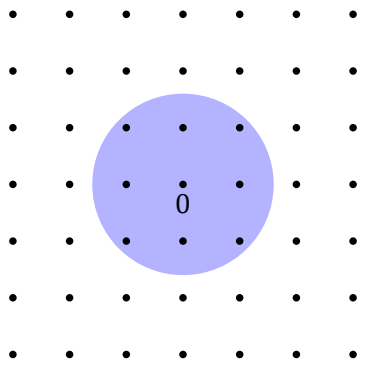
Todo conjunto convexo simétrico no vacío $X \subseteq V$ necesariamente contiene el punto 0. Ahora dado un retículo $\Lambda \subset V$, si X es suficientemente grande, entonces X contiene otro punto de Λ a parte de 0. Este es el contenido del siguiente teorema.

5.1.11. Teorema (Minkowski[*]). *Sean $\Lambda \subset V$ un retículo de rango completo y $X \subseteq V$ un conjunto convexo simétrico tal que*

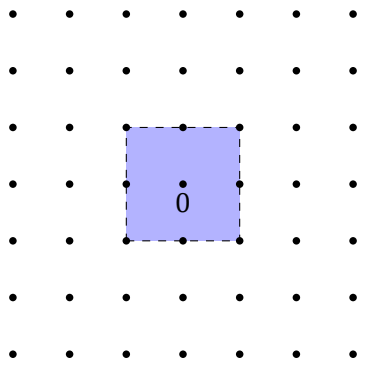
$$\operatorname{vol} X > 2^n \operatorname{covol} \Lambda.$$

Entonces, X contiene un punto no nulo de Λ.

En algún sentido, este resultado es una versión continua del principio del palomar.



5.1.12. Comentario. Para entender el significado del múltiplo 2^n en la cota del teorema, podemos considerar el hipercubo abierto con 2^n vértices en $(\pm 1, \pm 1, \ldots, \pm 1)$. Consideremos el retículo $\Lambda = \mathbb{Z}^n \subset \mathbb{R}^n$. El volumen del cubo es $2^n = \operatorname{covol} \Lambda$, pero el cubo no contiene ningún punto de Λ salvo 0.



Dejo como un ejercicio probar que si X es compacto, entonces también funcionaría $\operatorname{vol}(X) = 2^n \operatorname{covol} \Lambda$.

Para demostrar el teorema, necesitamos el siguiente resultado auxiliar.

5.1.13. Lema (Blichfeldt[**]). *Dado un conjunto medible $X \subset V$ tal que $\operatorname{vol} X > \operatorname{covol} \Lambda$, existen dos diferentes puntos $x, x' \in X$ tales que $x - x' \in \Lambda$.*

[*] Hermann Minkowski (1864–1909)
[**] Hans Frederick Blichfeldt (1873–1945), matemático danés.

Demostración. Puesto que

$$V = \bigsqcup_{\omega\in\Lambda} \Pi + \omega,$$

tenemos

$$X = \bigsqcup_{\omega\in\Lambda} X \cap (\Pi + \omega),$$

así que

$$\operatorname{vol} X = \sum_{\omega\in\Lambda} \operatorname{vol}(X \cap (\Pi + \omega)) = \sum_{\omega\in\Lambda} \operatorname{vol}((X - \omega) \cap \Pi).$$

Aquí los conjuntos $(X - \omega) \cap \Pi$ están en el dominio fundamental Π, y por nuestra hipótesis $\operatorname{vol} X > \operatorname{vol} \Pi$, así que podemos deducir que existen $\omega, \omega' \in \Lambda$ tales que

$$(X - \omega) \cap (X - \omega') \neq \varnothing.$$

Tomando $y \in (X - \omega) \cap (X - \omega')$, se obtiene

$$x = y + \omega, \quad x' = y + \omega' \in X, \quad x - x' = \omega - \omega' \in \Lambda. \qquad \blacksquare$$

Notamos que en realidad el lema no usa la covexidad de X y se aplica a cualquier conjunto medible, pero en particular, los conjuntos convexos son medibles.

Ahora estamos listos para demostrar el teorema de Minkowski, y aquí será importante la hipótesis de que X es convexo y simétrico. Consideremos el conjunto

$$\frac{1}{2} X = \left\{ \frac{1}{2} x \;\middle|\; x \in X \right\}.$$

Tenemos

$$\operatorname{vol}\left(\frac{1}{2} X\right) = \frac{1}{2^n} \operatorname{vol} X > \operatorname{covol} \Lambda,$$

así que por el lema de Blichfeldt existen dos puntos distintos $x, x' \in \frac{1}{2} X$ tales que $x - x' \in \Lambda$. Para terminar la demostración, sería suficiente ver que este punto pertenece a X. Por la hipótesis que X es simétrico, $-x' \in \frac{1}{2} X$, y luego

$$x = \frac{1}{2} y, \quad -x' = \frac{1}{2} y' \quad \text{para algunos } y, y' \in X.$$

El punto

$$x - x' = \frac{1}{2} y + \frac{1}{2} y'$$

pertenece a X, siendo una combinación convexa de dos puntos $y, y' \in X$. $\blacksquare$

Notamos que el argumento no es constructivo y no nos da una manera eficaz de obtener un punto no nulo en $X \cap \Lambda$.

5.2 Aplicación: teorema de cuatro cuadrados

Prácticamente todo este capítulo será dedicado a varias aplicaciones del teorema de Minkowski, pero primero sería instructivo ver algún ejemplo más sencillo de su uso. En esta sección vamos a probar el siguiente famoso resultado, conocido como el **teorema de cuatro cuadrados**.

5.2.1. Teorema (Lagrange). *Para todo entero $n \geq 0$ existen $a, b, c, d \in \mathbb{Z}$ tales que $n = a^2 + b^2 + c^2 + d^2$.*

Primero, gracias a la identidad

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

descubierta por Euler, notamos que es suficiente probar el teorema para el caso cuando $n=p$ es un número primo.

5.2.2. Comentario. He aquí una breve explicación. La identidad para las sumas de dos cuadrados

$$(a^2+b^2)(x^2+y^2)=(ax-by)^2+(ay+bx)^2$$

se sigue de la fórmula $N(\alpha\beta)=N(\alpha)N(\beta)$ para la norma $N(\alpha)=\alpha\overline{\alpha}$ sobre los enteros de Gauss $\mathbb{Z}[i]$.

De la misma manera, podemos considerar el **álgebra de cuaterniones** con coeficientes en $\mathbb{Z}$:

$$\mathbb{H}(\mathbb{Z})=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{Z}\},$$

donde la multiplicación está definida por

$$i^2=j^2=k^2=-1,$$
$$ij=k,\ ji=-k,$$
$$jk=i,\ kj=-i,$$
$$ki=j,\ ik=-j.$$

De manera más concreta, tenemos una representación fiel del álgebra de cuaterniones $\mathbb{H}(\mathbb{Z})$ por las matrices $M_2(\mathbb{Z}[i])$ dada por

$$(a+bi+cj+dk)\mapsto\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}.$$

Podemos definir el conjugado de $\alpha=a+bi+cj+dk$ mediante

$$\overline{\alpha}=a-bi-cj-dk.$$

La norma se define como

$$N(\alpha)=\alpha\overline{\alpha}=a^2+b^2+c^2+d^2,$$

o en términos de matrices,

$$\det\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}=a^2+b^2+c^2+d^2.$$

La norma es multiplicativa: $N(\alpha\beta)=N(\alpha)N(\beta)$.

5.2.3. Lema. *Para todo primo p existen $m,n\in\mathbb{Z}$ tales que*

$$m^2+n^2+1\equiv 0 \pmod{p}.$$

Demostración. Ejercicio. ■

Fijemos entonces m y n como arriba y consideremos los siguientes vectores en $V=\mathbb{R}^4$:

$$\omega_1=(1,0,m,n),\quad \omega_2=(0,1,n,-m),\quad \omega_3=(0,0,p,0),\quad \omega_4=(0,0,0,p).$$

Consideremos el producto escalar estándar sobre $\mathbb{R}^4$, y para un vector $v=\sum_i a_i e_i$ pongamos $\|v\|^2=\langle v,v\rangle=\sum_i a_i^2$. Calculando el determinante correspondiente, es fácil verificar que los ω_i generan un retículo de rango completo

$$\Lambda=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2+\mathbb{Z}\omega_3+\mathbb{Z}\omega_4\subset\mathbb{R}^4,$$

tal que

$$\operatorname{covol}\Lambda=p^2.$$

5.2.4. Lema. *Para todo $\omega \in \Lambda$ el número $\|\omega\|^2$ es un entero divisible por p.*

Demostración. Si

$$\omega = a_1\,\omega_1 + a_2\,\omega_2 + a_3\,\omega_3 + a_4\,\omega_4 = (a_1,\ a_2,\ a_1\,m + a_2\,n + a_3\,p,\ a_1\,n - a_2\,m + a_4\,p),$$

entonces

$$\begin{aligned}\|\omega\|^2 = a_1^2 + a_2^2 + (a_1\,m + a_2\,n + a_3\,p)^2 + (a_1\,n - a_2\,m + a_4\,p)^2 \\ \equiv a_1^2 + a_2^2 + (a_1\,m + a_2\,n)^2 + (a_1\,n - a_2\,m)^2 \pmod{p}.\end{aligned}$$

Luego,

$$a_1^2 + a_2^2 + (a_1\,m + a_2\,n)^2 + (a_1\,n - a_2\,m)^2 = (a_1^2 + a_2^2)\,(m^2 + n^2 + 1)$$

y $m^2 + n^2 + 1 \equiv 0 \pmod{p}$ por nuestra elección de m y n. ■

Sea X la bola abierta en $\mathbb{R}^4$ de radio $r = \sqrt{2p}$ centrada en el origen:

$$X = \{x \in \mathbb{R}^4 \mid \|x\|^2 < 2p\}.$$

Recordemos que en general la bola n-dimensional de radio r tiene volumen

$$\frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}\,r^n.$$

En este caso $n = 4$ y $\Gamma\left(\frac{n}{2}+1\right) = \Gamma(3) = 2! = 2$. Tenemos

$$\operatorname{vol} X = \frac{\pi^2 r^4}{2} = 2\pi^2 p^2 > 2^4 \operatorname{covol}\Lambda = 16\,p^2$$

(de hecho, $2\pi^2 = 19{,}73\ldots > 16$). Entonces, según el teorema de Minkowski, existe un punto no nulo $\omega \in \Lambda$ tal que $\omega \in X$. Ahora de

$$0 < \|\omega\|^2 < 2p, \quad p \mid \|\omega\|^2$$

podemos concluir que $\|\omega\|^2 = p$. Esto nos da una representación de p como una suma de cuatro cuadrados. ■

Cabe mencionar que la representación de números enteros por sumas de cuadrados es un problema clásico relacionado con mucha teoría de números profunda. Véase por ejemplo el libro [Gro1985].

5.3 Aplicación: teorema de aproximación de Dirichlet

Lectura adicional

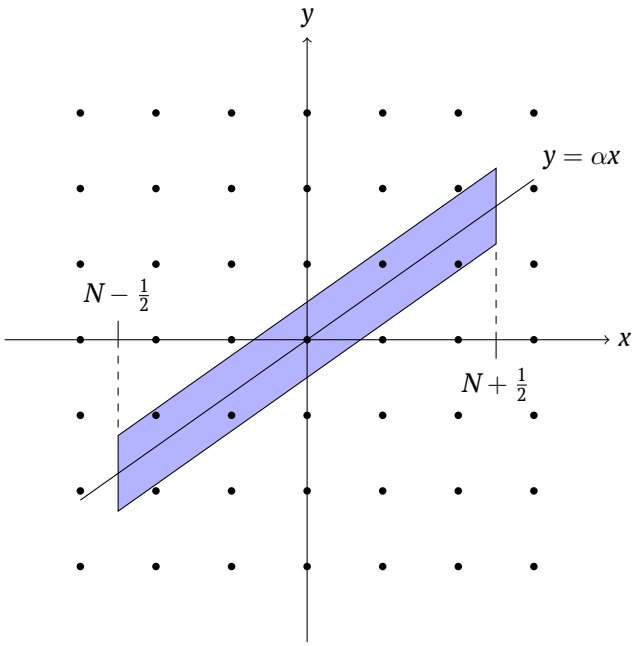
El siguiente famoso teorema de Dirichlet es el primer resultado en la **aproximación diofántica**.

5.3.1. Teorema. *Dados números reales α y $N \geq 1$, existen $p, q \in \mathbb{Z}$ tales que $1 \leq q \leq N$ y*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

Demostración. Consideremos el conjunto convexo simétrico

$$X = \left\{(x,y) \in \mathbb{R}^2 \;\middle|\; |x| \leq N + \frac{1}{2},\ |\alpha x - y| < \frac{1}{N}\right\}.$$



Este es un paralelogramo de área $(2N+1)\frac{2}{N} > 4$, y el teorema de Minkowski implica que existe un punto no nulo $(q,p) \in \mathbb{Z}^2$ tal que $(q,p) \in X$. Por la simetría, podemos asumir que $q \geq 1$. Tenemos entonces

$$1 \leq q \leq N, \quad |q\alpha - p| < \frac{1}{N}.$$

■

5.3.2. Corolario. *Para α irracional existe un número infinito de fracciones $\frac{p}{q}$ tales que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Demostración. Primero, el teorema de Dirichlet nos da una aproximación

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

Notamos que siempre podemos asumir que $\text{mcd}(p,q) = 1$. Escojamos

$$N' > \frac{1}{\left|\alpha - \frac{p}{q}\right|}$$

y tomamos otra aproximación

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q'N'} = \frac{\left|\alpha - \frac{p}{q}\right|}{q'} \leq \left|\alpha - \frac{p}{q}\right|.$$

Aquí necesariamente $\frac{p}{q} \neq \frac{p'}{q'}$, y continuando de esta manera se obtienen diferentes $\frac{p_i}{q_i}$, donde

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \cdots < \left|\alpha - \frac{p_1}{q_1}\right|$$

y $\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}$. ■

5.3.3. Ejemplo. Para $\alpha = \sqrt{2}$ las fracciones

$$\frac{p_n}{q_n} = \frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \ldots$$

cumplen la condición del corolario:

$\frac{p_n}{q_n}$:	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{7}{5}$	$\frac{17}{12}$	$\frac{41}{29}$	$\frac{99}{70}$
$\lvert\alpha - p_n/q_n\rvert$:	0,414213	0,085786	0,014213	0,002453	0,000420	0,000072
$1/q_n^2$:	1,000000	0,250000	0,040000	0,006944	0,001189	0,000204

▲

Las aproximaciones de 5.3.2 pueden ser obtenidas mediante las **fracciones continuas** para α. Vamos a revisarlas más adelante porque estas tendrán una relación con el grupo de unidades $\mathcal{O}_K^\times$ para $K = \mathbb{Q}(\sqrt{d})$ campo cuadrático real.

Para mayor información sobre la aproximación diofántica, véase por ejemplo [Sch1980].

5.4 Anillo de enteros como un retículo

Clase 20
21/10/20

Sea $K/\mathbb{Q}$ un campo de números. Este tiene $n = [K : \mathbb{Q}]$ encajes $\tau\colon K \hookrightarrow \mathbb{C}$, entre estos r_1 encajes reales $\rho\colon K \hookrightarrow \mathbb{R}$ y $2r_2$ encajes complejos $\sigma\colon K \hookrightarrow \mathbb{C}$ tales que $\overline{\sigma} \neq \sigma$. Consideremos el espacio complejo n-dimensional

$$K_{\mathbb{C}} = \prod_{\tau} \mathbb{C}$$

y el encaje correspondiente

$$\Phi\colon K \hookrightarrow K_{\mathbb{C}}, \quad \alpha \mapsto (\tau(\alpha))_\tau.$$

Vamos a dotar el espacio $K_{\mathbb{C}}$ del producto hermitiano habitual

$$\langle z, z' \rangle = \sum_{\tau} z_\tau \overline{z'_\tau}.$$

En particular, notamos que $\langle z', z\rangle = \overline{\langle z, z'\rangle}$ y $\langle z, z\rangle > 0$ para $z \neq 0$.

El grupo $G_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ actúa sobre $K_{\mathbb{C}}$ mediante la conjugación compleja y permutación de las coordenadas $\tau \mapsto \overline{\tau}$. Esto nos da un automorfismo $\mathbb{R}$-lineal de orden 2

$$F\colon K_{\mathbb{C}} \to K_{\mathbb{C}}, \quad (z_\tau)_\tau \mapsto (\overline{z}_{\overline{\tau}})_\tau.$$

Consideremos el subespacio real fijo por la acción de $G_{\mathbb{R}}$:

$$K_{\mathbb{R}} = (K_{\mathbb{C}})^{G_{\mathbb{R}}} = \{(z_\tau)_\tau \mid z_{\overline{\tau}} = \overline{z}_\tau\}.$$

Dado que $\langle Fz, Fz'\rangle = \overline{\langle z, z'\rangle}$, el producto hermitiano sobre $K_{\mathbb{C}}$ se restringe a un producto escalar

$$\langle \cdot, \cdot \rangle\colon K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}.$$

Efectivamente, para todo $x, y \in K_{\mathbb{R}}$ se tiene

$$\begin{gathered}\langle x, y\rangle = \langle Fx, Fy\rangle = \overline{\langle x, y\rangle},\\ \langle y, x\rangle = \overline{\langle x, y\rangle} = \langle x, y\rangle,\\ \langle x, x\rangle > 0 \text{ si } x \neq 0.\end{gathered}$$

Notamos que por la definición, para $\alpha \in K$ se tiene $\overline{\tau}(\alpha) = \overline{\tau(\alpha)}$, y entonces el encaje $\Phi\colon K \hookrightarrow K_{\mathbb{C}}$ toma valores en $K_{\mathbb{R}}$:

$$\begin{array}{ccc} K & \xhookrightarrow{\Phi} & K_{\mathbb{R}} \\ & \searrow^{\Phi} & \downarrow \\ & & K_{\mathbb{C}} \end{array}$$

5.4.1. Comentario. En términos de productos tensoriales,

- $K_{\mathbb{C}} \cong K \otimes_{\mathbb{Q}} \mathbb{C}$,
- el encaje $\Phi\colon K \hookrightarrow K_{\mathbb{C}}$ se identifica con $\alpha \mapsto \alpha \otimes 1$,
- la aplicación $F\colon K_{\mathbb{C}} \to K_{\mathbb{C}}$ corresponde a $\alpha \otimes z \mapsto \alpha \otimes \bar{z}$,
- $K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$, y la inclusión $K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$ está inducida por $\mathbb{R} \subset \mathbb{C}$.

El siguiente resultado explica el significado geométrico del discriminante Δ_K.

5.4.2. Proposición. *La imagen del anillo de enteros $\Lambda = \Phi(\mathcal{O}_K) \subset K_{\mathbb{R}}$ es un retículo de rango completo tal que* $\operatorname{covol}\Lambda = \sqrt{|\Delta_K|}$.

Demostración. Si $\mathcal{O}_K = \mathbb{Z}\,\alpha_1 + \cdots + \mathbb{Z}\,\alpha_n$, entonces $\Lambda = \mathbb{Z}\,\Phi(\alpha_1) + \cdots + \mathbb{Z}\,\Phi(\alpha_n)$. Ahora si $\tau_i\colon K \hookrightarrow \mathbb{C}$ son diferentes encajes, recordemos que $\Delta_K = \det(A)^2$, donde $A = (\tau_i\alpha_j)_{i,j}$.

Por otra parte, el covolumen de Λ se calcula mediante la matriz

$$(\langle \Phi(\alpha_i), \Phi(\alpha_j)\rangle)_{i,j} = \Big(\sum_k \tau_k\alpha_i, \overline{\tau_k\alpha_j}\Big)_{i,j} = A\,\overline{A}^t.$$

Ahora

$$\operatorname{covol}\Lambda = \sqrt{|\det(A\overline{A}^t)|} = \sqrt{|\Delta_K|}. \qquad \blacksquare$$

5.4.3. Corolario. *Para todo ideal no nulo $I \subseteq \mathcal{O}_K$, la imagen correspondiente $\Lambda = \Phi(I)$ es un retículo de rango completo tal que* $\operatorname{covol}\Lambda = \sqrt{|\Delta_K|} \cdot N_{K/\mathbb{Q}}(I)$.

Demostración. Si $I \neq 0$, entonces el índice

$$N_{K/\mathbb{Q}}(I) = \#(\mathcal{O}_K/I) = [\mathcal{O}_K : I]$$

es finito, y luego $\Lambda = \Phi(I)$ es un subretículo en $\Lambda' = \Phi(\mathcal{O}_K)$ tal que $[\Lambda' : \Lambda] = N_{K/\mathbb{Q}}(I)$. Dejo como un ejercicio verificar que

$$\operatorname{covol}\Lambda = \operatorname{covol}\Lambda' \cdot [\Lambda' : \Lambda]. \qquad \blacksquare$$

El último cálculo explica el significado geométrico de la norma $N_{K/\mathbb{Q}}(I)$.

5.4.4. Ejemplo. Volvamos a los enteros de Eisenstein $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$. Hay dos encajes complejos $\sigma, \overline{\sigma}\colon \mathbb{Q}(\zeta_3) \to \mathbb{C}$ dados por $\sigma\colon \zeta_3 \mapsto \zeta_3$ y $\overline{\sigma}\colon \zeta_3 \mapsto \zeta_3^2$. En este caso particular

$$K_{\mathbb{R}} = \{(z_\sigma, z_{\overline{\sigma}}) \in K_{\mathbb{C}} \mid z_{\overline{\sigma}} = \overline{z_\sigma}\}.$$

Esto nos da un isomorfismo de espacios vectoriales

$$\phi\colon K_{\mathbb{R}} \xrightarrow{\cong} \mathbb{R}^2, \quad (z_\sigma, z_{\overline{\sigma}}) \mapsto (x_\sigma, x_{\overline{\sigma}}) = (\operatorname{Re} z_\sigma, \operatorname{Im} z_\sigma).$$

Poniendo $z_\sigma = x_\sigma + iy_\sigma$, $z'_\sigma = x'_\sigma + iy'_\sigma$, calculamos que

$$z_\sigma\,\overline{z'_\sigma} + z_{\overline{\sigma}}\,\overline{z'_{\overline{\sigma}}} = z_\sigma\,\overline{z'_\sigma} + \overline{z_\sigma}\,z'_\sigma = 2\,(x_\sigma\,x'_\sigma + y_\sigma\,y'_\sigma) = 2\,(x_\sigma\,x'_\sigma + x_{\overline{\sigma}}\,x'_{\overline{\sigma}}).$$

Entonces, el producto escalar sobre $\mathbb{R}^2$ que corresponde al producto escalar sobre $K_\mathbb{R}$ es

$$\langle x, x' \rangle = 2\,(x_\sigma\, x'_\sigma + x_{\overline{\sigma}}\, x'_{\overline{\sigma}}).$$

Tenemos el encaje

$$\Phi\colon \mathbb{Z}[\zeta_3] \hookrightarrow K_\mathbb{R} \xrightarrow{\cong} \mathbb{R}^2$$

dado por

$$1 \mapsto (1,0), \quad \zeta_3 \mapsto (\operatorname{Re}\zeta_3, \operatorname{Im}\zeta_3).$$

Ahora el volumen del retículo correspondiente será

$$\left|\det\begin{pmatrix} \langle\Phi(1),\Phi(1)\rangle & \langle\Phi(1),\Phi(\zeta_3)\rangle \\ \langle\Phi(\zeta_3),\Phi(1)\rangle & \langle\Phi(\zeta_3),\Phi(\zeta_3)\rangle \end{pmatrix}\right|^{1/2} = \left|\det\begin{pmatrix} 2 & 2\operatorname{Re}\zeta_3 \\ 2\operatorname{Re}\zeta_3 & 2\cdot|\zeta_3|^2 \end{pmatrix}\right|^{1/2} = \sqrt{4 - 4\cdot\operatorname{Re}(\zeta_3)^2} = \sqrt{3}.$$

En este caso $\Delta_K = -3$. ▲

5.5 Cota de Minkowski

5.5.1. Comentario. Para ver el espacio $K_\mathbb{R}$ de manera más explícita, sean $\rho_1, \ldots, \rho_{r_1}\colon K \hookrightarrow \mathbb{R}$ los encajes reales, y $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_{r_2}, \overline{\sigma_{r_2}}\colon K \hookrightarrow \mathbb{C}$ los encajes complejos. Entonces,

$$K_\mathbb{R} = \{(z_\tau) \in K_\mathbb{C} \mid z_\rho \in \mathbb{R},\, z_{\overline{\sigma}} = \overline{z}_\sigma\}.$$

Tenemos un isomorfismo de espacios $\mathbb{R}$-vectoriales

$$\phi\colon K_\mathbb{R} \xrightarrow{\cong} \mathbb{R}^{r_1+2r_2}, \quad (z_\tau)_\tau \mapsto (x_\tau)_\tau,$$

donde

$$x_\rho = z_\rho, \quad x_\sigma = \operatorname{Re}(z_\sigma), \quad x_{\overline{\sigma}} = \operatorname{Im}(z_\sigma).$$

Un cálculo similar al de 5.4.4 demuestra que el producto escalar correspondiente sobre $\mathbb{R}^{r_1+2r_2}$ viene dado por

$$\langle x, y \rangle = \sum_\tau n_\tau\, x_\tau\, y_\tau,$$

donde

$$n_\tau = \begin{cases} 1, & \text{si } \tau \text{ es real,} \\ 2, & \text{si } \tau \text{ es complejo.} \end{cases}$$

Este producto escalar define una medida sobre $\mathbb{R}^{r_1+2r_2}$, respecto a cual

$$\operatorname{vol}(X) = 2^{r_2}\cdot \operatorname{vol}_{Leb}(\phi(X)),$$

donde vol_{Leb} denota el volumen respecto a la medida de Lebesgue habitual sobre $\mathbb{R}^n$. A partir de ahora, cuando hablamos del volumen de un subconjunto de $K_\mathbb{R}$, vamos a entender esta medida inducida por el producto escalar.

5.5.2. Lema. *Para $t > 0$ el conjunto convexo simétrico*

$$X_t = \{(z_\tau) \in K_\mathbb{R} \mid \sum_\tau |z_\tau| \le t\}$$

tiene volumen

$$\operatorname{vol}(X_t) = 2^{r_1}\,\pi^{r_2}\,\frac{t^n}{n!}.$$

Demostración. Como vimos, tenemos $\mathrm{vol}(X_t) = 2^{r_2}\ \mathrm{vol}_{Leb}(\phi(X_t))$, y el conjunto $\phi(X_t)$ en $\mathbb{R}^{r_1+2r_2}$ con coordenadas $(x_1,\dots,x_{r_1},\ y_1,z_1,\dots,y_{r_2},z_{r_2})$ es el conjunto definido por la desigualdad

$$|x_1| + \cdots + |x_{r_1}| + 2\sqrt{y_1^2+z_1^2} + \cdots + 2\ \sqrt{y_{r_2}+z_{r_2}} \leq t.$$

Pasando a las coordenadas polares $y_i = u_i\ \cos\theta_i$, $z_i = u_i\ \mathrm{sen}\,\theta_i$, tenemos

$$\mathrm{vol}_{Leb}(\phi(X_t)) = \int u_1 \cdots u_s\, dx_1 \cdots dx_{r_1}\, du_1 \cdots du_{r_2}\, d\theta_1 \cdots d\theta_{r_2},$$

donde la integración es sobre el dominio

$$0 \leq \theta_i \leq 2\pi, \quad u_i \geq 0, \quad |x_1| + \cdots + |x_{r_1}| + 2u_1 + \cdots + 2u_{r_2} \leq t.$$

Pasando a la integral sobre $x_i \geq 0$ y $2u_i = w_i$,

$$\mathrm{vol}_{Leb}(\phi(X_t)) = 2^{r_1}\, 4^{-r_2}\, (2\pi)^{r_2}\, I_{r_1,r_2}(t),$$

donde

$$I_{r_1,r_2}(t) = \int w_1 \cdots w_{r_2}\, dx_1 \cdots dx_{r_1} dw_1 \cdots dw_{r_2},$$

y la integral es sobre

$$x_i \geq 0, \quad w_i \geq 0, \quad x_1 + \cdots + x_{r_1} + w_1 + \cdots + w_{r_2} \leq t.$$

Tenemos

$$I_{r_1,r_2}(t) = t^{r_1+2r_2}\, I_{r_1,r_2}(1) = t^n\, I_{r_1,r_2}(1).$$

Reescribiendo el dominio como

$$x_2 + \cdots + x_{r_1} + w_1 + \cdots + w_{r_2} \leq t - x_1,$$

tenemos por el teorema de Fubini

$$I_{r_1,r_2}(1) = \int_0^1 I_{r_1-1,r_2}(1-x_1)\, dx_1 = \int_0^1 (1-x_1)^{n-1}\, dx_1 \cdot I_{r_1-1,r_2}(1) = \frac{1}{n}\, I_{r_1-1,r_2}(1),$$

y entonces por inducción

$$I_{r_1,r_2} = \frac{1}{n\,(n-1)\cdots(n-r_1+1)}\, I_{0,r_2}(1).$$

De la misma manera

$$I_{0,r_2}(1) = \int_0^1 w_1\,(1-w_1)^{2r_2-2}\, dw_1\, I_{0,r_2-1}(1),$$

de donde por inducción

$$I_{0,r_2}(1) = \frac{1}{(2r_2)!}\, I_{0,0}(1) = \frac{1}{(2r_2)!}.$$

Entonces,

$$I_{r_1,r_2}(1) = \frac{1}{n!},$$

así que

$$\mathrm{vol}(X_t) = 2^{r_2} \cdot 2^{r_1}\, 4^{-r_2}\, (2\pi)^{r_2}\, I_{r_1,r_2}(t) = 2^{r_1}\, \pi^{r_2}\, \frac{t^n}{n!}.$$ ■

5.5.3. Teorema (La cota de Minkowski). *Dado un ideal no nulo $I \subseteq \mathcal{O}_K$, existe un elemento no nulo $\alpha \in I$, tal que*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N_{K/\mathbb{Q}}(I),$$

donde

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$$

es una constante que depende solamente de K, llamada la ***cota de Minkowski****.*

Demostración. Consideremos el retículo $\Lambda = \Phi(I) \subset K_{\mathbb{R}}$, y el conjunto convexo simétrico compacto $X_t \subset K_{\mathbb{R}}$ del lema anterior, escogiendo t tal que

$$\operatorname{vol}(X_t) = 2^n \operatorname{covol} \Lambda;$$

es decir,

$$2^{r_1} \pi^{r_2} \frac{t^n}{n!} = 2^n \sqrt{|\Delta_K|} \cdot N_{K/\mathbb{Q}}(I) \iff t^n = n! \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|} \cdot N_{K/\mathbb{Q}}(I).$$

En este caso $X_t \cap \Phi(I) \neq \{0\}$; es decir, existe un elemento no nulo $\alpha \in I$ tal que $\Phi(\alpha) \in X_t$. (Basta tomar la igualdad $\operatorname{vol}(X_t) = 2^n \operatorname{covol} \Lambda$ porque X_t es compacto.) Notamos que

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{\tau} |\tau(\alpha)|,$$

y tenemos la desigualdad entre la media aritmética y geométrica

$$\frac{1}{n} \sum_{\tau} |\tau(\alpha)| \geq \left(\prod_{\tau} |\tau(\alpha)|\right)^{1/n}.$$

De aquí

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{\tau} |\tau(\alpha)| \leq \frac{1}{n^n} \Big(\sum_{\tau} |\tau(\alpha)|\Big)^n \leq \frac{t^n}{n^n} = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|} \cdot N_{K/\mathbb{Q}}(I). \qquad \blacksquare$$

En particular, si en 5.5.3 tomamos $I = \mathcal{O}_K$, entonces se obtiene la desigualdad $1 \leq |N_{K/\mathbb{Q}}(\alpha)| \leq M_K$, que puede ser escrita como

$$|\Delta_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2r_2} \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n.$$

Esta es una cota inferior para el discriminante en términos del grado de la extensión $n = [K : \mathbb{Q}]$. No es difícil verificar que la función de n que está a la derecha es creciente. (¡Ejercicio!) Para $n = 1$ a la derecha está $\frac{\pi}{4}$, y para $n = 2$ tenemos $\frac{\pi^2}{4}$ que es mayor que 1, así que $|\Delta_K| > 1$ para $n > 1$. Esto establece el siguiente resultado.

5.5.4. Teorema (Minkowski). *Si $K/\mathbb{Q}$ es una extensión no trivial, entonces $|\Delta_K| > 1$. En particular, en K necesariamente se ramifican algunos primos.*

5.6 Teorema de Hermite

Ahora vamos a probar un teorema de Hermite que establece la finitud de campos de números de discriminante acotado. Empecemos por un resultado auxiliar.

5.6.1. Lema. *Para todo campo de números $K/\mathbb{Q}$ existe $\alpha \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\alpha)$, y para cualquier encaje $\tau : K \hookrightarrow \mathbb{C}$ se tiene $|\tau(\alpha)| \leq C$, donde la constante C depende solamente del discriminante Δ_K.*

Demostración. Consideremos dos casos diferentes.

1) Supongamos que K tiene un encaje real $\rho\colon K \hookrightarrow \mathbb{R}$. En este caso para $t > 1$ definamos el conjunto convexo simétrico
$$X_t = \{(x_\tau)_\tau \in K_{\mathbb{R}} \mid |x_\rho| < t,\ |x_\tau| < 1 \text{ para } \tau \neq \rho\}.$$

2) Si K no tiene encajes reales, sean $\sigma, \overline{\sigma}\colon K \hookrightarrow \mathbb{C}$ un par de encajes complejos conjugados. Definamos X_t por las condiciones
$$x_\sigma, x_{\overline{\sigma}} \in (-1,+1) + (-t,+t)\, i \subseteq \mathbb{C}$$
y
$$|x_\tau| < 1 \text{ para } \tau \neq \sigma, \overline{\sigma}.$$

En ambos casos, podemos tomar t suficientemente grande de tal manera que $\mathrm{vol}(X_t) > 2^n \sqrt{|\Delta_K|}$. El teorema de Minkowski entonces implica que existe un elemento no nulo $\alpha \in \mathcal{O}_K$ tal que $\Phi(\alpha) \in X_t$. Nos gustaría probar que $K = \mathbb{Q}(\alpha)$. Todo encaje $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ se extiende a $[K : \mathbb{Q}(\alpha)]$ encajes $K \hookrightarrow \mathbb{C}$. Entonces, sería suficiente ver que para cualesquiera dos encajes $\tau_1, \tau_2\colon K \hookrightarrow \mathbb{C}$ se tiene $\tau_1(\alpha) \neq \tau_2(\alpha)$. Dejo al lector revisar las definiciones de X_t de arriba y verificar que en cualquier caso $\tau_1(\alpha) = \tau_2(\alpha)$ para $\tau_1 \neq \tau_2$ implicaría que $|\tau(\alpha)| < 1$ para todo encaje $\tau\colon K \hookrightarrow \mathbb{C}$, y luego
$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_\tau |\tau(\alpha)| < 1.$$
Sin embargo, $|N_{K/\mathbb{Q}}(\alpha)| \in \mathbb{Z}_{\geq 1}$, dado que α es un entero algebraico no nulo.

Entonces, podemos concluir que $K = \mathbb{Q}(\alpha)$. Por la defnición de X_t, sabemos que los valores $|\tau(\alpha)|$ están acotados en términos de t, y como consecuencia en términos de Δ_K. ■

5.6.2. Teorema (Hermite). *Para todo $C > 0$, salvo isomorfismo, hay un número finito de campos de números $K/\mathbb{Q}$ con discriminante $|\Delta_K| < C$.*

Demostración. Primero, gracias a la cota de Minkowski, una cota sobre $|\Delta_K|$ implica una cota sobre el grado $[K : \mathbb{Q}]$. Sería suficiente entonces ver que para todo grado fijo $n = [K : \mathbb{Q}]$ existe un número finito de campos de números de discriminante fijo $\Delta_K = \Delta$.

El lema anterior nos dice que $K = \mathbb{Q}(\alpha)$, donde las raíces del polinomio mínimo $f = f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[x]$ están acotadas en términos de Δ. Pero luego los coeficientes del polinomio mínimo pueden ser acotados en términos de Δ. El grado $n = \deg(f)$ está fijo, lo que nos deja un número finito de posibilidades para f. ■

Cabe mencionar que el argumento de arriba usa la teoría de Minkowski y es más reciente que los trabajos de Hermite. Para los detalles históricos (y qué exactamente fue probado por Hermite), véase [SO1985, Chapter 9].

5.6.3. Ejemplo. Hay solamente dos campos cúbicos con $|\Delta_K| \leq 100$. Estos están definidos por los polinomios
$$\begin{array}{ll} x^3 + x^2 - 2x - 1 & (\Delta_K = 49) \\ x^3 - 3x - 1 & (\Delta_K = 81) \end{array}$$

Por ejemplo, si aplicamos el lema de arriba a los campos cúbicos reales, entonces
$$X_t = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid |x_1| < t,\ |x_2|, |x_3| < 1\}.$$
Para que se cumpla $\mathrm{vol}(X_t) > 2^3 \cdot \sqrt{|\Delta_K|}$, basta tomar $t > 80$. Tenemos entonces
$$f = (x - \alpha_1)\,(x - \alpha_2)\,(x - \alpha_3) \in \mathbb{Z}[x],$$
donde α_i son raíces reales con $|\alpha_i| < t$ y $|\alpha_2|, |\alpha_3| < 1$. Despejando la expresión para f, se obtiene una cota para los coeficientes. Esto reduce las consideraciones a un número finito de polinomios (aunque no es un modo muy eficaz de hacer los cálculos). ▲

5.6.4. Comentario (Densidad de discriminantes). En general, si $N_n(C)$ es el número de campos de números $K/\mathbb{Q}$ (salvo isomorfismo) de grado n y $|\Delta_K| < C$, el comportamiento asintótico de la «densidad» $N_n(C)/C$ con $C \to \infty$ es un objeto de recientes estudios.

Por ejemplo, un teorema clásico de Davenport y Heilbronn (1971) dice que si $N_n(C)/C$ tiende a $\frac{1}{12\,\zeta(3)} = 0{,}069325\ldots$ si se consideran los campos cúbicos reales ($r_1 = 3$, $r_2 = 0$, $\Delta_K > 0$) y a $\frac{1}{4\,\zeta(3)} = 0{,}207976\ldots$ si se consideran los campos cúbicos complejos ($r_1 = r_2 = 1$, $\Delta_K < 0$).

El artículo [Bel1997] está dedicado a un algoritmo eficaz para enumerar los campos cúbicos de discriminante acotado; al final se encuentran unas tablas de campos de discriminantes pequeños y su número para $|\Delta_K| \leq 10^{11}$.

Para los resultados más recientes, véanse por ejemplo los artículos [Bha2005], [Bha2010], [BBP2010].

5.7 Finitud del grupo de clases

Clase 21
26/10/20

Ocupando la cota de Minkowski 5.5.3, no es difícil deducir la finitud del grupo de clases

$$\mathrm{Cl}(K) = \mathrm{Pic}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K).$$

5.7.1. Lema. *Para todo $C > 0$ hay un número finito de ideales $I \subseteq \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(I) \leq C$.*

Demostración. Primero, si $I = \mathfrak{p}$ es un ideal primo, entonces $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f$, donde p es un primo tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Para todo primo racional p hay un número finito de ideales primos $\mathfrak{p} \subset \mathcal{O}_K$ tales que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ (es decir, $\mathfrak{p} \mid p$), y de estas consideraciones se ve que la afirmación es cierta para los ideales primos.

En general, todo ideal no nulo $I \subset \mathcal{O}_K$ se factoriza de alguna manera en ideales primos: $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$, y luego

$$N_{K/\mathbb{Q}}(I) = N_{K/\mathbb{Q}}(\mathfrak{p}_1)^{e_1} \cdots N_{K/\mathbb{Q}}(\mathfrak{p}_s)^{e_s}.$$

De esta manera se ve que para encontrar los ideales de norma $\leq C$, podemos considerar los primos racionales $p \leq C$ y los ideales primos correspondientes $\mathfrak{p} \mid p$ con $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq C$, y luego tomar diferentes productos de estos ideales $\mathfrak{p}$. ■

5.7.2. Lema. *Para todo elemento $[I] \in \mathrm{Cl}(K)$ existe un ideal entero $J \subseteq \mathcal{O}_K$ tal que $[I] = [J]$ y $N_{K/\mathbb{Q}}(J) \leq M_K$, donde M_K es la cota de Minkowski, definida en 5.5.3.*

Demostración. Consideremos un elemento $[I] \in \mathrm{Cl}(K)$ representado por un $\mathcal{O}_K$-ideal fraccionario no nulo $I \subseteq K$. En este caso para algún $\beta \in \mathcal{O}_K$ no nulo se tiene $\beta I^{-1} \subseteq \mathcal{O}_K$. Según el teorema 5.5.3, existe entonces un elemento no nulo $\alpha \in \beta I^{-1}$ tal que

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N_{K/\mathbb{Q}}(\beta I^{-1}).$$

Notamos que $\alpha\beta^{-1} I \subseteq (\beta I^{-1})\,(\beta^{-1} I) = \mathcal{O}_K$, así que el ideal $\alpha\beta^{-1} I$ es entero. Además, $[I] = [\alpha\beta^{-1} I]$ en el grupo de clases. La desigualdad de arriba nos dice que

$$N_{K/\mathbb{Q}}(\alpha\beta^{-1} I) \leq M_K.$$ ■

5.7.3. Teorema. *El grupo $\mathrm{Cl}(K)$ es finito.*

Demostración. Hemos probado que cualquier elemento $[I] \in \mathrm{Cl}(K)$ puede ser representado por un ideal entero $J \subseteq \mathcal{O}_K$ tal que $[J] = [I]$ y $N_{K/\mathbb{Q}}(J) \leq M_K$. Aquí la constante M_K depende solamente de K, así que hay un número finito de ideales J. ■

5.7.4. Definición. Para un campo de números $K/\mathbb{Q}$ el número $h_K = \#\,\mathrm{Cl}(K)$ se llama el **número de clases** de K.

5.7.5. Comentario. Se puede probar que todo elemento de $\mathrm{Cl}(K)$ tiene forma $[\mathfrak{p}]$ para algún *ideal primo* $\mathfrak{p} \subset \mathcal{O}_K$.

Este es un resultado sutil porque es cierto para $\mathcal{O}_K$ y no se cumple para los dominios de Dedekind en general, así que no es un asunto de álgebra conmutativa sino de la aritmética. Esto se sigue del teorema que afirma que los ideales primos que están en una clase fija en $\mathrm{Cl}(K)$ tienen densidad $\frac{1}{h_K}$. Como todos los teoremas densidad, esto se demuestra considerando ciertas funciones L. Véase por ejemplo [Neu1999, §VII.13].

5.8 Ejemplo: campos cuadráticos imaginarios

5.8.1. Ejemplo. Consideremos los campos cuadráticos imaginarios $K = \mathbb{Q}(\sqrt{-d})$. En este caso $n = 2$ y $r_2 = 1$, así que la cota de Minkowski será $M_K = \frac{2}{\pi}\sqrt{|\Delta_K|}$, donde

$$\Delta_K = \begin{cases} -4d, & \text{si } d \equiv 1, 2 \pmod 4, \\ -d, & \text{si } d \equiv 3 \pmod 4. \end{cases}$$

d:	1	2	3	5	6	7	10	11	13	14
$M_{\mathbb{Q}(\sqrt{-d})}$:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,59	4,76

- Si $M_K < 2$, esto implica que $\mathrm{Cl}(K) = 0$. De esta manera sabemos que los campos

  $$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7})$$

  tienen el grupo de clases trivial. Esto no es algo nuevo: ya sabemos que los anillos de enteros correspondientes

  $$\mathbb{Z}[i],\ \mathbb{Z}[\sqrt{-2}],\ \mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}\Big],\ \mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big]$$

  son dominios euclidianos.

- El anillo de enteros de $\mathbb{Q}(\sqrt{-11})$ es $\mathbb{Z}\Big[\frac{1+\sqrt{-11}}{2}\Big]$, y es también un dominio euclidiano.

  La cota de Minkowski en este caso es $M_K \approx 2{,}11$. El primo $p = 2$ es inerte en $\mathbb{Q}(\sqrt{-11})$, así que no hay ideales de norma 2. Esto nos da otra prueba de que $\mathbb{Q}(\sqrt{-11})$ tiene el grupo de clases trivial.

- Consideremos el campo $K = \mathbb{Q}(\sqrt{-5})$. En este caso $M_K \approx 2{,}85$ nos dice que todo elemento en $\mathrm{Cl}(K)$ puede ser representado por un ideal entero de norma 1 o 2. El único ideal de norma 2 es el ideal primo que está arriba de $p = 2$:

  $$2\mathcal{O}_K = \mathfrak{p}^2, \quad \mathfrak{p} = (2, 1 + \sqrt{-5}).$$

  Afirmamos que el ideal $\mathfrak{p}$ no es principal: en el caso contrario tendríamos $\mathfrak{p} = (\alpha)$ para algún $\alpha \in \mathcal{O}_K$, y luego $N_{K/\mathbb{Q}}(\mathfrak{p}) = |N_{K/\mathbb{Q}}(\alpha)|$. Sin embargo, $N_{K/\mathbb{Q}}(\mathfrak{p}) = 2$, mientras que $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2 \neq 2$.

  Entonces, $[\mathfrak{p}]$ es el único elemento no trivial del grupo de clases, y podemos concluir que $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

- En el caso de $K = \mathbb{Q}(\sqrt{-6})$ tenemos que examinar los ideales de norma 2 y 3. Estos son

  $$\mathfrak{p}_2 = (2, \sqrt{-6}), \quad \mathfrak{p}_3 = (3, \sqrt{-6}).$$

  Calculamos que

  $$\mathfrak{p}_2^2 = 2\mathcal{O}_K, \quad \mathfrak{p}_3^2 = 3\mathcal{O}_K, \quad \mathfrak{p}_2\,\mathfrak{p}_3 = (\sqrt{-6}).$$

  Esto significa que en el grupo de clases los elementos $[\mathfrak{p}_2]$ y $[\mathfrak{p}_3]$ tienen orden 2, y además $[\mathfrak{p}_2]\cdot[\mathfrak{p}_3] = [\mathcal{O}_K]$ implica que $[\mathfrak{p}_2] = [\mathfrak{p}_3]$. Un argumento similar al de arriba demuestra que ideal $\mathfrak{p}_2$ no es principal, así que $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

- Para los campos $K = \mathbb{Q}(\sqrt{-10}), \mathbb{Q}(\sqrt{-13})$ de la misma manera se puede ver que $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. Dejo los detalles como un ejercicio.
- En fin, consideremos $K = \mathbb{Q}(\sqrt{-14})$. La cota de Minkowski es $M_K \approx 4{,}76$, así que basta considerar los ideales primos arriba de 2 y 3. Estos son los siguientes:

$$\mathfrak{p}_2 = (2, \sqrt{-14}), \quad 2\mathcal{O}_K = \mathfrak{p}_2^2,$$

y

$$\mathfrak{p}_3 = (3, 1+\sqrt{-14}), \quad \overline{\mathfrak{p}_3} = (3, 1-\sqrt{-14}), \quad 3\mathcal{O}_K = \mathfrak{p}_3\,\overline{\mathfrak{p}_3}.$$

En el anillo $\mathbb{Z}[\sqrt{-14}]$ no hay elementos de norma 2 y 3, así que los ideales $\mathfrak{p}_2, \mathfrak{p}_3, \overline{\mathfrak{p}_3}$ no son principales. Calculamos que

$$\mathfrak{p}_3^2 = (9, 3+\sqrt{-14}, -13+2\sqrt{-14}) = (1-\sqrt{-14}/2)\,\mathfrak{p}_2,$$

así que $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$. Por otra parte, $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = [\mathcal{O}_K]$. Entonces, $[\mathfrak{p}_3]$ tiene orden 4. Tenemos $[\overline{\mathfrak{p}_3}] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]^3$. Podemos concluir que $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$. ▲

5.8.2. Comentario. En los cálculos de arriba la parte más complicada es verificar si algún ideal $\mathfrak{p} \subset \mathcal{O}_K$ es principal, o en general si $[I] = [J]$ en el grupo de clases. Esto no se ve tan difícil para los campos cuadráticos imaginarios, pero también existe un algoritmo general para resolver este problema; véase por ejemplo [BW1987].

Una pequeña tabla de grupos de clases $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ se encuentra en el apéndice C.1. De allí se nota que estos grupos *no suelen* ser triviales, y es fácil explicarlo. Primero recordemos que

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}], & d \equiv 1, 2 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right], & d \equiv 3 \pmod 4. \end{cases}$$

Ahora la norma sobre $\mathbb{Z}[\sqrt{-d}]$ tiene forma

$$N_{K/\mathbb{Q}}(a + b\sqrt{-d}) = a^2 + d\,b^2,$$

y la norma sobre $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ tiene forma

$$N_{K/\mathbb{Q}}\left(a + b\,\frac{1+\sqrt{-d}}{2}\right) = a^2 + ab + \frac{1+d}{4}\,b^2 = \frac{1}{4}\,((2a+b)^2 + db^2).$$

De aquí se ve que en $\mathcal{O}_K$ no hay elementos de norma 2, con excepción de $d = 1, 2, 7$. Entonces, si en $\mathcal{O}_K$ el primo $p = 2$ se ramifica o se escinde:

$$2\mathcal{O}_K = \mathfrak{p}^2 \quad \text{o} \quad 2\mathcal{O}_K = \mathfrak{p}\,\overline{\mathfrak{p}},$$

el ideal $\mathfrak{p} \mid 2$ no tiene chances de ser principal: $\mathfrak{p} = (\alpha)$ implica que $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\mathfrak{p}) = 2$. Esto nos lleva al siguiente resultado.

5.8.3. Proposición. *Supongamos $d \neq 1, 2, 7$. Si $d \equiv 1, 2 \pmod 4$ o $d \equiv 7 \pmod 8$, entonces $\mathrm{Cl}(K) \neq 0$. Específicamente, en este caso un ideal $\mathfrak{p} \mid 2$ representa un elemento de orden 2 en $\mathrm{Cl}(K)$.*

Otra observación curiosa: si d no es primo, entonces $\mathrm{Cl}(K) \neq 0$.

5.8.4. Proposición. *Si d es un número compuesto y $p \mid d$, entonces el ideal $\mathfrak{p} \mid p$ representa un elemento de orden 2 en $\mathrm{Cl}(K)$.*

Demostración. Tenemos $\mathfrak{p}^2 = p\mathcal{O}_K$. En el caso que nos interesa $d > 3$, y luego $\mathcal{O}_K^\times = \{\pm 1\}$. Si $\mathfrak{p}$ fuera principal, tendríamos $\sqrt{\pm p} \in K$, pero esto implicaría $K = \mathbb{Q}(\sqrt{\pm p})$, lo cual no es cierto por nuestra hipótesis. ■

Dejo como un ejercicio probar que si $d = p_1 \cdots p_s$, entonces los ideales correspondientes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \subset \mathcal{O}_K$ generan un subgrupo en $\mathrm{Cl}(K)$ isomorfo a $(\mathbb{Z}/2\mathbb{Z})^{s-1}$.

5.8.5. Comentario. Gauss probó el siguiente resultado más fuerte: para $K = \mathbb{Q}(\sqrt{d})$ con $d < 0$ el subgrupo de 2-torsión $\mathrm{Cl}(K)[2]$ es isomorfo a $(\mathbb{Z}/2\mathbb{Z})^{\omega(\Delta_K)-1}$, donde $\omega(\Delta_K)$ es el número de divisores primos del discriminante Δ_K.

Por ejemplo, si $p \equiv 1 \pmod 4$, entonces $\Delta_{\mathbb{Q}(\sqrt{-p})} = -4 \cdot p$, y el subgrupo de 2-torsión será $\mathbb{Z}/2\mathbb{Z}$.

Otro ejemplo: para $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$ tenemos $\Delta_K = -4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$, y el grupo de clases (calculado con la computadora) es

$$\mathrm{Cl}(K) \cong \mathbb{Z}/24\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^6.$$

El rango de 2-torsión es 7, como nos dice el teorema de Gauss.

Para los campos cuadráticos reales, Gauss también calculó la 2-torsión en $\mathrm{Cl}(K)$, pero el resultado es un poco más difícil de formular, así que no entraré en los detalles. De la torsión $\mathrm{Cl}(K)[\ell]$ con $\ell \neq 2$ o $[K : \mathbb{Q}] > 2$, todavía no se sabe mucho, este es un tema de investigación contemporánea.

De lo que hemos visto hasta el momento se sigue que si nos interesan los campos cuadráticos imaginarios con $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d})) = 1$, entonces $d = p$ es necesariamente un primo tal que $p \equiv 3 \pmod 8$. La única excepción es $d = 1, 2, 7$.

5.8.6. Ejemplo. Para $p < 200$ nos interesan entonces

$$p = 19,\ 43,\ 59,\ 67,\ 83,\ 107,\ 131,\ 139,\ 163,\ 179.$$

Una observación útil es la siguiente: si todos los primos racionales $q < M_K$ son inertes en K, entonces $\mathrm{Cl}(K) = 0$. Hagamos una tabla con las cotas de Minkowski y el primer primo q que *no es* inerte en $K = \mathbb{Q}(\sqrt{-p})$. Es fácil encontrarlo: este será el primer q tal que $\left(\frac{-p}{q}\right) = +1$.

p:	11	19	43	59	67	83	107	131	139	163	179
Δ_K:	2,11	2,77	4,17	4,89	5,21	5,80	6,59	7,29	7,51	8,13	8,52
q:	3	5	11	3	17	3	3	3	5	41	3

De esta tabla se ve que $\mathrm{Cl}(\mathbb{Q}(\sqrt{-p})) = 0$ para $p = 11, 19, 43, 67, 163$. Curiosamente, para estos primos todo $q < (p+1)/4$ es inerte en $\mathbb{Q}(\sqrt{-p})$. Por otra parte, para $p = 59, 83, 107, 131, 139, 179$ el grupo de clases no será trivial.

- En $K = \mathbb{Q}(\sqrt{-59})$ tenemos
$$3\mathcal{O}_K = \mathfrak{p}_3\,\overline{\mathfrak{p}_3},$$
donde $\mathfrak{p}_3$ y $\overline{\mathfrak{p}_3}$ no son ideales principales: en $\mathcal{O}_K$ no hay elementos de norma 3. Además,
$$[\mathfrak{p}_3]^2 = [\overline{\mathfrak{p}_3}], \quad [\mathfrak{p}_3]^3 = [\mathfrak{p}_3\,\overline{\mathfrak{p}_3}] = [\mathcal{O}_K],$$
así que $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.
- En $K = \mathbb{Q}(\sqrt{-83})$ y $\mathbb{Q}(\sqrt{-107})$ el primo $q = 3$ se escinde y $q = 5$ es inerte. De nuevo, en $\mathcal{O}_K$ no hay elementos de norma 3, y los cálculos similares demuestran que $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.
- En $K = \mathbb{Q}(\sqrt{-131})$ los primos $q = 3, 5, 7$ se escinden, y en $\mathcal{O}_K$ no hay elementos de norma $3, 5, 7$. Pongamos
$$3\mathcal{O}_K = \mathfrak{p}_3\,\overline{\mathfrak{p}_3}, \quad 5\mathcal{O}_K = \mathfrak{p}_5\,\overline{\mathfrak{p}_5}, \quad 7\mathcal{O}_K = \mathfrak{p}_7\,\overline{\mathfrak{p}_7}.$$
Tenemos las siguientes relaciones en el grupo de clases:
$$[\mathfrak{p}_3]^2 = [\overline{\mathfrak{p}_5}] = [\overline{\mathfrak{p}_7}], \quad [\mathfrak{p}_3]^3 = [\mathfrak{p}_5] = [\mathfrak{p}_7], \quad [\mathfrak{p}_3]^4 = [\overline{\mathfrak{p}_3}], \quad [\mathfrak{p}_3]^5 = [\mathcal{O}_K].$$
Entonces, $\mathrm{Cl}(K) \cong \mathbb{Z}/5\mathbb{Z}$.

- En $K=\mathbb{Q}(\sqrt{-139})$ los primos $q=5,7$ se escinden, y en $\mathcal{O}_K$ no hay elementos de norma 5 y 7. Tenemos las siguientes relaciones:

$$[\mathfrak{p}_5]=[\overline{\mathfrak{p}_7}],\quad [\mathfrak{p}_5]^2=[\overline{\mathfrak{p}_5}]=[\overline{\mathfrak{p}_7}],\quad [\mathfrak{p}_5]^3=[\mathcal{O}_K].$$

  En este caso $\mathrm{Cl}(K)\cong\mathbb{Z}/3\mathbb{Z}$.

- En $K=\mathbb{Q}(\sqrt{-179})$ los primos $q=3,5$ se escinden, mientras que $q=7$ es inerte. De nuevo, en $\mathcal{O}_K$ no hay elementos de norma 3 y 5. Las relaciones

$$[\mathfrak{p}_3]^2=[\overline{\mathfrak{p}_5}],\quad [\mathfrak{p}_3]^3=[\mathfrak{p}_5],\quad [\mathfrak{p}_3]^4=[\overline{\mathfrak{p}_3}],\quad [\mathfrak{p}_3]^5=[\mathcal{O}_K]$$

  nos permiten concluir que $\mathrm{Cl}(K)\cong\mathbb{Z}/5\mathbb{Z}$.

Invito que el lector verifique todos los detalles. ▲

En el siguiente capítulo vamos a establecer la siguiente interpretación del número de clases de $\mathbb{Q}(\sqrt{-p})$.

5.8.7. Teorema (Dirichlet). *Sea $p>3$ un primo tal que $p\equiv 3 \pmod 4$. Consideremos el campo cuadrático imaginario $K=\mathbb{Q}(\sqrt{-p})$. Si $p\equiv 7 \pmod 8$, entonces*

$$h_K=\sum_{1\le a<p/2}\left(\frac{a}{p}\right),$$

y si $p\equiv 3 \pmod 8$, entonces

$$h_K=\frac{1}{3}\sum_{1\le a<p/2}\left(\frac{a}{p}\right).$$

5.8.8. Ejemplo. Si $p=7$, entonces

$$\left(\frac{1}{7}\right)+\left(\frac{2}{7}\right)+\left(\frac{3}{7}\right)=1+1-1=1$$

(tenemos $3^2\equiv 2 \pmod 7$).

Si $p=11$, entonces

$$\left(\frac{1}{11}\right)+\left(\frac{2}{11}\right)+\left(\frac{3}{11}\right)+\left(\frac{4}{11}\right)+\left(\frac{5}{11}\right)=1-1+1+1+1=3$$

(note que $5^2\equiv 3$ y $4^2\equiv 5 \pmod{11}$).

De estos cálculos se sigue que $\mathrm{Cl}(\mathbb{Q}(\sqrt{-7}))=0$ y $\mathrm{Cl}(\mathbb{Q}(\sqrt{-11}))=0$. ▲

Estas fórmulas tienen que ver con el siguiente fenómeno: aunque en $\mathbb{F}_p^\times$ hay el mismo número de cuadrados y no-cuadrados, resulta que para $p\equiv 3 \pmod 4$ el intervalo $[1,(p-1)/2]$ contiene más residuos cuadráticos que no-residuos (véase [Mos1951] para una prueba elemental). Este «defecto» tiene que ver con el grupo de clases.

En la figura 5.1 se encuentran los números de clases obtenidos mediante el último teorema.

Estos cálculos sugieren que *los únicos* campos cuadráticos imaginarios $K=\mathbb{Q}(\sqrt{-d})$ con $\mathrm{Cl}(K)=0$ corresponden a

$$d=1,\ 2,\ 3,\ 7,\ 11,\ 19,\ 43,\ 67,\ 163.$$

Esto fue conjeturado por Gauss. En 1936 Heilbronn y Linfoot probaron que a lo sumo existe un número más, pero en este caso $d>10^9$. Heegner, Baker, y Stark probaron que este número no existe. La prueba de Heegner fue publicada en 1952, pero contenía menores omisiones y no fue aceptada hasta que Stark dio una prueba similar completa en 1967. Otra prueba totalmente diferente fue publicada por Baker en 1966 (véase [Bak1990, Chapter 5]).

K	h_K	K	h_K	K	h_K	K	h_K
$\mathbb{Q}(\sqrt{-7})$	1	$\mathbb{Q}(\sqrt{-283})$	3	$\mathbb{Q}(\sqrt{-647})$	23	$\mathbb{Q}(\sqrt{-1063})$	19
$\mathbb{Q}(\sqrt{-11})$	1	$\mathbb{Q}(\sqrt{-307})$	3	$\mathbb{Q}(\sqrt{-659})$	11	$\mathbb{Q}(\sqrt{-1087})$	9
$\mathbb{Q}(\sqrt{-19})$	1	$\mathbb{Q}(\sqrt{-311})$	19	$\mathbb{Q}(\sqrt{-683})$	5	$\mathbb{Q}(\sqrt{-1091})$	17
$\mathbb{Q}(\sqrt{-23})$	3	$\mathbb{Q}(\sqrt{-331})$	3	$\mathbb{Q}(\sqrt{-691})$	5	$\mathbb{Q}(\sqrt{-1103})$	23
$\mathbb{Q}(\sqrt{-31})$	3	$\mathbb{Q}(\sqrt{-347})$	5	$\mathbb{Q}(\sqrt{-719})$	31	$\mathbb{Q}(\sqrt{-1123})$	5
$\mathbb{Q}(\sqrt{-43})$	1	$\mathbb{Q}(\sqrt{-359})$	19	$\mathbb{Q}(\sqrt{-727})$	13	$\mathbb{Q}(\sqrt{-1151})$	41
$\mathbb{Q}(\sqrt{-47})$	5	$\mathbb{Q}(\sqrt{-367})$	9	$\mathbb{Q}(\sqrt{-739})$	5	$\mathbb{Q}(\sqrt{-1163})$	7
$\mathbb{Q}(\sqrt{-59})$	3	$\mathbb{Q}(\sqrt{-379})$	3	$\mathbb{Q}(\sqrt{-743})$	21	$\mathbb{Q}(\sqrt{-1171})$	7
$\mathbb{Q}(\sqrt{-67})$	1	$\mathbb{Q}(\sqrt{-383})$	17	$\mathbb{Q}(\sqrt{-751})$	15	$\mathbb{Q}(\sqrt{-1187})$	9
$\mathbb{Q}(\sqrt{-71})$	7	$\mathbb{Q}(\sqrt{-419})$	9	$\mathbb{Q}(\sqrt{-787})$	5	$\mathbb{Q}(\sqrt{-1223})$	35
$\mathbb{Q}(\sqrt{-79})$	5	$\mathbb{Q}(\sqrt{-431})$	21	$\mathbb{Q}(\sqrt{-811})$	7	$\mathbb{Q}(\sqrt{-1231})$	27
$\mathbb{Q}(\sqrt{-83})$	3	$\mathbb{Q}(\sqrt{-439})$	15	$\mathbb{Q}(\sqrt{-823})$	9	$\mathbb{Q}(\sqrt{-1259})$	15
$\mathbb{Q}(\sqrt{-103})$	5	$\mathbb{Q}(\sqrt{-443})$	5	$\mathbb{Q}(\sqrt{-827})$	7	$\mathbb{Q}(\sqrt{-1279})$	23
$\mathbb{Q}(\sqrt{-107})$	3	$\mathbb{Q}(\sqrt{-463})$	7	$\mathbb{Q}(\sqrt{-839})$	33	$\mathbb{Q}(\sqrt{-1283})$	11
$\mathbb{Q}(\sqrt{-127})$	5	$\mathbb{Q}(\sqrt{-467})$	7	$\mathbb{Q}(\sqrt{-859})$	7	$\mathbb{Q}(\sqrt{-1291})$	9
$\mathbb{Q}(\sqrt{-131})$	5	$\mathbb{Q}(\sqrt{-479})$	25	$\mathbb{Q}(\sqrt{-863})$	21	$\mathbb{Q}(\sqrt{-1303})$	11
$\mathbb{Q}(\sqrt{-139})$	3	$\mathbb{Q}(\sqrt{-487})$	7	$\mathbb{Q}(\sqrt{-883})$	3	$\mathbb{Q}(\sqrt{-1307})$	11
$\mathbb{Q}(\sqrt{-151})$	7	$\mathbb{Q}(\sqrt{-491})$	9	$\mathbb{Q}(\sqrt{-887})$	29	$\mathbb{Q}(\sqrt{-1319})$	45
$\mathbb{Q}(\sqrt{-163})$	1	$\mathbb{Q}(\sqrt{-499})$	3	$\mathbb{Q}(\sqrt{-907})$	3	$\mathbb{Q}(\sqrt{-1327})$	15
$\mathbb{Q}(\sqrt{-167})$	11	$\mathbb{Q}(\sqrt{-503})$	21	$\mathbb{Q}(\sqrt{-911})$	31	$\mathbb{Q}(\sqrt{-1367})$	25
$\mathbb{Q}(\sqrt{-179})$	5	$\mathbb{Q}(\sqrt{-523})$	5	$\mathbb{Q}(\sqrt{-919})$	19	$\mathbb{Q}(\sqrt{-1399})$	27
$\mathbb{Q}(\sqrt{-191})$	13	$\mathbb{Q}(\sqrt{-547})$	3	$\mathbb{Q}(\sqrt{-947})$	5	$\mathbb{Q}(\sqrt{-1423})$	9
$\mathbb{Q}(\sqrt{-199})$	9	$\mathbb{Q}(\sqrt{-563})$	9	$\mathbb{Q}(\sqrt{-967})$	11	$\mathbb{Q}(\sqrt{-1427})$	15
$\mathbb{Q}(\sqrt{-211})$	3	$\mathbb{Q}(\sqrt{-571})$	5	$\mathbb{Q}(\sqrt{-971})$	15	$\mathbb{Q}(\sqrt{-1439})$	39
$\mathbb{Q}(\sqrt{-223})$	7	$\mathbb{Q}(\sqrt{-587})$	7	$\mathbb{Q}(\sqrt{-983})$	27	$\mathbb{Q}(\sqrt{-1447})$	23
$\mathbb{Q}(\sqrt{-227})$	5	$\mathbb{Q}(\sqrt{-599})$	25	$\mathbb{Q}(\sqrt{-991})$	17	$\mathbb{Q}(\sqrt{-1451})$	13
$\mathbb{Q}(\sqrt{-239})$	15	$\mathbb{Q}(\sqrt{-607})$	13	$\mathbb{Q}(\sqrt{-1019})$	13	$\mathbb{Q}(\sqrt{-1459})$	11
$\mathbb{Q}(\sqrt{-251})$	7	$\mathbb{Q}(\sqrt{-619})$	5	$\mathbb{Q}(\sqrt{-1031})$	35	$\mathbb{Q}(\sqrt{-1471})$	23
$\mathbb{Q}(\sqrt{-263})$	13	$\mathbb{Q}(\sqrt{-631})$	13	$\mathbb{Q}(\sqrt{-1039})$	23	$\mathbb{Q}(\sqrt{-1483})$	7
$\mathbb{Q}(\sqrt{-271})$	11	$\mathbb{Q}(\sqrt{-643})$	3	$\mathbb{Q}(\sqrt{-1051})$	5	$\mathbb{Q}(\sqrt{-1487})$	37

Figura 5.1: Números de clases $h_{\mathbb{Q}(\sqrt{-p})}$ para $p \equiv 3\ (4)$

Los d de arriba se conocen como los **números de Heegner**. Lamentablemente, Heegner falleció en 1965, antes de que su trabajo fuera reconocido por la comunidad matemática...

Gauss también hizo otras conjeturas:

- $h_{\mathbb{Q}(\sqrt{-d})} \to \infty$ con $d \to \infty$.
  Esto fue probado por Heilbronn en 1934.
- Para cualquier h fijo existe un número finito de campos cuadráticos imaginarios con $\#\,\mathrm{Cl}(K) = h$.
  Por ejemplo, Baker y Stark demostraron en 1971 que hay exactamente 18 campos $K = \mathbb{Q}(\sqrt{-d})$ con $h_K = 2$, y estos corresponden a

  $$d = 5,\ 6,\ 10,\ 13,\ 15,\ 22,\ 35,\ 37,\ 51,\ 58,\ 91,\ 115,\ 123,\ 187,\ 235,\ 267,\ 403,\ 427.$$

  Oesterlé demostró en 1985 que hay 16 campos $K = \mathbb{Q}(\sqrt{-d})$ con $h_K = 3$, y estos corresponden a

  $$d = 23,\ 31,\ 59,\ 83,\ 107,\ 139,\ 211,\ 283,\ 307,\ 331,\ 379,\ 499,\ 547,\ 643,\ 883,\ 907.$$

  De los trabajos de Goldfeld, Oesterlé, Gross y Zagier se sigue una cota explícita para d en términos de $h_{\mathbb{Q}(\sqrt{-d})}$. De esta manera el problema se reduce a un cálculo finito. Los campos correspondientes para pequeños valores de h han sido enumerados gradualmente; por ejemplo, en [Wat2004] se encuentra una tabla para $h \leq 100$.

Para la historia detrás de los campos cuadráticos imaginarios con $\mathrm{Cl}(K) = 0$, recomiendo el artículo [Gol1985].

5.9 Números de la suerte de Euler

Euler descubrió* que el polinomio $f(x) = x^2 + x + 41$ toma valores primos para todo $x = 0, 1, \ldots, 39$.

$f(1)$	$=$	43	$f(14)$	$=$	251	$f(27)$	$=$	797
$f(2)$	$=$	47	$f(15)$	$=$	281	$f(28)$	$=$	853
$f(3)$	$=$	53	$f(16)$	$=$	313	$f(29)$	$=$	911
$f(4)$	$=$	61	$f(17)$	$=$	347	$f(30)$	$=$	971
$f(5)$	$=$	71	$f(18)$	$=$	383	$f(31)$	$=$	1033
$f(6)$	$=$	83	$f(19)$	$=$	421	$f(32)$	$=$	1097
$f(7)$	$=$	97	$f(20)$	$=$	461	$f(33)$	$=$	1163
$f(8)$	$=$	113	$f(21)$	$=$	503	$f(34)$	$=$	1231
$f(9)$	$=$	131	$f(22)$	$=$	547	$f(35)$	$=$	1301
$f(10)$	$=$	151	$f(23)$	$=$	593	$f(36)$	$=$	1373
$f(11)$	$=$	173	$f(24)$	$=$	641	$f(37)$	$=$	1447
$f(12)$	$=$	197	$f(25)$	$=$	691	$f(38)$	$=$	1523
$f(13)$	$=$	223	$f(26)$	$=$	743	$f(39)$	$=$	1601

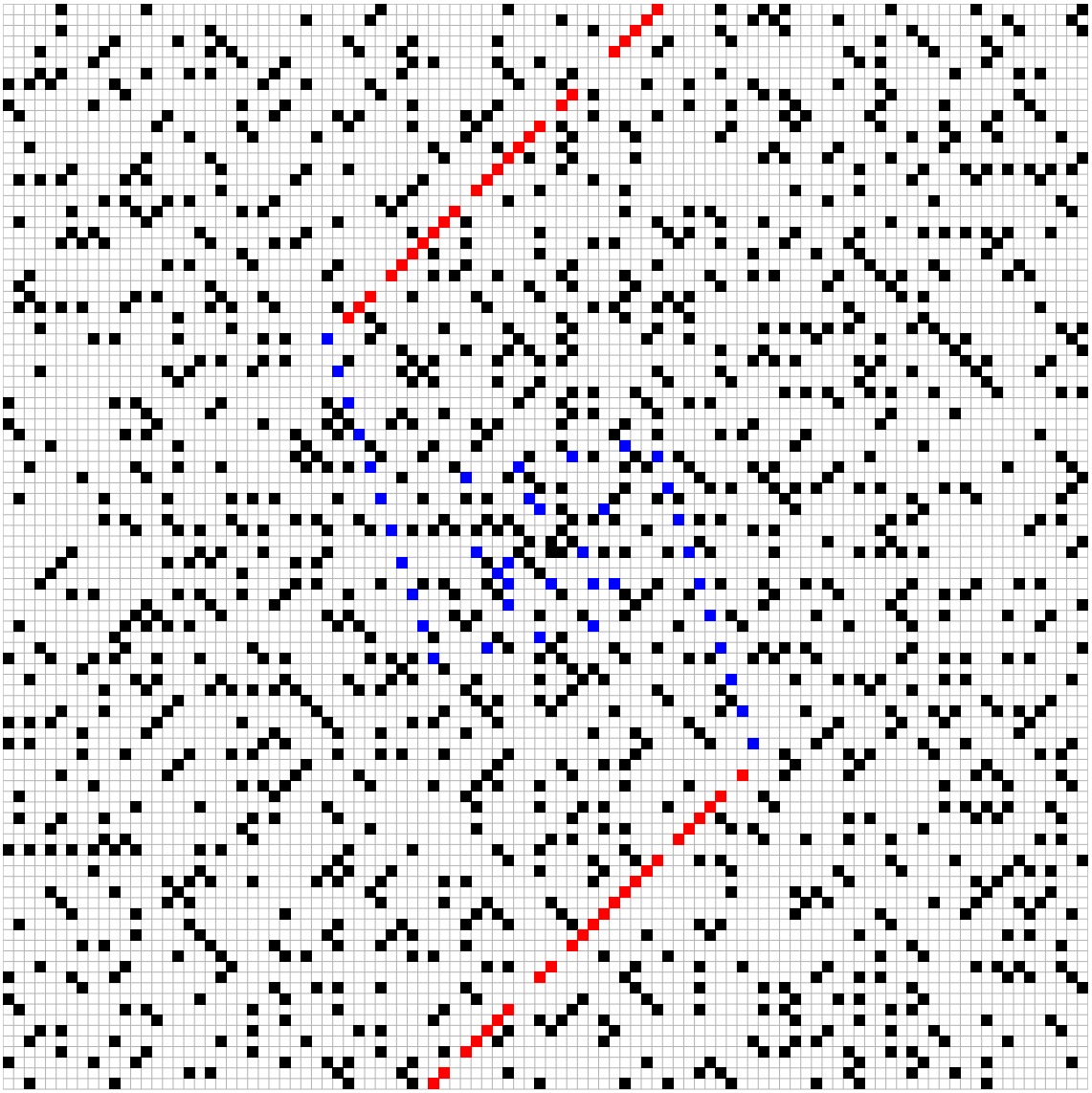


Figura 5.2: Los primos de la forma $x^2 + x + 41$ en la espiral de Ulam (los puntos en azul corresponden a $x = 0, 1, \ldots, 39$)

Para $x = 40$ se tiene $f(40) = 41^2$, así que este valor ya no es primo. De todos modos, es sorprendente que hasta este punto salgan números primos. Este fenómeno tiene una explicación en la teoría algebraica de números.

5.9.1. Teorema (Rabinowitsch[*], 1912). *Sean p un primo impar y $K = \mathbb{Q}(\sqrt{-p})$. Si $\mathrm{Cl}(K) = 0$, entonces el polinomio*[**]

$$f(x) = x^2 + x + \frac{p+1}{4}$$

toma valores primos para $0 \leq x < \frac{p-3}{4}$.

Obviamente, esta observación es trivial si uno asume el teorema de Baker–Heegner–Stark sobre los campos $K = \mathbb{Q}(\sqrt{-d})$ con $\mathrm{Cl}(K) = 0$, pero esto tampoco explicaría mucho... La prueba elemental que vamos a ver viene del artículo [AC1981].

5.9.2. Lema. *Si $\mathrm{Cl}(K) = 0$ y q es un primo tal que $q < \frac{p+1}{4}$, entonces $\left(\frac{q}{p}\right) = -1$.*

Demostración. Como ya vimos (5.8.3), la hipótesis $\mathrm{Cl}(K) = 0$ implica que $p \equiv 3 \pmod 4$, y luego $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$. Ahora si $\left(\frac{q}{p}\right) = +1$, entonces q se escinde en K: tenemos

$$q\mathcal{O}_K = \mathfrak{q}\,\overline{\mathfrak{q}}.$$

Por nuestra hipótesis, los ideales $\mathfrak{q}$ y $\overline{\mathfrak{q}}$ deben ser principales. Digamos que $\mathfrak{q}$ está generado por $a + b\,\frac{1+\sqrt{-p}}{2}$. Aquí necesariamente $b \neq 0$, y luego

$$q = N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}\left(a + b\,\frac{1+\sqrt{-p}}{2}\right) = \frac{1}{4}\left((2a+b)^2 + pb^2\right) \geq \frac{p+1}{4}. \qquad \blacksquare$$

5.9.3. Lema. *Si $\mathrm{Cl}(K) = 0$, entonces $f(0) = \frac{p+1}{4}$ es primo.*

Demostración. Si $\mathrm{Cl}(K) = 0$, entonces $\mathcal{O}_K$ es un dominio de factorización única. Supongamos que existe un primo q tal que $q < \frac{1+p}{4}$ y $q \mid \frac{1+p}{4}$. En este caso $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right) = -1$ por el lema anterior, y luego q es inerte en K, y por lo tanto un elemento primo en $\mathcal{O}_K$. Ahora

$$q \mid \frac{p+1}{4} = \left(\frac{1+\sqrt{-p}}{2}\right)\left(\frac{1-\sqrt{-p}}{2}\right) \Longrightarrow q \mid \left(\frac{1 \pm \sqrt{-p}}{2}\right).$$

Esto es imposible. $\blacksquare$

Demostración del teorema de Rabinowitsch. Supongamos que para el polinomio $f(x)$ para algún $x < \frac{p-3}{4}$ el valor $f(x)$ no es primo. Sea q un primo impar tal que $q \mid f(x)$ y $q^2 \leq f(x)$. Tenemos entonces la desigualdad

$$4q^2 \leq (2x+1)^2 + p < \left(\frac{p+1}{2}\right)^2.$$

Por el lema 5.9.2, tenemos $\left(\frac{q}{p}\right) = -1$. Por otra parte,

$$x^2 + x + \frac{p+1}{4} = aq$$

para algún $a \in \mathbb{Z}$, y luego

$$(2x+1)^2 + p = 4aq,$$

de donde $\left(\frac{-p}{q}\right) = +1$. Pero bajo nuestra hipótesis $\left(\frac{-p}{q}\right) = \left(\frac{q}{p}\right)$. Contradicción. $\blacksquare$

[*] La publicación original es la carta de Euler a Bernoulli [E461]. Allí el polinomio es $g(x) = x^2 - x + 41$, pero $g(x+1) = f(x)$.

[*] Seudónimo de George Yuri Rainich (1886–1968). El mismo Rabinowitsch del famoso «truco de Rabinowitsch» en la prueba del Nullstellensatz.

[**] Recuerde que en este caso $p \equiv 3 \pmod 4$ según 5.8.3.

5.9.4. Ejemplo. Si en lugar de $p = 163$ tomamos $p = 67$, se obtiene el polinomio $f(x) = x^2 + x + 17$ que toma valores primos para $x = 0, 1, \ldots, 15$.

$f(1)$	$=$	19	$f(6)$	$=$	59	$f(11)$	$=$	149
$f(2)$	$=$	23	$f(7)$	$=$	73	$f(12)$	$=$	173
$f(3)$	$=$	29	$f(8)$	$=$	89	$f(13)$	$=$	199
$f(4)$	$=$	37	$f(9)$	$=$	107	$f(14)$	$=$	227
$f(5)$	$=$	47	$f(10)$	$=$	127	$f(15)$	$=$	257

De la misma manera, para $p = 43$ se obtiene $f(x) = x^2 + x + 11$ que toma valores primos para $x = 0, 1, \ldots, 9$. ▲

Los primos q que dan lugar a $f(x) = x^2 + x + q$ que toma valores primos para $x = 0, 1, \ldots, q-2$ se conocen como los **números de la suerte de Euler**[*]. Tampoco es difícil probar que en este caso necesariamente se tiene $\mathrm{Cl}(\mathbb{Q}(\sqrt{1-4q})) = 0$ (véase [Rib2000, Chapter 5]). Entonces, el teorema de Baker–Heegner–Stark implica que hay solo un número finito de números de la suerte: estos se obtienen de $p = 7, 11, 19, 43, 67, 163$.

5.10 Ejemplo: campos cuadráticos reales

Ahora veamos algunos campos cuadráticos reales. En este caso la cota de Minkowski será $\frac{1}{2}\sqrt{|\Delta_K|}$.

5.10.1. Ejemplo. Calculemos M_K para los primeros $K = \mathbb{Q}(\sqrt{d})$.

d:	2	3	5	6	7	10	11	13	14	15
$\Delta_{\mathbb{Q}(\sqrt{d})}$:	8	12	5	24	28	40	44	13	56	60
$M_{\mathbb{Q}(\sqrt{d})}$:	1,41	1,73	1,12	2,45	2,65	3,16	3,32	1,80	3,74	3,87

De aquí notamos que para $d = 2, 3, 5, 13$ el grupo de clases es trivial. Podemos ver otros casos de la tabla uno por uno.

- Para $d = 6$, el primo 2 se ramifica en $\mathcal{O}_K$: tenemos $2\mathcal{O}_K = \mathfrak{p}_2^2$, donde $\mathfrak{p}_2 = (2, \sqrt{6})$. Este ideal es principal: tenemos $\mathfrak{p}_2 = (2 + \sqrt{6})$. Para verlo, basta notar que $N_{K/\mathbb{Q}}(2 + \sqrt{6}) = 2^2 - 6 \cdot 1^2 = -2$, así que el elemento $2 + \sqrt{6}$ genera un ideal primo que está sobre $p = 2$.
- Para $d = 7$ pasa lo mismo: se puede ver que el ideal $\mathfrak{p}_2 = (2, 1 + \sqrt{7})$ es principal, generado por $3 + \sqrt{7}$.
- Para $d = 10$ tenemos
$$2\mathcal{O}_K = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, \sqrt{10})$$
y
$$3\mathcal{O}_K = \mathfrak{p}_3\,\overline{\mathfrak{p}_3}, \quad \mathfrak{p}_3 = (3, 1 + \sqrt{10}).$$
Estos ideales no son principales. La norma es $N_{K/\mathbb{Q}}(a + b\sqrt{10}) = a^2 - 10\,b^2$, y esta no puede ser igual a 2 o 3. Para verlo, basta por ejemplo reducir la norma módulo 5.
Además, podemos calcular que
$$(1 - \sqrt{10}/2)\,\mathfrak{p}_2 = \mathfrak{p}_3,$$
así que $[\mathfrak{p}_3] = [\mathfrak{p}_2]$ en el grupo de clases. De la misma manera $[\overline{\mathfrak{p}_3}] = [\mathfrak{p}_2]$. Entonces, $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

[*] *Euler's lucky numbers*.

- Dejo al lector ver que para $d = 11$ y 14 el grupo de clases será trivial.
- Para $d = 15$ tenemos
$$2\mathcal{O}_K = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, 1 + \sqrt{15})$$
y
$$3\mathcal{O}_K = \mathfrak{p}_3^2, \quad \mathfrak{p}_3 = (3, \sqrt{15}).$$
De nuevo, reduciendo la norma $N_{K/\mathbb{Q}}(a+b\sqrt{15}) = a^2+15\,b^2$ módulo 5, notamos que no hay elementos de norma 2 y 3, así que los ideales $\mathfrak{p}_2$ y $\mathfrak{p}_3$ no son principales. Por otra parte, podemos verificar que $[\mathfrak{p}_2] = [\mathfrak{p}_3]$, y luego $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. ▲

Una tabla de grupos de clases para los campos cuadráticos reales se encuentra en el apéndice C.2. Aquí la situación es mucho más misteriosa que con los campos imaginarios. Una conjetura de Gauss, todavía abierta, afirma que $\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = 0$ para un número infinito de $d > 1$. Cohen y Lenstra predicen que $\mathrm{Cl}(\mathbb{Q}(\sqrt{p})) = 0$ para aproximadamente 75,445 % de los primos. La densidad exacta (conjetural) es

$$\frac{1}{2\,C_\infty\,\eta_\infty(2)}, \quad \text{donde } \eta_\infty(p) = \prod_{n\geq 1} \frac{1}{1-p^{-n}},\ C_\infty = \prod_{n\geq 2} \zeta(n).$$

Es algo que se puede verificar con la computadora, solo hay que tomar *bastantes* primos:

primos	$\mathrm{Cl}(K) = 0$
100	91
1000	845
10000	7970
100000	77962
1000000	769230
10000000	7638446

Cohen y Lenstra tienen otras conjeturas de este tipo sobre la estructura de grupos de clase; para más detalles, consulte el artículo [CL1984].

En general, para un campo de números específico K, hay un algoritmo para calcular $\mathrm{Cl}(K)$. Sin embargo, si nos interesa el comportamiento de grupos de clases para una familia de campos de números, no se sabe mucho. Por ejemplo, no se conoce *ninguna* familia infinita de campos de números con $\mathrm{Cl}(K) = 0$. Como mencionamos, esta es una gran conjetura para los campos cuadráticos reales.

5.11 Perspectiva: campos ciclotómicos

Para los campos ciclotómicos $K = \mathbb{Q}(\zeta_n)$ nuestros cálculos con la cota de Minkowski ya no serán muy prácticos porque los discriminantes Δ_K serán bastante grandes. He aquí un pequeño ejemplo que sí es posible hacer a mano.

5.11.1. Ejemplo. Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_7)$. En este caso $n = 6$, $r_2 = 3$, y $\Delta_K = -7^5$, así que la cota de Minkowski viene dada por

$$M_K = \frac{6!}{6^6}\left(\frac{4}{\pi}\right)^3 7^{5/2} \approx 4{,}12.$$

En este caso el orden de $p = 2$ mód 7 es igual a $f = 3$, así que

$$2\mathcal{O}_K = \mathfrak{p}_2\,\mathfrak{p}_2'.$$

Por otra parte, el orden de $p = 3$ mód 7 es igual a $f = 6$, lo que significa que $p = 3$ es inerte en K.

Factorizando el polinomio ciclotómico, se obtiene

$$\Phi_7(x) \equiv (x^3 + x + 1)\,(x^3 + x^2 + 1) \pmod 2.$$

Entonces,

$$\mathfrak{p}_2 = (2, 1 + \zeta_7 + \zeta_7^3), \quad \mathfrak{p}_2' = (2, 1 + \zeta_7^2 + \zeta_7^3).$$

Afirmamos que estos ideales son principales. En efecto,

$$(1 + \zeta_7 + \zeta_7^3)\,(1 + \zeta_7^2 + \zeta_7^3) = 2\zeta_7^3,$$

así que

$$\mathfrak{p}_2 = (1 + \zeta_7 + \zeta_7^3), \quad \mathfrak{p}_2' = (1 + \zeta_7^2 + \zeta_7^3).$$

Esto demuestra que $\mathrm{Cl}(K) = 0$. ▲

De hecho, Kummer descubrió que el primer campo ciclotómico con el grupo de clases no trivial es $K = \mathbb{Q}(\zeta_{23})$, donde $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$. Como generador, se puede tomar uno de los ideales primos sobre $p = 2$, o también uno de los 22 ideales no principales sobre $p = 47$ que encontramos en 3.10.8.

Las cotas de Minkowski para los campos ciclotómicos son las siguientes.

K:	$\mathbb{Q}(\zeta_3)$	$\mathbb{Q}(\zeta_4)$	$\mathbb{Q}(\zeta_5)$	$\mathbb{Q}(\zeta_7)$	$\mathbb{Q}(\zeta_8)$	$\mathbb{Q}(\zeta_9)$	$\mathbb{Q}(\zeta_{11})$	$\mathbb{Q}(\zeta_{12})$	$\mathbb{Q}(\zeta_{13})$	$\cdots$	$\mathbb{Q}(\zeta_{23})$
M_K:	1,10	1,27	1,70	4,13	2,43	4,47	58,96	1,82	306,42	$\cdots$	9324406,48

¡oops!

En el apéndice C.3 se encuentra una pequeña tabla de grupos de clases para los campos ciclotómicos. Se sabe que el grupo $\mathrm{Cl}(\mathbb{Q}(\zeta_n))$ es trivial precisamente para

$n = 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.$

Aquí para evitar las redundancias, se consideran $n \not\equiv 2 \pmod 4$ (sino, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$ para $n \equiv 2 \pmod 4$). Para la prueba véase [Was1997, Chapter 11].

La **teoría de Iwasawa** es una rama de la teoría de números que se origina en el estudio de grupos de clases de campos ciclotómicos. Un texto introductorio en español sobre el tema es [FV2020].

5.12 Campos con número de clases 2

Lectura adicional

Ya sabemos que el anillo de enteros $\mathcal{O}_K$ es un dominio de factorización única si y solamente si se tiene $h_K = 1$. Recordemos que la factorización única significa que para todo elemento no nulo $\alpha \in \mathcal{O}_K$, si hay dos factorizaciones

$$\alpha = \pi_1 \cdots \pi_r = \pi_1' \cdots \pi_s', \tag{*}$$

donde los π_i y π_j son irreducibles, entonces $r = s$, y salvo una permutación, los factores son asociados: $\pi_i \sim \pi_i'$ (lo que equivale a $\pi_i\mathcal{O}_K = \pi_i'\mathcal{O}_K$). Supongamos ahora que $\mathcal{O}_K$ no tiene factorización única, pero pidamos una propiedad más débil: dada una factorización en elementos irreducibles (*), se tiene $r = s$. La caracterización de esta propiedad fue obtenida por Leonard Carlitz en un breve artículo [Car1960].

5.12.1. Teorema. *La unicidad de longitud de factorización se cumple si y solamente si* $h_K = 1, 2$.

Ya conocemos el caso de $h_K = 1$, así que vamos a suponer que $h_K > 1$. Primero asumamos que $h_K = 2$. Empecemos por la siguiente observación.

5.12.2. Lema. *Sea $K/\mathbb{Q}$ un campo de números con $h_K = 2$. Supongamos que $\pi \in \mathcal{O}_K$ es un elemento irreducible que no es primo. Entonces, $\pi\mathcal{O}_K = \mathfrak{q}\,\mathfrak{q}'$, donde $\mathfrak{q}$ y $\mathfrak{q}'$ son ideales primos no principales (no necesariamente distintos).*

Demostración. Consideramos una factorización en ideales primos

$$\pi\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r\, \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

donde los ideales $\mathfrak{p}_i = \pi_i\mathcal{O}_K$ son principales y los $\mathfrak{q}_j$ no son principales. Por nuestra hipótesis de que $h_K = 2$, todos $\mathfrak{q}_j$ representan el mismo elemento no trivial $[\mathfrak{q}]$ en el grupo de clases. La factorización de arriba nos dice que $[\mathfrak{q}]^s = [\mathcal{O}_K]$, y luego s es necesariamente par, así que la factorización tiene forma

$$\pi\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r\, \mathfrak{q}_1\mathfrak{q}_1' \cdots \mathfrak{q}_t\mathfrak{q}_t'$$

(donde $t = s/2$). Pero ahora $[\mathfrak{q}_j\mathfrak{q}_j'] = [\mathfrak{q}]^2 = [\mathcal{O}_K]$, así que los ideales $\mathfrak{q}_j\mathfrak{q}_j' = \rho_j\mathcal{O}_K$ son principales. Entonces, se obtiene una factorización

$$\pi \sim \pi_1 \cdots \pi_r\, \rho_1 \cdots \rho_t.$$

Aquí π es irreducible, y el ideal $\pi\mathcal{O}_K$ no es principal por nuestra hipótesis, así que se tiene $r = 0$, $t = 1$, y $\pi \sim \rho$. Esto nos da la factorización deseada $\pi\mathcal{O}_K = \mathfrak{q}\,\mathfrak{q}'$. ■

Ahora ocupando el lema, supongamos que para $\alpha \neq 0$ hay dos factorizaciones en elementos irreducibles

$$\alpha = \pi_1 \cdots \pi_r\rho_1 \cdots \rho_s = \pi_1' \cdots \pi_{r'}'\rho_1' \cdots \rho_{s'}',$$

donde los π_i son primos y ρ_j no lo son. El lema nos da entonces una factorización en ideales primos

$$\alpha\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r\, \mathfrak{q}_1 \cdots \mathfrak{q}_{2s} = \mathfrak{p}_1' \cdots \mathfrak{p}_{r'}'\, \mathfrak{q}_1' \cdots \mathfrak{q}_{2s'}',$$

donde los $\mathfrak{p}_i$ son ideales principales y $\mathfrak{q}_j$ no lo son. Ahora por la unicidad de factorizaciones en ideales primos, esto implica que $r' = r$ y $s' = s$.

Esta es una de las implicaciones del teorema de Carlitz, y la otra es más difícil: para esto necesitamos usar que toda clase en $\mathrm{Cl}(K)$ puede ser representada por un ideal primo (véase el comentario 5.7.5).

Nos gustaría probar que si para las factorizaciones irreducibles en $\mathcal{O}_K$ se tiene la unicidad de longitud, entonces $h_K \leq 2$. Para esto asumamos que $h_K > 2$. Esto nos deja dos posibilidades: o en el grupo de clases existe un elemento de orden > 2, o hay por lo menos dos distintos elementos de orden 2.

Primero, supongamos que algún elemento tiene orden $n > 2$. En este caso por el resultado mencionado, existen ideales primos $\mathfrak{p}_1$ y $\mathfrak{p}_2$, donde $[\mathfrak{p}_i]$ tiene orden n y $[\mathfrak{p}_2] = [\mathfrak{p}_1]^{-1}$, así que

$$\mathfrak{p}_1^n = \pi_1\mathcal{O}_K, \quad \mathfrak{p}_2^n = \pi_2\mathcal{O}_K, \quad \mathfrak{p}_1\,\mathfrak{p}_2 = \rho\mathcal{O}_K.$$

Aquí los elementos π_1, π_2, ρ son necesariamente irreducibles. Por ejemplo, si $\pi_1 = \alpha\,\beta$ con $\alpha, \beta \notin \mathcal{O}_K^\times$, entonces $\pi_1\mathcal{O}_K = \alpha\mathcal{O}_K\,\beta\mathcal{O}_K = \mathfrak{p}_1^\ell\mathfrak{p}_1^m$, donde $\mathfrak{p}_1^\ell = \alpha\mathcal{O}_K$ y $\mathfrak{p}_1^m = \beta\mathcal{O}_K$, $\ell, m > 0$ y $\ell + m = n$. Sin embargo, esto contradice el hecho de que n es el orden de $\mathfrak{p}_1$ en el grupo de clases. Se obtiene entonces $\rho^n \sim \pi\,\pi'$, y estas son dos factorizaciones en elementos irreducibles de diferente longitud.

Supongamos ahora que en el grupo de clases hay dos elementos de orden 2. En este caso tenemos tres ideales primos $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ donde $[\mathfrak{p}_i]$ son diferentes elementos de orden 2 y $[\mathfrak{p}_3] = [\mathfrak{p}_1\mathfrak{p}_2]$, así que

$$\mathfrak{p}_1^2 = \pi_1\mathcal{O}_K, \quad \mathfrak{p}_2^2 = \pi_2\mathcal{O}_K, \quad \mathfrak{p}_3^2 = \pi_3\mathcal{O}_K, \quad \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = \pi\mathcal{O}_K,$$

donde de nuevo se puede verificar que π_1, π_2, π_3 son elementos irreducibles. Pero ahora $\pi^2 \sim \pi_1\pi_2\pi_3$.

Esto concluye la prueba del teorema de Carlitz. ■

5.12.3. Ejemplo. El grupo de clases de $K = \mathbb{Q}(\sqrt{-14})$ es isomorfo a $\mathbb{Z}/4\mathbb{Z}$, y podemos tomar como el generador la clase de $\mathfrak{p}_3 = (3, 1+\sqrt{-14})$. En este caso $[\mathfrak{p}_3]^{-1} = [\overline{\mathfrak{p}_3}]$, y tenemos

$$\mathfrak{p}_3^4 = (5+2\sqrt{-14}), \quad \overline{\mathfrak{p}_3}^4 = (5-2\sqrt{-14}), \quad \mathfrak{p}_3\mathfrak{p}_3 = 3\mathcal{O}_K.$$

Analizando las normas, no es difícil ver directamente que los elementos 3 y $5 \pm 2\sqrt{-14}$ son irreducibles en $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. Ahora

$$3^4 = (5+2\sqrt{-14})\,(5-2\sqrt{-14})$$

son dos factorizaciones irreducibles de diferente longitud. ▲

5.12.4. Ejemplo. El grupo de clases de $K = \mathbb{Q}(\sqrt{-21})$ es isomorfo a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En este caso

$$2\mathcal{O}_K = \mathfrak{p}_2^2, \quad 3\mathcal{O}_K = \mathfrak{p}_3^2, \quad 5\mathcal{O}_K = \mathfrak{p}_5\,\overline{\mathfrak{p}_5},$$

y $[\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_5]$ son diferentes clases no triviales: analizando $N_{K/\mathbb{Q}}(a+b\sqrt{-21}) = a^2+21b^2$, se ve que no hay elementos de norma $2, 3, 5$.

Se tiene $[\mathfrak{p}_1\,\mathfrak{p}_2] = [\mathfrak{p}_5]$. Específicamente, $\mathfrak{p}_2 = (2, 1+\sqrt{-21})$, $\mathfrak{p}_3 = (3, \sqrt{-21})$, $\mathfrak{p}_5 = (5, 2+\sqrt{-21})$, y calculamos que

$$\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_5 = (3-\sqrt{-21}), \quad \mathfrak{p}_5^2 = (2+\sqrt{-21}).$$

Los elementos 2, 3, 5, $2+\sqrt{-21}$, $3-\sqrt{-21}$ son irreducibles: esto se sigue del hecho de que en $\mathcal{O}_K$ no hay elementos de norma $2, 3, 5, 6, 10, 15$. Tenemos entonces factorizaciones irreducibles de diferente longitud

$$(3-\sqrt{-21})^2 = 2 \cdot 3 \cdot (-2-\sqrt{-21}).$$ ▲

5.13 Ecuación de Pell

Clase 22
28/10/20

Nuestro próximo objetivo es probar el teorema de unidades de Dirichlet, pero primero vamos a ver su caso particular relacionado con los campos cuadráticos reales.

5.13.1. Teorema. *Sea $d > 1$ un entero libre de cuadrados. La ecuación*

$$x^2 - dy^2 = 1$$

tiene una solución entera distinta de $(\pm 1, 0)$.

Demostración. Consideremos el campo de números $K = \mathbb{Q}(\sqrt{d})$. Nuestra ecuación puede ser interpretada como

$$N_{K/\mathbb{Q}}(x + y\sqrt{d}) = 1.$$

Vamos a encajar el anillo de números $\mathbb{Z}[\sqrt{d}]$ como un retículo Λ en $\mathbb{R}^2$ mediante

$$a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d}).$$

Respecto a este encaje, las soluciones que nos interesan son los puntos del retículo Λ en la hipérbola $xy = 1$. Sea X un conjunto convexo simétrico acotado suficientemente grande para que $X \cap \Lambda \neq \{0\}$. Según el teorema de Minkowski, hay que tomar X tal que $\operatorname{vol} X > 4 \operatorname{covol} \Lambda$.

Ahora para todo $\lambda > 0$ podemos considerar el conjunto

$$X_\lambda = (\lambda, \lambda^{-1})\,X = \{(\lambda x, \lambda^{-1} y) \mid (x, y) \in X\}.$$

Este tiene el mismo volumen que X, así que $X_\lambda \cap \Lambda \neq \{0\}$ (véase la figura 5.3)

De esta manera para todo $\lambda > 0$ se obtiene un elemento $\alpha_\lambda \in \mathbb{Z}[\sqrt{d}]$. Los puntos que corresponden a $X \cap \Lambda$ tienen norma acotada, y la transformación (λ, λ^{-1}) preserva la cota sobre la norma. Entonces, tenemos $|N_{K/\mathbb{Q}}(\alpha_\lambda)| \leq C$ para todo α_λ. Hay un número finito de ideales de norma acotada, así que existen $\lambda \neq \lambda'$ tales que $(\alpha_\lambda) = (\alpha_{\lambda'})$ y $\alpha_\lambda \neq \pm\alpha_{\lambda'}$. En este caso $u = \alpha_\lambda / \alpha_{\lambda'}$ es una unidad en el anillo $\mathbb{Z}[\sqrt{d}]$ distinta de ± 1. Tenemos $N_{K/\mathbb{Q}}(u) = \pm 1$. Si $N_{K/\mathbb{Q}}(u) = -1$, entonces $N_{K/\mathbb{Q}}(u^2) = +1$. De esta manera se obtiene una solución no trivial de la ecuación de Pell. ■

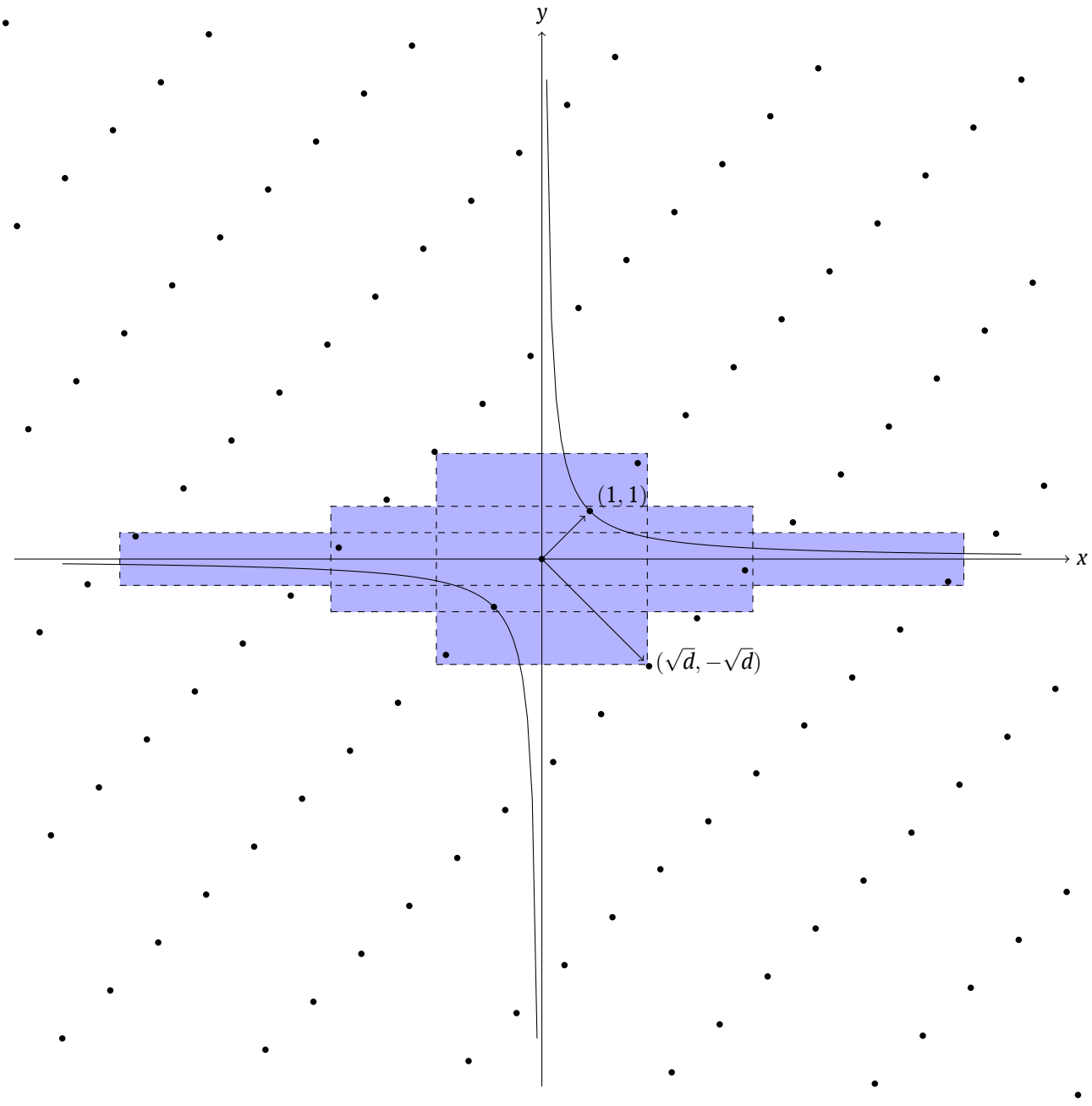


Figura 5.3: Argumento de 5.13.1

5.13.2. Corolario. *El grupo de unidades $\mathbb{Z}[\sqrt{d}]^\times$ es infinito.*

Demostración. Hemos encontrado una unidad $u \in \mathbb{Z}[\sqrt{d}]^\times$ distinta de ± 1, y luego u^n para $n \in \mathbb{Z}$ son distintas unidades. ■

A continuación vamos a probar un resultado más preciso y para el anillo de enteros $\mathcal{O}_K$ de cualquier campo de números $K/\mathbb{Q}$.

5.14 Teorema de unidades de Dirichlet

5.14.1. Teorema (Teorema de unidades de Dirichlet). *Sea $K/\mathbb{Q}$ un campo de números con r_1 encajes reales y $2r_2$ encajes complejos. Entonces tenemos un isomorfismo (no canónico)*

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1},$$

donde μ_K es el grupo finito de las raíces de unidad que están en K y $\mathbb{Z}^{r_1+r_2-1}$ es la parte libre (escrita en la notación aditiva).

En otras palabras, existen **unidades fundamentales** $u_1, \ldots, u_{r_1+r_2-1} \in \mathcal{O}_K^\times$ tales que

$$\mathcal{O}_K^\times = \mu_K \times \langle u_1 \rangle \times \cdots \langle u_{r_1+r_2-1} \rangle.$$

5.14.2. Ejemplo. Si $K = \mathbb{Q}(\sqrt{d})$ es un campo cuadrático, hay dos diferentes posibilidades. Si $d < 0$, entonces $r_1 = 0$ y $r_2 = 2$, y luego $\mathcal{O}_K^\times$ es un grupo finito. Para las raíces de la unidad tenemos $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, así que necesariamente $\mu_K = \mu_2(\mathbb{C}) = \{\pm 1\}$, o $\mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$ (si $d = -1$), o $\mu_6(\mathbb{C})$ (si $d = -3$). Ya lo hemos visto porque en este caso $\mathcal{O}_K^\times$ se calcula fácilmente usando la norma.

Notamos que $r_1 + 2r_2 = [K : \mathbb{Q}]$, así que el teorema de unidades nos dice que las únicas extensiones no triviales $K/\mathbb{Q}$ con el grupo de unidades $\mathcal{O}_K^\times$ finito son los campos cuadráticos imaginarios.

Por otra parte, si $d > 1$, entonces $r_1 = 2$ y $r_2 = 0$. Las raíces de la unidad reales son $\{\pm 1\}$, y el rango libre será igual a 1. En este caso si u es un generador de la parte libre, entonces $\pm u^{\pm 1}$ son también generadores, y normalmente como la unidad fundamental se toma el generador $u > 1$. Esto es algo especial para los campos cuadráticos reales; en general no hay manera canónica de escoger las unidades fundamentales. ▲

Volviendo a lo que vimos al inicio del capítulo, consideremos el encaje

$$\Phi \colon K \hookrightarrow K_{\mathbb{R}}, \quad \alpha \mapsto (\tau(\alpha))_\tau.$$

Este se restringe a un encaje

$$\Phi \colon K^\times \hookrightarrow K_{\mathbb{R}}^\times = \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid z_\tau \neq 0\}.$$

Para pasar a grupos aditivos, vamos a tomar los logaritmos

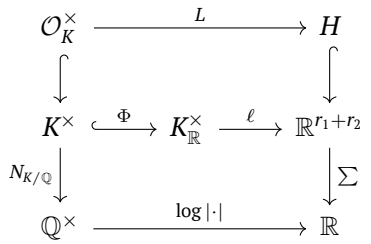
$$\ell \colon K_{\mathbb{R}}^\times \to \mathbb{R}^{r_1+r_2}, \quad (z_\tau) \mapsto (n_\tau \log |z_\tau|)_\tau,$$

donde

$$n_\tau = \begin{cases} 1, & \text{si } \tau \text{ es } \textit{real}, \\ 2, & \text{si } \tau \text{ es } \textit{complejo}. \end{cases}$$

Puesto que $|z_{\overline{\sigma}}| = |\overline{z_\sigma}| = |z_\sigma|$, las coordenadas que corresponden a encajes complejos conjugadas no se repiten, pero los contamos dos veces con coeficiente $n_\sigma = 2$. Por esto la imagen es $\mathbb{R}^{r_1+r_2}$ y no es $\mathbb{R}^{r_1+2r_2}$.

Tenemos el siguiente diagrama conmutativo de homomorfismos de grupos abelianos:



El homomorfismo $\sum$ es la suma de coordenadas y H es su núcleo:

$$H = \{x \in \mathbb{R}^{r_1+r_2} \mid \sum_i x_i = 0\}.$$

Tenemos $\dim_\mathbb{R} H = r_1 + r_2 - 1$. La aplicación L es la restricción natural: si $\alpha \in \mathcal{O}_K^\times$, entonces

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_\tau |\tau(\alpha)| = 1,$$

y luego

$$\sum_\tau \log|\tau(\alpha)| = 0.$$

Primero calculemos el núcleo de L. Esto es bastante fácil: tenemos

$$\ker L = \{\alpha \in \mathcal{O}_K^\times \mid |\tau(\alpha)| = 1 \text{ para todo encaje } \tau\colon K \hookrightarrow \mathbb{C}\}.$$

Recordemos que $\Phi(\mathcal{O}_K)$ es un retículo en $K_\mathbb{R}$; es decir un subgrupo discreto. La condición $|z_\tau| = 1$ define un subconjunto acotado en $K_\mathbb{R}$, y allí cabe solamente un número finito de elementos de $\Phi(\mathcal{O}_K^\times) \subset \Phi(\mathcal{O}_K)$. Esto significa que $\ker L$ es un grupo finito, y entonces consiste en elementos de orden finito de $\mathcal{O}_K^\times$. Por otra parte, cualquier elemento de orden finito en $\mathcal{O}_K^\times$ se encaja en $\mathbb{C}$ como una raíz de la unidad $\zeta_n^k = \exp(2\pi ik/n)$, y entonces está en $\ker L$. Esto demuestra que

$$\ker L = (\mathcal{O}_K)_{tors} = \mu_\infty(\mathbb{C}) \cap K = \mu_\infty(\mathbb{C}) \cap \mathcal{O}_K = \mu_K$$

es el subgrupo de las raíces de la unidad en K.

Denotemos por Λ la imagen de L en H. Tenemos una sucesión exacta corta

$$1 \to \mu_K \to \mathcal{O}_K^\times \xrightarrow{L} \Lambda \to 0$$

Aquí siendo un subgrupo de un espacio vectorial real, Λ es libre. Un resultado general nos dice que el homomorfismo L admite una sección (no canónica) $s\colon \Lambda \to \mathcal{O}_K^\times$ tal que $L \circ s = id_\Lambda$, y luego se obtiene un isomorfismo (no canónico)

$$\mathcal{O}_K^\times \cong \mu_K \times \Lambda.$$

(Estas son generalidades del álgebra homológica básica; refiero al ejercicio 5.10 para los detalles.)

Nuestro objetivo será probar que Λ es un retículo de rango completo en H, así que $\operatorname{rk}\Lambda = r_1 + r_2 - 1$. Con esto terminaríamos la demostración del teorema de unidades de Dirichlet.

Para ver que Λ es un retículo, tenemos que ver que este es un subgrupo discreto de H. Esto no es difícil: si tomamos un subconjunto acotado en H, este corresponde a ciertas cotas sobre $\log|\tau(\alpha)|$ para $\alpha \in \mathcal{O}_K^\times$, y luego cotas para los coeficientes del polinomio característico $f_{K/\mathbb{Q}}^\alpha \in \mathbb{Z}[x]$, lo que nos da un número finito de los α.

Para ver que Λ tiene rango completo, hay que trabajar más y emplear la teoría de Minkowski. Recordemos que $\Phi(\mathcal{O}_K)$ es un retículo en $K_\mathbb{R}$ de volumen $\sqrt{|\Delta_K|}$. Para $t > 0$ consideremos el conjunto

$$X_t = \{(x_\tau)_\tau \in K_\mathbb{R} \mid |x_\tau| < t \text{ para todo } \tau\}.$$

El volumen de X_t (respecto a nuestra estructura euclidiana sobre $K_\mathbb{R}$) es $2^{r_1}(2\pi)^{r_2} t^n$. Podemos escoger t suficientemente grande para que $\mathrm{vol}(X_t) > 2^n \sqrt{|\Delta_K|}$.

Consideremos el conjunto

$$S = \{(x_\tau)_\tau \in K_\mathbb{R}^\times \mid \left|\prod_\tau x_\tau\right| = 1\} \subset K_\mathbb{R}^\times.$$

Ahora para todo $s \in S$ por el teorema de Minkowski existe un entero no nulo $\alpha_s \in \mathcal{O}_K$ tal que $\Phi(\alpha_s) \in s\,X_t$. Aquí la multiplicación por s se entiende coordenada por coordenada, y esta no afecta el volumen de X_t. (Recuerde la sección anterior donde se consideraban los conjuntos $(\lambda, \lambda^{-1})\,X$.) Entonces, $s \in \Phi(\alpha_s)^{-1} X_t$.

Tenemos

$$S \subseteq \bigcup_{s\in S} \Phi(\alpha_s)^{-1} X_t.$$

Notamos que $\Phi(\alpha_s) \in s\,X_t$ implica que

$$|N_{K/\mathbb{Q}}(\alpha_s)| = \prod_\tau |\tau(\alpha_s)| < t^n.$$

Hay un número finito de ideales (α_s) con la norma acotada por t^n, así que salvo multiplicación por unidades $u \in \mathcal{O}_K^\times$, hay solo un número finito de elementos α_s. Entonces, existe un subconjunto finito $S_0 \subset S$ tal que

$$S \subseteq \bigcup_{s\in S_0} \Phi(\alpha_s)^{-1}\,\Phi(\mathcal{O}_K^\times)\,X_t.$$

Ahora la imagen de $S \subset K_\mathbb{R}^\times$ respecto a ℓ es precisamente el subespacio H, y la fórmula de arriba nos dice que

$$H = \bigcup_{\omega\in\Lambda} Y + \omega,$$

donde Y es el conjunto acotado. Esto precisamente significa que Λ es un retículo completo, y hemos terminado nuestra prueba del teorema de unidades. ■

Notamos que la prueba usa el teorema de Minkowski, así que no es constructiva y no nos da explícitamente las unidades fundamentales.

5.14.3. Comentario. Si $R \subset \mathcal{O}_K$ es un **orden**; es decir un $\mathbb{Z}$-submódulo de rango $n = [K : \mathbb{Q}] = \mathrm{rk}\,\mathcal{O}_K$, entonces todo lo que hemos probado se generaliza a la fórmula $R^\times \cong \mu_R \times \mathbb{Z}^{r_1+r_2-1}$. En este caso hay que notar que $\Phi(R)$ es un retículo en $K_\mathbb{R}$ de volumen $\sqrt{|\Delta_R|}$.

Sin embargo, si $R \subset K$ es un anillo de números que no es un orden, el teorema de unidades ya no se cumple. Por ejemplo, el mismo $\mathbb{Q}$ no es un grupo abeliano finitamente generado.

De hecho, el mismo Dirichlet probó el teorema para los órdenes de la forma $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, donde α es un entero algebraico y $K = \mathbb{Q}(\alpha)$. Un artículo sobre las contribuciones de Dirichlet es [Els2007].

5.14.4. Comentario. En general, se puede probar que si R es un anillo que es finitamente generado como $\mathbb{Z}$-módulo, entonces $R^\times$ es un grupo finitamente generado. Véase [Sam1967, §4.7]. Esto también es cierto si R es reducido* y finitamente generado *como anillo*** [Sam1966].

*Sin nilpotentes.

**$R = \mathbb{Z}[a_1, \ldots, a_n]$ para un número finito de elementos $a_1, \ldots, a_n \in R$.

5.15 Aplicación: unidades en $\mathbb{Z}[\zeta_p]$

Para ver algún ejemplo interesante de grupos de unidades mas allá de los campos cuadráticos, consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_n)$. En este caso $r_1 = 0$ y $r_2 = \phi(n)/2$. Tomemos el subcampo real fijo por la conjugación compleja $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Para este se tiene $r_1 = \phi(n)/2$ y $r_2 = 0$; este es un campo **totalmente real**.

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ \Big| 2 \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ \Big| \phi(n)/2 \\ \mathbb{Q} \end{array}$$

Entonces, los grupos de unidades $\mathcal{O}_K^\times$ y $\mathcal{O}_{K^+}^\times$ tienen el mismo rango, y por lo tanto el índice $[\mathcal{O}_K^\times : \mathcal{O}_{K^+}^\times]$ es finito. De hecho, en el caso de $n = p$ un primo impar no es difícil entender cuál es el índice.

5.15.1. Proposición. *Consideremos los campos $K = \mathbb{Q}(\zeta_p)$ y $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*
Toda unidad $u \in \mathcal{O}_K^\times$ puede ser escrita como $u = \zeta_p^a\, u'$, donde $u' \in \mathcal{O}_{K^+}^\times$. Como consecuencia, $[\mathcal{O}_K^\times : \mathcal{O}_{K^+}^\times] = p$.

Demostración. Dada una unidad $u \in \mathcal{O}_K^\times$, consideremos el número $\alpha = u/\overline{u}$. Para todo encaje $\tau\colon K \hookrightarrow \mathbb{C}$ tenemos $|\tau(\alpha)| = |\tau(u)|/|\overline{\tau(u)}| = 1$, así que $\alpha \in \mu_K$. Esto significa que $\alpha = \pm\zeta_p^k$.

En realidad, el signo debe ser «+». Recordemos que arriba de p en K está el ideal primo $\mathfrak{p} = (\zeta_p - 1)$ y $p\mathcal{O}_K = (\zeta_p - 1)^{p-1}$. Ahora

$$u = \sum_k a_k\, \zeta_p^k \equiv \sum_k a_k \pmod{\mathfrak{p}},$$

y de la misma manera

$$\overline{u} \equiv \sum_k a_k \pmod{\mathfrak{p}} \equiv u.$$

Si $u/\overline{u} \equiv -\zeta_p^k$, esto implicaría que $1 = -1$ en $\mathbb{Z}[\zeta_p]/\mathfrak{p} \cong \mathbb{F}_p$ pero p es un primo impar... Entonces, $u/\overline{u} = +\zeta_p^k$ para algún k. Escojamos $a \in \mathbb{Z}$ tal que $2a \equiv k \pmod{p}$ y pongamos $u' = \zeta_p^{-a}\, u$. En este caso tenemos $u = \zeta_p^a\, u'$, y además, $\overline{u'} = u'$, así que $u' \in \mathcal{O}_{K^+}^\times$. ■

5.15.2. Ejemplo. Si $p = 5$, tenemos el campo ciclotómico $K = \mathbb{Q}(\zeta_5)$ de grado 4 y el subcampo cuadrático real $K^+ = \mathbb{Q}(\sqrt{5})$ con $\mathcal{O}_{K^+}^\times = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. En este caso la unidad fundamental será

$$\phi = \frac{1+\sqrt{5}}{2} = -(\zeta_5^2 + \zeta_5^3)$$

(véase §1.12). Entonces, las unidades en $\mathcal{O}_K$ tienen forma $\pm\zeta_5\,(\zeta_5^2 + \zeta_5^3)^n$ para $n \in \mathbb{Z}$. Multiplicando la unidad fundamental $\zeta_5^2 + \zeta_5^3$ por ζ_5^3, podemos cambiarla por otra unidad fundamental $1 + \zeta_5$. Como conclusión,

$$\mathcal{O}_K^\times = \mu_{10}(\mathbb{C}) \times \langle 1 + \zeta_5 \rangle.$$ ▲

Cabe mencionar que $\mathbb{Q}(\zeta_n)$ es un ejemplo de algo que se llama **campo con multiplicación compleja** o **campo CM**. En general, $K/\mathbb{Q}$ es un campo con multiplicación compleja si K es totalmente imaginario ($r_1(K) = 0$, $r_2(K) = [K : \mathbb{Q}]/2$), y existe un subcampo $F \subset K$ tal que $[K : F] = 2$ y F es totalmente real ($r_1(F) = [F : \mathbb{Q}]$ y $r_2(F) = 0$). Del teorema de unidades se sigue que el índice $[\mathcal{O}_K^\times : \mathcal{O}_F^\times]$ es finito en este caso. Esto puede pasar solamente con los campos con multiplicación compleja.

5.15.3. Proposición (Einheitsdefekt). *Supongamos que $\mathbb{Q} \subset F \subsetneq K$ son campos tales que $[\mathcal{O}_K^\times : \mathcal{O}_F^\times]$ es finito. En este caso necesariamente F es un campo totalmente real, K totalmente imaginario, y $[K : F] = 2$.*

Demostración. Si $\operatorname{rk} \mathcal{O}_K^\times = \operatorname{rk} \mathcal{O}_F^\times$, entonces por el teorema de Dirichlet

$$r_1(K) + r_2(K) = r_1(F) + r_2(F).$$

Ahora, denotando $n = [K : F]$,

$$r_1(K) + 2\, r_2(K) = [K : \mathbb{Q}] = n\, [F : \mathbb{Q}] = n\, r_1(F) + 2n\, r_2(F).$$

De aquí expresamos

$$r_2(K) = (n-1)\, r_1(F) + (2n-1)\, r_2(F),$$

y luego

$$r_1(K) = r_1(F) + r_2(F) - r_2(K) = (2-n)\, r_1(F) + (2-2n)\, r_2(F).$$

Dado que $r_1, r_2 \geq 0$, esto implica que necesariamente $n = 2$ y $r_2(F) = r_1(K) = 0$. ■

5.16 Fracciones continuas

Clase 23
04/11/20

En esta sección vamos a revisar la teoría de fracciones continuas necesaria para encontrar la unidad fundamental de un campo cuadrático real. Este material es elemental y no usa la teoría algebraica desarrollada en el curso. Una buena referencia sobre el tema es [Khi1997].

5.16.1 Valor de una fracción continua infinita

Las **fracciones continuas finitas** vienen dadas por

$$\begin{aligned}
[a_0] &= a_0, \\
[a_0, a_1] &= a_0 + \frac{1}{a_1}, \\
[a_0, a_1, a_2] &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \\
[a_0, a_1, a_2, a_3] &= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}}, \\
&\dots
\end{aligned}$$

Por inducción, podemos definirlas mediante

$$[a_0, \dots, a_n] = a_0 + \frac{1}{[a_1, \dots, a_n]}.$$

Estas expresiones finitas pueden ser consideradas de manera formal, pero a continuación nos interesará el caso particular cuando $a_n \in \mathbb{Z}$ y $a_n \geq 1$ para $n \geq 1$.

5.16.1. Definición. Sea $a_0, a_1, a_2, \ldots$ una sucesión de números enteros con $a_n \geq 1$ para $n \geq 1$. Luego, el valor que corresponde a la fracción continua infinita

$$[a_0, a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

es

$$\lim_{n\to\infty} x_n, \quad \text{donde } x_n = [a_0, a_1, \ldots, a_n].$$

Hay que verificar que el límite existe. Esto se hace de la siguiente manera.

5.16.2. Lema. *A partir de una sucesión (a_n) como arriba, definamos las sucesiones de números enteros*

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a_n\, p_{n-1} + p_{n-2}, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a_n\, q_{n-1} + q_{n-2}. \end{aligned}$$

1) Para cualquier número real $\alpha > 0$ y $n \geq 1$ se cumple

$$[a_0, a_1, \ldots, a_{n-1}, \alpha] = \frac{\alpha\, p_{n-1} + p_{n-2}}{\alpha\, q_{n-1} + q_{n-2}}, \tag{5.1}$$

y en particular,

$$x_n = [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

2) Se cumplen las identidades

$$p_n\, q_{n-1} - p_{n-1}\, q_n = (-1)^{n+1}, \tag{5.2}$$

$$x_n - x_{n-1} = \frac{(-1)^{n+1}}{q_n\, q_{n-1}}, \tag{5.3}$$

$$p_n\, q_{n-2} - p_{n-2}\, q_n = (-1)^n\, a_n, \tag{5.4}$$

$$x_n - x_{n-2} = \frac{(-1)^n\, a_n}{q_n\, q_{n-2}}. \tag{5.5}$$

Demostración. Ejercicio. ■

Notamos que la ecuación (5.2) implica que

$$\operatorname{mcd}(p_n, q_n) = 1.$$

De la definición de q_n se sigue que

$$1 = q_0 \leq q_1 < q_2 < q_3 < \cdots$$

y luego gracias a (5.3),

$$\lim_{n\to\infty} (x_n - x_{n-1}) = 0.$$

De (5.3) y (5.5) se sigue que

$$\begin{aligned} &x_0 < x_2 < x_4 < \cdots < x_1, \\ &x_1 > x_3 > x_5 > \cdots > x_0. \end{aligned}$$

En palabras: la sucesión (x_{2n}) es creciente y acotada superiormente por x_1, mientras que (x_{2n+1}) es decreciente y acotada inferiormente por x_0[*]. Ambas sucesiones (x_{2n}) y (x_{2n+1}) tienen límites, y dado que $\lim_{n\to\infty}(x_n - x_{n-1}) = 0$, los dichos límites coinciden con $\lim_{n\to\infty} x_n$. De esta manera se obtienen intervalos

$$(x_0, x_1) \supset (x_2, x_3) \supset (x_4, x_5) \supset \cdots$$

tales que $\alpha \in (x_{2n}, x_{2n+1})$.

5.16.3. Ejemplo. Evaluemos la fracción continua

$$[1,1,1,1,1,\ldots] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1+\cdots}}}}$$

Tenemos $x_n = \frac{p_n}{q_n}$, y las recurrencias que definen a los p_n y q_n corresponden a los números de Fibonacci:

$$x_0 = 1, \quad x_1 = 2, \quad x_2 = \frac{3}{2}, \quad x_3 = \frac{5}{3}, \quad x_4 = \frac{8}{5}, \quad x_5 = \frac{13}{8}, \quad x_6 = \frac{21}{13}, \quad \ldots, \quad x_n = \frac{F_{n+2}}{F_{n+1}}.$$

En PARI/GP las fracciones $[a_0, \ldots, a_n] = p_n/q_n$ pueden ser calculadas mediante `contfracpnqn([`$a_0, \ldots, a_n$`],`N`)`. En este caso se calculan p_n/q_n para $n = 0, \ldots, N$ y se devuelven como una matriz $\begin{pmatrix} p_0 & p_1 & \cdots & p_N \\ q_0 & q_1 & \cdots & q_N \end{pmatrix}$.

```
? vec = vector (10,i,1)
% = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1]

? contfracpnqn(vec, #vec-1)
% =
[1 2 3 5 8 13 21 34 55 89]

[1 1 2 3 5  8 13 21 34 55]
```

Denotando el valor de la fracción continua por α, tenemos

$$\alpha = [1, \alpha] \iff \alpha = 1 + \frac{1}{\alpha} \iff \alpha^2 - \alpha - 1 = 0,$$

de donde (escogiendo la raíz positiva de la ecuación cuadrática)

$$\alpha = \frac{1+\sqrt{5}}{2}$$

es el número áureo. En particular, nuestros cálculos demuestran la fórmula bien conocida

$$\lim_{n\to\infty} \frac{F_{n+2}}{F_{n+1}} = \frac{1+\sqrt{5}}{2}.$$

La figura 5.4 demuestra la sucesión $x_0, x_1, x_2, \ldots$ en este caso. ▲

5.16.4. Proposición. *Para una fracción continua infinita $[a_0, a_1, a_2, \ldots]$ el valor correspondiente está definido de manera única por los números a_n y es irracional.*

[*] En general, $x_{2m} < x_{2n+1}$ para cualesquiera m y n.

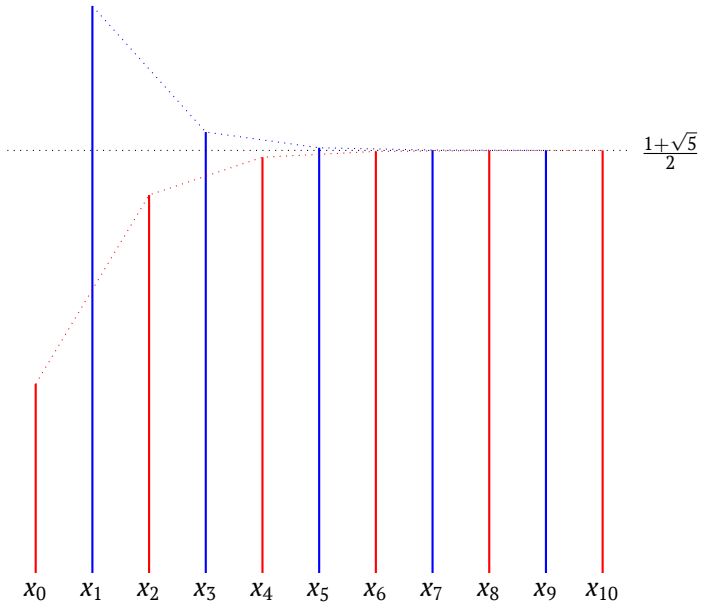


Figura 5.4: Valores de $x_n = [a_0, \ldots, a_n]$ (el caso de $[1, 1, 1, \ldots]$)

Demostración. Para la unicidad, observamos que $x_0 < \alpha < x_1$, es decir $a_0 < \alpha < a_0 + \frac{1}{a_1}$. Dado que $a_1 \geq 1$, esto implica que

$$a_0 = \lfloor \alpha \rfloor. \tag{5.6}$$

Además, es fácil comprobar que

$$[a_0, a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1, a_2, \ldots]}. \tag{5.7}$$

Usando (5.6) y (5.7), se ve por inducción sobre n que el valor de una fracción continua define de manera única sus coeficientes:

$$[a_0, a_1, a_2, \ldots] = [b_0, b_1, b_2, \ldots] \iff a_n = b_n \text{ para todo } n.$$

Ahora para ver que el valor correspondiente es irracional, escribamos como antes

$$x_n = [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Si $[a_0, a_1, a_2, \ldots] = \alpha$, entonces como hemos visto arriba, $x_n < \alpha < x_{n+1}$ para todo n. Ahora

$$0 < |\alpha - x_n| < |x_{n+1} - x_n| = \frac{1}{q_{n+1}\, q_n}$$

(véase (5.3)). Multiplicando todo por q_n, se obtiene

$$0 < |\alpha q_n - p_n| < \frac{1}{q_{n+1}}.$$

Ahora supongamos que $\alpha = a/b$ es racional, donde $b > 0$. Se obtiene la desigualdad

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}.$$

Pero para n suficientemente grande se tiene $\frac{b}{q_{n+1}} < 1$, y esto nos lleva a una contradicción. ■

5.16.2 Fracción continua asociada a un número irracional

Sea α un número irracional. Pongamos

$$\alpha_0 = \alpha, \quad a_0 = \lfloor \alpha_0 \rfloor,$$

y luego por inducción para $n \geq 1$

$$\alpha_n = \frac{1}{\alpha_{n-1} - a_{n-1}}, \quad a_n = \lfloor \alpha_n \rfloor.$$

Por inducción se ve que los α_n son números irracionales y $0 < \alpha_{n-1} - a_{n-1} < 1$, así que $a_n \geq 1$ para $n \geq 1$. Esto nos da una fracción continua

$$[a_0, a_1, a_2, \ldots],$$

y de hecho su valor coincide con α.

En efecto, se tiene para todo n

$$\alpha = [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, \ldots, a_{n-1}, \alpha_n].$$

Usando (5.1), podemos escribir

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}.$$

Luego,

$$\alpha - [a_0, a_1, \ldots, a_{n-1}] = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} = \frac{-(p_{n-1} q_{n-2} - p_{n-2} q_{n-1})}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} = \frac{(-1)^{n+1}}{q_{n-1}(\alpha_n q_{n-1} + q_{n-2})} \xrightarrow{n\to\infty} 0.$$

Para resumir, hemos obtenido una biyección

$$\{\text{fracciones continuas infinitas } [a_0, a_1, a_2, \ldots]\} \leftrightarrow \{\text{números reales irracionales}\}.$$

5.16.5. Ejemplo. Para $\alpha = \pi$ el algoritmo general nos da

$$\begin{aligned}
\alpha_0 &= \pi = 3{,}14\ldots, & a_0 &= \lfloor \alpha_0 \rfloor = 3,\\
\alpha_1 &= \frac{1}{\alpha_0 - a_0} = \frac{1}{\pi - 3} = 7{,}06\ldots, & a_1 &= \lfloor \alpha_1 \rfloor = 7,\\
\alpha_2 &= \frac{1}{\alpha_1 - a_1} = 15{,}99\ldots, & a_2 &= \lfloor \alpha_2 \rfloor = 15,\\
\alpha_3 &= \frac{1}{\alpha_2 - a_2} = 1{,}003\ldots, & a_3 &= \lfloor \alpha_3 \rfloor = 1.
\end{aligned}$$

Luego,

$$\pi = [3, 7, 15, 1, \ldots].$$

Las primeras aproximaciones son

$$\begin{aligned}
3 + \frac{1}{7} &= \frac{22}{7} = 3{,}1428571\ldots,\\
3 + \cfrac{1}{7 + \cfrac{1}{15}} &= \frac{333}{106} = 3{,}1415094\ldots,\\
3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1}}} &= \frac{355}{113} = 3{,}1415929\ldots
\end{aligned}$$

La aproximación $\frac{22}{7}$ era conocida a Arquímedes, mientras que $\frac{355}{113}$ fue descubierta por los matemáticos chinos[*]. ▲

En PARI/GP la función `contfrac(`α`)` calcula la fracción continua para α. Por ejemplo,

```
? contfrac(Pi)
% = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2,
     1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, 6]
? contfracpnqn(%)
% =
[2646693125139304345 430010946591069243]

[ 842468587426513207 136876735467187340]

? %[1,2]/%[2,2] * 1.0
% = 3.1415926535897932384626433832795028929
? % - Pi
% = 8.663606142479168328 E-36

? contfrac (exp(1))
% = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14,
     1, 1, 16, 1, 1, 18, 1, 1, 20, 1, 1, 22, 1, 1, 24, 1, 1, 26, 2]
```

La fórmula curiosa

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \ldots]$$

fue descubierta por Euler; véase [San2006], [Old1970], y [Coh2006]. En particular, con esta fracción continua Euler estableció la irracionalidad de «su número» e.

La fracción continua para π no cumple ningún patrón aparente.

Las aproximaciones $\frac{p_n}{q_n}$ que salen de la fracción continua son las mejores posibles en cierto sentido. A saber, si tenemos

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right|,$$

entonces $b > q_n$. Esto se deduce del siguiente resultado (recuerde que $q_{n+1} > q_n$).

5.16.6. Proposición. *Si* $|\alpha b - a| < |\alpha q_n - p_n|$, *entonces* $b \geq q_{n+1}$.

Demostración. Supongamos que $b < q_{n+1}$. Consideremos el sistema de ecuaciones lineales

$$\begin{cases} xq_n + yq_{n+1} &= b, \\ xp_n + yp_{n+1} &= a. \end{cases}$$

Aquí $\det \begin{pmatrix} q_n & q_{n+1} \\ p_n & p_{n+1} \end{pmatrix} = \pm 1$, así que existe una solución única $x, y \in \mathbb{Z}$, donde $(x, y) \neq (0, 0)$. De hecho, bajo nuestras hipótesis, $x \neq 0$ e $y \neq 0$. Efectivamente, si $x = 0$, entonces nos queda $b = yq_{n+1} \geq q_{n+1}$, que no es el caso. Por otra parte, si $y = 0$, entonces $x \neq 0$, y se tiene

$$|\alpha b - a| = |x| \cdot |\alpha q_n - p_n| \geq |\alpha q_n - p_n|.$$

Notamos que x e y necesariamente tienen diferentes signos: si $y < 0$, entonces $x = \frac{b - yq_{n+1}}{q_n} > 0$. De manera similar, si $y > 0$, entonces $x < 0$ por nuestra hipótesis de que $b < q_{n+1}$. Los números $\alpha q_n - p_n$ y

[*] https://en.wikipedia.org/wiki/Milü

$\alpha q_{n+1} - p_{n+1}$ también tienen diferentes signos: si n es par, entonces $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$, y si n es impar, entonces $\frac{p_{n+1}}{q_{n+1}} < \alpha < \frac{p_n}{q_n}$.

Esto implica que $x\,(\alpha q_n - p_n)$ e $y\,(\alpha q_{n+1} - p_{n+1})$ tienen el mismo signo, y luego

$$|\alpha b - a| = |x| \cdot |\alpha q_n - p_n| + |y| \cdot |\alpha q_{n+1} - p_n| > |\alpha q_n - p_n|. \qquad \blacksquare$$

5.16.7. Corolario. *Si* $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$, *entonces* $\frac{a}{b} = \frac{p_n}{q_n}$ *para algún* n.

Demostración. La sucesión (q_n) es creciente, así que para algún n se tiene $q_n \leq b < q_{n+1}$. Según la proposición anterior, tenemos entonces

$$|\alpha q_n - p_n| \leq |\alpha b - a| < \frac{1}{2b},$$

y luego

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$

Ahora ocupando la desigualdad triangular,

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2b^2} + \frac{1}{2bq_n}.$$

Por otra parte, si $\frac{a}{b} \neq \frac{p_n}{q_n}$, entonces

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| = \frac{|aq_n - bp_n|}{bq_n} \geq \frac{1}{bq_n}.$$

Todo esto nos lleva a la desigualdad

$$\frac{1}{bq_n} < \frac{1}{2b^2} + \frac{1}{2bq_n},$$

de donde $b < q_n$, pero esto contradice nuestra hipótesis. $\blacksquare$

5.16.3 Fracciones continuas periódicas

5.16.8. Definición. Se dice que una fracción continua $\alpha = [a_0, a_1, a_2, \ldots]$ es **periódica** si existen números naturales n_0 y $k \geq 1$ tales que $a_n = a_{n+k}$ para todo $n \geq n_0$. En este caso se escribe

$$\alpha = [a_0, a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, \ldots, a_{n_0+k-1}}].$$

Si $n_0 = 0$; es decir, si $\alpha = [\overline{a_0, a_1, \ldots, a_{k-1}}]$, se dice que la fracción continua es **puramente periódica**.

5.16.9. Ejemplo. Evaluemos la fracción periódica $[\overline{1, 2, 3}]$. La periodicidad nos da la relación

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{\alpha}}}.$$

Esta relación corresponde a la ecuación cuadrática

$$7\alpha^2 - 8\alpha - 3 = 0,$$

de donde se obtiene

$$\alpha = \frac{4 + \sqrt{37}}{7}. \qquad \blacktriangle$$

5.16.10. Proposición. *Si la fracción continua para α es periódica, entonces α es un número cuadrático irracional: se tiene $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$.*

Demostración. Primero, si $\alpha=[\overline{a_0,a_1,\dots,a_{k-1}}]$ es una fracción puramente periódica, entonces

$$\alpha=[a_0,\dots,a_{k-1},\alpha]=\frac{\alpha\,p_{k-1}+p_{k-2}}{\alpha\,q_{k-1}+q_{k-2}},$$

lo que nos da una ecuación cuadrática

$$q_{k-1}\,\alpha^2+(q_{k-2}-p_{k-1})\,\alpha-p_{k-2}=0.$$

En general, podemos escribir $\alpha=[a_0,\dots,a_{k-1},\beta]$, donde β es la parte puramente periódica, y luego

$$\alpha=\frac{\beta\,p_{k-1}+p_{k-2}}{\beta\,q_{k-1}+q_{k-2}}\in\mathbb{Q}(\beta).$$ ■

Resulta que también se cumple la otra implicación: si α es un número cuadrático, entonces la fracción continua correspondiente es periódica. Veamos primero un ejemplo.

5.16.11. Ejemplo. Para $\alpha=\sqrt{11}$ calculamos

$$\begin{aligned}
\alpha_0&=\sqrt{11}=3{,}31\dots, & a_0&=\lfloor\alpha_0\rfloor=3,\\
\alpha_1&=\frac{1}{\alpha_0-a_0}=\frac{3+\sqrt{11}}{2}=3{,}15\dots, & a_1&=\lfloor\alpha_1\rfloor=3,\\
\alpha_2&=\frac{1}{\alpha_1-a_1}=3+\sqrt{11}=6{,}31\dots, & a_2&=\lfloor\alpha_2\rfloor=6,\\
\alpha_3&=\frac{1}{\alpha_2-a_2}=\frac{1}{\sqrt{11}-3}=\alpha_1, & a_3&=a_1.
\end{aligned}$$

Se ve que los cálculos se vuelven periódicos y el resultado es

$$\sqrt{11}=[3,\overline{3,6}]=3+\cfrac{1}{3+\cfrac{1}{6+\cfrac{1}{3+\cfrac{1}{6+\cdots}}}}$$

Las aproximaciones correspondientes son

$$\begin{aligned}
[3,3]&=3{,}33333333\dots\\
[3,3,6]&=3{,}31578947\dots\\
[3,3,6,3]&=3{,}31666666\dots\\
[3,3,6,3,6]&=3{,}31662269\dots\\
[3,3,6,3,6,3]&=3{,}31662489\dots\\
&\dots\\
\sqrt{11}&=3{,}31662479\dots
\end{aligned}$$ ▲

Clase 24
09/11/20

5.16.12. Teorema (Lagrange). *La fracción continua de α es periódica si y solamente si $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$.*

Demostración ([Ste1992]). Ya lo probamos en una dirección. Ahora para un número cuadrático α hay que ver que $\alpha_m = \alpha_n$ para algunos $m \neq n$. Por la hipótesis sobre α, su polinomio mínimo

$$f(x) = A\,x^2 + B\,x + C$$

tiene discriminante

$$\Delta = \Delta(f) = B^2 - 4AC,$$

donde $\Delta > 0$ (porque α es real) y Δ no es un cuadrado. Por inducción podemos definir una sucesión de polinomios cuadráticos

$$f_n(x) = A_n\,x^2 + B_n\,x + C_n \in \mathbb{Z}[x]$$

que cumplen

$$f_n(\alpha_n) = 0, \quad \Delta(f_n) = \Delta.$$

Para $n = 0$ tomamos $f_0 = f$. Para el paso inductivo, no es difícil comprobar que

$$\alpha_{n+1}^2\, f_n\Big(a_n + \frac{1}{\alpha_{n+1}}\Big) = \alpha_{n+1}^2\, f_n(\alpha_n) = 0$$

corresponde a la ecuación cuadrática

$$f_{n+1}(\alpha_{n+1}) = 0, \quad f_{n+1}(x) = A_{n+1}\,x^2 + B_{n+1}\,x + C_{n+1},$$

donde

$$A_{n+1} = a_n^2\,A_n + a_n\,B_n + C_n, \quad B_{n+1} = 2\,a_n\,A_n + B_n, \quad C_{n+1} = A_n. \tag{5.8}$$

Un cálculo directo demuestra que

$$\Delta(f_{n+1}) = \Delta(f_n).$$

Notamos que la sucesión (A_n) cambia su signo un número infinito de veces. Por ejemplo, si $A_n > 0$ para todo n suficientemente grande, entonces de (5.8) se ve que también $B_n, C_n > 0$ para n suficientemente grande. Pero $\alpha_n > 0$ para $n \geq 1$, y en este caso tendríamos

$$f_n(\alpha_n) = A_n\,\alpha_n^2 + B_n\,\alpha_n + C_n > 0.$$

Entonces, para un número infinito de n se tiene $A_n\,A_{n-1} = A_n\,C_n < 0$, y en este caso el discriminante

$$\Delta(f_n) = \Delta = B_n^2 - 4\,A_n\,C_n$$

nos da la cota

$$|B_n| < \sqrt{\Delta}, \quad |A_n|, |C_n| \leq \frac{1}{4}\,\Delta.$$

Puesto que esto se cumple para un número infinito de n, habrá $m \neq n$ tales que $f_m = f_n$ y $\alpha_m = \alpha_n$. ■

También sería interesante investigar cuándo la fracción continua es *puramente* periódica. La caracterización es la siguiente.

5.16.13. Teorema. *Sea $\alpha \in \mathbb{Q}(\sqrt{d})$ un número real cuadrático. Denotemos por $\bar{\cdot}$ el automorfismo no trivial $\sqrt{d} \mapsto -\sqrt{d}$. La fracción continua para α es puramente periódica si y solamente si $\alpha > 1$ y $-1 < \overline{\alpha} < 0$.*

Demostración. Supongamos primero que la fracción continua para α es puramente periódica y $\alpha = [\overline{a_0, a_1, \ldots, a_{k-1}}]$. En todo caso se cumple $q_n \geq 1$, y luego, $a_0 = a_k \geq 1$ implica por inducción que también $p_n = a_n\,p_{n-1} + p_{n-2} \geq 1$ para todo n. Entonces, $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n} > 1$. Como ya notamos en 5.16.10, α, y luego $\overline{\alpha}$, es una raíz del polinomio cuadrático

$$f(x) = q_{k-1}\,\alpha^2 + (q_{k-2} - p_{k-1})\,\alpha - p_{k-2} = 0.$$

Es fácil verificar que $f(0) < 0$ y $f(-1) > 0$, así que f tiene una raíz entre -1 y 0, y luego $-1 < \overline{\alpha} < 0$.

En la otra dirección, supongamos que $\alpha > 1$ y $-1 < \overline{\alpha} < 0$. Esto implica por inducción que $\alpha_n > 1$ y $-1 < \overline{\alpha_n} < 0$ para todo $n \geq 0$. Notamos que

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} \Longrightarrow \overline{\alpha_n} = a_n + \frac{1}{\overline{\alpha_{n+1}}}.$$

Ahora la desigualdad $-1 < \overline{\alpha_n} < 0$ puede ser escrita como

$$0 < -\frac{1}{\overline{\alpha_{n+1}}} - a_n < 1,$$

de donde

$$a_n = \left\lfloor -\frac{1}{\overline{\alpha_{n+1}}} \right\rfloor.$$

Dado que α es un número cuadrático, la sucesión (α_n) es periódica, y existe k tal que $\alpha_n = \alpha_{n+k}$ para n *suficientemente grande*, y nos gustaría ver que esto es cierto para $n = 0$. Tenemos

$$a_{n-1} = \left\lfloor -\frac{1}{\overline{\alpha_n}} \right\rfloor = \left\lfloor -\frac{1}{\overline{\alpha_{n+k}}} \right\rfloor = a_{n-1+k}.$$

De aquí

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n} = a_{n-1+k} + \frac{1}{\alpha_{n+k}} = \alpha_{n-1+k}.$$

Aplicando este razonamiento, llegaremos a $\alpha_0 = \alpha_k$. ■

5.16.14. Corolario. *Sea $d > 1$ un entero que no es un cuadrado. Entonces,*

$$\sqrt{d} = [\lfloor \sqrt{d} \rfloor, \overline{a_1, \ldots, a_k}],$$

donde $a_k = 2\lfloor \sqrt{d} \rfloor$.

Demostración. Notamos que para el número $\alpha = \sqrt{d} + \lfloor \sqrt{d} \rfloor$ se cumple $\alpha > 0$ y $-1 < \overline{\alpha} < 0$, así que la fracción continua de α es puramente periódica: $\alpha = [\overline{a_0, a_1, \ldots, a_{k-1}}]$, donde $a_0 = a_k = \lfloor \alpha \rfloor = 2\lfloor \sqrt{d} \rfloor$. Luego,

$$\sqrt{d} = \alpha - \lfloor \sqrt{d} \rfloor = [\lfloor \sqrt{d} \rfloor, \overline{a_1, \ldots, a_{k-1}, a_k}].$$ ■

5.16.15. Comentario. El número más pequeño k tal que $\sqrt{d} = [\lfloor \sqrt{d} \rfloor, \overline{a_1, \ldots, a_k}]$ se llama el **período**. El mismo Lagrange obtuvo una cota $< 2d$, pero los cálculos sugieren la cota $O(\sqrt{d})$. Véase las referencias en https://oeis.org/A003285 para más detalles.

En la figura 5.5 se encuentran las fracciones continuas para $\sqrt{d}$, donde $d < 100$.

5.17 Volviendo a la ecuación de Pell

La ecuación de Pell $x^2 - dy^2 = \pm 1$ está relacionada con la fracción continua de $\sqrt{d}$ de la siguiente manera.

5.17.1. Proposición. *Toda solución entera con $x, y > 0$ de la ecuación $x^2 + dy^2 = \pm 1$ tiene forma $(x, y) = (p_n, q_n)$ para algún n, donde los $\frac{p_n}{q_n}$ vienen de la fracción continua para $\sqrt{d}$.*

Demostración. De manera un poco más general, sean x, y enteros positivos tales que $\mathrm{mcd}(x, y) = 1$ y s, t números reales tales que

$$x^2 - ry^2 = s, \quad 0 < s < \sqrt{r}, \quad \sqrt{r} \text{ es irracional.}$$

$\sqrt{2} = [1, \overline{2}]$
$\sqrt{3} = [1, \overline{1, 2}]$
$\sqrt{5} = [2, \overline{4}]$
$\sqrt{6} = [2, \overline{2, 4}]$
$\sqrt{7} = [2, \overline{1, 1, 1, 4}]$
$\sqrt{10} = [3, \overline{6}]$
$\sqrt{11} = [3, \overline{3, 6}]$
$\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$
$\sqrt{14} = [3, \overline{1, 2, 1, 6}]$
$\sqrt{15} = [3, \overline{1, 6}]$
$\sqrt{17} = [4, \overline{8}]$
$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}]$
$\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}]$
$\sqrt{22} = [4, \overline{1, 2, 4, 2, 1, 8}]$
$\sqrt{23} = [4, \overline{1, 3, 1, 8}]$
$\sqrt{26} = [5, \overline{10}]$
$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$
$\sqrt{30} = [5, \overline{2, 10}]$
$\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$
$\sqrt{33} = [5, \overline{1, 2, 1, 10}]$
$\sqrt{34} = [5, \overline{1, 4, 1, 10}]$
$\sqrt{35} = [5, \overline{1, 10}]$
$\sqrt{37} = [6, \overline{12}]$
$\sqrt{38} = [6, \overline{6, 12}]$
$\sqrt{39} = [6, \overline{4, 12}]$
$\sqrt{41} = [6, \overline{2, 2, 12}]$
$\sqrt{42} = [6, \overline{2, 12}]$
$\sqrt{43} = [6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}]$
$\sqrt{46} = [6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}]$
$\sqrt{47} = [6, \overline{1, 5, 1, 12}]$
$\sqrt{51} = [7, \overline{7, 14}]$
$\sqrt{53} = [7, \overline{3, 1, 1, 3, 14}]$
$\sqrt{55} = [7, \overline{2, 2, 2, 14}]$
$\sqrt{57} = [7, \overline{1, 1, 4, 1, 1, 14}]$
$\sqrt{58} = [7, \overline{1, 1, 1, 1, 1, 1, 14}]$
$\sqrt{59} = [7, \overline{1, 2, 7, 2, 1, 14}]$
$\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$
$\sqrt{62} = [7, \overline{1, 6, 1, 14}]$
$\sqrt{65} = [8, \overline{16}]$
$\sqrt{66} = [8, \overline{8, 16}]$
$\sqrt{67} = [8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}]$
$\sqrt{69} = [8, \overline{3, 3, 1, 4, 1, 3, 3, 16}]$
$\sqrt{70} = [8, \overline{2, 1, 2, 1, 2, 16}]$
$\sqrt{71} = [8, \overline{2, 2, 1, 7, 1, 2, 2, 16}]$
$\sqrt{73} = [8, \overline{1, 1, 5, 5, 1, 1, 16}]$
$\sqrt{74} = [8, \overline{1, 1, 1, 1, 16}]$
$\sqrt{77} = [8, \overline{1, 3, 2, 3, 1, 16}]$
$\sqrt{78} = [8, \overline{1, 4, 1, 16}]$
$\sqrt{79} = [8, \overline{1, 7, 1, 16}]$
$\sqrt{82} = [9, \overline{18}]$
$\sqrt{83} = [9, \overline{9, 18}]$
$\sqrt{85} = [9, \overline{4, 1, 1, 4, 18}]$
$\sqrt{86} = [9, \overline{3, 1, 1, 1, 8, 1, 1, 1, 3, 18}]$
$\sqrt{87} = [9, \overline{3, 18}]$
$\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}]$
$\sqrt{91} = [9, \overline{1, 1, 5, 1, 5, 1, 1, 18}]$
$\sqrt{93} = [9, \overline{1, 1, 1, 4, 6, 4, 1, 1, 1, 18}]$
$\sqrt{94} = [9, \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}]$
$\sqrt{95} = [9, \overline{1, 2, 1, 18}]$
$\sqrt{97} = [9, \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}]$

Figura 5.5: Fracciones continuas para $\sqrt{d}$, donde $d < 100$

Escribiendo $(x - y\sqrt{r})\,(x + y\sqrt{r}) = s$, se obtiene la desigualdad

$$\frac{x}{y} - \sqrt{r} = \frac{s}{y\,(x + y\sqrt{r})} < \frac{\sqrt{r}}{y\,(x + y\sqrt{r})} = \frac{1}{y^2\left(\frac{x}{y\sqrt{r}} + 1\right)} < \frac{1}{2y^2},$$

usando que $\frac{x}{y\sqrt{r}} > 1$, como consecuencia de $\frac{x}{y} - \sqrt{r} > 0$. Ahora, dado que

$$\left|\frac{x}{y} - \sqrt{r}\right| < \frac{1}{2y^2},$$

el resultado de 5.16.7 nos dice que $\frac{x}{y} = \frac{p_n}{q_n}$ para algún n, donde los $\frac{p_n}{q_n}$ salen de la fracción continua para $\sqrt{r}$.

Si nos interesa la ecuación $x^2 - dy^2 = +1$, basta aplicar nuestro argumento a $r = d$ y $s = 1$. Por otra parte, si la ecuación es $x^2 - dy^2 = -1$, entonces podemos tomar $r = s = \frac{1}{d}$. En este caso la ecuación será

$$x^2 - \frac{1}{d}\,y^2 = \frac{1}{d} \iff y^2 - dx^2 = -1.$$

Tenemos $\frac{x}{y} = \frac{p'_n}{q'_n}$ para algún n, donde los $\frac{p'_n}{q'_n}$ salen de la fracción continua para $\frac{1}{\sqrt{d}}$. Pero no es difícil verificar que $\frac{p'_n}{q'_n} = \frac{q_{n-1}}{p_{n-1}}$, donde las fracciones $\frac{p_n}{q_n}$ vienen de $\sqrt{d}$ (¡ejercicio!). ■

Ahora la pregunta es cuándo $\frac{p_n}{q_n}$ nos da una solución de la ecuación de Pell. Para verlo, nos conviene describir la fracción continua de $\sqrt{d}$ de manera más explícita.

5.17.2. Proposición. *Consideremos la fracción continua*

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_k}],$$

donde k es el periodo. Como antes, consideremos $\alpha_0 = \alpha$ y

$$a_n = \lfloor \alpha_n \rfloor, \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}.$$

1) Se tiene $\alpha_n = \frac{A_n + \sqrt{d}}{B_n}$, donde $A_0 = 0$, $B_0 = 1$, y

$$A_{n+1} = a_n B_n - A_n, \quad B_{n+1} = \frac{d - A_{n+1}^2}{B_n} \in \mathbb{Z}. \tag{5.9}$$

2) $B_n = +1$ si y solamente si $k \mid n$.

3) $B_n \neq -1$ para ningún n.

4) Para todo n se tiene $p_n^2 - d\,q_n^2 = (-1)^{n+1} B_{n+1}$.

Demostración. La parte 1) se deja como un ejercicio.

En la parte 2), primero consideremos B_k, donde k es el período. Tenemos $\alpha_{k+1} = \alpha_1$, y luego

$$A_{k+1} = A_1 = \lfloor \sqrt{d} \rfloor, \quad B_{k+1} = \frac{d - A_{k+1}^2}{B_k} = B_1 = d - \lfloor \sqrt{d} \rfloor^2.$$

Esto implica que $B_k = 1$. Viceversa, si $B_n = 1$ para algún n, entonces $\alpha_n = A_n + \sqrt{d}$, y podemos escribir $\alpha = [a_0, a_1, \ldots, a_{n-1}, \alpha_n]$, donde el número α_n tiene fracción continua puramente periódica, y por lo tanto $-1 < \overline{\alpha_n} < 0$. Esto implica que $\sqrt{d} - 1 < A_n < \sqrt{d}$, y luego $A_n = \lfloor \sqrt{d} \rfloor$. Ahora $\alpha_n = \sqrt{d} + \lfloor \sqrt{d} \rfloor = \alpha_1$, y esto es posible precisamente si $k \mid n$.

En la parte 3) de manera similar, si $B_n = -1$, entonces $\alpha_n = -A_n - \sqrt{d}$ tiene fracción continua puramente periódica, y luego

$$\alpha_n > 1, \ -1 < \overline{\alpha_n} < 0 \iff -A_n - \sqrt{d} > 1, \ -1 < -A_n + \sqrt{d} < 0,$$

pero estas desigualdades implican que $\sqrt{d} < A_n < -\sqrt{d} - 1$. Contradicción.

En fin, en 4) escribamos

$$\sqrt{d} = \alpha = \frac{\alpha_{n+1}\, p_n + p_{n-1}}{\alpha_{n+1}\, q_n + q_{n-1}} = \frac{(A_{n+1} + \sqrt{d})\, p_n + B_{n+1}\, p_{n-1}}{(A_{n+1} + \sqrt{d})\, q_n + B_{n+1}\, q_{n-1}}.$$

Dejo al lector analizar la ecuación correspondiente en $\mathbb{Q}(\sqrt{d})$, expresar de allí A_{n+1} en términos de B_{n+1} y verificar que nos queda

$$p_n^2 - d\, q_n^2 = (p_n\, q_{n-1} - p_{n-1}\, q_n)\, B_{n+1} = (-1)^{n+1}\, B_{n+1}. \qquad \blacksquare.$$

Entonces, hemos probado que las soluciones de la ecuación de Pell son (p_n, q_n) para algún n, y además que $p_n^2 - d\, q_n^2 = (-1)^{n+1}\, B_{n+1}$. Aquí $B_{n+1} \neq -1$ y $B_{n+1} = +1$ si y solamente si $k \mid (n+1)$. Esto nos lleva al siguiente resultado.

5.17.3. Teorema. *Para un entero libre de cuadrados d consideremos la fracción continua para $\sqrt{d}$. Si k es el período, entonces las soluciones enteras positivas de la ecuación $x^2 - dy^2 = \pm 1$ tienen forma $(x, y) = (p_{kn-1}, q_{kn-1})$, donde $n = 1, 2, 3, \ldots$*

5.17.4. Ejemplo. Consideremos la ecuación $x^2 - 41\, y^2 = \pm 1$. En este caso primero calculamos la fracción continua $\sqrt{41} = [6, \overline{2, 2, 12}]$. Las soluciones no triviales son $(x, y) = (p_{3n-1}, q_{3n-1})$. En particular, la solución más pequeña será $(x, y) = (p_2, q_2) = (32, 5)$. Efectivamente, verificamos que $32^2 - 41 \cdot 5^2 = -1$. ▲

5.17.5. Ejemplo. Las soluciones de la ecuación de Pell suelen ser bastante grandes, pero tenemos un algoritmo eficaz de entontrarlas. Por ejemplo, para la ecuación $x^2 - 151\, y^2 = \pm 1$, primero calculamos la fracción continua

$$\sqrt{151} = [12, \overline{3, 2, 7, 1, 3, 4, 1, 1, 1, 11, 1, 1, 1, 4, 3, 1, 7, 2, 3, 24}]$$

(no es difícil hacerlo con la computadora ocupando las fórmulas (5.9)). Aquí el periodo es igual a 21, y luego la solución más pequeña será (p_{20}, q_{20}). Calculámosla con PARI/GP:

```
? fr = [12,3,2,7,1,3,4,1,1,1,11,1,1,1,4,3,1,7,2,3,24];
? contfracpnqn(fr)
% =
[41973615123 1728148040]

[ 3415764356  140634693]

? [p,q] = [%[1,2], %[2,2]]
% = [1728148040, 140634693]
? p^2 - 151*q^2
% = 1
```

▲

5.18 Unidades fundamentales en campos cuadráticos reales

Consideremos un campo cuadrático real $K = \mathbb{Q}(\sqrt{d})$. En este caso el teorema de unidades nos dice que

$$\mathcal{O}_K^\times = \{\pm 1\} \times \langle u \rangle,$$

donde u es la unidad fundamental. Nuestro objetivo será encontrarla de manera explícita.

Si $d \equiv 1 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Para una unidad $v = a + b\,\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K^\times$ tenemos

$$N_{K/\mathbb{Q}}(v) = a^2 + ab + \frac{1-d}{4}\,b^2 = \pm 1.$$

Si $d \equiv 1 \pmod 8$, entonces considerando diferentes opciones mód 8, se ve que b tiene que ser par en cualquier caso, así que $v \in \mathbb{Z}[\sqrt{d}]^\times$. Por otra parte, si $d \equiv 5 \pmod 8$, un cálculo directo y tedioso demuestra que $v^3 \in \mathbb{Z}[\sqrt{d}]^\times$. Todo esto significa lo siguiente.

- Si $d \equiv 2, 3 \pmod 4$ o $d \equiv 1 \pmod 8$, entonces $\mathcal{O}_K^\times = \mathbb{Z}[\sqrt{d}]^\times$.
- si $d \equiv 5 \pmod 8$, entonces $[\mathcal{O}_K^\times : \mathbb{Z}[\sqrt{d}]^\times] = 1$ o 3. Si u es la unidad fundamental de $\mathbb{Z}[\sqrt{d}]^\times$, entonces para encontrar la unidad fundamental de $\mathcal{O}_K^\times$, basta resolver la ecuación $u^3 = v$ en $\mathcal{O}_K$. Si esta no tiene soluciones, entonces $\mathcal{O}_K^\times = \mathbb{Z}[\sqrt{d}]^\times$.

En cualquier caso, para encontrar las unidades en $\mathcal{O}_K$, bastará conocer las unidades en $\mathbb{Z}[\sqrt{d}]$. Tenemos

$$\{x + y\sqrt{d} \mid x, y > 0,\ x^2 - dy^2 = \pm 1\} = \{u^n \mid n = 1, 2, 3, \ldots\},$$

donde u es la unidad fundamental de $\mathbb{Z}[\sqrt{d}]$, definida como la unidad más pequeña tal que $u > 1$. Por otra parte, sabemos que las unidades de arriba tienen forma $p_{kn-1} + q_{kn-1}\sqrt{d}$, donde k es el período de la fracción continua para $\sqrt{d}$. La más pequeña entre estas corresponde a $n = 1$, así que

$$u = p_{k-1} + q_{k-1}\sqrt{d}.$$

5.18.1. Ejemplo. Para $K = \mathbb{Q}(\sqrt{2})$, empezamos por la fracción continua $\sqrt{2} = [1, \overline{2}]$. En este caso nos interesan $p_0 = 1$ y $q_0 = 1$. Entonces, la unidad fundamental es $u = 1 + \sqrt{2}$. ▲

5.18.2. Ejemplo. Para $K = \mathbb{Q}(\sqrt{5})$ tenemos $\sqrt{5} = [2, \overline{4}]$. En este caso $p_0 = 2$, $q_0 = 1$, así que la unidad fundamental de $\mathbb{Z}[\sqrt{5}]^\times$ es $u = 2 + \sqrt{5}$. El anillo de enteros es $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Para $v = A + B\frac{1+\sqrt{5}}{2}$ consideremos la ecuación $v^3 = u$. Esta nos da

$$\begin{cases} A^3 + \frac{3}{2}A^2B + \frac{9}{2}AB^2 + 2B^3 &= 2, \\ \frac{3}{2}A^2B + \frac{3}{2}AB^2 + B^2 &= 1. \end{cases}$$

Se ve que $A = 0$, $B = 1$ nos da una solución, así que la unidad fundamental de $\mathcal{O}_K^\times$ es $v = \frac{1+\sqrt{5}}{2}$. ▲

5.18.3. Ejemplo. Consideremos $K = \mathbb{Q}(\sqrt{13})$. En este caso $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$, y la unidad fundamental de $\mathbb{Z}[\sqrt{13}]^\times$ es $u = p_4 + q_4\sqrt{13} = 18 + 5\sqrt{13}$. Luego resolviendo la ecuación $v^3 = u$ en $\mathbb{Z}\left[\frac{1+\sqrt{13}}{2}\right]$ se obtiene la unidad fundamental $v = 1 + \frac{1+\sqrt{13}}{2}$. ▲

5.18.4. Ejemplo. Consideremos $K = \mathbb{Q}(\sqrt{37})$. Tenemos $\sqrt{37} = [6, \overline{12}]$, y entonces la unidad fundamental de $\mathbb{Z}[\sqrt{37}]^\times$ será $u = p_0 + q_0\sqrt{37} = 6 + \sqrt{37}$. Ahora la ecuación $v^3 = u$ en $\mathbb{Z}\left[\frac{1+\sqrt{37}}{2}\right]$ corresponde a

$$\begin{cases} A^3 + \frac{3}{2}A^2B + \frac{57}{2}AB^2 + 14B^3 &= 6, \\ \frac{3}{2}A^2B + \frac{3}{2}AB^2 + 5B^3 &= 1. \end{cases}$$

Escribamos la segunda ecuación como

$$B\,(3A^2 + 3AB + 10B^2) = 2.$$

De aquí se sigue que $B = \pm 1$ o ± 2. Sustituyendo estos valores, se obtiene una ecuación cuadrática en A que no tiene soluciones enteras. Entonces, $v^3 = u$ no tiene solución. Esto significa que $\mathcal{O}_K^\times = \mathbb{Z}[\sqrt{37}]^\times$, y la unidad fundamental es la misma u. ▲

En la figura 5.6 se encuentran las unidades fundamentales en $\mathbb{Z}[\sqrt{d}]^\times$ y $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$ para $d < 100$.

5.19 Cálculo del grupo de clases y unidades en PARI/GP

En esta sección explicaré brevemente cómo calcular el grupo de clases $\mathrm{Cl}(K)$ y grupo de unidades $\mathcal{O}_K^\times$ en PARI/GP. Mientras los invariantes básicos como el anillo de enteros $\mathcal{O}_K$ y el discriminante Δ_K se calculan mediante la función `nfinit(f)`, ahora necesitaremos otra función más poderosa `bnfinit(f)`. Aquí «nf» como antes viene de «number field», mientras que «b» se debe al hecho de que los cálculos de $\mathrm{Cl}(K)$ y $\mathcal{O}_K^\times$ se hacen mediante un algoritmo diseñado por Johannes Buchmann. Todas las funciones que aceptan la estructura calculada por `nfinit` también aceptan la estructura de `bnfinit` que es más general.

Ahora si `K = bnfinit(f)`, entonces los invariantes que nos interesan son los siguientes:

- `K.clgp` — el grupo de clases;
- `K.no` — el número de clases $h_K = \#\,\mathrm{Cl}(K)$;
- `K.cyc` — vector `[`a_1`,...,`a_n`]`, tal que $\mathrm{Cl}(K) \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$;
- `K.gen` — el generador de cada componente cíclica del grupo de clases, representado en la forma normal de Hermite,
- `K.tu` — las raíces de la unidad; vector `[`n`,`ζ`]`, donde n es el orden del grupo μ_K y ζ su generador;
- `K.fu` — las unidades fundamentales.

(Aquí «`tu`» son *torsion units* y «`fu`» son *fundamental units*.)

5.19.1. Ejemplo. Si nos interesa el campo $K = \mathbb{Q}(\sqrt[3]{19})$.

```
? K = bnfinit(x^3-19);
? K.no
% = 3
? K.cyc
% = [3]
? K.gen
% = [[2, 1, 1; 0, 1, 0; 0, 0, 1]]
? P = K.gen[1];
? idealdown(K,P)
% = 2
? K.fu
% = [Mod(-1/3*x^2 + 2/3*x + 2/3, x^3 - 19)]
? K.tu
% = [2, -1]
? K.fu
% = [Mod(-1/3*x^2 + 2/3*x + 2/3, x^3 - 19)]
```

d	$d\,(8)$	$u \in \mathbb{Z}[\sqrt{d}]^\times$	$v \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$	$N(u)$	d	$d\,(8)$	$u \in \mathbb{Z}[\sqrt{d}]^\times$	$v \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$	$N(u)$
2	2	$1+\sqrt{2}$		-1	51	3	$50+7\sqrt{51}$		$+1$
3	3	$2+\sqrt{3}$		$+1$	53	5	$182+25\sqrt{53}$	$3+\frac{1+\sqrt{53}}{2}$	-1
5	5	$2+\sqrt{5}$	$\frac{1+\sqrt{5}}{2}$	-1	55	7	$89+12\sqrt{55}$		$+1$
6	6	$5+2\sqrt{6}$		$+1$	57	1	$152+20\sqrt{57}$	$152+20\sqrt{57}$	$+1$
7	7	$8+3\sqrt{7}$		$+1$	58	2	$99+13\sqrt{58}$		-1
10	2	$3+\sqrt{10}$		-1	59	3	$530+69\sqrt{59}$		$+1$
11	3	$10+3\sqrt{11}$		$+1$	61	5	$29718+3805\sqrt{61}$	$17+5\,\frac{1+\sqrt{61}}{2}$	-1
13	5	$18+5\sqrt{13}$	$1+\frac{1+\sqrt{13}}{2}$	-1	62	6	$63+8\sqrt{62}$		$+1$
14	6	$15+4\sqrt{14}$		$+1$	65	1	$8+\sqrt{65}$	$8+\sqrt{65}$	-1
15	7	$4+\sqrt{15}$		$+1$	66	2	$65+8\sqrt{66}$		$+1$
17	1	$4+\sqrt{17}$	$4+\sqrt{17}$	-1	67	3	$48842+5967\sqrt{67}$		$+1$
19	3	$170+39\sqrt{19}$		$+1$	69	5	$7775+936\sqrt{69}$	$11+3\,\frac{1+\sqrt{69}}{2}$	$+1$
21	5	$55+12\sqrt{21}$	$2+\frac{1+\sqrt{21}}{2}$	$+1$	70	6	$251+30\sqrt{70}$		$+1$
22	6	$197+42\sqrt{22}$		$+1$	71	7	$3480+413\sqrt{71}$		$+1$
23	7	$24+5\sqrt{23}$		$+1$	73	1	$1068+125\sqrt{73}$	$1068+125\sqrt{73}$	-1
26	2	$5+\sqrt{26}$		-1	74	2	$43+5\sqrt{74}$		-1
29	5	$70+13\sqrt{29}$	$2+\frac{1+\sqrt{29}}{2}$	-1	77	5	$351+40\sqrt{77}$	$4+\frac{1+\sqrt{77}}{2}$	$+1$
30	6	$11+2\sqrt{30}$		$+1$	78	6	$53+6\sqrt{78}$		$+1$
31	7	$1520+273\sqrt{31}$		$+1$	79	7	$80+9\sqrt{79}$		$+1$
33	1	$23+4\sqrt{33}$	$23+4\sqrt{33}$	$+1$	82	2	$9+\sqrt{82}$		-1
34	2	$35+6\sqrt{34}$		$+1$	83	3	$82+9\sqrt{83}$		$+1$
35	3	$6+\sqrt{35}$		$+1$	85	5	$378+41\sqrt{85}$	$4+\frac{1+\sqrt{85}}{2}$	-1
37	5	$6+\sqrt{37}$	$6+\sqrt{37}$	-1	86	6	$10405+1122\sqrt{86}$		$+1$
38	6	$37+6\sqrt{38}$		$+1$	87	7	$28+3\sqrt{87}$		$+1$
39	7	$25+4\sqrt{39}$		$+1$	89	1	$500+53\sqrt{89}$	$500+53\sqrt{89}$	-1
41	1	$32+5\sqrt{41}$	$32+5\sqrt{41}$	-1	91	3	$1574+165\sqrt{91}$		$+1$
42	2	$13+2\sqrt{42}$		$+1$	93	5	$12151+1260\sqrt{93}$	$13+3\,\frac{1+\sqrt{93}}{2}$	$+1$
43	3	$3482+531\sqrt{43}$		$+1$	94	6	$2143295+221064\sqrt{94}$		$+1$
46	6	$24335+3588\sqrt{46}$		$+1$	95	7	$39+4\sqrt{95}$		$+1$
47	7	$48+7\sqrt{47}$		$+1$	97	1	$5604+569\sqrt{97}$	$5604+569\sqrt{97}$	-1

Figura 5.6: Unidades fundamentales en $\mathbb{Z}[\sqrt{d}]^\times$ y $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$, donde $d < 100$

Interpretación de la salida:

$$\mathrm{Cl}(\mathbb{Q}(\sqrt[3]{19})) \cong \mathbb{Z}/3\mathbb{Z},$$

donde como el generador se puede tomar un ideal $\mathfrak{p}$ que está arriba de $p = 2$. El grupo de unidades es

$$\mathcal{O}_K^\times \cong \{\pm 1\} \times \langle u \rangle, \quad u = \frac{2}{3} + \frac{2}{3}\,19^{1/3} - \frac{1}{3}\,19^{2/3}.$$

▲

5.19.2. Ejemplo. Podemos compilar las listas de campos cuadráticos imaginarios con $h_K = 1, 2, 3$. Vamos a tomar $K = \mathbb{Q}(\sqrt{d})$ con $d \leq 10^4$. De hecho, estas serán las listas completas.

```
? l = vector(3,x,List())
%65 = [List([]), List([]), List([])]
? { for (d=1,10^4,
      if (issquarefree(d),
        n = bnfinit(x^2+d).no;
        if (n <= 3, listput (l[n],d))
      )
) };

? l[1]
% = List([1, 2, 3, 7, 11, 19, 43, 67, 163])
? l[2]
% = List([5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427])
? #l[2]
% = 18
? l[3]
% = List([23, 31, 59, 83, 107, 139, 211, 283, 307, 331, 379, 499, 547, 643, 883, 907])
? #l[3]
% = 16
```

▲

5.19.3. Ejemplo. Calculemos los grupos de clases de algunos campos ciclotómicos.

```
? for (n=3,50, if (n%4 != 2, print ([n, bnfinit(polcyclo(n)).cyc])))
[3, []]
[4, []]
[5, []]
[7, []]
[8, []]
[9, []]
[11, []]
[12, []]
[13, []]
[15, []]
[16, []]
[17, []]
[19, []]
[20, []]
[21, []]
```

```
[23, [3]]
[24, []]
[25, []]
[27, []]
[28, []]
[29, [2, 2, 2]]
[31, [9]]
[32, []]
[33, []]
[35, []]
[36, []]
  ***   at top-level: ...=3,50,if(n%4!=2,print([n,
  ***   bnfinit(polcyclo(n)).
  ***   ^---------------------
  *** bnfinit: the PARI stack overflows !
  current stack size: 8000000 (7.629 Mbytes)
  [hint] set 'parisizemax' to a nonzero value in your GPRC

  ***   Break loop: type 'break' to go back to GP
  ***   prompt
```

Aquí PARI/GP ya no pudo calcular el grupo de clases de $\mathbb{Q}(\zeta_{37})$: no le bastó la memoria disponible (el tamaño de la pila[*]). Se puede aumentarlo ocupando el comando `default(parisizemax,...)`, pero hay que tomar en cuenta que los grupos de clases de campos ciclotómicos suelen ser bastante grandes, y su cálculo requiere tiempo y memoria.

```
? default(parisizemax,10^10)
  ***   Warning: new maximum stack size = 10000003072 (9536.746 Mbytes).
? #
   timer = 1 (on)
? bnfinit(polcyclo(37)).cyc
  *** bnfinit: Warning: increasing stack size to 16000000.
cpu time = 1,690 ms, real time = 1,711 ms.
% = [37]
? bnfinit(polcyclo(41)).cyc
  *** bnfinit: Warning: increasing stack size to 16000000.
  *** bnfinit: Warning: increasing stack size to 32000000.
cpu time = 3,329 ms, real time = 3,355 ms.
% = [11, 11]
? bnfinit(polcyclo(43)).cyc
  *** bnfinit: Warning: increasing stack size to 16000000.
  *** bnfinit: Warning: increasing stack size to 32000000.
  *** bnfinit: Warning: increasing stack size to 64000000.
cpu time = 6,524 ms, real time = 6,646 ms.
% = [211]
? bnfinit(polcyclo(47)).cyc
```

[*] *stack*

```
  *** bnfinit: Warning: increasing stack size to 16000000.
  *** bnfinit: Warning: increasing stack size to 32000000.
  *** bnfinit: Warning: increasing stack size to 64000000.
  *** bnfinit: Warning: increasing stack size to 128000000.
cpu time = 12,276 ms, real time = 12,435 ms.
% = [695]
```

▲

Otras funciones útiles:

- `bnfisprincipal(K,a)` — verifica si el ideal $\mathfrak{a}$ es principal en $\mathcal{O}_K$. La salida será un vector `[e,t]`, donde $e = 0$ si y solamente si $\mathfrak{a}$ es principal (es decir, $[\mathfrak{a}] = [\mathcal{O}_K]$).
- `bnfisintnorm(K,n)` — devuelve todos los elementos $\alpha \in \mathcal{O}_K$ con $N_{K/\mathbb{Q}}(\alpha) = n$, módulo unidades $u \in \mathcal{O}_K^\times$ con $N_{K/\mathbb{Q}}(u) = +1$.

5.19.4. Ejemplo. Supongamos que nos interesa el grupo de clases de $K = \mathbb{Q}(\sqrt{-6})$. Calculemos la cota de Minkowski y factorizaciones de ideales primos correspondientes.

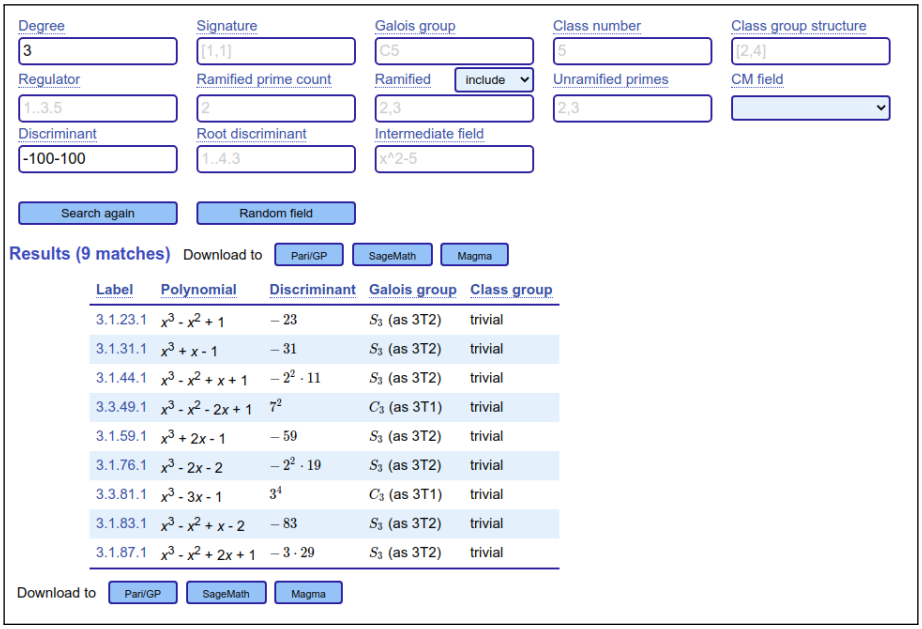
```
? K = bnfinit(x^2+6);
? 2/Pi * sqrt(abs(K.disc))
% = 3.1187872049347044316234722010930270438
? P2 = idealprimedec(K,2)[1]
% = [2, [0, 1]~, 2, 1, [0, -6; 1, 0]]
? P3 = idealprimedec(K,3)[1]
% = [3, [0, 1]~, 2, 1, [0, -6; 1, 0]]
? bnfisprincipal(K,P2)
% = [[1]~, [-1, 0]~]
? bnfisprincipal(K,P3)
% = [[1]~, [0, 1/2]~]
? bnfisintnorm(K,2)
% = []
? bnfisintnorm(K,3)
% = []
? bnfisprincipal(K,idealdiv(K,P2,P3))
% = [[0]~, [0, -1/3]~]
```

Aquí arriba de 2 y 3 están ideales primos $\mathfrak{p}_2$ y $\mathfrak{p}_3$ respectivamente. Verificamos que estos no son principales. El motivo: en $\mathcal{O}_K$ no hay elementos de norma 2 y 3. Luego verificamos que el ideal $\mathfrak{p}_2\,\mathfrak{p}_3^{-1}$ sí es principal; es decir, $[\mathfrak{p}_2] = [\mathfrak{p}_3]$. ▲

Recomiendo que el lector revise la documentación para más detalles y otras funciones.

5.20 LMFDB

Un recurso indispensable para la teoría de números experimental y computacional es *L-functions and Modular Forms Database*, lmfdb.org. Allí en particular en la sección «Number Fields» se pueden buscar los campos de números con los invariantes precalculados. Véase la página https://www.lmfdb.org/NumberField/



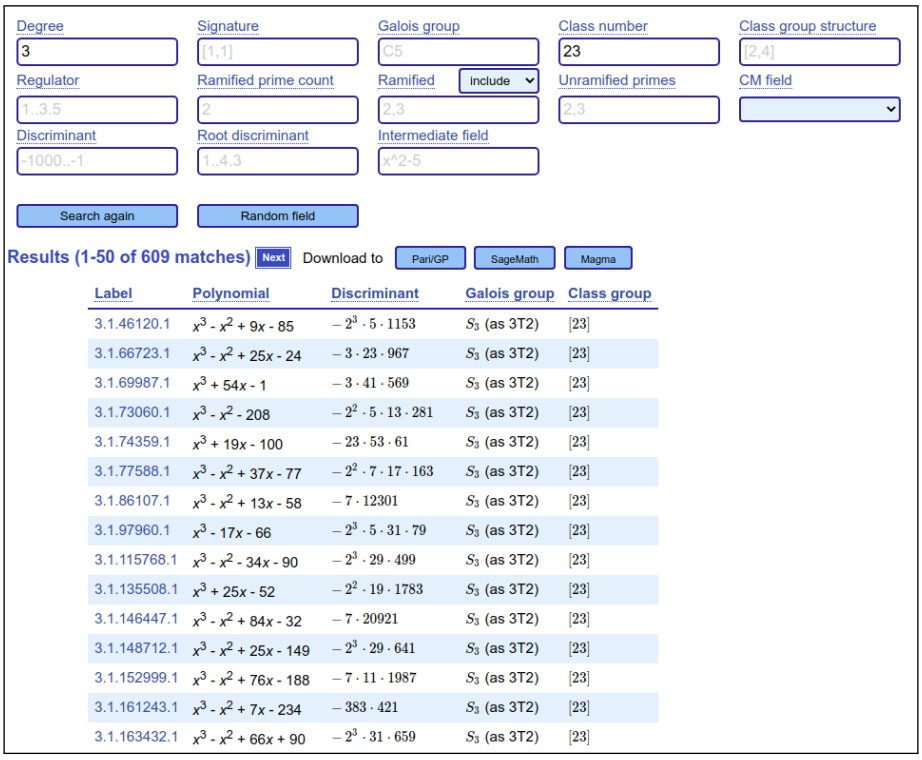


Figura 5.7: Ejemplos de búsqueda en LMFDB: la lista completa de campos cúbicos con $|\Delta_K| \leq 100$ y algunos campos cúbicos con $\mathrm{Cl}(K) \cong \mathbb{Z}/23\mathbb{Z}$

Conclusión

En este capítulo investigamos los invariantes más importantes de un campo de números $K/\mathbb{Q}$: el grupo de clases $\mathrm{Cl}(K)$ y el grupo de unidades $\mathcal{O}_K^\times$. Probamos que $\mathrm{Cl}(K)$ es un grupo finito, mientras que $\mathcal{O}_K^\times$ es finitamente generado de rango $r_1 + r_2 - 1$. En general, no es fácil encontrar generadores explícitos para $\mathcal{O}_K^\times$, pero vimos cómo hacerlo en el caso especial cuando $K = \mathbb{Q}(\sqrt{d})$ es un campo cuadrático real. El siguiente capítulo será dedicado a los métodos analíticos, en particular la **función zeta de Dedekind** $\zeta_K(s)$. La última nos ayudará a relacionar $\mathrm{Cl}(K)$ con $\mathcal{O}_K^\times$, mediante la **fórmula analítica del número de clases**, que es otro resultado fundamental descubierto por Dirichlet (en el caso de campos cuadráticos, y luego generalizado a todo $K/\mathbb{Q}$ por Dedekind).

Ejercicios

Ejercicio 5.1. Demuestre que si G es un grupo topológico Hausdorff, entonces todo subgrupo discreto $H \subset G$ es cerrado.

Ejercicio 5.2. Demuestre directamente que $\mathbb{Z}[\sqrt{2}]$ no es un subgrupo discreto de $\mathbb{R}$.

Ejercicio 5.3. Demuestre que si X es un conjunto convexo simétrico compacto tal que $\operatorname{vol} X = 2^n \cdot \operatorname{covol} \Lambda$, entonces $X \cap \Lambda \neq \{0\}$.

Ejercicio 5.4. Demuestre que para todo primo p existen $m, n \in \mathbb{Z}$ tales que $m^2 + n^2 + 1 \equiv 0 \pmod{p}$.

Ejercicio 5.5. Demuestre que

$$a_n = \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n$$

crece con n.

Ejercicio 5.6. Para $t > 0$ consideremos el conjunto convexo simétrico

$$X_t = \{(x_\tau)_\tau \in K_{\mathbb{R}} \mid |x_\tau| < t \text{ para todo } \tau\}.$$

Calcule que

$$\operatorname{vol}(X_t) = 2^{r_1} (2\pi)^{r_2} t^n.$$

Ejercicio 5.7. Supongamos que $d = p_1 \cdots p_s$, donde $s > 1$ y los p_i son diferentes primos y consideremos el campo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-d})$. Demuestre que los ideales correspondientes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \subset \mathcal{O}_K$ generan un subgrupo en $\mathrm{Cl}(K)$ isomorfo a $(\mathbb{Z}/2\mathbb{Z})^{s-1}$.

Ejercicio 5.8. Calcule los grupos de clases de campos

$$\mathbb{Q}(\sqrt{-110}), \quad \mathbb{Q}(\sqrt{-127}), \quad \mathbb{Q}(\sqrt{33}), \quad \mathbb{Q}(\sqrt[3]{19}), \quad \mathbb{Q}(\sqrt{-3}, \sqrt{-5}).$$

Ejercicio 5.9. Sea $K/\mathbb{Q}$ un campo de números. Demuestre que para cualquier ideal $I \subset \mathcal{O}_K$ existe una extensión finita L/K tal que el ideal correspondiente $I\mathcal{O}_L$ es principal.
(Use que $[I]$ tiene orden finito en $\mathrm{Cl}(K)$.)

Ejercicio 5.10. Consideremos una sucesión exacta corta de R-módulos

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

1) Demuestre que si M'' es un R-módulo libre, entonces el homomorfismo p admite una **sección** $s\colon M'' \to M$ tal que $p \circ s = id_{M''}$.

2) Demuestre si existe una sección s como arriba, entonces $M' \oplus M'' \cong M$.

Ejercicio 5.11. Encuentre el número cuadrático α tal que $\alpha = [3, \overline{2, 1}]$.

Ejercicio 5.12. Demuestre que si $\alpha = [a_0, a_1, a_2, \ldots]$, entonces $\frac{1}{\alpha} = [0, a_0, a_1, a_2, \ldots]$. Concluya que si las fracciones parciales para α y $\frac{1}{\alpha}$ son $\frac{p_n}{q_n}$ y $\frac{p'_n}{q'_n}$ respectivamente, entonces $\frac{p'_n}{q'_n} = \frac{q_{n-1}}{p_{n-1}}$.

Ejercicio 5.13. Encuentre las fracciones continuas para $\sqrt{n^2+1}$, $\sqrt{n\,(n+1)}$, $\sqrt{m^2\,n^2+n}$.

Ejercicio 5.14. Describa el grupo de unidades $\mathcal{O}_K^\times$ para $K = \mathbb{Q}(\sqrt{29})$ (justifique todos los cálculos sin usar las tablas).

Capítulo 6

Función zeta de Dedekind

Clase 25
11/11/20

Para un campo de números $K/\mathbb{Q}$, la **función zeta de Dedekind** correspondiente es una especie de función generatriz definida por la serie

$$\zeta_K(s) = \sum_{I \neq 0} \frac{1}{N_{K/\mathbb{Q}}(I)^s},$$

donde la suma se toma sobre los ideales enteros no nulos $I \subseteq \mathcal{O}_K$. Resulta que la función zeta de Dedekind codifica mucha información aritmética sobre K. Nos interesará $\zeta_K(s)$ como un objeto analítico, y en particular hay que ver la convergencia de la serie.

Primero notamos que si $K = \mathbb{Q}$, entonces los ideales no nulos en $\mathcal{O}_K = \mathbb{Z}$ tienen forma $n\mathbb{Z}$ para $n = 1, 2, 3, \ldots$, así que $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ es la función zeta de Riemann.

6.0.1. Lema. *La serie* $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$ *converge absolutamente para* $\operatorname{Re} s > 1$*, y se tiene*

$$\lim_{s \to 1^+} (s-1)\,\zeta(s) = 1.$$

Demostración. Primero, notamos que $|1/n^s| = 1/n^{\operatorname{Re} s}$, así que será suficiente establecer la convergencia para $s > 1$ real. Tenemos

$$\int_n^{n+1} \frac{dx}{x^s} \leq \frac{1}{n^s} \leq \int_{n-1}^{n} \frac{dx}{x^s},$$

donde la primera desigualdad se cumple para $n \geq 1$ y la segunda para $n \geq 2$ (véase la figura 6.1). Tomando la suma sobre $n \geq 1$, nos sale la desigualdad

$$\int_1^{\infty} \frac{dx}{x^s} \leq \zeta(s) \leq 1 + \int_1^{\infty} \frac{dx}{x^s}.$$

Ahora, dado que $\int_1^{\infty} \frac{dx}{x^s} = \frac{1}{s-1}$, tenemos

$$\frac{1}{s-1} \leq \zeta(s) \leq \frac{s}{s-1},$$

y luego

$$1 \leq (s-1)\,\zeta(s) \leq s.$$

Esto establece la convergencia y también calcula $(s-1)\,\zeta(s)$ para $s \to 1^+$. ∎

Ahora podemos probar la convergencia de $\zeta_K(s)$.

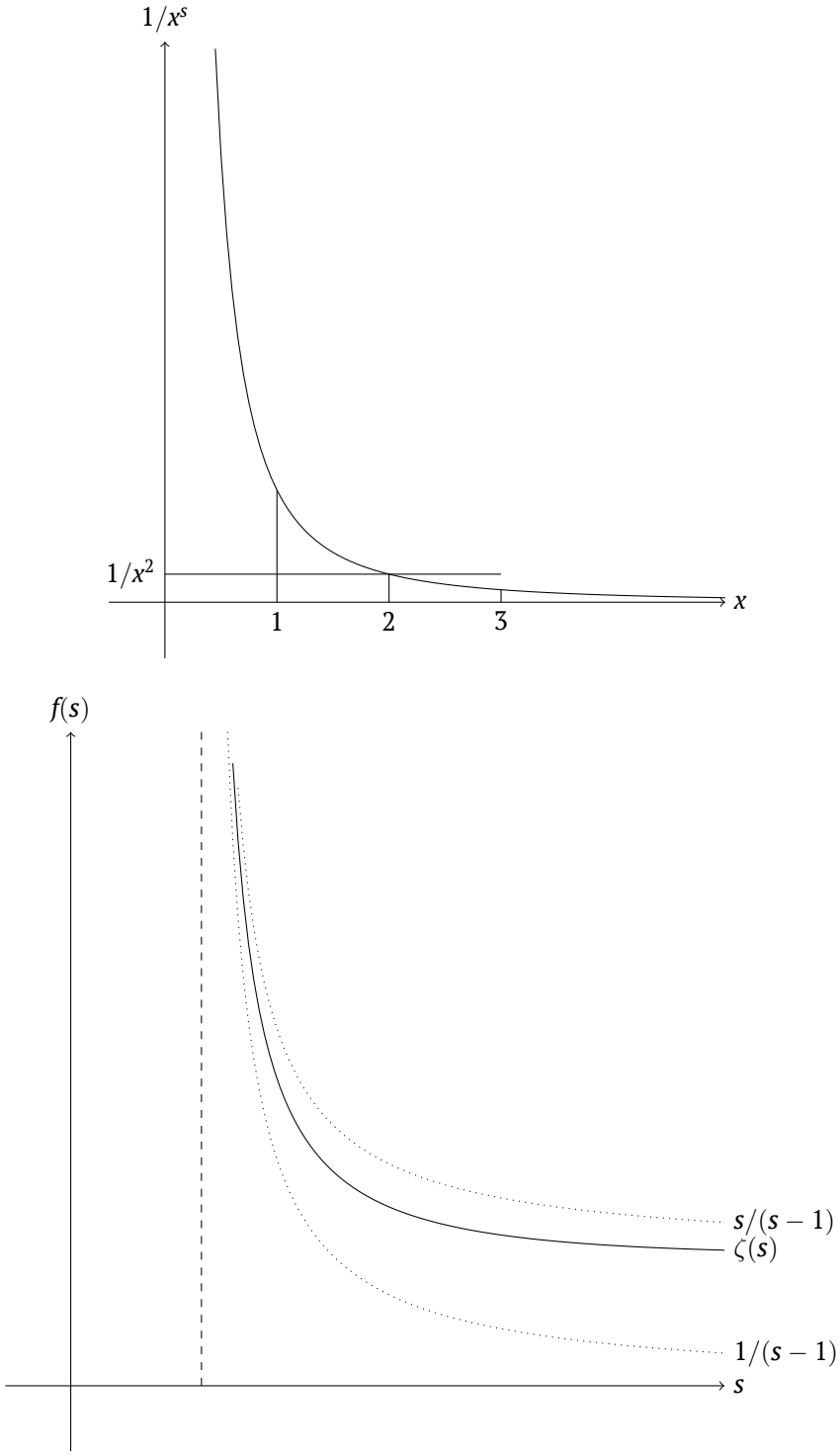


Figura 6.1: Demostración de 6.0.1

6.0.2. Proposición. *La serie* $\zeta_K(s) = \sum_{I\neq 0} \frac{1}{N_{K/\mathbb{Q}}(I)^s}$ *converge absolutamente para* $\operatorname{Re} s > 1$. *Además, se cumple la* ***fórmula del producto de Euler***

$$\sum_{I\neq 0} \frac{1}{N_{K/\mathbb{Q}}(I)^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

donde el producto es sobre todos los ideales primos (no nulos) $\mathfrak{p} \subset \mathcal{O}_K$.

Demostración. De nuevo, la convergencia absoluta para $\operatorname{Re} s > 1$ se sigue de la convergencia para $s > 1$ real. Será suficiente probar la convergencia absoluta del producto de Euler

$$\prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

y luego,

$$\prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \sum_{e\geq 0} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p}^e)^s} = \sum_{I\neq 0} \frac{1}{N_{K/\mathbb{Q}}(I)^s}.$$

Aquí hemos usado la serie geométrica, la multiplicatividad de la norma, y que todo ideal entero no nulo $I \subseteq \mathcal{O}_K$ tiene factorización única en ideales primos $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$.

Un producto $\prod_{n\geq 1}(1 + |x_n|)$ converge si y solamente si la serie $\sum_{n\geq 1} |x_n|$ converge. Entonces, la convergencia del producto de Euler se sigue de la convergencia de $\prod_{\mathfrak{p}}(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s})$, y luego de $\sum_{\mathfrak{p}} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s}$.

Recordemos que para todo primo racional p, existen $\leq [K : \mathbb{Q}]$ ideales primos $\mathfrak{p} \mid p$, y luego para cada uno de estos se tiene $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f \geq p$. Entonces,

$$\sum_{\mathfrak{p}} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s} = \sum_{p} \sum_{\mathfrak{p}\mid p} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s} \leq \sum_{p} \frac{[K : \mathbb{Q}]}{p^s} < [K : \mathbb{Q}]\, \zeta(s).$$

Aquí hemos usado la convergencia de la función zeta de Riemann. ∎

6.1 Ejemplo: la función zeta de $\mathbb{Q}(i)$

Tomemos $K = \mathbb{Q}(i)$. Para entender cómo se ve la función zeta correspondiente $\zeta_K(s)$, sería más fácil trabajar con el producto de Euler

$$\prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}.$$

Los primos en $\mathcal{O}_K = \mathbb{Z}[i]$ son los siguientes.

- Al primo ramificado $p = 2$ corresponde un ideal primo $\mathfrak{p}_2$ de norma 2.
- Si $p \equiv 1 \pmod 4$, entonces p se escinde en dos ideales primos $\mathfrak{p}$ y $\overline{\mathfrak{p}}$, cada uno de norma p.
- Si $p \equiv 3 \pmod 4$, entonces p es inerte y corresponde a un ideal primo $\mathfrak{p}$ de norma p^2.

Entonces,

$$\zeta_K(s) = \frac{1}{1 - 2^{-s}} \prod_{p\equiv 1\ (4)} \frac{1}{(1 - p^{-s})^2} \prod_{p\equiv 1\ (4)} \frac{1}{1 - p^{-2s}}.$$

Notamos que $\frac{1}{1-p^{-2s}} = \frac{1}{1-p^{-s}} \frac{1}{1+p^{-s}}$, así que

$$\zeta_K(s) = \prod_{p} \frac{1}{1 - p^{-s}} \prod_{p} \frac{1}{1 - \chi(p)\, p^{-s}},$$

donde

$$\chi(p) = \begin{cases} +1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

Este es un **carácter de Dirichlet** mód 4, y a este se asocia la **serie L de Dirichlet** correspondiente

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)\,p^{-s}} = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

Entonces, se tiene

$$\zeta_K(s) = \zeta(s)\,L(s,\chi).$$

Invito que el lector revise el apéndice D para más detalles.

Recordamos que $\mathcal{O}_K = \mathbb{Z}[i]$ es un dominio de ideales principales y $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$. Como consecuencia, todo ideal tiene forma $I = (\alpha)$, y para $I \neq 0$ hay precisamente cuatro maneras de escoger un generador α. Si $\alpha = x + yi$, entonces $N_{K/\mathbb{Q}}(I) = x^2 + y^2$. Pongamos

$$C(n) = \#\{(x,y) \in \mathbb{Z}^2 \mid x,y \geq 0,\ x^2+y^2 = n\}.$$

Tenemos entonces una identidad con series de Dirichlet

$$\zeta_K(s) = \sum_{n\geq 1} \frac{C(n)}{n^s} = \Big(\sum_{n\geq 1} \frac{1}{n^s}\Big)\Big(\sum_{n\geq 1} \frac{\chi(n)}{n^s}\Big).$$

Comparando los coeficientes, nos sale

$$C(n) = \sum_{d\mid n} \chi(d).$$

De la multiplicatividad del carácter χ se sigue también que $C(mn) = C(m)\,C(n)$ si m y n son coprimos. Calculando ahora

$$C(p^e) = \begin{cases} 1, & \text{si } p = 2, \\ e+1, & \text{si } p \equiv 1\ (4), \\ 0, & \text{si } p \equiv 3\ (4),\ e \text{ impar}, \\ 1, & \text{si } p \equiv 3\ (4),\ e \text{ par}, \end{cases}$$

se obtiene el siguiente curioso resultado que generaliza el teorema de Fermat sobre los primos de la forma x^2+y^2 (véase 1.6.5).

6.1.1. Teorema. *Supongamos que $n = p_1^{e_1}\cdots p_k^{e_k}$, donde los p_i son diferentes primos.*

- *Si $p_i \equiv 3 \pmod 4$ para algún i y e_i es impar, entonces n no es una suma de dos cuadrados.*
- *En el caso contrario, hay precisamente*

$$C(n) = \prod_{p_i \equiv 1\ (4)} (e_i + 1)$$

representaciones de n como una suma de dos cuadrados x^2+y^2 con $x,y \in \mathbb{N}$ (o $4\,C(n)$ si contamos $x,y \in \mathbb{Z}$ con diferentes signos).

6.1.2. Comentario. Más adelante veremos que para cualquier extensión finita abeliana $K/\mathbb{Q}$ se tiene una descomposición en ciertas series L de Dirichlet

$$\zeta_K(s) = \prod_\chi L(s,\chi).$$

En particular, para el carácter trivial sale el factor $\zeta(s)$. Más adelante veremos que $\zeta_K(s)$ determina la factorización de primos racionales en $\mathcal{O}_K$. La fórmula de arriba significa que *en el caso abeliano* la factorización depende de p mód N para algún N. El caso no-abeliano es más complicado.

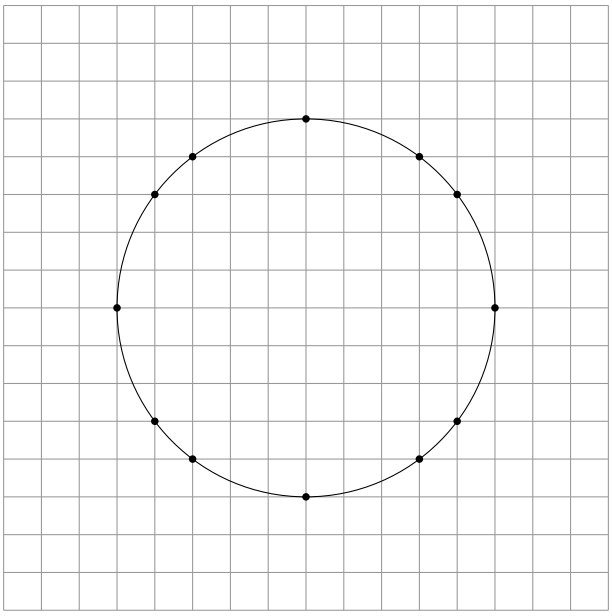


Figura 6.2: 12 puntos enteros en el círculo de radio 5

6.2 Fórmula analítica del número de clases

Nuestro próximo gran objetivo será calcular el residuo en $s = 1$:

$$\lim_{s\to 1^+} (s-1)\,\zeta_K(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\,h_k}{\#\mu_K\,\sqrt{|\Delta_K|}}.$$

Esta fórmula contiene todos los invariantes básicos de K que hemos considerado.

- El número de encajes reales r_1 y el número de pares de encajes complejos r_2.
- El número de clases $h_K = \#\operatorname{Cl}(K)$.
- El número de las raíces de la unidad $\#\mu_K = \#(\mathcal{O}_K^\times)_{tors}$.
- El discriminante Δ_K. Específicamente, aparece $\sqrt{|\Delta_K|}$ que es el covolumen de $\mathcal{O}_K$ realizado como un retículo en el espacio $K_\mathbb{R}$.
- En fin, Reg_K es el **regulador** que, salvo una normalización, corresponde al covolumen de la parte libre del grupo de unidades $\mathcal{O}_K^\times$, realizada como un retículo en el espacio H de dimensión $r_1 + r_2 - 1$. En la siguiente sección vamos a dar una definición más precisa.

Para $K = \mathbb{Q}$ se pone $\operatorname{Reg}_\mathbb{Q} = 1$, y la fórmula se reduce a $\lim_{s\to 1^+}(s-1)\,\zeta(s) = 1$.

La fórmula del número de clases fue descubierta por Dirichlet para el caso de campos cuadráticos, y la versión general es de Dedekind.

6.3 Regulador

Vamos a ver con más detalle qué es el regulador y cómo calcularlo. Recordemos nuestra prueba del teorema de unidades en §5.14 con el encaje logarítmico de $\mathcal{O}_K^\times$. Será conveniente numerar diferentes encajes

$K \hookrightarrow \mathbb{C}$ por

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}},$$

donde los primeros r_1 encajes son reales y el resto son complejos.

Tenemos la aplicación

$$\Phi\colon K^\times \hookrightarrow K_{\mathbb{R}}^\times, \quad \alpha \mapsto (\sigma_i(\alpha))_i,$$

y el encaje logarítmico

$$\ell\colon K_{\mathbb{R}}^\times \to \mathbb{R}^{r_1+r_2}, \quad (z_{\sigma_i}) \mapsto (n_i \log |z_{\sigma_i}|)_i,$$

donde

$$n_i = \begin{cases} 1, & \text{si } 1 \le i \le r_1, \\ 2, & \text{si } r_1 < i \le r_1 + r_2. \end{cases}$$

Esto nos da el diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{O}_K^\times & & \xrightarrow{\quad L \quad} & & H \\ \big\downarrow & & & & \big\downarrow \\ K^\times & \xhookrightarrow{\Phi} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & \mathbb{R}^{r_1+r_2} \\ {\scriptstyle N_{K/\mathbb{Q}}}\big\downarrow & & & & \big\downarrow{\scriptstyle \Sigma} \\ \mathbb{Q}^\times & & \xrightarrow{\log|\cdot|} & & \mathbb{R} \end{array}$$

Hemos probado que la aplicación L realiza la parte libre de $\mathcal{O}_K^\times$ como un retículo de rango completo $r = r_1 + r_2 - 1$ en el subespacio

$$H = \{x \in \mathbb{R}^{r_1+r_2} \mid \sum_i x_i = 0\}.$$

Como consecuencia, $L(u_1), \dots, L(u_r)$ forman una base de H, y podemos completarla a una base de $\mathbb{R}^{r_1+r_2}$ añadiendo el vector

$$L = \frac{1}{\sqrt{r_1 + r_2}}\,(1, \dots, 1) \in \mathbb{R}^{r_1+r_2}.$$

El vector $(1, \dots, 1)$ es ortogonal a H, y con la normalización de arriba, la longitud de L es 1. Esto significa que el covolumen de $L(\mathcal{O}_K^\times)$ en H es igual al volumen del paralelepípedo en $\mathbb{R}^{r_1+r_2}$ generado por los vectores $L, L(u_1), \dots, L(u_r)$; es decir,

$$\operatorname{covol} L(\mathcal{O}_K^\times) = \pm \det \begin{pmatrix} L_1 & L_1(u_1) & L_1(u_2) & \cdots & L_1(u_{r_1+r_2-1}) \\ L_2 & L_2(u_1) & L_2(u_1) & \cdots & L_2(u_{r_1+r_2-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ L_{r_1+r_2} & L_{r_1+r_2}(u_1) & L_{r_1+r_2}(u_2) & \cdots & L_{r_1+r_2-1}(u_{r_1+r_2-1}) \end{pmatrix}$$

Ahora podemos sumar a la i-ésima fila de la matriz de arriba todas las filas. Como resultado, en la i-ésima fila estará el vector

$$(\sqrt{r_1 + r_2}, 0, \dots, 0)$$

—puesto que $L(u_j) \in H$, se tiene $\sum_i L_i(u_j) = 0$. Esto nos lleva al siguiente resultado.

6.3.1. Proposición-definición. *El covolumen del retículo $L(\mathcal{O}_K^\times)$ en H es igual a*

$$\sqrt{r_1 + r_2}\ \operatorname{Reg}_K,$$

donde Reg_K *es el valor absoluto del determinante de cualquier menor de rango $r_1 + r_2 - 1$ de la matriz*

$$(L_i(u_j))_{\substack{1 \le i \le r_1+r_2 \\ 1 \le j \le r_1+r_2-1}} = (n_i \log |\sigma_i(u_j)|)_{\substack{1 \le i \le r_1+r_2 \\ 1 \le j \le r_1+r_2-1}}.$$

El número $\operatorname{Reg}_K > 0$ *se llama el* ***regulador*** *de K.*

Si $\mathcal{O}_K^\times = \mu_K$ es un grupo finito (lo que puede pasar solo si $K = \mathbb{Q}$ o $K = \mathbb{Q}(\sqrt{-d})$ es un campo cuadrático imaginario), entonces se pone $\mathrm{Reg}_K = 1$.

6.3.2. Ejemplo. Si $K = \mathbb{Q}(\sqrt{d})$ es un campo cuadrático real, entonces su regulador será $\log|u|$, donde u es la unidad fundamental de $\mathcal{O}_K^\times$. ▲

6.3.3. Ejemplo. Para el campo $K = \mathbb{Q}(\zeta_7)$ podemos calcular con ayuda de computadora que como unidades fundamentales, se pueden tomar

$$u_1 = 1 + \zeta_7, \quad u_2 = \zeta_7 + \zeta_7^4.$$

En este caso $r_1 = 0$ y $r_2 = 3$. Los encajes complejos, salvo conjugación, serán

$$\sigma_1 \colon \zeta_7 \mapsto \zeta_7, \quad \sigma_2 \colon \zeta_7 \mapsto \zeta_7^2, \quad \sigma_3 \colon \zeta_7 \mapsto \zeta_7^3.$$

Tenemos entonces

$$\mathrm{Reg}_K = \pm \det \begin{pmatrix} 2\log|1+\zeta_7| & 2\log|\zeta_7+\zeta_7^4| \\ 2\log|1+\zeta_7^2| & 2\log|\zeta_7^2+\zeta_7| \end{pmatrix} = 2{,}101818\ldots$$ ▲

6.4 Ejemplos de uso de la fórmula del número de clases

Clase 26
18/11/20

Antes de probar la fórmula, podemos ver algunos ejemplos de su uso. Consideremos el campo cuadrático real $K = \mathbb{Q}(\sqrt{5})$. Argumentando de la misma manera que en §6.1, se demuestra la identidad

$$\zeta_K(s) = \zeta(s)\, L(s,\chi),$$

donde $\chi(n) = \left(\frac{n}{5}\right)$. Ahora $L(s,\chi)$ converge en $s = 1$ a un valor no nulo, mientras que $\lim_{s\to 1^+}(s-1)\,\zeta(s) = 1$, así que

$$\lim_{s\to 1^+}(s-1)\,\zeta_K(s) = L(1,\chi).$$

En general, para el carácter cuadrático $\chi(n) = \left(\frac{n}{p}\right)$ mód p se tiene

$$\exp(g(\chi)\,L(1,\chi)) = \prod_n (1-\zeta_p^n) \prod_r (1-\zeta_p)^{-1},$$

donde

$$g(\chi) = \sum_{1\le a\le p-1} \chi(a)\,\zeta_p^a$$

es la **suma de Gauss**, y los productos son sobre los no-residuos y residuos cuadráticos mód p respectivamente. Para la prueba, véase el ejercicio 6.4.

En nuestro caso calculamos que

$$g(\chi) = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$$

y

$$(1-\zeta_p^2)\,(1-\zeta_5^3)\,(1-\zeta_5)^{-1}\,(1-\zeta_5^4)^{-1} = \frac{3+\sqrt{5}}{2}.$$

Entonces,

$$\lim_{s\to 1^+}(s-1)\,\zeta_K(s) = L(1,\chi) = \frac{1}{\sqrt{5}}\,\log\frac{3+\sqrt{5}}{2}. \tag{6.1}$$

El regulador en este caso será igual a $\log u$, donde $u = \frac{1+\sqrt{5}}{2}$ es la unidad fundamental de $\mathcal{O}_K^\times$. Tenemos $r_1 = 2$, $r_2 = 0$ y $\mu_K = \{\pm 1\}$, $\Delta_K = 5$, y la fórmula del número de clases nos da entonces

$$\lim_{s\to 1^+}(s-1)\,\zeta_K(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\,\mathrm{Reg}_K\,h_K}{\#\mu_K\,\sqrt{|\Delta_K|}} = \frac{1}{\sqrt{5}}\,h_K \cdot 2\,\log\frac{1+\sqrt{5}}{2}. \tag{6.2}$$

En fin,

$$2\,\log\frac{1+\sqrt{5}}{2}=\log\left(\frac{1+\sqrt{5}}{2}\right)^2=\log\frac{3+\sqrt{5}}{2}.$$

Comparando (6.1) y (6.2), podemos concluir que $h_K=1$.

Si $K=\mathbb{Q}[x]/(f)$, entonces para calcular el residuo de $\zeta_K(s)$ en $s=1$ en PARI/GP, basta digitar `lfun(`f`, 1)`. Calculamos el residuo para $K=\mathbb{Q}(\sqrt{10})$.

```
? lfun (x^2 - 10, 1)
% = 1.1500865228483708943221826442284221318*x^-1 + O(x^0)
```

La unidad fundamental en este caso es $u=3+\sqrt{10}$, el discriminante es $\Delta_K=40$, así que

$$\lim_{s\to1^+}(s-1)\,\zeta_K(s)=\frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\,h_k}{\#\mu_K\,\sqrt{|\Delta_K|}}=\frac{2}{\sqrt{40}}\,\log(3+\sqrt{10})\cdot h_K.$$

```
? 2 / sqrt (40) * log (3 + sqrt(10))
% = 0.57504326142418544716109132211421106589
? polcoef (lfun (x^2 - 10, 1), -1) / %
% = 2.0000000000000000000000000000000000000
```

Esto nos permite concluir que $h_K=2$.

De hecho, en este caso también se puede ocupar una descomposición $\zeta_K(s)=\zeta(s)\,L(s,\chi)$ para cierto carácter de Dirichlet χ (véase ejercicio 6.3), y luego obtener el valor de $L(1,\chi)$, pero no quiero entrar en los detalles de este cálculo.

6.5 Número de clases de $\mathbb{Q}(\sqrt{-p})$

Ahora vamos a aplicar la fórmula del número de clases a campos cuadráticos imaginarios $K=\mathbb{Q}(\sqrt{-d})$. En particular, tomemos $d=p$ primo, $p>3$ y $p\equiv3\pmod 4$. En este caso $\Delta_K=-p$, $\mathcal{O}_K^\times=\mu_K=\{\pm1\}$, y $Reg_K=1$. Tenemos entonces

$$\lim_{s\to1^+}(s-1)\,\zeta_K(s)=\frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\,h_k}{\#\mu_K\,\sqrt{|\Delta_K|}}=\frac{\pi}{\sqrt{p}}\,h_K.$$

Notamos que bajo nuestra hipótesis de que $p\equiv3\pmod 4$, la factorización de un primo racional q en $\mathcal{O}_K$ depende del símbolo de Legendre $\left(\frac{q}{p}\right)$, y como en §6.1 se demuestra la identidad

$$\zeta_K(s)=\zeta(s)\,L(s,\chi),$$

donde $\chi(n)=\left(\frac{n}{p}\right)$. Esto implica que

$$\lim_{s\to1^+}(s-1)\,\zeta_K(s)=L(1,\chi),$$

y luego

$$h_K = \frac{\sqrt{p}}{\pi} L(1,\chi).$$

Podemos de nuevo ocupar la fórmula

$$\exp(g(\chi)\, L(1,\chi)) = \prod_n (1-\zeta_p^n) \prod_r (1-\zeta_p)^{-1}.$$

Usando el lema 1.4.10 sobre las sumas cuadráticas de Gauss, tenemos

$$g(\chi) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & p \equiv 3 \pmod 4. \end{cases}$$

De hecho, el famoso cálculo de Gauss dice que el signo es $+1$ en ambos casos. Para la prueba, véase por ejemplo [IR1990, Chapter 6]. De todos modos, estamos calculando h_K que es un número positivo, así que el signo no es tan relevante y podríamos determinarlo al final del cálculo.

Tomando los logaritmos, se obtiene (módulo $2\pi i\mathbb{Z}$)

$$L(1,\chi) = -\frac{1}{i\sqrt{p}} \sum_{1\le a\le p-1} \chi(a)\, \log(1-\zeta_p^a).$$

Nos interesa la suma

$$S_\chi = -\sum_{1\le a\le p-1} \chi(a)\, \log(1-\zeta_p^a).$$

Notamos que $\chi(-1) = -1$ (usando la hipótesis $p \equiv 3 \pmod 4$), así que podemos escribir

$$2S_\chi = \sum_{1\le a\le p-1} \chi(a) \left(\log(1-\zeta_p^{-a}) - \log(1-\zeta_p^a) \right) = \sum_{1\le a\le p-1} \chi(a)\, \log \frac{1-\zeta_p^{-a}}{1-\zeta_p^a}.$$

Aquí

$$\log \frac{1-\zeta_p^{-a}}{1-\zeta_p^a} = \log(-\zeta_p^{-a}) = \log \exp\left(\pi i - \frac{2\pi i a}{p} \right) = 2\pi i \left(\frac{1}{2} - \frac{a}{p} \right).$$

Entonces,

$$S_\chi = -\frac{\pi i}{p} \sum_{1\le a\le p-1} \chi(a)\, a,$$

y luego

$$h_K = \frac{\sqrt{p}}{\pi} L(1,\chi) = \frac{\sqrt{p}}{\pi} \frac{1}{i\sqrt{p}} S_\chi = -\frac{1}{p} \sum_{1\le a\le p-1} \chi(a)\, a.$$

Esta expresión todavía puede ser simplificada.

6.5.1. Lema. *Sea p un primo, $p > 3$ tal que $p \equiv 3 \pmod 4$. Entonces, para el carácter $\chi(a) = \left(\frac{a}{p}\right)$ se tiene*

$$\frac{1}{p} \sum_{1\le a\le p-1} \chi(a)\, a = \begin{cases} -\frac{1}{3} \sum\limits_{1\le a<p/2} \chi(a), & \text{si } p \equiv 3 \pmod 8, \\ -\sum\limits_{1\le a<p/2} \chi(a), & \text{si } p \equiv 7 \pmod 8 \end{cases}$$

Demostración. Pongamos

$$C = \frac{1}{p} \sum_{1\le a\le p-1} \chi(a)\, a.$$

Podemos escribir (recordamos que $p \equiv 3 \pmod 4$, así que $\chi(-1) = -1$)

$$pC = \sum_{1\le a\le p-1} \chi(a)\, a = \sum_{1\le a<p/2} \chi(a)\, a + \sum_{1\le a<p/2} \chi(p-a)\,(p-a)$$
$$= 2 \sum_{1\le a<p/2} \chi(a)\, a - p \sum_{1\le a<p/2} \chi(a). \quad (6.3)$$

Por otra parte,

$$pC = \sum_{1\le a\le p-1} \chi(a)\, a = \sum_{\substack{1\le a\le p-1 \\ a \text{ par}}} \chi(a)\, a + \sum_{\substack{1\le a\le p-1 \\ a \text{ par}}} \chi(p-a)\,(p-a) =$$
$$\sum_{1\le a<p/2} \chi(2a)\, 2a + \sum_{1\le a<p/2} \chi(p-2a)\,(p-2a) =$$
$$= 4\,\chi(2) \sum_{1\le a<p/2} \chi(a)\, a - p\,\chi(2) \sum_{1\le a<p/2} \chi(a). \quad (6.4)$$

Ahora comparando (6.3) y (6.4), nos sale

$$C\,(2\chi(2) - 1) = -\chi(2) \sum_{1\le a<p/2} \chi(a).$$

Recordamos que

$$\chi(2) = \begin{cases} -1, & p \equiv 3 \pmod 8, \\ +1, & p \equiv 7 \pmod 8. \end{cases}$$

■

Nuestros cálculos nos llevan entonces al siguiente resultado (que ya fue mencionado en §5.8).

6.5.2. Teorema (Dirichlet). *Sea $p > 3$ un primo tal que $p \equiv 3 \pmod 4$. Consideremos el campo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-p})$. Si $p \equiv 7 \pmod 8$, entonces*

$$h_K = \sum_{1\le a<p/2} \left(\frac{a}{p}\right),$$

y si $p \equiv 3 \pmod 8$, entonces

$$h_K = \frac{1}{3} \sum_{1\le a<p/2} \left(\frac{a}{p}\right).$$

6.5.3. Corolario. *Si $p \equiv 3 \pmod 4$, entonces el intervalo $[1, (p-1)/2]$ contiene más residuos que no-residuos cuadráticos.*

La fórmula de arriba implica una cota lineal sobre h_K en términos de p. De hecho, para las sumas de caracteres existen cotas mejores, no triviales.

6.5.4. Proposición (Pólya–Vinogradov). *Para el carácter $\chi = \left(\frac{\cdot}{p}\right)$ tenemos*

$$\left| \sum_{m\le t\le n} \chi(t) \right| < \sqrt{p}\,\log p$$

para cualesquiera m y n.

Demostración. Según el lema 1.4.9 se cumple

$$\chi(t)\, g(\chi) = g_t(\chi),$$

donde

$$g_t(\chi) = \sum_{1\le a\le p-1} \chi(t)\, \zeta_p^{at},$$

y en particular $g(\chi) = g_1(\chi)$. Ahora

$$\sum_{m\le t\le n} \chi(t) = \frac{1}{g(\chi)} \sum_{m\le t\le n} g_t(\chi) = \frac{1}{g(\chi)} \sum_{m\le t\le m+k} g_t(\chi),$$

donde $k \le p$ (usando que $\sum_{1\le t\le p-1} \chi(t) = 0$). Vamos a analizar la expresión

$$\Big|\sum_{m\le t\le m+k} g_t(\chi)\Big| = \Big|\sum_{m\le t\le m+k} \sum_{1\le a\le p-1} \chi(a)\zeta_p^{at}\Big| = \Big|\sum_{1\le a\le p-1} \chi(a) \sum_{m\le t\le m+k} \zeta_p^{at}\Big| = \left|\sum_{1\le a\le p-1} \chi(a)\zeta_p^{am}\, \frac{\zeta_p^{a\,(k+1)} - 1}{\zeta_p^a - 1}\right|.$$

Ocuparemos la cota

$$\Big|\sum_{m\le t\le m+k} g_t(\chi)\Big| \le \sum_{1\le a\le p-1} \left|\frac{\zeta_p^{a\,(k+1)} - 1}{\zeta_p^a - 1}\right|.$$

Notamos que

$$|\zeta_p^{a\,(k+1)} - 1| \le 2, \quad |\zeta_p^a - 1| = 2\left|\operatorname{sen}\left(\frac{a\pi}{p}\right)\right|.$$

Además,

$$\left|\operatorname{sen}\left(\frac{a\pi}{p}\right)\right| = \left|\operatorname{sen}\left(\frac{(p-a)\,\pi}{p}\right)\right|.$$

Juntando todo esto, se obtiene

$$\Big|\sum_{m\le t\le m+k} g_t(\chi)\Big| \le \sum_{1\le a\le p-1} \left|\frac{1}{\operatorname{sen}\left(\frac{a\pi}{p}\right)}\right| = 2 \sum_{1\le a\le \frac{p-1}{2}} \left|\frac{1}{\operatorname{sen}\left(\frac{a\pi}{p}\right)}\right|.$$

Usando la desigualdad $\operatorname{sen} x \ge \frac{2}{\pi}\, x$ para un ángulo agudo x, obtenemos la cota

$$\Big|\sum_{m\le t\le m+k} g_t(\chi)\Big| \le 2 \sum_{1\le a\le \frac{p-1}{2}} \frac{1}{\frac{2}{\pi}\frac{a\pi}{p}} = p \sum_{1\le a\le \frac{p-1}{2}} \frac{1}{a} \le p\, \log p.$$

Aquí la última desigualdad viene de $\log p = \int_1^p \frac{dx}{x}$. En fin,

$$\Big|\sum_{m\le t\le n} \chi(t)\Big| = \frac{1}{|g(\chi)|}\Big|\sum_{m\le t\le m+k} g_t(\chi)\Big| \le \frac{1}{\sqrt{p}}\, p\, \log p = \sqrt{p}\, \log p. \qquad \blacksquare$$

6.5.5. Comentario. En general, para cualquier carácter de Dirichlet χ mód N la suma de caracteres puede ser acotada como $O(\sqrt{N}\log N)$. Bajo la hipótesis de Riemann generalizada, esta cota se generaliza a $O(\sqrt{N}\log\log N)$.

6.5.6. Comentario. En general, para *cualquier* campo cuadrático $K = \mathbb{Q}(\sqrt{d})$ (imaginario o real) se puede definir un carácter χ módulo $|\Delta_K|$ que gobierna la factorización de primos en $\mathcal{O}_K$ y nos lleva a la fórmula

$$\zeta_K(s) = \zeta(s)\, L(s,\chi)$$

—véase ejercicio 6.3. Luego los métodos parecidos a los de arriba nos permiten calcular h_K en términos de $L(1,\chi)$ (y $\log u$ para la unidad fundamental u en el caso de campos reales). Para los detalles, véase [BS1966, Chapter 5].

6.6 Demostración de la fórmula del número de clases

Clase 27
23/11/20

El objetivo de esta sección será probar la fórmula analítica del número de clases

$$\lim_{s\to 1^+}(s-1)\,\zeta_K(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\,h_k}{\#\mu_K\,\sqrt{|\Delta_K|}}.$$

La prueba es algo larga y técnica, así que al principio explicaré la estrategia general, omitiendo algunos detalles técnicos. Mi referencia es [BS1966].

Primero vamos a partir $\zeta_K(s)$ en h_K series

$$\zeta_K(s) = \sum_{I\neq 0}\frac{1}{N_{K/\mathbb{Q}}(I)^s} = \sum_{c\in \mathrm{Cl}(K)}\zeta_c(s), \quad \text{donde } \zeta_c(s) = \sum_{[I]=c}\frac{1}{N_{K/\mathbb{Q}}(I)^s}.$$

A continuación veremos que cada una de estas series tiene el mismo residuo

$$\lim_{s\to 1^+}(s-1)\,\zeta_c(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K}{\#\mu_K\,\sqrt{|\Delta_K|}}.$$

Esto claramente implicaría la fórmula del número de clases.

Para cada clase $c\in \mathrm{Cl}(K)$ fijemos un ideal entero $I'\subseteq \mathcal{O}_K$ tal que $[I'] = c^{-1}$. Ahora para todo ideal entero $I\subseteq\mathcal{O}_K$ tal que $[I]=c$ se tiene $II' = \alpha\mathcal{O}_K$ para algún $\alpha\in\mathcal{O}_K$ no nulo. Esto nos da una biyección

$$\{I\subseteq\mathcal{O}_K \mid [I]=c\} \leftrightarrow \{\text{ideales principales } \alpha\mathcal{O}_K \mid \alpha\in I'\}.$$

Tenemos $N_{K/\mathbb{Q}}(I)\,N_{K/\mathbb{Q}}(I') = |N_{K/\mathbb{Q}}(\alpha)|$, y entonces

$$\zeta_c(s) = N_{K/\mathbb{Q}}(I')^s \sum_{\substack{0\neq(\alpha)\subseteq\mathcal{O}_K\\ \alpha\in I'}}\frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s}.$$

La suma es sobre todos los ideales principales generados por los elementos $\alpha\in I'$, que es lo mismo que la suma sobre los $\alpha\in I'$ considerados módulo la relación $\sim$.

El grupo de unidades $\mathcal{O}_K^\times$ actúa sobre el espacio complejo $K_\mathbb{C}$ mediante la multiplicación punto por punto

$$u\cdot x = \Phi(u)\,x,$$

y no es difícil ver que esta acción se restringe al subconjunto $K_\mathbb{R}^\times$. Para esta acción se puede obtener una construcción explícita de un dominio fundamental $X\subset K_\mathbb{R}^\times$ en términos de las raíces de la unidad μ_K y las unidades fundamentales $u_1,\dots,u_{r_1+r_2-1}\in\mathcal{O}_K^\times$. La daremos más adelante, y la conclusión será la siguiente.

6.6.1. Teorema. *Existe un subconjunto $X\subset K_\mathbb{R}^\times$ que satisface las siguientes condiciones.*

1) *X es un **cono**: si $x\in X$, entonces $\lambda x\in X$ para todo $\lambda>0$.*
2) *X es un dominio fundamental de la acción de $\mathcal{O}_K^\times$ sobre $K_\mathbb{R}^\times$: para todo punto $y\in K_\mathbb{R}^\times$ existen únicos $u\in\mathcal{O}_K^\times$ y $x\in X$ tales que $y=\Phi(u)\,x$.*
3) *El subconjunto $T=\{x\in X \mid \prod_i |x_i|\le 1\}$ es acotado y se tiene*

$$\operatorname{vol} T = \frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K}{\#\mu_K}. \tag{6.5}$$

Para la construcción de X, véase §6.6.2, y para el cálculo de vol T, refiero a §6.6.3. Por el momento propongo considerar un par de ejemplos particulares cuando $K=\mathbb{Q}(\sqrt{d})$ es un campo cuadrático.

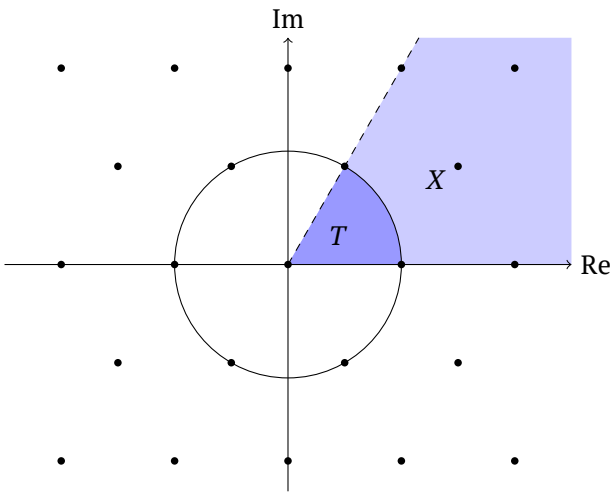
6.6.2. Ejemplo. Consideremos el campo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-3})$. Tenemos un isomorfismo

$$K_{\mathbb{R}} \cong \mathbb{R}^2, \quad (z_\sigma, z_{\overline{\sigma}}) \mapsto (\operatorname{Re} z_\sigma, \operatorname{Im} z_\sigma).$$

El grupo de unidades es $\mathcal{O}_K^\times = \mu_6(\mathbb{C})$. La multiplicación por $\sigma(\zeta_6) = \exp\left(\frac{2\pi i}{6}\right)$ corresponde a la rotación del plano complejo respecto al origen por el ángulo $\pi/3$, y entonces como un dominio fundamental podemos tomar

$$X = \{z \in \mathbb{C} \mid 0 \leq \arg z < \frac{\pi}{3}\}.$$

El conjunto T es la intersección de X con el círculo definido por $|z| = 1$.



El área de T es

$$\operatorname{vol}(T) = 2^{r_2} \operatorname{vol}_{Leb.}(T) = \frac{\pi}{3}.$$

Esto corresponde a la fórmula general $\operatorname{vol} T = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}_K}{\#\mu_K}$. ▲

6.6.3. Ejemplo. Consideremos el campo cuadrático real $K = \mathbb{Q}(\sqrt{3})$. En este caso $K_{\mathbb{R}} \cong \mathbb{R}^2$. El grupo de unidades será

$$\mathcal{O}_K^\times = \{\pm u^n \mid n \in \mathbb{Z}\},$$

donde $u = 2 + \sqrt{3}$ es la unidad fundamental.

Primero podemos ponernos de acuerdo que para $(x, y) \in X$ se tiene $x > 0$. De esta manera se escogen representantes únicos respecto a la acción de $\mu_K = \{\pm 1\}$, y nos queda ver qué sucede con la acción de la parte libre $\langle u \rangle$. Esta viene dada por

$$\Phi(u^n) \cdot (x, y) = ((2 + \sqrt{3})^n x, (2 - \sqrt{3})^n y).$$

Consideremos el encaje logarítmico

$$\ell \colon K_{\mathbb{R}}^\times = (\mathbb{R}^\times)^2 \to \mathbb{R}^2, \quad (x, y) \mapsto (\log|x|, \log|y|).$$

Como una base del subespacio

$$H = \{(x, y) \in \mathbb{R}^2 \mid x + y = 0\}$$

se puede tomar el vector

$$L(u) = (\log(2 + \sqrt{3}), \log(2 - \sqrt{3})).$$

Podemos completarlo a una base de $\mathbb{R}^2$ con el vector $(1,1)$. Todo elemento de $\mathbb{R}^2$ se expresa entonces de manera única como

$$\lambda L(u) + \mu\,(1,1)$$

para algunos $\lambda, \mu \in \mathbb{R}$. En particular, para todo $(x,y) \in K_{\mathbb{R}}^{\times}$

$$\ell(x,y) = (\log|x|, \log|y|) = \lambda L(u) + \mu\,(1,1). \qquad (*)$$

Afirmamos que como dominio fundamental X se pueden tomar los $(x,y) \in K_{\mathbb{R}}^{\times}$ tales que $0 \leq \lambda < 1$ en la expresión de arriba. En efecto, si $(x,y) \in K_{\mathbb{R}}^{\times}$ es cualquier punto tal que $\ell(x,y)$ tiene coordenadas λ y μ en (*), entonces tomamos $n = \lfloor \lambda \rfloor$, y luego

$$\ell(\Phi(u^{-n})\,(x,y)) = L(u^{-n}) + \ell(x,y) = (\underbrace{\lambda - n}_{<1})\,L(u) + \mu\,(1,1).$$

Entonces, cualquier punto de $K_{\mathbb{R}}^{\times}$ puede ser enviado al dominio fundamental X actuando por alguna unidad en $\mathcal{O}_K^{\times}$. Por otra parte, podemos ver que los elementos de X no pueden ser identificados por una acción de $\mathcal{O}_K^{\times}$. Consideremos dos puntos (x,y), $(x',y') \in X$:

$$\ell(x,y) = \lambda L(u) + \mu\,(1,1),$$
$$\ell(x',y') = \lambda' L(u) + \mu'\,(1,1),$$

con $0 \leq \lambda, \lambda' \leq 1$, y supongamos que para algún $n \in \mathbb{Z}$ se tiene

$$\Phi(u^n)\,(x,y) = (x',y').$$

Aplicando el encaje logarítmico ℓ, se obtiene

$$(\lambda + n)\,L(u) + \ell(x,y) = \lambda' L(u) + \ell(x',y'),$$

y entonces

$$\lambda + n = \lambda', \quad \mu + \mu'.$$

Dado que $0 \leq \lambda, \lambda' \leq 1$, esto es posible si y solamente si $n = 0$, pero luego $(x,y) = (x',y')$.

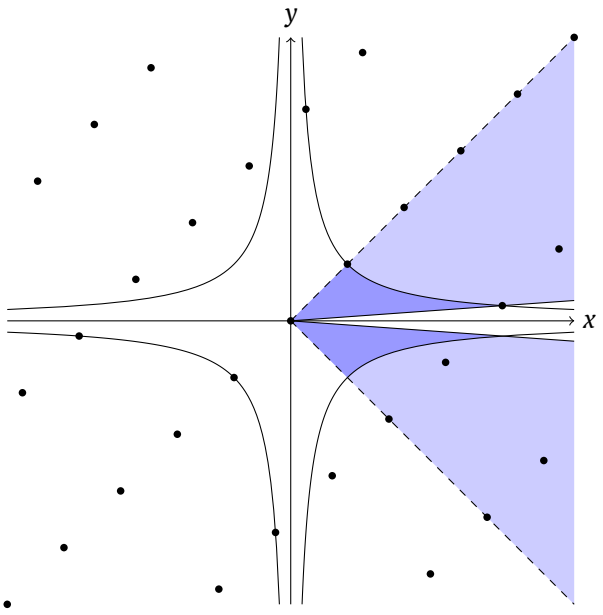
Llegamos a la conclusión que X consiste en los puntos $(x,y) \in K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^2$ tales que

$$\log|x| = \lambda\,\log(2+\sqrt{3}) + \mu,$$
$$\log|y| = \lambda\,\log(2-\sqrt{3}) + \mu,$$

donde $0 \leq \lambda < 1$ y $x > 0$. De aquí es fácil ver que X será la unión de dos conos

$$C_1 = \langle (1,+1),\,(2+\sqrt{3},+2-\sqrt{3})\rangle, \quad C_2 = \langle (1,-1),\,(2+\sqrt{3},-2+\sqrt{3})\rangle.$$

El subconjunto $T \subset X$ está acotado por la curva $xy = \pm 1$.



No es difícil calcular que el área de T es

$$2\int_1^{2+\sqrt{3}} \frac{dx}{x} = 2\log(2+\sqrt{3}),$$

lo que corresponde a la fórmula vol $T = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_K}{\#\mu_K}$. ▲

De la parte 2) del teorema 6.6.1 se deduce fácilmente el siguiente resultado.

6.6.4. Corolario. *Para todo $\alpha \in \mathcal{O}_K$ no nulo existe único $\beta \sim \alpha$ tal que $\Phi(\beta) \in X$.*

Demostración. La acción de $\mathcal{O}_K^\times$ sobre $K_\mathbb{R}^\times$ se restringe a una acción sobre $\Lambda \setminus \{0\} = \Phi(\mathcal{O}_K \setminus \{0\})$. ■

Volvamos a nuestra expresión

$$\zeta_c(s) = N_{K/\mathbb{Q}}(I')^s \sum_{\substack{0\neq(\alpha)\subseteq\mathcal{O}_K \\ \alpha\in I'}} \frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s}.$$

Denotemos por Λ el retículo $\Phi(I') \subset K_\mathbb{R}$. Denotemos por $N\colon K_\mathbb{R} \to \mathbb{R}$ el producto de coordenadas $x \mapsto \prod_i x_i$. En este caso $N_{K/\mathbb{Q}}(\alpha) = N(\Phi(\alpha))$. Ocupando el último corolario, podemos escribir entonces

$$\zeta_c(s) = N_{K/\mathbb{Q}}(I')^s \sum_{\omega\in\Lambda\cap X} \frac{1}{|N(\omega)|^s}.$$

Para calcular el residuo de esta serie en $s = 1$, vamos a formular el siguiente teorema general.

6.6.5. Teorema. *Sean X un cono en $(\mathbb{R}^\times)^n$, $F\colon X \to \mathbb{R}_{>0}$ una función positiva, y $\Lambda \subset X$ un retículo de rango completo. Supongamos que se cumplen las siguientes condiciones.*

a) Para cualesquiera $x \in X$ y $\lambda > 0$ se cumple $F(\lambda x) = \lambda^n F(x)$.

b) El subconjunto $T = \{x \in X \mid F(x) \leq 1\}$ es acotado y tiene volumen no nulo.

Entonces, la serie

$$Z(s) = \sum_{\omega \in \Lambda \cap X} \frac{1}{F(x)^s}$$

converge para $s > 1$, y se tiene

$$\lim_{s \to 1^+} (s-1)\, Z(s) = \frac{\operatorname{vol} T}{\operatorname{covol} \Lambda}.$$

Veremos la prueba en §6.6.1. En nuestra situación, podemos aplicar el teorema a la función $F\colon x \mapsto |N(x)|$ sobre $X \subset K_{\mathbb{R}}^{\times}$, y el subconjunto $T \subset X$. Recordamos que el espacio $K_{\mathbb{R}}$ no es precisamente $\mathbb{R}^n$, sino tiene estructura euclidiana ligeramente distinta, respecto a cual $\mathrm{vol} = 2^{r_2}\ \mathrm{vol}_{Leb.}$, pero esto será irrelevante porque nos sale el cociente de dos volúmenes.

Como ya sabemos,

$$\operatorname{covol} \Lambda = \sqrt{|\Delta_K|}\, N_{K/\mathbb{Q}}(I'),$$

y por otra parte, calcularemos que el volumen de T viene dado por (6.5). Esto nos permite concluir que

$$\lim_{s \to 1^+} (s-1)\, \zeta_c(s) = \frac{2^{r_1}\, (2\pi)^{r_2}\ \mathrm{Reg}_K}{\#\mu_K \sqrt{|\Delta_K|}}.$$

Entonces, para terminar la prueba, nos falta lo siguiente:

1) demostrar el teorema 6.6.5 sobre el residuo de $Z(s) = \sum_{\omega \in \Lambda \cap X} \frac{1}{F(x)^s}$ en $s = 1$;
2) obtener una buena descripción para un dominio fundamental $X \subset K_{\mathbb{R}}^{\times}$ de la acción de $\mathcal{O}_K^{\times}$;
3) calcular el volumen (6.5) del subconjunto $T \subset X$.

6.6.1 Conos, retículos y residuo en $s = 1$

Primero vamos a probar el teorema 6.6.5. Tenemos un retículo de rango completo $\Lambda \subset \mathbb{R}^n$ y un cono $X \subset (\mathbb{R}^{\times})^n$ junto con una función $F\colon X \to \mathbb{R}_{>0}$ que es homogénea en el sentido de que

$$F(\lambda x) = \lambda^n F(x).$$

Consideremos el conjunto

$$T = \{x \in X \mid F(x) \leq 1\}$$

que es acotado y de volumen finito no nulo. Nos interesa probar que la serie

$$Z(s) = \sum_{\omega \in \Lambda \cap X} \frac{1}{F(x)^s}$$

converge para $s > 1$ y tiene residuo $\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda}$ en $s = 1$.

El punto clave es una interpretación de volúmenes en términos del conteo de puntos en retículos. Para un parámetro $r > 0$ vamos a considerar el retículo $\frac{1}{r}\Lambda$. Notamos que $\operatorname{covol}\left(\frac{1}{r}\Lambda\right) = \frac{1}{r^n} \operatorname{covol}(\Lambda)$. Definamos

$$C(r) = \#\{\omega \in \frac{1}{r}\Lambda \mid \omega \in T\} = \#\{\omega \in \Lambda \mid \omega \in rT\} = \#\{\omega \in \Lambda \cap X \mid F(\omega) \leq r^n\}.$$

Tenemos entonces

$$\operatorname{vol} T = \lim_{r \to \infty} C(r)\, \operatorname{covol}\left(\frac{1}{r}\,\Lambda\right) = \operatorname{covol} \Lambda\, \lim_{r \to \infty} \frac{C(r)}{r^n}.$$

Podemos ordenar los puntos $\omega \in \Lambda \cap X$ de tal manera que

$$0 < F(\omega_1) \leq F(\omega_2) \leq F(\omega_3) \leq \cdots$$

Pongamos $r_k = \sqrt[n]{F(\omega_k)}$. Tenemos $\{\omega_1, \ldots, \omega_k\} \subseteq r_k\, T$, así que $C(r_k) \geq k$. Por otra parte, para todo $\epsilon > 0$ se tiene $x_k \notin (r_k - \epsilon)\, T$, así que $C(r_k - \epsilon) < k$. Esto nos da la desigualdad

$$C(r_k - \epsilon) < k \leq C(r_k),$$

y luego

$$\frac{C(r_k - \epsilon)}{(r_k - \epsilon)^n} \frac{(r_k - \epsilon)^n}{r_k^n} < \frac{k}{r_k^n} \leq \frac{C(r_k)}{r_k^n}.$$

Pasando al límite $k \to \infty$, tenemos $r_k \to \infty$, y luego

$$\lim_{k\to\infty} \frac{k}{F(\omega_k)} = \frac{\operatorname{vol} T}{\operatorname{covol} \Lambda}.$$

Esto significa que para todo $\epsilon > 0$ se tiene

$$\Big(\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} - \epsilon\Big)\frac{1}{k} < \frac{1}{F(\omega_k)} < \Big(\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} + \epsilon\Big)\frac{1}{k}$$

para todo k suficientemente grande, digamos $k \geq k_0$. Elevando todo a $s > 1$ y sumando sobre $k \geq k_0$, tenemos

$$\Big(\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} - \epsilon\Big)^s \sum_{k\geq k_0} \frac{1}{k^s} < \sum_{k\geq k_0} \frac{1}{F(\omega_k)^s} < \Big(\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} + \epsilon\Big)^s \sum_{k\geq k_0} \frac{1}{k^s}.$$

Aquí

$$\sum_{k\geq k_0} \frac{1}{k^s} = \zeta(s) - \sum_{1\leq k<k_0} \frac{1}{k^s},$$

donde $\zeta(s)$ converge para $s > 1$. Por otra parte, nuestra serie es

$$Z(s) = \sum_{k\geq 1} \frac{1}{F(\omega_k)^s}.$$

Las desigualdades de arriba que se cumplen para todo $\epsilon > 0$ establecen la convergencia de $Z(s)$ para $s > 1$.

Ahora multiplicando la desigualdad por $(s-1)$ y pasando al límite $s \to 1^+$, en vista de la fórmula

$$\lim_{s\to 1^+} (s-1) \sum_{k\geq k_0} \frac{1}{k^s} = \lim_{s\to 1^+} (s-1)\, \zeta(s) = 1,$$

se obtiene

$$\frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} - \epsilon < \liminf_{s\to 1^+} (s-1)\, Z(s) \leq \limsup_{s\to 1^+} (s-1)\, Z(s) < \frac{\operatorname{vol} T}{\operatorname{covol} \Lambda} + \epsilon.$$

Esto se cumple para todo $\epsilon > 0$, así que podemos concluir que

$$\lim_{s\to 1^+} (s-1)\, Z(s) = \frac{\operatorname{vol} T}{\operatorname{covol} \Lambda}.$$

Hemos entonces probado el teorema 6.6.5. ■

6.6.2 Dominio fundamental X de la acción de unidades sobre $K_{\mathbb{R}}^{\times}$

Ahora vamos a probar la primera mitad del teorema 6.6.1 que nos da un cono $X \subset K_{\mathbb{R}}^{\times}$ que es un dominio fundamental de la acción de $\mathcal{O}_K^{\times}$.

Consideremos unidades fundamentales $u_1, \dots, u_r \in \mathcal{O}_K^\times$. Entonces los vectores $L(u_1), \dots, L(u_r)$ forman una base del espacio $H \subset \mathbb{R}^{r_1+r_2}$. Por otra parte, el vector

$$L = (\underbrace{1, \dots, 1}_{r_1}, \underbrace{2, \dots, 2}_{r_2})$$

no está en H, así que los $L(u_i)$ junto con L forman una base de $\mathbb{R}^{r_1+r_2}$: todo $x \in \mathbb{R}^{r_1+r_2}$ puede ser expresado como

$$\lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \lambda L \tag{6.6}$$

para algunos $\lambda_1, \dots, \lambda_r, \lambda \in \mathbb{R}$.

A partir de ahora vamos a denotar por $m = \#\mu_K$ el número de las raíces de la unidad en K.

6.6.6. Definición. Sea $X \subset K_\mathbb{R}^\times$ el subconjunto definido por las siguientes condiciones.

a) Para todo $x \in X$ en la expresión de $\ell(x)$ en la base (6.6) se tiene $0 \le \lambda_i < 1$ para $i = 1, \dots, r$.

b) Se tiene $0 \le \arg x_1 < \frac{2\pi}{m}$.

La condición b) merece alguna explicación. Si K tiene un encaje real, entonces $\mu_K = \{\pm 1\}$ (otras raíces de la unidad no se encajan en $\mathbb{R}$), así que $m = 2$ y la condición b) nos dice simplemente que $x_1 > 0$. En general, la condición b) sirve para tomar en cuenta la acción de $\mu_K = (\mathcal{O}_K^\times)_{tors}$ como en el ejemplo 6.6.2. La condición a) es similar a lo que vimos en el ejemplo 6.6.3.

6.6.7. Proposición. *X es un **cono**: si $x \in X$, entonces $\lambda x \in X$ para todo $\lambda > 0$.*

Demostración. Para $x \in X$ y $\lambda > 0$ tenemos

$$\ell(\lambda x) = \log|\lambda|\, L + \ell(x),$$

y esto no afecta los coeficientes $\lambda_1, \dots, \lambda_r$, así que la condición a) se preserva. Por otra parte, $\arg(\lambda x_1) = \arg x_1$, así que b) se preserva también. Notamos que $X \neq \varnothing$: por ejemplo, el punto $\Phi(1)$ está en X. ■

6.6.8. Proposición. *X es un dominio fundamental de la acción de $\mathcal{O}_K^\times$ sobre $K_\mathbb{R}^\times$: para todo punto $y \in K_\mathbb{R}^\times$ existen únicos $u \in \mathcal{O}_K^\times$ y $x \in X$ tales que $y = \Phi(u)\, x$.*

Demostración. Primero para la existencia, escribamos $\ell(y)$ en términos de nuestra base de $\mathbb{R}^{r_1+r_2}$:

$$\ell(y) = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \lambda L.$$

Para $i = 1, \dots, r$ pongamos

$$\lambda_i = a_i + \mu_i,$$

donde

$$a_i \in \mathbb{Z}, \quad 0 \le \mu_i < 1.$$

Consideremos la unidad $v = u_1^{a_1} \cdots u_r^{a_r}$ y el punto $z = \Phi(v^{-1})\, y$. Ahora

$$\ell(z) = L(v^{-1}) + \ell(y) = -a_1 L(u_1) - \cdots - a_r L(u_r) + \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \lambda L = \mu_1 L(u_1) + \cdots + \mu_r L(u_r) + \lambda L.$$

Esto nos asegura la condición a) de la definición de X, y falta analizar la condición b). Si $\arg z_1 = \phi$, entonces para algún k se tiene

$$\frac{2\pi k}{m} \le \phi < \frac{2\pi k + 1}{m}.$$

Sea $\zeta \in \mu_K$ la m-ésima raíz de la unidad tal que $\sigma_1(\zeta) = \exp\left(\frac{2\pi i}{m}\right)$. En este caso el punto $x = \Phi(\zeta^{-k})\, z$ está en X: primero tenemos

$$\ell(x) = L(\zeta^{-k}) + \ell(z) = \ell(z),$$

dado que $\mu_K = \ker L$, así que la condición a) se preserva. Por otra parte,

$$\arg x_1 = \arg z_1 - \frac{2\pi k}{m} = \phi - \frac{2\pi k}{m},$$

y luego

$$0 \leq \arg x_1 < \frac{2\pi}{m}.$$

Entonces,

$$y = \Phi(v)\, z = \Phi(\zeta^k v)\, x$$

es la representación que estábamos buscando.

Ahora para ver que la representación es única, supongamos que

$$y = \Phi(u)\, x = \Phi(u')\, x'$$

para algunos $u, u' \in \mathcal{O}_K^\times$, $x, x' \in X$. Tomando los logaritmos, se obtiene

$$L(u) + \ell(x) = L(u') + \ell(x').$$

Aquí por nuestra hipótesis

$$\ell(x) = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \lambda L,$$
$$\ell(x') = \lambda_1' L(u_1) + \cdots + \lambda_r' L(u_r) + \lambda' L,$$

donde $0 \leq \lambda_i, \lambda_i' < 1$. Por otra parte,

$$L(u) = a_1 L(u_1) + \cdots + a_r L(u_r),$$
$$L(u') = a_1' L(u_1) + \cdots + a_r' L(u_r),$$

donde $a_i, a_i' \in \mathbb{Z}$. Esto nos permite concluir que $L(u) = L(u')$, así que $u' = \zeta u$ para alguna raíz de la unidad $\zeta \in \mu_K = \ker L$. Ahora $\Phi(u') = \Phi(\zeta)\, \Phi(u)$, y entonces $x = \Phi(\zeta)\, x'$, y en particular $x_1 = \sigma_1(\zeta)\, x_1'$. La condición b) nos dice que

$$0 \leq \arg x_1, \arg x_1' < \frac{2\pi}{m}.$$

Tenemos

$$0 \leq |\sigma_1(\zeta)| < \frac{2\pi}{m},$$

pero $\sigma_1(\zeta)$ es una raíz m-ésima compleja, así que la única opción es $\sigma_1(\zeta) = 1$, y luego $\zeta = 1$. Podemos concluir que $u = u'$ y $x = x'$. ■

6.6.3 Cálculo del volumen de T

Para terminar la prueba de la fórmula del número de clases, tenemos que ver que

$$T = \{x \in X \mid |N(x)| \leq 1\}$$

es un conjunto acotado y calcular su volumen

$$\operatorname{vol} T = \frac{2^{r_1}\, (2\pi)^{r_2}\, \operatorname{Reg}_K}{m}.$$

El cálculo esencialmente consiste en una reducción a ciertas integrales iteradas, lo que no suena muy interesante. Sin embargo, este es precisamente el punto donde aparece el regulador y $m = \#\mu_K$.

6.6.9. Lema. *$T \subset X$ es un conjunto acotado.*

Demostración. Recordemos que $X \subset K_{\mathbb{R}}^{\times}$ es un cono. Todo rayo en X que sale del origen contiene único punto $x \in X$ tal que $|N(x)| = 1$. Ahora si S es el conjunto de tales puntos, entonces $T = \bigcup_{0<\lambda\leq 1} \lambda S$.

Para todo punto $x \in K_{\mathbb{R}}^{\times}$ consideremos

$$\ell(x) = (n_i \log |x_i|)_i = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \lambda L.$$

Calculando la suma de coordenadas de los vectores en la parte derecha e izquierda, nos sale $\log |N(x)| = n(r_1 + 2r_2) = n\lambda$, usando que $L(u_i) \in H$. Podemos entonces escribir

$$\ell(x) = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \frac{1}{n} \log |N(x)|\, L.$$

Ahora si $x \in S$, entonces $\log |N(x)| = 1$, y nos queda

$$\ell(x) = (n_i \log |x_i|)_i = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r),$$

donde $0 \leq \lambda_1 < 1$, puesto que $x \in S \subset X$. Esto nos da una cota sobre los $\log |x_i|$, y luego sobre los x_i. Esto significa que S es acotado, y por ende T también lo es. ■

6.6.10. Lema. *Para toda unidad $u \in \mathcal{O}_K^{\times}$ la transformación $x \mapsto \Phi(u) \cdot x$ sobre $K_{\mathbb{R}}^{\times}$ preserva el volumen.*

Demostración. El determinante de esta transformación será $N(\Phi(u)) = K_{K/\mathbb{Q}}(u) = \pm 1$. ■

En particular, sea $\zeta \in \mu_K$ una raíz de la unidad tal que

$$\sigma_1(\zeta) = \exp\Big(\frac{2\pi i}{m}\Big).$$

Para $k = 0, 1, \ldots, m-1$ consideremos los conjuntos

$$T_k = \Phi(\zeta^k) \cdot T.$$

Tenemos entonces $\mathrm{vol}(T_k) = \mathrm{vol}(T)$. Ahora

$$\begin{gathered} |N(\Phi(\zeta^k) \cdot x)| = |N(x)|, \\ \ell(\Phi(\zeta^k) \cdot x) = \ell(x), \\ \arg(\Phi(\zeta^k) \cdot x)_1 = \arg x_1 + \frac{2\pi k}{m}. \end{gathered}$$

Entonces, cada conjunto T_k está definido por las condiciones

1) $0 < |N(x)| \leq 1$;

2) $\ell(x) = \lambda_1 L(u_1) + \cdots + \lambda_r L(u_r) + \frac{1}{n} \log |N(x)|\, L$, donde $0 \leq \lambda_i < 1$.

3) $\frac{2\pi k}{m} \leq \arg x_1 < \frac{2\pi\,(k+1)}{m}$.

De la condición 3) se ve que los T_k son disjuntos y su unión $\bigcup_{0\leq k\leq m-1} T_k$ está definida por las condiciones 1) y 2). Sea $\overline{T}$ el subconjunto de la unión tal que $x_1, \ldots, x_{r_1} > 0$. Tenemos entonces

$$\mathrm{vol}(T) = \frac{2^{r_1}}{m}\ \mathrm{vol}(\overline{T}) = \frac{2^{r_1+r_2}}{m}\ \mathrm{vol}_{Leb.}(\overline{T}).$$

6.6.11. Proposición. *Se tiene* $\mathrm{vol}_{Leb.}(\overline{T}) = \pi^{r_2}\ \mathrm{Reg}_K$, *y por lo tanto* $\mathrm{vol}(T) = \frac{2^{r_1}\,(2\pi)^{r_2}\ \mathrm{Reg}_K}{m}$.

Demostración. Para $x \in \overline{T}$ se tiene

$$\ell(x)_i = \sum_{1 \le k \le r} \lambda_k L(u_k) + \frac{n_i}{n} \log |N(x)|,$$

donde $n_i = 1$ para las coordenadas que corresponden a encajes reales (es decir, $1 \le i \le r_1$) y $n_i = 2$ para las coordenadas que corresponden a encajes complejos (es decir, $r_1 + 1 \le i \le r_1 + r_2$).

Escribamos las coordenadas de $K_{\mathbb{R}} \cong \mathbb{R}^{r_1+2r_2}$ como

$$(x_1, \dots, x_r, y_1, z_1, \dots, y_{r_2}, z_{r_2}).$$

Hagamos un cambio de variables

$$x_i = \rho_i, \quad y_j = \rho_{r_1+j} \cos \phi_j, \quad z_j = \rho_{r_1+j} \operatorname{sen} \phi_j,$$

donde $1 \le i \le r_1$ y $1 \le j \le r_2$. El jacobiano correspondiente será

$$\left(\begin{array}{ccc|ccccc}
\frac{\partial x_1}{\partial \rho_1} & \cdots & \frac{\partial x_1}{\partial \rho_{r_1}} & \frac{\partial x_1}{\partial \rho_{r_1+1}} & \frac{\partial x_1}{\partial \phi_1} & \cdots & \frac{\partial x_1}{\partial \rho_{r_1+r_2}} & \frac{\partial x_1}{\partial \phi_{r_2}} \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\frac{\partial x_{r_1}}{\partial \rho_1} & \cdots & \frac{\partial x_{r_1}}{\partial \rho_{r_1}} & \frac{\partial x_{r_1}}{\partial \rho_{r_1+1}} & \frac{\partial x_{r_1}}{\partial \phi_1} & \cdots & \frac{\partial x_{r_1}}{\partial \rho_{r_1+r_2}} & \frac{\partial x_{r_1}}{\partial \phi_{r_2}} \\
\hline
\frac{\partial y_1}{\partial \rho_1} & \cdots & \frac{\partial y_1}{\partial \rho_{r_1}} & \frac{\partial y_1}{\partial \rho_{r_1+1}} & \frac{\partial y_1}{\partial \phi_1} & \cdots & \frac{\partial y_1}{\partial \rho_{r_1+r_2}} & \frac{\partial y_1}{\partial \phi_{r_2}} \\
\frac{\partial z_1}{\partial \rho_1} & \cdots & \frac{\partial z_1}{\partial \rho_{r_1}} & \frac{\partial z_1}{\partial \rho_{r_1+1}} & \frac{\partial z_1}{\partial \phi_1} & \cdots & \frac{\partial z_1}{\partial \rho_{r_1+r_2}} & \frac{\partial z_1}{\partial \phi_{r_2}} \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\frac{\partial y_{r_2}}{\partial \rho_1} & \cdots & \frac{\partial y_{r_2}}{\partial \rho_{r_1}} & \frac{\partial y_{r_2}}{\partial \rho_{r_1+1}} & \frac{\partial y_{r_2}}{\partial \phi_1} & \cdots & \frac{\partial y_{r_2}}{\partial \rho_{r_1+r_2}} & \frac{\partial y_{r_2}}{\partial \phi_{r_2}} \\
\frac{\partial z_{r_2}}{\partial \rho_1} & \cdots & \frac{\partial z_{r_2}}{\partial \rho_{r_1}} & \frac{\partial z_{r_2}}{\partial \rho_{r_1+1}} & \frac{\partial z_{r_2}}{\partial \phi_1} & \cdots & \frac{\partial z_{r_2}}{\partial \rho_{r_1+r_2}} & \frac{\partial z_{r_2}}{\partial \phi_{r_2}}
\end{array}\right).$$

Calculándolo con cuidado, nos sale la matriz

$$\left(\begin{array}{ccc|ccccc}
1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 \\
\hline
0 & \cdots & 0 & \cos \phi_1 & -\rho_{r_1+1} \operatorname{sen}(\phi_1) & \cdots & 0 & 0 \\
0 & \cdots & 0 & \operatorname{sen} \phi_1 & +\rho_{r_1+1} \cos(\phi_1) & \cdots & 0 & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \cdots & 0 & 0 & 0 & \cdots & \cos \phi_{r_2} & -\rho_{r_1+r_2} \operatorname{sen}(\phi_{r_2}) \\
0 & \cdots & 0 & 0 & 0 & \cdots & \operatorname{sen} \phi_{r_2} & +\rho_{r_1+r_2} \cos(\phi_{r_2})
\end{array}\right).$$

de determinante $\rho_{r_1+1} \cdots \rho_{r_1+r_2}$.

En términos de nuevas coordenadas, el conjunto $\overline{T} \subset \mathbb{R}^{r_1+2r_2}$ viene dado por

1) $\rho_1, \dots, \rho_{r_1+r_2} > 0$, $\displaystyle\prod_{1 \le i \le r_1+r_2} \rho_i^{e_i} \le 1$;

2) $\log \rho_j^{e_j} = \sum_{1\le k\le r} \lambda_k \,(L(u_k))_j + \frac{e_j}{n} \log \prod_{1\le i\le r_1+r_2} \rho_i^{e_i}$, donde $0 \le \lambda_k < 1$;

3) $0 \le \phi_j < 2\pi$.

Ahora pasemos a otras coordenadas $\lambda_1, \ldots, \lambda_r, \lambda$, definidas por

$$\log \rho_j^{e_j} = \sum_{1\le k\le r} \lambda_k L(u_k)_j + \frac{e_j}{n} \log \lambda.$$

Sumando estas ecuaciones para $j = 1, \ldots, r_1 + r_2$ y notando que $\sum_j e_j = n$ y $\sum_j L(u_k)_j = 0$, se obtiene

$$\lambda = \prod_{1\le j\le r_2+r_2} \rho_j^{e_j}.$$

Entonces, el conjunto $\overline{T}$ está definido por las condiciones

$$0 \le \lambda_k < 1, \quad 0 < \lambda \le 1$$

para $k = 1, \ldots, r$. Calculamos el jacobiano

$$J = \left(\begin{array}{c|ccc} \frac{\partial \rho_1}{\partial \lambda} & \frac{\partial \rho_1}{\partial \lambda_1} & \cdots & \frac{\partial \rho_1}{\partial \lambda_r} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \rho_{r_1}}{\partial \lambda} & \frac{\partial \rho_{r_1}}{\partial \lambda_1} & \cdots & \frac{\partial \rho_{r_1}}{\partial \lambda_r} \\ \hline \frac{\partial \rho_{r_1+1}}{\partial \lambda} & \frac{\partial \rho_{r_1+1}}{\partial \lambda_1} & \cdots & \frac{\partial \rho_{r_1+1}}{\partial \lambda_r} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial \rho_{r_1+r_2}}{\partial \lambda} & \frac{\partial \rho_{r_1+r_2}}{\partial \lambda_1} & \cdots & \frac{\partial \rho_{r_1+r_2}}{\partial \lambda_r} \end{array}\right) = \left(\begin{array}{c|ccc} \frac{\rho_1}{n\lambda} & \frac{\rho_1}{e_1} L(u_1)_1 & \cdots & \frac{\rho_1}{e_1} L(u_r)_1 \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r_1}}{n\lambda} & \frac{\rho_{r_1}}{e_{r_1}} L(u_1)_{r_1} & \cdots & \frac{\rho_{r_1}}{e_{r_1}} L(u_r)_{r_1} \\ \hline \frac{\rho_{r_1+1}}{n\lambda} & \frac{\rho_{r_1+1}}{e_{r_1+1}} L(u_1)_{r_1+1} & \cdots & \frac{\rho_{r_1+1}}{e_{r_1+1}} L(u_r)_{r_1+1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r_1+r_2}}{n\lambda} & \frac{\rho_{r_1+r_2}}{e_{r_1+r_2}} L(u_1)_{r_1+r_2} & \cdots & \frac{\rho_{r_1+r_2}}{e_{r_1+r_2}} L(u_r)_{r_1+r_2} \end{array}\right).$$

El determinante correspondiente será

$$|\det J| = \frac{\rho_1 \cdots \rho_{r_1+r_2}}{n\lambda\, 2^{r_2}} \det \left(\begin{array}{c|ccc} 1 & L(u_1)_1 & \cdots & L(u_r)_1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & L(u_1)_{r_1} & \cdots & L(u_r)_{r_1} \\ \hline 2 & L(u_1)_{r_1+1} & \cdots & L(u_r)_{r_1+1} \\ \vdots & \vdots & \ddots & \vdots \\ 2 & L(u_1)_{r_1+r_2} & \cdots & L(u_r)_{r_1+r_2} \end{array}\right).$$

Sumando todas las filas a la primera, allí nos quedará el vector $(n, 0, \ldots, 0)$. Recordando la definición del regulador,

$$\det |J| = \frac{\rho_1 \cdots \rho_{r_1+r_2}}{\lambda\, 2^{r_2}} \operatorname{Reg}_K = \frac{1}{\rho_{r_1+1} \cdots \rho_{r_1+r_2}\, 2^{r_2}} \operatorname{Reg}_K.$$

Juntando todos los cálculos de arriba,

$$\begin{aligned}
\operatorname{vol}_{Leb.}(\overline{T}) &= \int \cdots \int dx_1 \cdots dx_{r_1}\, dy_1\, dz_1 \cdots dy_{r_2} dz_{r_2} \\
&= \int \cdots \int \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, d\rho_1 \cdots d\rho_{r_1+r_2}\, d\phi_1 \cdots d\phi_{r_2} \\
&= \int_0^{2\pi} d\phi_1 \cdots \int_0^{2\pi} d\phi_{r_2} \int \cdots \int \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, d\rho_1 \cdots d\rho_{r_1+r_2} \\
&= (2\pi)^{r_2} \int \cdots \int \det|J|\, \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, d\lambda_1 \cdots d\lambda_r\, d\lambda \\
&= \pi^{r_2}\, \operatorname{Reg}_K \int_0^1 d\lambda_1 \cdots \int_0^1 d\lambda_r \int_0^1 d\lambda = \pi^{r_2}\, \operatorname{Reg}_K .
\end{aligned}$$

■

Con esto ya tenemos todos los detalles de nuestra prueba de la fórmula de clases.

6.7 Función zeta y series L

Clase 28
25/11/20

En esta sección me gustaría explicar cómo la función zeta se factoriza en ciertas series L de Dirichlet

$$\zeta_K(s) = \prod_{\chi} L(s, \chi),$$

en el caso cuando $K/\mathbb{Q}$ es una extensión abeliana. Aquí voy a seguir la exposición de [Was1997].

La idea es bastante sencilla: recordemos que un carácter de Dirichlet mód m es un homomorfismo multiplicativo $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. Dado que para un campo ciclotómico $\mathbb{Q}(\zeta_m)$ se tiene $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, es útil considerar los caracteres de Dirichlet como caracteres de Galois $\chi\colon \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathbb{C}^\times$. Ahora los subgrupos $H \subseteq \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ corresponden a subcampos $K \subseteq \mathbb{Q}(\zeta_m)$. Como ya mencionamos en el capítulo 4, el **teorema de Kronecker–Weber** afirma que cualquier extensión abeliana $K/\mathbb{Q}$ puede ser realizada como una subextensión de $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ para algún m.

Ahora para el grupo de caracteres $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \cong \operatorname{Gal}(\widehat{\mathbb{Q}(\zeta_m)}/\mathbb{Q})$ se tiene $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \cong (\mathbb{Z}/m\mathbb{Z})^\times$, así que los subcampos de $\mathbb{Q}(\zeta_m)$ están en correspondencia con grupos de caracteres de Dirichlet mód m. Sin embargo, aquí el isomorfismo $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \cong (\mathbb{Z}/m\mathbb{Z})^\times$ no es canónico, y por esto hay que proceder con cuidado. Vamos a empezar por una revisión más sistemática de los caracteres de grupos abelianos finitos.

6.7.1 Caracteres de grupos abelianos finitos

Sea G un grupo abeliano finito. Vamos a usar la notación multiplicativa. Un **carácter** de G es un homomorfismo $\chi\colon G \to \mathbb{C}^\times$. Los caracteres forman un grupo respecto a la multiplicación punto por punto que será denotado por $\widehat{G}$. Esta construcción es contravariante: un homomorfismo de grupos $f\colon G \to H$ induce un homomorfismo de grupos de caracteres $\widehat{f}\colon \widehat{H} \to \widehat{G}$ mediante la composición con f.

6.7.1. Lema. *Se tiene* $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.

Demostración. Para los grupos abelianos el producto $\times$ coincide con coproducto, y luego $\operatorname{Hom}(G \times H, \mathbb{C}^\times) \cong \operatorname{Hom}(G, \mathbb{C}^\times) \times \operatorname{Hom}(H, \mathbb{C}^\times)$ por las propiedades universales de productos y coproductos. ■

6.7.2. Lema. *Hay un isomorfismo no canónico* $\widehat{G} \cong G$. *En particular,* $\#\widehat{G} = \#G$.

Demostración. Primero, si $G = C_n$ es un grupo cíclico finito, entonces

$$\widehat{C_n} = \operatorname{Hom}(C_n, \mathbb{C}^\times) = \operatorname{Hom}(C_n, \mu_n(\mathbb{C})) \cong \operatorname{Hom}(C_n, C_n) \cong C_n.$$

En general, tenemos un isomorfismo no canónico $G \cong C_{n_1} \times \cdots \times C_{n_s}$, y luego

$$\widehat{G} \cong \widehat{C_{n_1}} \times \cdots \times \widehat{C_{n_s}} \cong C_{n_1} \times \cdots \times C_{n_s} \cong G. \qquad \blacksquare$$

Las siguientes propiedades es un caso muy particular de la **dualidad Pontriaguin** que funciona para los grupos abelianos localmente compactos. En este caso el **grupo dual** $\widehat{G}$ se define como el grupo de homomorfismos continuos $\chi\colon G \to \mathbb{T}$, donde $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ es el grupo compacto del círculo. En el caso cuando G es finito, es trivialmente compacto, y todo homomorfismo $\chi\colon G \to \mathbb{C}^\times$ toma valores en las raíces n-ésimas de la unidad $\mu_n(\mathbb{C}) \subset \mathbb{T}$, donde $n = \#G$. En general la prueba de la dualidad de Pontriaguin es bastante complicada, pero para G finito podemos usar la observación de arriba de que $\#\widehat{G} = \#G$ y ocupar el conteo de elementos.

6.7.3. Proposición. *Sean G un grupo abeliano finito y $\widehat{G}$ su grupo de caracteres.*

a) Hay isomorfismo canónico $G \cong \widehat{\widehat{G}}$ dado por el homomorfismo de evaluación $ev\colon g \mapsto (\chi \mapsto \chi(g))$.

b) Tenemos un apareamiento no degenerado

$$G \times \widehat{G} \to \mathbb{C}^\times, \quad (g, \chi) \mapsto \chi(g);$$

Es decir, si $\chi(g) = 1$ para todo $g \in G$, entonces $\chi = 1$, y si $\chi(g) = 1$ para todo $\chi \in \widehat{G}$, entonces $g = 1$.

c) Dado un subgrupo $H \subset G$, consideremos el subgrupo ortogonal respecto al apareamiento de arriba:

$$H^\perp = \{\chi \in \widehat{G} \mid \chi(h) = 1 \text{ para todo } h \in H\}.$$

Tenemos isomorfismos naturales

$$H^\perp \cong \widehat{G/H}, \quad \widehat{H} \cong \widehat{G}/H^\perp.$$

d) Bajo la identificación de $\widehat{\widehat{G}}$ con G, se tiene $(H^\perp)^\perp = H$.

Demostración. El homomorfismo *ev* es inyectivo: si tenemos $\chi(g) = 1$ para todo carácter $\chi\colon G \to \mathbb{C}^\times$, entonces todo χ se factoriza de manera única por el cociente $G/\langle g\rangle$, y luego $\widehat{G} = \widehat{G/\langle g\rangle}$. Sin embargo, $\#\widehat{G} = \#G$ y $\#\widehat{G/\langle g\rangle} = G/\langle g\rangle$, así que necesariamente $g = 1$. Por otra parte, el homomorfismo es sobreyectivo, dado que $\#G = \#\widehat{G} = \#\widehat{\widehat{G}}$. Esto establece la parte a). Notamos que el argumento es similar a la prueba del isomorfismo canónico $V \cong (V^\vee)^\vee$ para un espacio vectorial de dimensión finita V.

La parte b) es una consecuencia inmediata de lo que acabamos de ver.

En c), observamos que si $H \subset \ker\chi$, entonces χ se factoriza de manera única por el cociente G/H, así que $H^\perp \cong \widehat{G/H}$. Además, la inclusión $H \hookrightarrow G$ induce la restricción de caracteres $\widehat{G} \to \widehat{H}$, y por la definición $H^\perp$ es el núcleo. Esto nos da un homomorfismo inyectivo $\widehat{G}/H^\perp \hookrightarrow \widehat{H}$. Para la sobreyectividad, calculamos que

$$\#(\widehat{G}/H^\perp) = \frac{\#G}{\#H^\perp} = \frac{\#G}{\#\widehat{G/H}} = \frac{\#G}{\#(G/H)} = \#H = \#\widehat{H}.$$

En fin, en la parte d), primero tenemos por la definición $H \subseteq (H^\perp)^\perp$, y luego

$$\#(H^\perp)^\perp = \#(\widehat{G/H})^\perp = \#\left(\frac{\widehat{G}}{\widehat{G/H}}\right) = \#H. \qquad \blacksquare$$

6.7.2 Caracteres de Dirichlet

6.7.4. Definición. Un carácter de Dirichlet mód m es un homomorfismo $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Notamos que si $m \mid m'$, entonces χ induce un carácter

$$(\mathbb{Z}/m'\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times.$$

6.7.5. Definición. El m más pequeño tal que χ puede ser considerado como un carácter mód m se llama el **conductor** de χ y se denota por f_χ.[*] Cuando χ se considera como un carácter mód f_χ, se dice que χ es **primitivo**.

6.7.6. Ejemplo. Consideremos el homomorfismo $\chi\colon (\mathbb{Z}/6\mathbb{Z})^\times \to \mathbb{C}^\times$ definido por $1 \mapsto 1$ y $5 \mapsto -1$. En realidad este χ se induce por el homomorfismo no trivial $\chi'\colon (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ definido por $1 \mapsto 1$, $2 \mapsto -1$:

$$\chi\colon (\mathbb{Z}/6\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times.$$

Entonces χ tiene conductor $f_\chi = 3$ y no es primitivo. ▲

6.7.7. Definición. Si $\chi(-1) = +1$, se dice que χ es **par**, y si $\chi(-1) = -1$, se dice que χ es **impar**.

Un carácter de Dirichlet $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ se extiende a una aplicación $\chi\colon \mathbb{Z} \to \mathbb{C}$ poniendo

$$\chi(n) = 0, \text{ si } \operatorname{mcd}(n, f_\chi) \neq 1.$$

Si χ y χ' son caracteres primitivos, entonces su producto punto por punto se define como un carácter

$$\chi\chi'\colon (\mathbb{Z}/\operatorname{mcm}(f_\chi, f_{\chi'})\mathbb{Z})^\times \to \mathbb{C}^\times,$$

y es también primitivo. Si $\operatorname{mcd}(f_\chi, f_{\chi'}) = 1$, entonces $f_{\chi\chi'} = f_\chi f_{\chi'}$.

Sea $K/\mathbb{Q}$ una extensión abeliana. En este caso gracias al teorema de Kronecker–Weber tenemos $K \subseteq \mathbb{Q}(\zeta_m)$ para algún m. El mínimo posible m con esta propiedad se llama el **conductor** de K. En este caso todo carácter de Galois $\chi\colon \operatorname{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$ puede ser interpretado como un carácter de Dirichlet mód m:

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times \cong \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \longrightarrow & \mathbb{C}^\times \\ & \searrow \quad \nearrow_{\chi} & \\ & \operatorname{Gal}(K/\mathbb{Q}) & \end{array}$$

De esta manera el grupo de caracteres $\widehat{\operatorname{Gal}(K/\mathbb{Q})}$ se identifica con cierto grupo de caracteres de Dirichlet X y se tiene el apareamiento perfecto correspondiente

$$\operatorname{Gal}(K/\mathbb{Q}) \times X \to \mathbb{C}^\times.$$

Para un subcampo $F \subseteq K$ consideremos el subgrupo $\operatorname{Gal}(K/F) \subseteq \operatorname{Gal}(K/\mathbb{Q})$ y el correspondiente subgrupo ortogonal de X

$$Y = \operatorname{Gal}(K/F)^\perp = \{\chi \in X \mid \chi(g) = 1 \text{ para todo } g \in \operatorname{Gal}(K/F)\}.$$

Viceversa, dado un subgrupo $Y \subseteq X$, podemos considerar el grupo $Y^\perp \subseteq \operatorname{Gal}(K/\mathbb{Q})$ y el subcampo fijo correspondiente $F = K^{Y^\perp}$. De esta manera se obtiene la siguiente versión de la correspondencia de Galois para $K/\mathbb{Q}$.

[*] Nota políticamente incorrecta: aquí «*f*» viene del alemán *Führer*, lo que literalmente significa líder o conductor.

6.7.8. Teorema. *Para un campo $K \subseteq \mathbb{Q}(\zeta_m)$, sea $X \cong \widehat{\mathrm{Gal}(K/\mathbb{Q})}$ un grupo de caracteres de Dirichlet correspondiente. Tenemos una biyección*

$$\{\textit{subgrupos } Y \subseteq X\} \underset{\mathrm{Gal}(K/F)^\perp \hookleftarrow F}{\overset{Y \mapsto K^{(Y^\perp)}}{\rightleftarrows}} \{\textit{subcampos } F \subseteq K\}$$

Esta correspondencia cumple con las siguientes propiedades:

a) $[F : \mathbb{Q}] = \#Y$.

b) Se tiene $F_1 \subseteq F_2$ *si y solamente si* $Y_1 \subseteq Y_2$.

c) Al subgrupo generado por los elementos Y_1 *e* Y_2 *corresponde el compositum* F_1F_2.

En particular, hay una biyección

$$\{\textit{subgrupos } X \subseteq \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}\} \rightleftarrows \{\textit{subcampos } K \subseteq \mathbb{Q}(\zeta_m)\}$$

Demostración. Si $F = K^{(Y^\perp)}$, entonces $Y^\perp = \mathrm{Gal}(K/F)$ por la teoría de Galois, y luego $\mathrm{Gal}(K/F)^\perp = (Y^\perp)^\perp = Y$. De manera similar, si $Y = \mathrm{Gal}(K/F)^\perp$, entonces $K^{(Y^\perp)} = K^{(\mathrm{Gal}(K/F)^\perp)^\perp} = K^{\mathrm{Gal}(K/F)} = F$. Esto establece la biyección.

Para verificar la propiedad a), notamos que $[F : \mathbb{Q}] = \#\,\mathrm{Gal}(F/\mathbb{Q})$. Por otra parte,

$$\mathrm{Gal}(K/F)^\perp \cong (\mathrm{Gal}(K/\mathbb{Q})/\,\mathrm{Gal}(K/F))\widehat{\ } \cong \widehat{\mathrm{Gal}(F/\mathbb{Q})},$$

y $\#\widehat{\mathrm{Gal}(F/\mathbb{Q})} = \#\,\mathrm{Gal}(F/\mathbb{Q})$.

La propiedad b) nada más viene del hecho de que para la correspondencia de Galois habitual, se tiene $F_1 \subseteq F_2$ si y solamente si $\mathrm{Gal}(K/F_2) \subseteq \mathrm{Gal}(K/F_1)$, y lo último se cumple si y solamente si $\mathrm{Gal}(K/F_1)^\perp \subseteq \mathrm{Gal}(K/F_2)^\perp$.

Como consecuencia, en la propiedad c), el subgrupo de X más pequeño que contiene Y_1 e Y_2 corresponderá al subcampo más pequeño de K que contiene F_1 y F_2. ■

6.7.9. Ejemplo. En el campo ciclotómico $\mathbb{Q}(\zeta_7)$ consideremos el subcampo cúbico real $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Este debe corresponder a algún grupo de caracteres de Dirichlet $X \subset \widehat{(\mathbb{Z}/7\mathbb{Z})^\times}$ de orden 3. El grupo $(\mathbb{Z}/7\mathbb{Z})^\times$ tiene solamente dos caracteres cúbicos; estos corresponden a 2 y 4 que tienen orden 3 mód 7.

Para definir un carácter cúbico, podemos escoger un generador de $(\mathbb{Z}/7\mathbb{Z})^\times$, por ejemplo 3, y mandarlo a la raíz de la unidad ζ_3:

$$\chi\colon 1 \mapsto 1, \quad 2 \equiv 3^2 \mapsto \zeta_3^2, \quad 3 \mapsto \zeta_3, \quad 4 \equiv 3^4 \mapsto \zeta_3, \quad 5 \equiv 3^5 \mapsto \zeta_3^2, \quad 6 \equiv 3^3 \mapsto 1.$$

El otro carácter cúbico será $\chi^2 = \overline{\chi}$. Entonces, $X = \{1, \chi, \chi^2\}$. ▲

6.7.10. Ejemplo. Consideremos el campo $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. La extensión $K/\mathbb{Q}$ es abeliana, y el teorema de Kronecker–Weber nos dice que $K \subset \mathbb{Q}(\zeta_m)$ para algún m.

Nos conviene considerar por separado dos campos cuadráticos $F_1 = \mathbb{Q}(\sqrt{2})$ y $F_2 = \mathbb{Q}(\sqrt{3})$. Tenemos $F_1 \subset \mathbb{Q}(\zeta_8)$ y $F_2 \subset \mathbb{Q}(\zeta_{12})$, y luego $K = F_1F_2 \subset \mathbb{Q}(\zeta_{24})$.

El encaje $F_1 \subset \mathbb{Q}(\zeta_8)$ corresponde a un carácter cuadrático χ_1 mód 8, y sería instructivo entender cuál es este, ocupando las consideraciones de arriba. El automorfismo no trivial de $\mathbb{Q}(\zeta_8)$ que deja fijo a $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ es $\sigma\colon \zeta_8 \mapsto \zeta_8^7$, así que

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/F_1) = \{1, \sigma\}.$$

Nos interesa el grupo ortogonal

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/F_1)^\perp = \{\chi \in \mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})\widehat{\ } \mid \chi(\sigma) = 1\}.$$

Todos los elementos no triviales de $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$ tienen orden 2, así que los caracteres $\chi \in \widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})} \cong \widehat{(\mathbb{Z}/8\mathbb{Z})^\times}$ toman valores ± 1. Bajo la identificación $\widehat{\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})} \cong \widehat{(\mathbb{Z}/8\mathbb{Z})^\times}$, notamos que el elemento no trivial de $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/F_1)^\perp$ debe mandar 7 a $+1$, y esto ya nos define todo el carácter:

$$\chi_1 \colon 1 \mapsto +1, \quad 3 \mapsto -1, \quad 5 \mapsto -1, \quad 7 \mapsto +1$$

Dejo al lector investigar el caso de $F_2 \subset \mathbb{Q}(\zeta_{12})$ y ver que el carácter correspondiente mód 12 será

$$\chi_2 \colon 1 \mapsto +1, \quad 5 \mapsto -1, \quad 7 \mapsto -1, \quad 11 \mapsto +1.$$

Podemos concluir que K corresponde al grupo de caracteres de Dirichlet

$$X = \{1, \chi_1, \chi_2, \chi_1\chi_2\}. \qquad \blacktriangle$$

6.7.3 Caracteres de Dirichlet y ramificación

Empezamos por un par de pequeños lemas sobre los índices de ramificación en extensiones. Invito que el lector revise el material de §§4.3–4.4 sobre el grupo de descomposición e inercia y automorfismo de Frobenius.

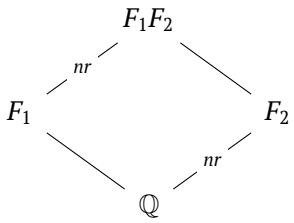
Primero, nos conviene introducir la siguiente terminología: se dice que un primo racional p es **totalmente ramificado**[*] en una extensión $K/\mathbb{Q}$ si en $\mathcal{O}_K$ hay único ideal primo $\mathfrak{p} \mid p$ y $p\mathcal{O}_K = \mathfrak{p}^e$, donde $e = [K : \mathbb{Q}]$. Notamos que esto es equivalente a tener $f(\mathfrak{p}|p) = 1$.

6.7.11. Lema. *En una torre de extensiones $\mathbb{Q} \subseteq F \subseteq K$, si p es totalmente ramificado en K, entonces es totalmente ramificado en F.*

Demostración. Si $\mathfrak{P}$ es el único primo en $\mathcal{O}_K$ que está sobre p, entonces $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$ es el único primo en $\mathcal{O}_F$ que está sobre p. Ahora $f(\mathfrak{P}|\mathfrak{p})\, f(\mathfrak{p}|p) = f(\mathfrak{P}|p) = 1$ implica que $f(\mathfrak{p}|p) = 1$. ■

6.7.12. Lema. *Sean F_1 y F_2 dos campos de números, donde $F_2/\mathbb{Q}$ es una extensión de Galois. Dado un primo racional p, consideremos ideales primos $\mathfrak{P} \subset \mathcal{O}_{F_1F_2}$, $\mathfrak{p}_1 \subset \mathcal{O}_{F_1}$, $\mathfrak{p}_1 \subset \mathcal{O}_{F_2}$ tales que $\mathfrak{P} \mid \mathfrak{p}_1 \mid p$ y $\mathfrak{p}_2 \mid p$.*

1) *Si p no se ramifica en F_2, entonces $e(\mathfrak{P} \mid \mathfrak{p}_1) = 1$.*
2) *En particular, si $F_2/\mathbb{Q}$ es también una extensión de Galois, y p no se ramifica en F_2, entonces el índice de ramificación de p en $F_1/\mathbb{Q}$ es el mismo que el índice de ramificación de p en $F_1F_2/\mathbb{Q}$.*



Demostración. Recordemos que si $F_2/\mathbb{Q}$ es una extensión de Galois, entonces F_1F_2/F_1 es también una extensión de Galois. Consideremos los grupos de descomposición

$$D(\mathfrak{P}|\mathfrak{p}_1) = \{\sigma \in \mathrm{Gal}(F_1F_2/F_1) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$
$$D(\mathfrak{p}_2|p) = \{\sigma \in \mathrm{Gal}(F_2/\mathbb{Q}) \mid \sigma(\mathfrak{p}_2) = \mathfrak{p}_2\}.$$

[*] No hemos mencionado este término hasta el momento solo porque por el carácter introductorio de este curso, no hemos tratado de manera más sistemática la teoría de ramificación...

Dejo al lector verificar que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I(\mathfrak{P}|\mathfrak{p}_1) & \longrightarrow & D(\mathfrak{P}|\mathfrak{p}_1) & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}_1)) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I(\mathfrak{p}_2|p) & \longrightarrow & D(\mathfrak{p}_2|p) & \longrightarrow & \mathrm{Gal}(\kappa(\mathfrak{p}_2)/\mathbb{F}_p) & \longrightarrow & 1 \end{array}$$

Aquí el homomorfismo en el medio está inducido por el homomorfismo inyectivo de restricción

$$\mathrm{Gal}(F_1F_2/F_1) \hookrightarrow \mathrm{Gal}(F_2/\mathbb{Q}), \quad \sigma \mapsto \sigma|_{F_2}$$

(véase A.13.4). Como consecuencia, tenemos un homomorfismo inyectivo $I(\mathfrak{P}|\mathfrak{p}_1) \hookrightarrow I(\mathfrak{p}_2|p)$. En particular, si p no se ramifica en F_2, entonces $I(\mathfrak{p}_2|p) = 1$, y luego $I(\mathfrak{P}|\mathfrak{p}_1) = 1$, así que $e(\mathfrak{P} \mid \mathfrak{p}_1) = 1$.

Para la parte 2) del lema, dado un primo racional p, sean $\mathfrak{P} \subset \mathcal{O}_{F_1F_2}$ un ideal primo tal que $\mathfrak{P} \mid p$ y $\mathfrak{p}_1 = \mathfrak{P} \cap \mathcal{O}_{F_1}$, $\mathfrak{p}_2 = \mathfrak{P} \cap \mathcal{O}_{F_2}$. Entonces,

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}_1)\, e(\mathfrak{p}_1|p) = e(\mathfrak{p}_1|p). \qquad \blacksquare$$

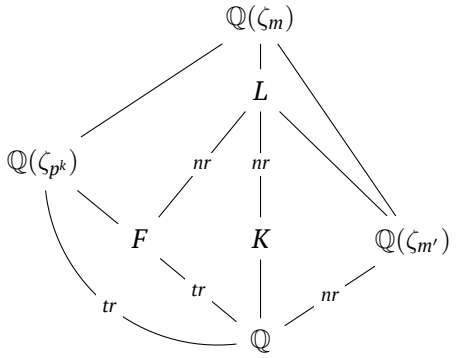
Ahora si $m = \prod_p p^k$, entonces $(\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_p (\mathbb{Z}/p^k\mathbb{Z})^\times$, y luego $\widehat{(\mathbb{Z}/m\mathbb{Z})}^\times \cong \prod_p \widehat{(\mathbb{Z}/p^k\mathbb{Z})}^\times$. De esta manera todo carácter de Dirichlet χ mód m se descompone como $\chi = \prod_p \chi_p$, donde χ_p es un carácter mód p^k. Dado un grupo de caracteres de Dirichlet X, pongamos

$$X_p = \{\chi_p \mid \chi \in X\}.$$

6.7.13. Teorema. *Para $K \subseteq \mathbb{Q}(\zeta_m)$, sea $X \cong \widehat{\mathrm{Gal}(K/\mathbb{Q})}$ el grupo de caracteres de Dirichlet correspondiente. Para un primo racional p el índice de ramificación en K es $e_p = \#X_p$.*

Demostración. Escribamos $m = p^k m'$, donde $p \nmid m'$. El campo $L = K\mathbb{Q}(\zeta_{m'})$ corresponde al grupo de caracteres de Dirichlet generado por X y $\widehat{(\mathbb{Z}/m'\mathbb{Z})}^\times$. Los caracteres mód m' son precisamente los caracteres mód m de conductor f_χ tal que $p \nmid f_\chi$. Entonces, L corresponde al producto directo $X_p \times \widehat{(\mathbb{Z}/m'\mathbb{Z})}^\times$, y por ende $L = F\mathbb{Q}(\zeta_{m'})$, donde F es el subcampo de $\mathbb{Q}(\zeta_{p^k})$ que corresponde a X_p.

Tenemos el siguiente diagrama, donde está marcada la ramificación de p en las extensiones.



Aquí p no se ramifica en la extensión $\mathbb{Q}(\zeta_{m'})/\mathbb{Q}$, así que el índice de ramificación de p en $K/\mathbb{Q}$ es el mismo que en la extensión $L/\mathbb{Q}$. En la extensión L/F el primo p tampoco se ramifica, así que el índice de ramificación es el mismo que en $F/\mathbb{Q}$. En fin, $F/\mathbb{Q}$ es una subextensión de $\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}$ donde p es totalmente ramificado. Se sigue que p es totalmente ramificado en $F/\mathbb{Q}$ y $e_p = [F : \mathbb{Q}] = \#X_p$. $\blacksquare$

Esto nos lleva a la siguiente caracterización de ramificación.

6.7.14. Corolario. *En la situación anterior, un primo p no se ramifica en K si y solamente si $\chi(p) \neq 0$ para todo $\chi \in X$.*

Demostración. Según el teorema, p se ramifica en $K/\mathbb{Q}$ si y solamente si $\#X_p \neq 1$. Esto es equivalente a tener un carácter no trivial $\chi \in X$ tal que

$$\chi_p \neq 1 \iff p \mid f_\chi \iff \chi(p) = 0. \qquad \blacksquare$$

6.7.15. Teorema. *Sean $K \subseteq \mathbb{Q}(\zeta_m)$ y $X \cong \widehat{\mathrm{Gal}(K/\mathbb{Q})}$ el grupo de caracteres de Dirichlet correspondiente. Para un primo racional p consideremos los subgrupos de X dados por*

$$Y = \{\chi \in X \mid \chi(p) \neq 0\}, \quad Z = \{\chi \in X \mid \chi(p) = 1\}.$$

En este caso el grupo Y/Z es cíclico, y se tiene

$$e_p = [X : Y], \quad f_p = [Y : Z], \quad g_p = \#Z.$$

Demostración. Recordamos que

$$e_p f_p g_p = [K : \mathbb{Q}] = \#X.$$

Entonces, bastará verificar que $e_p = [X : Y]$ y $f_p = [Y : Z]$, y luego

$$g_p = \frac{\#X}{[X : Y] \cdot [Y : Z]} = \#Z.$$

Sea F el subcampo de K que corresponde al subgrupo $Y \subseteq X$. Entonces, $\mathbb{Q} \subseteq F \subseteq K$ es la subextensión más grande donde p no se ramifica. Esto significa que F es precisamente el campo de inercia de p (véase 4.3.6). Tenemos entonces $F = K^{I(\mathfrak{p}|p)} = K^{\mathrm{Gal}(K/F)}$, así que $I(\mathfrak{p}|p) = \mathrm{Gal}(K/F)$. Luego, $e_p = \#I(\mathfrak{p}|p) = \#\,\mathrm{Gal}(K/F)$ (véase 4.3.4).

Recordemos que bajo el apareamiento $\mathrm{Gal}(K/\mathbb{Q}) \times X \to \mathbb{C}^\times$ se tiene $Y = \mathrm{Gal}(K/F)^\perp$, así que

$$X/Y = \widehat{\mathrm{Gal}(K/\mathbb{Q})}/\,\mathrm{Gal}(K/F)^\perp \cong \widehat{\mathrm{Gal}(K/F)}.$$

Entonces, $e_p = \#\,\mathrm{Gal}(K/F) = \#\widehat{\mathrm{Gal}(K/F)} = [X : Y]$.

Ahora nos vamos a fijar en la extensión $F/\mathbb{Q}$ donde p no se ramifica. En este caso el grupo de descomposición correspondiente es cíclico, generado por el automorfismo de Frobenius $\mathrm{Frob}_p \in \mathrm{Gal}(F/\mathbb{Q})$, y se tiene $f_p = \#\langle \mathrm{Frob}_p \rangle$.

Sea n el mcm de los conductores f_χ para $\chi \in Y$. En este caso $F \subseteq \mathbb{Q}(\zeta_n)$, donde $p \nmid n$, y p tampoco se ramifica en la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Recordemos que el grupo de descomposición de p respecto a $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es cíclico, generado por el automorfismo de Frobenius $\zeta_n \mapsto \zeta_n^p$.

El grupo $\mathrm{Gal}(F/\mathbb{Q})$ es el cociente de $\mathrm{Gal}(\zeta_n)/\mathbb{Q} \cong (\mathbb{Z}/n\mathbb{Z})^\times$ por $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/F)$, y el automorfismo Frob_p es precisamente la clase lateral de $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. Ahora si $\chi \in Y$, entonces se tiene $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/F) \subseteq \ker \chi$, así que $\chi(\mathrm{Frob}_p) = \chi(p)$. En particular, $\chi(\mathrm{Frob}_p) = 1$ si y solamente si $\chi(p) = 1$. Esto significa que respecto al apareamiento $\mathrm{Gal}(F/\mathbb{Q}) \times Y \to \mathbb{C}^\times$, tenemos precisamente $Z = \langle \mathrm{Frob}_p \rangle^\perp$. Ahora

$$Y/Z \cong \widehat{\langle \mathrm{Frob}_p \rangle},$$

y luego $[Y : Z] = \#\widehat{\langle \mathrm{Frob}_p \rangle} = \#\langle \mathrm{Frob}_p \rangle = f_p$. $\blacksquare$

6.7.4 Factorización de la función zeta en series L de Dirichlet

Recordemos que a un carácter de Dirichlet χ se asocia la serie L correspondiente

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)\, p^{-s}}.$$

Aquí para levantar χ a una aplicación $\chi \colon \mathbb{Z} \to \mathbb{C}$, vamos a usar nuestra convención de que χ se considera módulo su conductor f_χ.

6.7.16. Teorema. *Para un subcampo $K \subseteq \mathbb{Q}(\zeta_m)$, sea X el grupo de caracteres de Dirichlet correspondiente. Se tiene*

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi).$$

Demostración. Escribamos la función zeta como el producto de Euler

$$\zeta_K(s) = \prod_p \prod_{\mathfrak{p}|p} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}.$$

Pongamos

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_{g_p})^{e_p}, \quad \text{donde } N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_p}.$$

El factor de Euler que corresponde a p será entonces

$$\prod_{1 \le i \le g_p} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{-s}} = \prod_p \frac{1}{(1 - p^{-f_p s})^{g_p}}.$$

Por otra parte, en el producto $\prod_{\chi \in X} L(s, \chi)$ el factor que corresponde a p será

$$\prod_{\chi \in X} \frac{1}{1 - \chi(p)\, p^{-s}} = \prod_{\chi \in Y} \frac{1}{1 - \chi(p)\, p^{-s}},$$

donde

$$Y = \{\chi \in X \mid \chi(p) \neq 0\}.$$

Hemos pasado al producto sobre $\chi \in Y$ porque los términos con $\chi(p) = 0$ no contribuyen nada. De la misma manera, podemos considerar el subgrupo de Y dado por

$$Z = \{\chi \in X \mid \chi(p) = 1\}.$$

Para cada clase lateral $\chi Z \in Y/Z$ los caracteres en χZ toman el mismo valor en p. Esto nos permite reescribir nuestro factor de Euler como

$$\left(\prod_{\overline{\chi} \in Y/Z} \frac{1}{1 - \chi(p)\, p^{-s}} \right)^{\#Z},$$

donde por $\overline{\chi} \in Y/Z$ se entienden diferentes representantes del grupo cociente. Recordemos de 6.7.15 que Y/Z es un grupo cíclico de orden f_p y $\#Z = g_p$. Entonces, los valores $\chi(p)$ para diferentes representantes $\overline{\chi} \in Y/Z$ serán precisamente las f_p-ésimas raíces de la unidad. Usando la identidad $\prod_{0 \le k \le n-1}(1 - \zeta_n^k x) = 1 - x^n$, calculamos

$$\prod_{0 \le k \le f_p - 1} \frac{1}{1 - \zeta_{f_p}^k\, p^{-s}} = \frac{1}{1 - p^{-f_p s}}.$$

Esto nos dice que

$$\prod_{\chi \in X} \frac{1}{1 - \chi(p)\, p^{-s}} = \frac{1}{(1 - \chi(p)\, p^{-f_p s})^{g_p}}.$$

■

Como consecuencia, se obtiene el siguiente resultado que es el punto clave en la prueba del teorema de Dirichlet sobre primos en progresiones aritméticas (véase el apéndice D).

6.7.17. Corolario. *Para $\chi \neq 1$ se tiene $L(1, \chi) \neq 0$.*

Demostración. Consideremos el grupo de caracteres de Dirichlet $X = \langle \chi \rangle$ y el campo correspondiente $K \subseteq \mathbb{Q}(\zeta_m)$, donde m es el conductor de χ. Sea $n = \#X$. El teorema anterior nos da

$$\zeta_K(s) = \prod_{0 \le k \le n-1} L(s, \chi^k) = \zeta(s) \prod_{1 \le k \le n-1} L(s, \chi^k).$$

Sabemos que las funciones $\zeta_K(s)$ y $\zeta(s)$ tienen un polo simple en $s = 1$, y esto implica que ninguno de los factores $L(s, \chi^k)$ se anulan en $s = 1$. ■

6.7.18. Ejemplo. En el ejemplo 6.7.9 vimos que el campo cúbico real $K = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ corresponde al grupo de caracteres de Dirichlet $X = \{1, \chi, \chi^2\}$, donde χ es un carácter cúbico mód 7. Entonces,

$$\zeta_K(s) = \zeta(s)\, L(s, \chi)\, L(s, \chi^2).$$ ▲

6.7.19. Ejemplo. En el ejemplo 6.7.10 vimos que el campo bicuadrático $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ se encaja en $\mathbb{Q}(\zeta_{24})$ y corresponde al grupo de caracteres

$$X = \{1, \chi_1, \chi_2, \chi_1\chi_2\},$$

donde χ_1 es un carácter mód 8 y χ_2 es un carácter mód 12. (De hecho, estos caracteres también pueden ser recuperados del ejercicio 6.3.) Tenemos como consecuencia

$$\zeta_K(s) = \zeta(s)\, L(s, \chi_1)\, L(s, \chi_2)\, L(s, \chi_1\chi_2).$$ ▲

6.7.20. Comentario. Todo lo que hemos hecho en esta sección funciona para extensiones abelianas $K/\mathbb{Q}$. Para factorizar la función $\zeta_K(s)$ en el caso no abeliano, Artin introdujo funciones $L(s, \rho)$, donde ρ es una representación lineal del grupo $\mathrm{Gal}(K/\mathbb{Q})$; es decir, un homomorfismo $\rho\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$. Aquí n es la dimensión de la representación. El resultado general es la factorización

$$\zeta_K(s) = \prod_{\rho} L(s, \rho),$$

donde el producto es sobre todas las representaciones irreducibles del grupo de Galois.

Cuando $G = \mathrm{Gal}(K/\mathbb{Q})$ es un grupo abeliano, un resultado básico de la teoría de representación (véase por ejemplo [Ser1978]) nos dice que todas las representaciones irreducibles de G son unidimensionales, y entonces corresponden a los caracteres $\chi\colon G \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. En este caso las funciones L de Artin serán las series L de Dirichlet.

El caso no abeliano es más complicado y de este se origina una gran parte de las matemáticas contemporáneas.

6.8 Perspectiva: Prolongación analítica

Clase 29
30/11/20

En muchos casos una función de variable compleja definida por una serie sobre el dominio de convergencia (como la función $\zeta_K(s)$ que al principio se define para $\mathrm{Re}\, s > 1$) puede ser extendida a una función meromorfa sobre todo $s \in \mathbb{C}$. Este es el caso con la función zeta de Dedekind.

6.8.1. Teorema. *La función zeta de Dedekind admite prolongación analítica a todo plano complejo con el único polo en $s = 1$ de residuo dado por la fórmula del número de clases. Se cumple la ecuación funcional*

$$\zeta_K(1 - s) = A(s)\, \zeta_K(s),$$

donde

$$A(s) = |\Delta_K|^{s-1/2} \left(\cos \frac{\pi s}{2}\right)^{r_1 + r_2} \left(\mathrm{sen}\, \frac{\pi s}{2}\right)^{r_2} \left(2\,(2\pi)^{-s}\,\Gamma(s)\right)^n,$$

$n = [K : \mathbb{Q}]$, y r_1 (resp. $2r_2$) es el número de encajes reales (resp. complejos) de K.

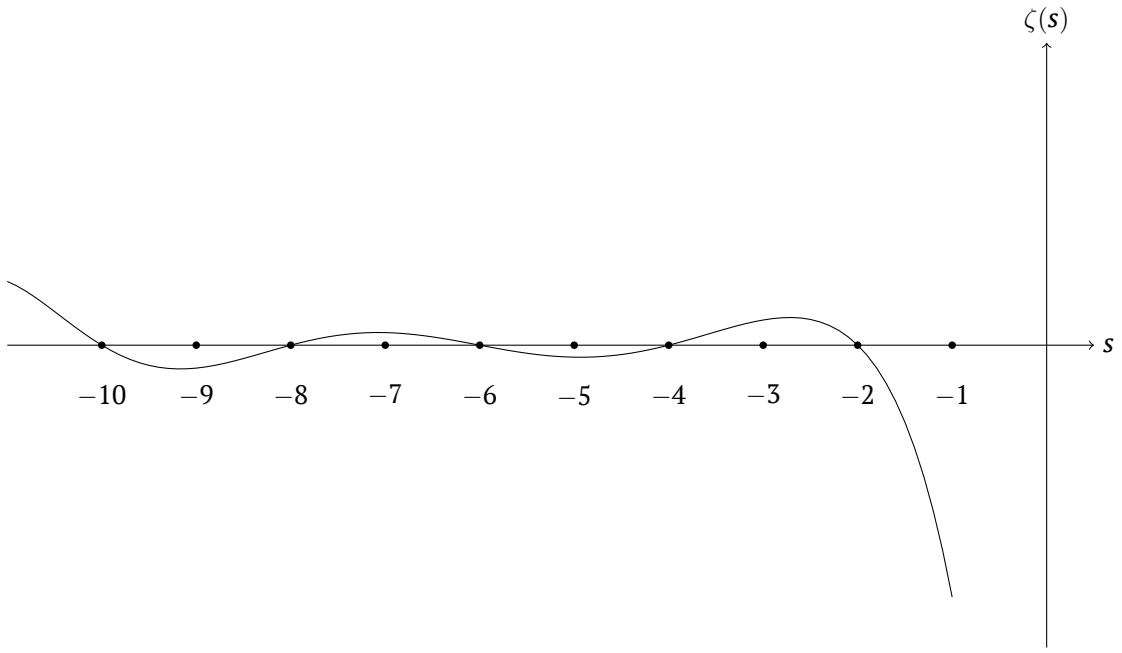


Figura 6.3: Valores negativos de $\zeta(s)$

Demostración. Véase [Neu1999, §VII.5]. ■

Aquí

$$\Gamma(s) = \int_0^\infty e^{-t}\, t^{s-1}\, dt, \quad \operatorname{Re} s > 0$$

es la **función Gamma**. En particular, $\Gamma(k) = (k-1)!$ para $k = 1, 2, 3, \ldots$

Tomando $K = \mathbb{Q}$, se obtiene la ecuación funcional para la función zeta de Riemann

$$\zeta(1-s) = \left(\cos\frac{\pi s}{2}\right)\, 2\,(2\pi)^{-s}\,\Gamma(s)\,\zeta(s). \tag{6.7}$$

Sustituyendo $s = 1$ en la ecuación funcional, notamos que el término $\left(\cos\frac{\pi s}{2}\right)^{r_1+r_2}$ tiene cero de orden $r_1 + r_2$, mientras que $\zeta_K(s)$ tiene polo de orden 1. Esto nos permite concluir que $\zeta_K(s)$ tiene cero en $s = 0$ de orden $r_1 + r_2 - 1$. Curiosamente, este es también el rango del grupo de unidades $\mathcal{O}_K^\times$. Dejo al lector calcular que el residuo correspondiente será

$$\zeta_K^*(0) = \lim_{s\to 0} s^{-(r_1+r_2-1)}\,\zeta_K(s) = -\frac{\operatorname{Reg}_K\, h_k}{\#\mu_K}.$$

En particular,

$$\zeta(0) = -\frac{1}{2}.$$

La ecuación funcional nos da los **ceros triviales** de la función $\zeta_K(s)$ que aparecen para $s = 0, -1, -2, -3, \ldots$ gracias a los términos cos $\frac{\pi s}{2}$ y sen $\frac{\pi s}{2}$. Aquí están los ordenes de estos ceros.

s:	0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10	$\cdots$
ord:	r_1+r_2-1	r_2	r_1+r_2	r_2	r_1+r_2	r_2	r_1+r_2	r_2	r_1+r_2	r_2	r_1+r_2	$\cdots$

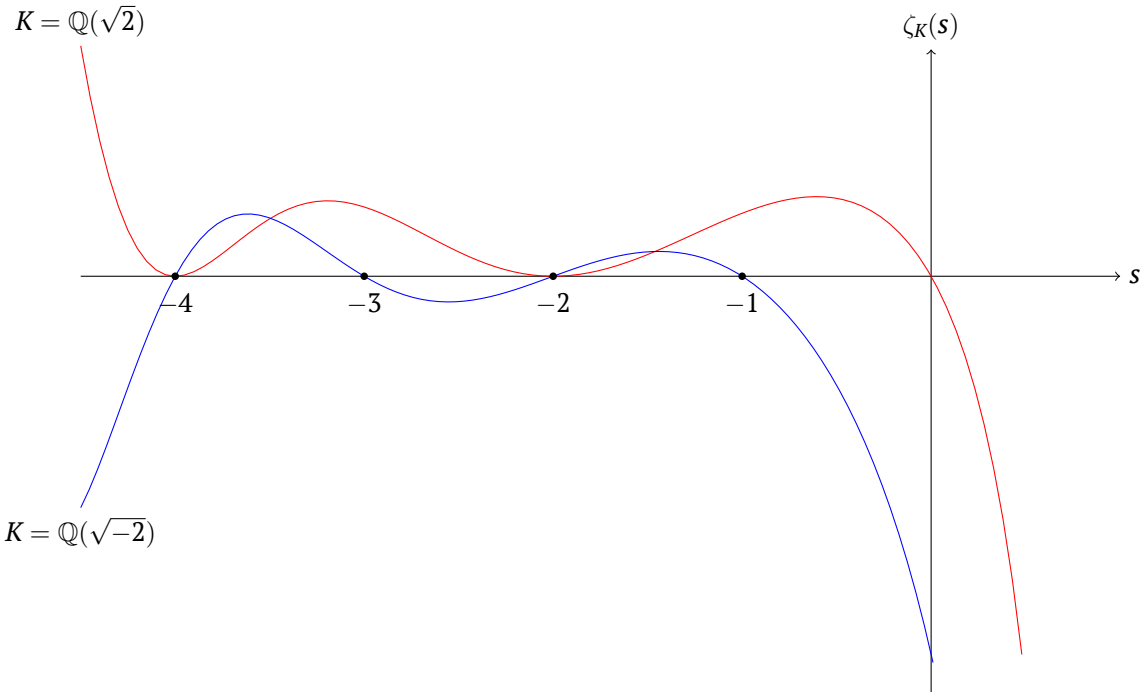


Figura 6.4: Valores negativos de $\zeta_{\mathbb{Q}(\sqrt{\pm 2})}(s)$

La **hipótesis de Riemann extendida** afirma que todos los ceros *no triviales* de $\zeta_K(s)$ tienen $\operatorname{Re} s = \frac{1}{2}$. El mismo Riemann formuló su conjetura para el caso de $K = \mathbb{Q}$, y este es uno de los problemas abiertos más importantes en matemáticas.

Las series L de Dirichlet también admiten prolongación a todo el plano complejo.

6.8.2. Teorema. *Sea χ un carácter de Dirichlet primitivo mód m. La serie $L(s,\chi)$ admite prolongación analítica a todo plano complejo que satisface la ecuación funcional*

$$L(1-s,\chi) = A(s)\,L(s,\overline{\chi}), \tag{6.8}$$

donde

$$A(s) = \frac{m^{s-1}\,\Gamma(s)}{(2\pi)^s}\left(e^{-\pi i s/2} + \chi(-1)\,e^{\pi i s/2}\right) g(\chi)$$

y

$$g(\chi) = \sum_{1\le a\le m-1} \chi(a)\,\zeta_m^a.$$

Demostración. Véase [Neu1999, §VII.2] o [Apo1976, Chapter 12]. ■

Más adelante veremos que $g(\chi) \neq 0$. Además, de la fórmula del producto de Euler se ve que $L(s,\overline{\chi}) \neq 0$ para $s > 1$. Entonces, los ceros triviales de $L(s,\chi)$ en $s = 0, -1, -2, -3, \ldots$ vienen del término

$$e^{-\pi i s/2} + \chi(-1)\,e^{\pi i s/2} = \begin{cases} 2\,\cos\left(\frac{\pi s}{2}\right), & \text{si } \chi(-1) = +1, \\ -2i\,\operatorname{sen}\left(\frac{\pi s}{2}\right), & \text{si } \chi(-1) = -1. \end{cases}$$

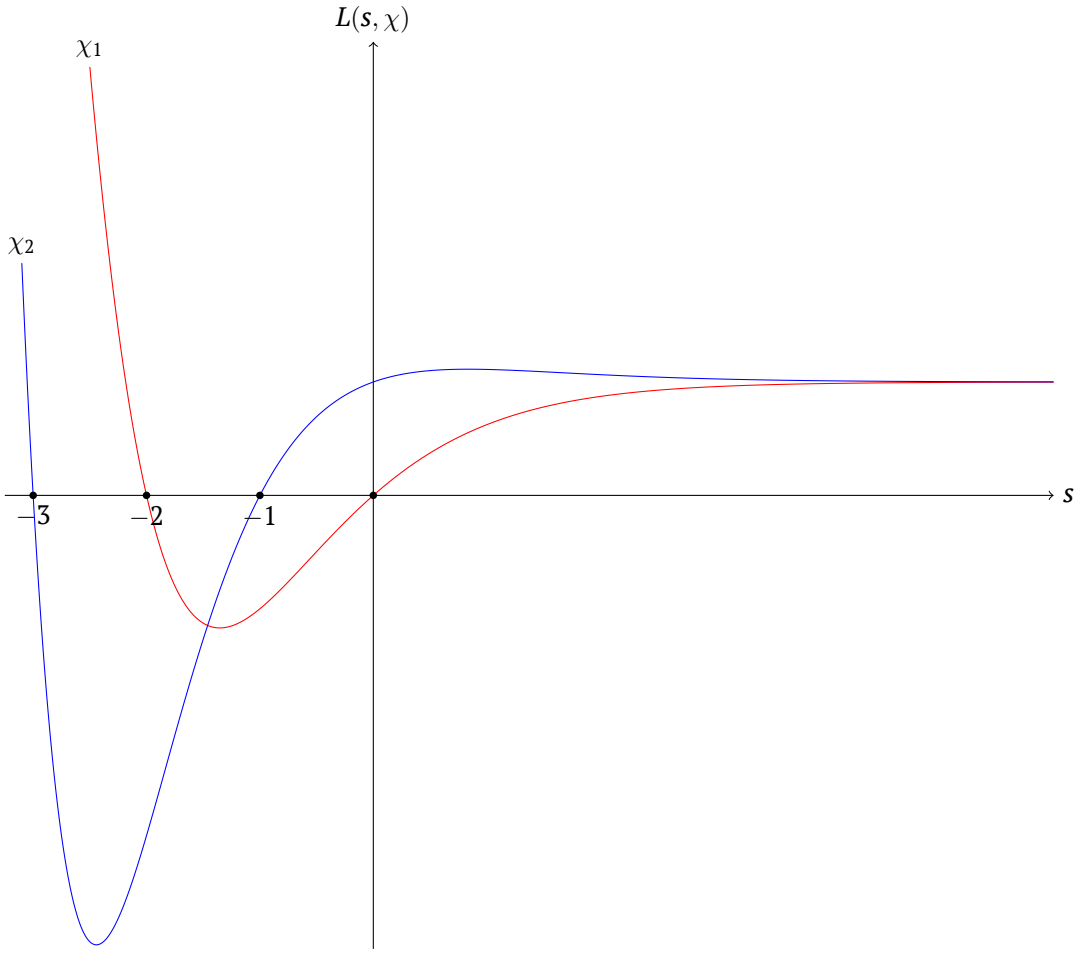


Figura 6.5: $L(s,\chi)$ para $\chi_1(n) = \left(\frac{+8}{n}\right)$ (par) y $\chi_2(n) = \left(\frac{-8}{n}\right)$ (impar)

Podemos concluir que si $\chi(-1) = +1$, entonces $L(s,\chi)$ tiene ceros simples en $s = 0, -2, -4, -6, \ldots$, y si $\chi(-1) = -1$, entonces $L(s,\chi)$ tiene ceros simples en $s = -1, -3, -5, \ldots$ La **hipótesis de Riemann generalizada** afirma que los ceros *no triviales* de $L(s,\chi)$ tienen $\operatorname{Re} s = \frac{1}{2}$.

Nuestro próximo objetivo será calcular los valores $L(s,\chi)$ para $s = 0, -1, -2, -3, \ldots$ de manera explícita.

6.9 Perspectiva: Valores especiales

Los valores de la función zeta $\zeta_K(s)$ en enteros $s = n \in \mathbb{Z}$ se conocen como los **valores especiales**. Como vimos, la función zeta suele tener ceros en $s = n$ negativos, así que normalmente por el valor especial se entiende más bien el residuo correspondiente

$$\zeta_K^*(n) = \lim_{s\to n}(s-n)^{-d_n}\,\zeta_K(s),$$

donde d_n denota el orden de cero en $s = n$ (para el polo en $s = 1$ tenemos $d_1 = -1$).

Para las funciones $L(s,\chi)$ los valores especiales se definen de manera similar.

Un ejemplo primordial de valores especiales es

$$\zeta_K^*(0) = \lim_{s\to 0} s^{-(r_1+r_2-1)}\,\zeta_K(s) = -\frac{\operatorname{Reg}_K\, h_k}{\#\mu_K} \longleftrightarrow \zeta_K^*(1) = \frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\, h_k}{\#\mu_K\,\sqrt{|\Delta_K|}}.$$

Hay varias identidades (en gran parte conjeturales) que generalizan estas fórmulas a todo $s = n \in \mathbb{Z}$. La idea general es definir *ciertos invariantes algebraicos* análogos a $\mathrm{Cl}(K)$ y $\mathcal{O}_K^\times$; estos deben ser algunos grupos abelianos finitamente generados. De sus partes de torsión vendrá algún número racional, similar a $\frac{h_K}{\#\mu_K}$. Por otra parte, debería haber ciertos «reguladores superiores» $\operatorname{Reg}_{K,n}$ responsables por la parte trascendente del valor especial. Estos reguladores superiores también serán covolúmenes de algunos retículos, pero son más difíciles de definir.

Las construcciones técnicas necesarias para escribir estas fórmulas para los valores especiales nos llevarían demasiado lejos. El lector interesado en los resultados y conjeturas contemporáneos acerca de los valores especiales puede empezar por el artículo de Kontsevich y Zagier sobre períodos [KZ2001], y también ver el artículo de Nekovář sobre las conjeturas de Beilinson en [Motives-I], y el libro [CRSS2015] sobre las conjeturas de Bloch–Kato para la función zeta de Riemann. Aquí me gustaría explicar un resultado clásico.

6.9.1. Teorema (Siegel–Klingen). *Para un campo totalmente real $K/\mathbb{Q}$ los valores $\zeta_K(-1)$, $\zeta_K(-3)$, $\zeta_K(-5)$, ... son números racionales.*

Aquí se trata literalmente de valores $\zeta_K(-n)$, no de residuos $\zeta_K^*(-n)$. Hemos calculado arriba los ordenes de ceros triviales $\zeta_K(-n)$, y estos son r_2 o $r_1 + r_2$, dependiendo de la paridad de n. En particular, si K no es totalmente real y $r_2 > 0$, entonces $\zeta_K(-n) = 0$ para todo $n \le 0$. Por esto la hipótesis dice que $K/\mathbb{Q}$ es totalmente real.

Para la prueba completa del teorema véase [Neu1999, §VII.9]. A continuación veremos una prueba para $K/\mathbb{Q}$ una extensión abeliana. En este caso, como ya vimos, se tiene $\zeta_K(s) = \prod_\chi L(s,\chi)$ para ciertos caracteres de Dirichlet χ, y bastaría saber calcular los valores de $L(s,\chi)$ en $s = n \le 0$. Estos cálculos son muy clásicos.

6.9.1 Números y polinomios de Bernoulli

Hay diferentes definiciones equivalentes de los números y polinomios de Bernoulli. Nos conviene usar las funciones generatrices exponenciales.

6.9.2. Definición. Los **números de Bernoulli** $B_k \in \mathbb{Q}$ se definen mediante

$$\frac{t\,e^t}{e^t - 1} = \sum_{k\ge 0} \frac{B_k}{k!}\,t^k,$$

y los **polinomios de Bernoulli** $B_k(x) \in \mathbb{Q}[x]$ se definen mediante

$$\frac{t\,e^{tx}}{e^t - 1} = \sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!}.$$

No es difícil verificar que la función generatriz para B_k es equivalente a la recurrencia

$$\sum_{0\leq i\leq k} \binom{k+1}{i} B_i = k+1.$$

6.9.3. Proposición. *Los números y polinomios de Bernoulli cumplen las siguientes propiedades.*

a) $B_k(1) = B_k$.

b) $B_k(x+1) - B_k(x) = k\,x^{k-1}$.
En particular, para $x = 0$ *se obtiene* $B_k(0) = B_k$ *para* $k \neq 1$.

c) $B_k(1-x) = (-1)^k B_k(x)$.
En particular, para $x = 0$*, se obtiene que* $B_k = 0$ *para* $k \geq 3$ *impar.*

d) Para todo $k \geq 1$ *se tiene* $B_k'(x) = k\,B_{k-1}(x)$ *y* $\int_0^1 B_k(x)\,dx = 0$.

Demostración. La propiedad a) se sigue de las funciones generatrices para B_k y $B_k(x)$, y la propiedad b) se sigue de la identidad

$$\sum_{k\geq 0}(B_k(x+1) - B_k(x))\,\frac{t^k}{k!} = \frac{t\,e^{(x+1)\,t}}{e^t - 1} - \frac{t\,e^{t\,x}}{e^t - 1} = t\,e^{t\,x} = \sum_{k\geq 0}\frac{x^k}{k!}\,t^{k+1}.$$

De manera similar, c) se sigue de

$$\sum_{k\geq 0} B_k(1-x)\,\frac{t^k}{k!} = \frac{t\,e^{(1-x)\,t}}{e^t - 1} = \frac{(-t)\,e^{x\,(-t)}}{e^{-t} - 1} = \sum_{k\geq 0}(-1)^k B_k(x)\,\frac{t^k}{k!}.$$

En fin, para d), tomando as derivadas formales de la identidad $\frac{t\,e^{tx}}{e^t-1} = \sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!}$ respecto a x, se obtiene

$$\frac{\partial}{\partial x}\left(\frac{t\,e^{tx}}{e^t - 1}\right) = \frac{t\cdot t\,e^{tx}}{e^t - 1} = t\sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!} = \sum_{k\geq 1} B_{k-1}(x)\,\frac{t^k}{(k-1)!} = \sum_{k\geq 0} B_k'(x)\,\frac{t^k}{k!}.$$

Se tiene $\int B_k(x)\,dx = \frac{1}{k+1}\,B_{k+1}(x) + C$, donde $B_{k+1}(0) = B_{k+1}(1)$, y luego $\int_0^1 B_k(x)\,dx = 0$. ■

De hecho, la última propiedad *caracteriza* los polinomios de Bernoulli: estos se definen de manera única por las condiciones

$$B_0(x) = 1, \quad B_k'(x) = k\,B_{k-1}(x), \quad \int_0^1 B_k(x)\,dx = 0 \text{ para } k \geq 1.$$

(La identidad $B_k'(x) = k\,B_{k-1}(x)$ define $B_k(x)$ salvo el término constante que luego se recupera de la condición $\int_0^1 B_k(x)\,dx = 0$.)

A continuación nos servirá el siguiente caso particular de series de Fourier. Sea $f\colon \mathbb{R} \to \mathbb{R}$ una función continua por trozos y periódica tal que $f(x+1) = f(x)$. Luego, para todo $x_0 \in \mathbb{R}$ donde f es continua y las derivadas izquierda y derecha de f existen, se cumple

$$f(x_0) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)\,e^{2\pi i n x_0}, \quad \text{donde } \widehat{f}(n) = \int_0^1 e^{-2\pi i n x} f(x)\,dx.$$

k	$B_k(x)$	B_k
0	1	1
1	$x - \frac{1}{2}$	$\frac{1}{2}$
2	$x^2 - x + \frac{1}{6}$	$\frac{1}{6}$
3	$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$	0
4	$x^4 - 2x^3 + x^2 - \frac{1}{30}$	$-\frac{1}{30}$
5	$x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x$	0
6	$x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}$	$\frac{1}{42}$
7	$x^7 - \frac{7}{2}x^6 + \frac{7}{2}x^5 - \frac{7}{6}x^3 + \frac{1}{6}x$	0
8	$x^8 - 4x^7 + \frac{14}{3}x^6 - \frac{7}{3}x^4 + \frac{2}{3}x^2 - \frac{1}{30}$	$-\frac{1}{30}$
9	$x^9 - \frac{9}{2}x^8 + 6x^7 - \frac{21}{5}x^5 + 2x^3 - \frac{3}{10}x$	0
10	$x^{10} - 5x^9 + \frac{15}{2}x^8 - 7x^6 + 5x^4 - \frac{3}{2}x^2 + \frac{5}{66}$	$\frac{5}{66}$
11	$x^{11} - \frac{11}{2}x^{10} + \frac{55}{6}x^9 - 11x^7 + 11x^5 - \frac{11}{2}x^3 + \frac{5}{6}x$	0
12	$x^{12} - 6x^{11} + 11x^{10} - \frac{33}{2}x^8 + 22x^6 - \frac{33}{2}x^4 + 5x^2 - \frac{691}{2730}$	$-\frac{691}{2730}$
13	$x^{13} - \frac{13}{2}x^{12} + 13x^{11} - \frac{143}{6}x^9 + \frac{286}{7}x^7 - \frac{429}{10}x^5 + \frac{65}{3}x^3 - \frac{691}{210}x$	0
14	$x^{14} - 7x^{13} + \frac{91}{6}x^{12} - \frac{1001}{30}x^{10} + \frac{143}{2}x^8 - \frac{1001}{10}x^6 + \frac{455}{6}x^4 - \frac{691}{30}x^2 + \frac{7}{6}$	$\frac{7}{6}$
15	$x^{15} - \frac{15}{2}x^{14} + \frac{35}{2}x^{13} - \frac{91}{2}x^{11} + \frac{715}{6}x^9 - \frac{429}{2}x^7 + \frac{455}{2}x^5 - \frac{691}{6}x^3 + \frac{35}{2}x$	0

Figura 6.6: Polinomios y números de Bernoulli

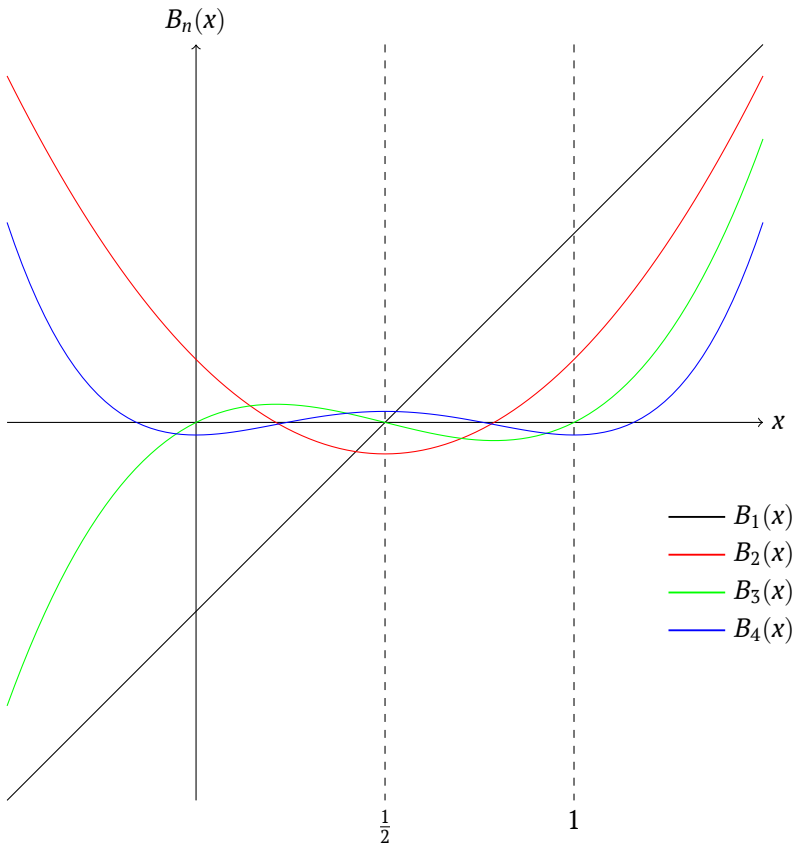


Figura 6.7: Polinomios de Bernoulli $B_n(x)$

6.9.4. Proposición. *Tenemos la serie de Fourier*

$$B_k(x-\lfloor x\rfloor) = -\frac{k!}{(2\pi i)^k}\sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}}\frac{e^{2\pi inx}}{n^k}. \tag{6.9}$$

Demostración. Necesitamos calcular los coeficientes de Fourier de la función $f(x) = B_k(x-\lfloor x\rfloor)$. Para $n=0$ tenemos

$$\widehat{f}(0) = \int_0^1 B_k(x)\,dx = 0.$$

Para $n\neq 0$ y $k=1$ usamos la integración por partes ($\int_a^b f'(x)\,g(x)\,dx = [f(x)\,g(x)]_a^b - \int_a^b f(x)\,g'(x)\,dx$):

$$\begin{aligned}\int_0^1 e^{-2\pi inx}\left(x-\frac{1}{2}\right)dx &= -\frac{1}{2\pi in}\int_0^1 \left(e^{-2\pi inx}\right)'\left(x-\frac{1}{2}\right)dx\\ &= -\frac{1}{2\pi in}\left(\left[e^{-2\pi inx}\left(x-\frac{1}{2}\right)\right]_0^1 - \underbrace{\int_0^1 e^{-2\pi inx}\,dx}_{=0}\right) = -\frac{1}{2\pi in}.\end{aligned}$$

Para $k>1$ la integración por partes junto con la identidad $B_k'(x) = k\,B_{k-1}(x)$ nos da

$$\begin{aligned}\widehat{f}(n) &= \int_0^1 e^{-2\pi inx}B_k(x)\,dx\\ &= -\frac{1}{2\pi in}\int_0^1 (e^{-2\pi inx})'\,B_k(x)\,dx\\ &= -\frac{1}{2\pi in}\left(\left[e^{-2\pi inx}B_k(x)\right]_0^1 - k\int_0^1 e^{-2\pi inx}B_{k-1}(x)\,dx\right)\\ &= \frac{k}{2\pi in}\int_0^1 e^{-2\pi inx}B_{k-1}(x)\,dx\\ &= \frac{k(k-1)}{(2\pi in)^2}\int_0^1 e^{-2\pi inx}B_{k-2}(x)\,dx\\ &= \cdots\\ &= \frac{k!}{(2\pi in)^{k-1}}\int_0^1 e^{-2\pi inx}\left(x-\frac{1}{2}\right)dx\\ &= \frac{k!}{(2\pi in)^{k-1}}\cdot\left(-\frac{1}{2\pi in}\right) = -\frac{k!}{(2\pi in)^k}.\end{aligned}$$

■

La serie de Fourier (6.9) nos lleva al siguiente famoso resultado.

6.9.5. Teorema (Euler). *Para todo $k\geq 1$ se tiene*

$$\zeta(2k) = (-1)^{k+1}B_{2k}\frac{2^{2k-1}}{(2k)!}\pi^{2k}.$$

Demostración. Sustituyendo $x=0$ en (6.9) y $2k$ en lugar de k, se obtiene

$$B_{2k} = B_{2k}(0) = -\frac{(2k)!}{(-1)^k(2\pi)^{2k}}\,2\sum_{n\geq 1}\frac{1}{n^{2k}} = (-1)^{k+1}\frac{(2k)!}{2^{2k-1}\pi^{2k}}\,\zeta(2k).$$

■

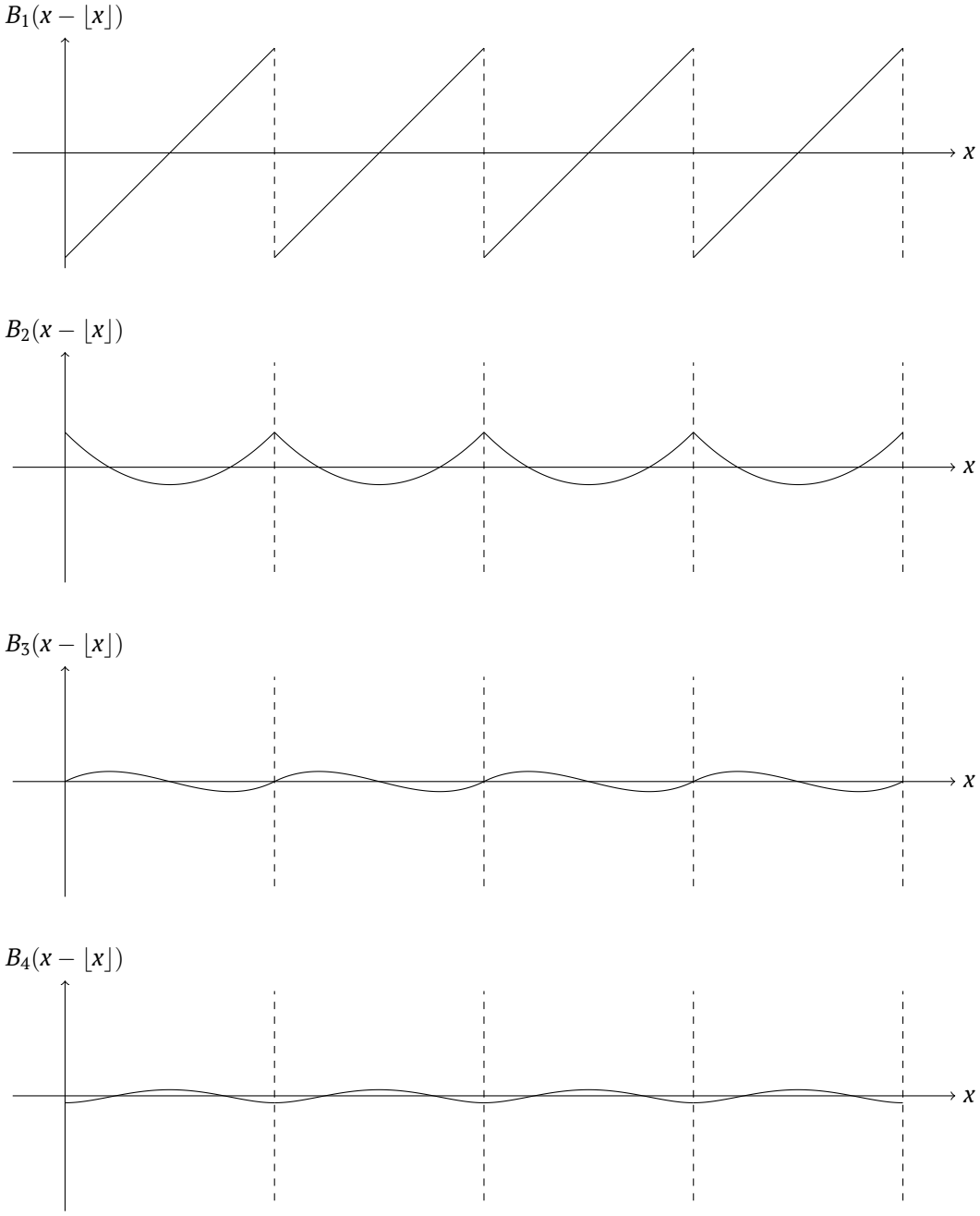


Figura 6.8: Funciones periódicas $B_n(x - \lfloor x \rfloor)$

6.9.6. Ejemplo. Los primeros valores $\zeta(2k)$ son

$$\begin{aligned}
\zeta(2) &= \frac{\pi^2}{6} \approx 1{,}644934\ldots,\\
\zeta(4) &= \frac{\pi^4}{90} \approx 1{,}082323\ldots,\\
\zeta(6) &= \frac{\pi^6}{945} \approx 1{,}017343\ldots,\\
\zeta(8) &= \frac{\pi^8}{9450} \approx 1{,}004077\ldots,\\
\zeta(10) &= \frac{\pi^{10}}{93\,555} \approx 1{,}000994\ldots,\\
\zeta(12) &= \frac{691\,\pi^{12}}{638\,512\,875} \approx 1{,}000246\ldots
\end{aligned}$$

▲

6.9.7. Comentario. Los valores $\zeta(3), \zeta(5), \zeta(7), \ldots$ son más misteriosos. *Al parecer*, son números trascendentes. Por supuesto, los números

$$\zeta(2k) = (-1)^{k+1}\, B_{2k}\, \frac{2^{2k-1}}{(2k)!}\, \pi^{2k}$$

son también trascendentes, ya que π es trascendente. Los valores $\zeta(2k+1)$ deberían de ser trascendentes por alguna razón más sofisticada, y se supone que entre $\zeta(2k+1)$ distintos no hay ninguna relación algebraica. Sin embargo, todavía no hay demostraciones ni siquiera de que los $\zeta(2k+1)$ sean irracionales. En 1977 el matemático francés Roger Apéry demostró que el número

$$\zeta(3) \approx 1{,}202056903159594285399738 16\ldots$$

es irracional. La tumba de Apéry en París lleva la inscripción

Roger APÉRY 1916–1994

$$1 + \tfrac{1}{8} + \tfrac{1}{27} + \tfrac{1}{64} + \cdots \neq \tfrac{p}{q}$$

Para más información sobre el teorema de Apéry, véase el artículo [vdP1979]. Los métodos de Apéry no se generalizan para demostrar que $\zeta(5)$ es irracional. Hay pocos resultados en esta dirección. Rivoal demostró en 2000 que entre los números $\zeta(3), \zeta(7), \zeta(9), \ldots$ hay una infinidad de irracionales [Riv2000], mientras que Zudilin demostró que por lo menos un número entre $\zeta(5)$, $\zeta(7)$, $\zeta(9)$ y $\zeta(11)$ es irracional [Zud2004].

6.9.8. Corolario. $(-1)^{k+1}\, B_{2k} > 0$ *para* $k \geq 1$. *Es decir,* $B_{2k} \neq 0$*, y los signos son alternantes.*

Demostración. Se sigue inmediatamente de la fórmula $(-1)^{k+1}\, B_{2k} = \frac{(2k)!}{2^{2k-1}\,\pi^{2k}}\, \zeta(2k)$. Esto también puede ser deducido directamente de la definición de B_{2k}, pero la fórmula para $\zeta(2k)$ nos da mejor explicación. ■

6.9.9. Corolario. *Se tiene* $|B_{2k+2}| > |B_{2k}|$ *para* $k \geq 3$.

Demostración. Basta aplicar la fórmula

$$|B_{2k}| = \frac{2 \cdot (2k)!}{(2\pi)^{2k}}\, \zeta(2k),$$

y notar que la función $\zeta(s+c)/\zeta(s)$ crece para todo $c > 0$ (por ejemplo, calcule que $\frac{d}{ds} \log \zeta(s+c)/\zeta(s) > 0$, usando la fórmula del producto). ■

6.9.10. Corolario. *Para $n = 0, 1, 2, 3, \ldots$ se tiene*

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

Demostración. De la ecuación funcional (6.7) se ve que $\zeta(-2k) = 0$ (se anula $\operatorname{sen}(-\pi k/2)$). Esto coincide con el hecho de que $B_n = 0$ para $n > 1$ impar. Por otra parte, para $s = -(2k+1)$ impar la fórmula de Euler se simplifica a $\zeta(-(2k+1)) = -\frac{B_{2k+2}}{2k+2}$. En fin, de la ecuación funcional se deduce que $\zeta(0) = -\frac{1}{2} = -B_1$. ■

6.9.2 Números de Bernoulli torcidos por un carácter de Dirichlet

Recordemos que la función zeta de Riemann es un caso particular de las series L de Dirichlet $L(s, \chi)$ cuando $\chi = 1$. A continuación nos gustaría generalizar la fórmula $\zeta(-n) = -\frac{B_{n+1}}{n+1}$ a $L(-n, \chi) = -\frac{B_{\chi,n+1}}{n+1}$, donde $B_{\chi,n+1}$ son números racionales que generalizan los números de Bernoulli.

6.9.11. Definición. Dado un carácter de Dirichlet χ mód m, los **números de Bernoulli generalizados** («torcidos» por χ) se definen mediante la función generatriz

$$\sum_{k\geq 0} B_{k,\chi}\,\frac{t^k}{k!} = \sum_a \frac{\chi(a)\,t\,e^{at}}{e^{mt}-1},$$

donde la suma es sobre $1 \leq a \leq m-1$. A partir de ahora estas sumas serán denotadas simplemente por $\sum_a$.

Notamos que $B_{k,\chi} \in \mathbb{Q}(\zeta_m)$.

6.9.12. Proposición. *a) Para $\chi \neq 1$ se tiene $B_{k,\chi} = 0$ si $\chi(-1) = (-1)^{k+1}$.*

b) Los números de Bernoulli $B_{k,\chi}$ están relacionados con los polinomios de Bernoulli mediante la fórmula

$$B_{k,\chi} = m^{k-1} \sum_a \chi(a)\,B_k(a/m).$$

Demostración. Para la propiedad a), basta notar que para la función generatriz $f(t) = \sum_a \frac{\chi(a)\,t\,e^{at}}{e^{mt}-1}$ se tiene $f(t) = \chi(-1)\,f(-t)$. Entonces, $f(t)$ es una función par o impar, dependiendo de la paridad de χ.

Para la propiedad b), podemos considerar la función generatriz para los polinomios de Bernoulli

$$\sum_{k\geq 0} B_k(x)\,\frac{t^k}{k!} = \frac{t\,e^{tx}}{e^t-1}.$$

Al sustituir $x = a/m$ y remplazar t por mt, nos queda

$$\sum_{k\geq 0}\sum_a \chi(a)\,B_k(a/m)\,\frac{(mt)^k}{k!} = \sum_a \frac{\chi(a)\,mt\,e^{t\,a}}{e^{mt}-1} = m\sum_{k\geq 0} B_{k,\chi}\,\frac{t^k}{k!}.$$

Basta comparar los coeficientes. ■

6.9.13. Ejemplo. Un carácter no trivial mód 4 viene dado por

$$\chi\colon 1 \mapsto +1, \quad 3 \mapsto -1.$$

Entonces, los números de Bernoulli correspondientes se definen por por la función generatriz

$$\sum_{k\geq 0} B_{k,\chi}\,\frac{t^k}{k!} = t\,\frac{e^t - e^{3t}}{e^{4t}-1} = -\frac{te^t}{e^{2t}+1}.$$

El carácter χ es impar, así que $B_{k,\chi} = 0$ para los k pares. Para los impares, calculamos los siguientes valores.

k:	1	3	5	7	9	11	13	15
$B_{k,\chi}$:	$-\frac{1}{2}$	$+\frac{3}{2}$	$-\frac{25}{2}$	$+\frac{427}{2}$	$-\frac{12465}{2}$	$+\frac{555731}{2}$	$-\frac{35135945}{2}$	$+\frac{2990414715}{2}$

```
? default(seriesprecision,16);
? f = -t*exp(t)/(exp(2*t)+1);
? vector (8,k, (2*k-1)!*polcoeff(f,2*k-1))
% = [-1/2, 3/2, -25/2, 427/2, -12465/2, 555731/2, -35135945/2, 2990414715/2]
```

▲

6.9.3 Sumas de Gauss para caracteres de Dirichlet

6.9.14. Definición. Sea χ un carácter de Dirichlet primitivo mód m. La **suma de Gauss** correspondiente viene dada por

$$g(\chi) = \sum_a \chi(a)\,\zeta_m^a,$$

donde $\zeta_m = e^{2\pi i/m}$. En general, para todo entero n pongamos

$$g_n(\chi) = \sum_a \chi(a)\,\zeta_m^{an}.$$

Vamos a necesitar un par de propiedades básicas de sumas de Gauss. El caso de $m = p$ primo ya fue considerado en nuestra prueba de la reciprocidad cuadrática en §1.4.

6.9.15. Lema. *Para todo $n \in \mathbb{Z}$ se tiene*

$$\overline{\chi(n)}\,g(\chi) = g_n(\chi).$$

En particular (tomando $n = -1$ y los conjugados),

$$\overline{g(\chi)} = \chi(-1)\,g(\overline{\chi}).$$

Demostración. Si $\mathrm{mcd}(n,m) = 1$, entonces la multiplicación por n nos da un automorfismo de $(\mathbb{Z}/m\mathbb{Z})^\times$, y luego

$$\begin{aligned}
\overline{\chi(n)}\,g(\chi) &= \overline{\chi(n)} \sum_a \chi(a)\,\zeta_m^a \\
&= \chi(n)^{-1} \sum_a \chi(an)\,\zeta_m^{an} \\
&= \sum_a \chi(a)\,\zeta_m^{an} \\
&= g_n(\chi).
\end{aligned}$$

Por otra parte, si $\mathrm{mcd}(n,m) \neq 1$, entonces $\chi(n) = 0$, y afirmamos que

$$g_n(\chi) = \sum_a \chi(a)\,\zeta_m^{an} = 0.$$

Para esto escribamos $d = \mathrm{mcd}(n,m)$. Notamos que ζ_m^{an} depende de a mód m/d, y los elementos que satisfacen $\mathrm{mcd}(a, m/d) = 1$ forman un subgrupo de $(\mathbb{Z}/m\mathbb{Z})^\times$, que es el núcleo del homomorfismo canónico sobreyectivo $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/\frac{m}{d}\mathbb{Z})^\times$. Ahora

$$\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\,\zeta_m^{an} = \sum_{b\in(\mathbb{Z}/\frac{m}{d}\mathbb{Z})^\times} \left(\sum_{a\equiv b\ (m/d)} \chi(a) \right) \zeta_m^{an},$$

donde

$$\sum_{a\equiv b\ (m/d)} \chi(a) = \chi(b) \sum_{a\equiv 1\ (m/d)} \chi(a) = 0.$$

En efecto, aquí χ es un carácter no trivial, así que siempre existe algún $c \in (\mathbb{Z}/m\mathbb{Z})^\times$ tal que $\chi(c) \neq 1$. Luego,

$$\sum_{a\equiv 1\ (m/d)} \chi(a) = \sum_{a\equiv 1\ (m/d)} \chi(ac) = \chi(c) \sum_{a\equiv 1\ (m/d)} \chi(a),$$

lo que implica que la suma es nula. ■

6.9.16. Lema.

$$|g(\chi)|^2 = g(\chi)\,\overline{g(\chi)} = m.$$

En particular (usando 6.9.15),

$$g(\chi)^{-1} = \frac{1}{m}\,\chi(-1)\,g(\overline{\chi}).$$

Demostración. Según el lema anterior, para todo n se cumple

$$|\chi(n)|^2\,|g(\chi)|^2 = |g_n(\chi)|^2.$$

Aquí

$$|\chi(n)| = \begin{cases} 1, & \operatorname{mcd}(n,m) = 1, \\ 0, & \operatorname{mcd}(n,m) \neq 1. \end{cases}$$

Calculamos que

$$\phi(m)\,|g(\chi)|^2 = \sum_{1\leq n\leq m-1} |\chi(n)|^2\,|g(\chi)|^2 = \sum_{1\leq n\leq m-1} |g_n(\chi)|^2.$$

Por otra parte, la última suma es

$$\begin{aligned} \sum_{1\leq n\leq m-1} |g_n(\chi)|^2 &= \sum_{1\leq n\leq m-1} g_n(\chi)\,\overline{g_n(\chi)} \\ &= \sum_{1\leq a,b\leq m-1} \chi(a)\,\overline{\chi(b)} \sum_{1\leq n\leq m-1} \zeta_m^{(a-b)\,n}, \\ &= \phi(m)\,m, \end{aligned}$$

usando

$$\sum_{1\leq n\leq m-1} \zeta_m^{(a-b)\,n} = \begin{cases} 0, & a \neq b, \\ m, & a = b. \end{cases}$$

Esto concluye la prueba. ■

6.9.4 Valores especiales de las series L de Dirichlet

Estamos listos para formular y probar el resultado principal de esta sección.

6.9.17. Teorema. *Sean χ un carácter de Dirichlet primitivo mód m y $k > 1$ un número natural tal que $\chi(-1) = (-1)^k$. Entonces,*

$$L(k,\chi) = (-1)^{k+1}\,\frac{(2\pi i)^k}{2\cdot k!\,m^k}\,g(\chi)\,B_{k,\overline{\chi}}.$$

Esto nos da *la mitad* de los valores especiales: $L(k,\chi)$, donde la paridad de k corresponde a la paridad del carácter.

Demostración. La fórmula del lema 6.9.15 nos da para todo $n \in \mathbb{Z}$

$$\chi(n)\, g(\overline{\chi}) = \sum_a \overline{\chi(a)}\, \zeta_m^{an}.$$

Gracias a esto, podemos escribir

$$L(k,\chi)\, g(\overline{\chi}) = \sum_a \overline{\chi(a)} \sum_{n\geq 1} \frac{\zeta_m^{an}}{n^k}.$$

Puesto que $\chi(-1) = (-1)^k$, tenemos

$$L(k,\chi)\, g(\overline{\chi}) = \frac{1}{2} \sum_a \overline{\chi(a)} \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \frac{\zeta_m^{an}}{n^k}.$$

Recordemos la serie de Fourier para los polinomios de Bernoulli:

$$B_k(x - \lfloor x \rfloor) = -\frac{k!}{(2\pi i)^k} \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \frac{e^{2\pi i n x}}{n^k}.$$

En particular, sustituyendo $x = a/m$, se obtiene

$$\sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \frac{\zeta_m^{an}}{n^k} = -\frac{(2\pi i)^k}{k!}\, B_k(a/m).$$

Y usando la expresión para $B_{k,\chi}$ en términos de $B_k(x)$,

$$L(k,\chi)\, g(\overline{\chi}) = -\frac{(2\pi i)^k}{2\cdot k!} \sum_a \overline{\chi(a)} B_k(a/m) = -\frac{(2\pi i)^k}{2\cdot k!\, m^{k-1}}\, B_{k,\overline{\chi}}.$$

En fin, dado que

$$g(\overline{\chi})^{-1} = \frac{1}{m}\, \chi(-1)\, g(\chi) = \frac{1}{m}\, (-1)^k\, g(\chi)$$

por el lema 6.9.16, llegamos a la fórmula deseada

$$L(k,\chi) = (-1)^{k+1}\, \frac{(2\pi i)^k}{2\cdot k!\, m^k}\, g(\chi)\, B_{k,\overline{\chi}}.$$ ■

6.9.18. Corolario. *Si $\chi(-1) = (-1)^k$ para $k > 1$, entonces $B_{k,\chi} \neq 0$.*

Demostración. La fórmula del producto de Euler $L(s,\chi) = \prod_p \frac{1}{1-\chi(p)\, p^{-s}}$ implica que $L(s,\chi) \neq 0$ para $s > 1$. ■

6.9.19. Corolario. *Para todo $n = 0, 1, 2, 3, \ldots$ se tiene*

$$L(-n,\chi) = -\frac{B_{n+1,\chi}}{n+1}.$$

Demostración. Se sigue de la ecuación funcional (6.8). Los detalles se dejan como un ejercicio. ■

6.9.5 Ejemplo: Campos reales abelianos

Estamos listos para probar el teorema de Siegel–Klingen para las extensiones abelianas.

6.9.20. Teorema. *Si $K/\mathbb{Q}$ es un campo de números totalmente real abeliano, entonces $\zeta_K(-n)$ son números racionales no nulos para $n = 1, 3, 5, \ldots$*

Demostración. Dado que $K/\mathbb{Q}$ es una extensión abeliana, tenemos la descomposición de la función zeta

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi),$$

donde $X \subseteq \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ es el grupo de caracteres de Dirichlet que corresponde a $K \subseteq \mathbb{Q}(\zeta_m)$. Ahora ocupando nuestras fórmulas para los valores especiales de funciones L de Dirichlet (corolario 6.9.19),

$$\zeta_K(-n) = (-1)^{[K:\mathbb{Q}]} \prod_{\chi \in X} \frac{B_{n+1,\chi}}{n+1}.$$

Puesto que K es un campo totalmente real, para todo $\chi \in X$ se tiene $\chi(-1) = +1$, así que $B_{n+1,\chi} \neq 0$ para n impar (corolario 6.9.18). Esto también se sigue del hecho de que el orden de anulación de $\zeta_K(s)$ para $s = -1, -3, -5, \ldots$ es igual a r_2, y en nuestro caso $r_2 = 0$. Los números de Bernoulli generalizados $B_{n+1,\chi}$ están en la extensión ciclotómica $\mathbb{Q}(\zeta_m)$, y nos gustaría ver que el producto $\prod_{\chi \in X} B_{n+1,\chi}$ es un número racional. Para esto podemos ocupar la fórmula

$$B_{n+1,\chi} = m^n \sum_{1 \leq a \leq m-1} \chi(a)\, B_{n+1}(a/m)$$

(proposición 6.9.12). Los caracteres $\chi \in X$ pueden ser identificados con caracteres de Galois $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^\times$, y el grupo $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ actúa sobre $\chi \in X$ permutando las raíces de la unidad complejas. Entonces, para todo automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ se tiene $\sigma(B_{n+1,\chi}) = B_{n+1,\sigma\cdot\chi}$. En particular, σ deja fijo el producto $\prod_{\chi \in X} B_{n+1,\chi}$, así que este es un número racional. ∎

Veamos un par de ejemplos particulares.

6.9.21. Ejemplo. En el ejemplo 6.7.18 hemos calculado que si K es el subcampo cúbico real en $\mathbb{Q}(\zeta_7)$, entonces

$$\zeta_K(s) = \zeta(s)\, L(s, \chi)\, L(s, \chi^2),$$

donde χ es el carácter cúbico mód 7. Calculamos los números de Bernoulli correspondientes. Notamos que $B_{k,\chi^2} = B_{k,\overline{\chi}} = \overline{B_{k,\chi}}$, así que $B_{k,\chi}\, B_{k,\chi^2} = |B_{k,\chi}|^2$.

k:	1	2	3	4	5	6	7	8	9	10
B_k:	$\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$
$B_{k,\chi}$:	0	$\frac{8-4\,\zeta_3}{7}$	0	$\frac{-128+88\,\zeta_3}{7}$	0	$672 - 516\,\zeta_3$	0	$\frac{-324736+257456\,\zeta_3}{7}$	0	$\frac{36199840-28945220\,\zeta_3}{7}$
$B_{k,\chi}\, B_{k,\chi^2}$:	0	$\frac{16}{7}$	0	$\frac{5056}{7}$	0	1064592	0	$\frac{36477470464}{7}$	0	$\frac{456580929948400}{7}$
$\zeta_K(1-k)$:	0	$-\frac{1}{21}$	0	$\frac{79}{210}$	0	$-\frac{7393}{63}$	0	$\frac{142490119}{420}$	0	$-\frac{1141452324871}{231}$

```
? f = x^3 + x^2 - 2*x - 1;
? for (k=1,10, print ([-k, bestappr (lfun(f,-k))]))
[-1, -1/21]
[-2, 0]
[-3, 79/210]
[-4, 0]
[-5, -7393/63]
[-6, 0]
[-7, 142490119/420]
[-8, 0]
[-9, -1141452324871/231]
[-10, 0]
```

▲

6.9.22. Ejemplo. En 6.7.19 notamos que para $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ se tiene

$$\zeta_K(s) = \zeta(s)\,\zeta(s, \chi_1)\,\zeta(s, \chi_2)\,\zeta(s, \chi_1)\,\zeta(s, \chi_1\chi_2),$$

donde χ_1 y χ_2 son ciertos caracteres mód 8 y mód 12 respectivamente. Calculamos los números de Bernoulli correspondientes.

k:	1	2	3	4	5	6	7	8	9	10
B_k:	$\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$
B_{k,χ_1}:	0	2	0	−44	0	2166	0	−196888	0	28730410
B_{k,χ_2}:	0	4	0	−184	0	20172	0	−4120688	0	1352745620
$B_{k,\chi_1\chi_2}$:	0	12	0	−2088	0	912996	0	−745928016	0	979492656060
$\zeta_K(1-k)$:	0	1	0	$\frac{22011}{10}$	0	$\frac{2198584943}{3}$	0	$\frac{98499651123679091}{20}$	0	$\frac{3172326639386146564271121}{11}$

Por ejemplo,

$$\zeta_K(-1) = \frac{B_2}{2}\,\frac{B_{2,\chi_1}}{2}\,\frac{B_{2,\chi_2}}{2}\,\frac{B_{2,\chi_1\chi_2}}{2} = 1.$$

```
? f = x^4 - 10*x^2 + 1;
? for (k=0,9, print ([-k, bestappr (lfun(f,-k))]))
[0, 0]
[-1, 1]
[-2, 0]
[-3, 22011/10]
[-4, 0]
[-5, 2198584943/3]
[-6, 0]
[-7, 98499651123679091/20]
[-8, 0]
[-9, 260964086896692937464123458824946270239074535638249907774210 65 /
     904889465108514745889183529986516625 32]
```

```
? bestappr (lfun (f,-9), 11)
% = 3172326639386146564271121/11

? default(realprecision, 100)
? bestappr (lfun (f,-9))
% = 3172326639386146564271121/11
```

Aquí la primera aproximación racional a $\zeta_K(-9)$ es equivocada porque con la precisión por defecto, PARI/GP obtiene el valor aproximado 288393330853286051297374,63636363636364, y aquí hay muy pocos dígitos después de la coma flotante. Para el valor correcto, se puede especificar que nos interesa aproximación con el denominador ≤ 11, o aumentar la precisión. ▲

6.10 Equivalencia aritmética

Clase 30
02/12/20

La fórmula del número de clases nos sugiere que la función zeta $\zeta_K(s)$ trae mucha información aritmética sobre el campo de números K, pero $\zeta_K(s)$ no sabe *todo* de K: es posible que $\zeta_K(s) = \zeta_{K'}(s)$ para dos campos no isomorfos $K \ncong K'$. Aún así, si dos campos comparten la misma función zeta, estos tienen muchas propiedades en común. Este será el tema de la presente sección. La referencia original es el artículo [Per1977], y también recomiendo los apuntes [Sut2018].

6.10.1. Definición. Se dice que dos campos de números $K/\mathbb{Q}$ y $K/\mathbb{Q}$ son **aritméticamente equivalentes** si $\zeta_K(s) = \zeta_{K'}(s)$.

Está claro que esta es una relación de equivalencia, y si $K \cong K'$, entonces los campos son aritméticamente equivalentes. Nuestro objetivo es entender qué precisamente significa la equivalencia aritmética. Primero vamos a revisar la ecuación funcional para $\zeta_K(s)$. Nos conviene reescribirla de manera más simétrica.

6.10.2. Teorema. *Definamos la* ***función zeta de Dedekind completada*** *por*

$$Z_K(s) = |\Delta_K|^{s/2}\, \Gamma_{\mathbb{R}}(s)^{r_1}\, \Gamma_{\mathbb{C}}(s)^{r_2}\, \zeta_K(s),$$

donde

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\, \Gamma\Big(\frac{s}{2}\Big), \quad \Gamma_{\mathbb{C}}(s) = 2\,(2\pi)^{-s}\, \Gamma(s).$$

Luego, $Z_K(s)$ se extiende a una función meromorfa sobre todo el plano complejo con polos simples en $s = 0$ y $s = 1$ que satisface la ecuación funcional

$$Z_K(s) = Z_K(1 - s).$$

Demostración. Véase por ejemplo [Neu1999, §VII.5]. ■

La ecuación funcional impone cierta rigidez sobre $Z_K(s)$ y en particular implica que esta función se determina por el producto de Euler para $\zeta_K(s)$, posiblemente con un número finito de factores quitados. Para verlo, necesitamos la siguiente observación.

6.10.3. Lema. *Dados números reales $1 < x_1 \leq x_2 \leq \cdots \leq x_m$ y $1 < y_1 \leq y_2 \leq \cdots \leq y_n$, definamos las funciones complejas*

$$f(s) = \prod_{1 \leq i \leq m} (1 - x_i^{-s}), \quad g(s) = \prod_{1 \leq j \leq n} (1 - y_j^{-s}), \quad h(s) = \frac{f(s)}{g(s)}.$$

Sea $\phi(s)$ una función meromorfa que no tiene ceros y polos en s que coincide con los ceros o polos de $h(s)$. Supongamos que se cumple una ecuación funcional

$$h(s) = \phi(s)\, h(1 - s).$$

Luego, $f(s) = g(s)$ *y* $\phi(s) = 1$.

Demostración. Las funciones $f(s)$ y $g(s)$ no tienen polos, y sus ceros son $\frac{2\pi ik}{\log x_i}$ y $\frac{2\pi ik}{\log y_j}$ respectivamente para $k \in \mathbb{Z}$. Todo cero de $h(s)$ debe ser un cero de $f(s)$, y por nuestra hipótesis, este no puede ser un cero de $\phi(s)$. Además, las funciones $f(s)$ y $f(1-s)$ no tienen ceros en común (los ceros de $f(s)$ cumplen $\operatorname{Re} s = 0$, mientras que los ceros de $f(1-s)$ cumplen $\operatorname{Re} s = 1$). Entonces, los ceros de $h(s)$ no pueden coincidir con los ceros de $h(1-s)$. Dado que $h(s) = \phi(s)\, h(1-s)$, esto implica que $h(s)$ no tiene ceros. De manera similar se demuestra que $h(s)$ no tiene polos. Entonces, $f(s)$ y $g(s)$ deben tener los mismos ceros de las mismas multiplicidades, así que $(x_1, \ldots, x_m) = (y_1, \ldots, y_n)$ y $f(s) = g(s)$. Se sigue que $h(s) = 1$ y $\phi(s) = 1$. ■

6.10.4. Proposición. *Sean* $K/\mathbb{Q}$ *y* $K'/\mathbb{Q}$ *dos campos de números, y supongamos que salvo un número finito de primos racionales* $p \in \mathbb{Z}$ *se cumple*

$$\prod_{\mathfrak{p} \mid p\mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p} \mid p\mathcal{O}_{K'}} (1 - N_{K'/\mathbb{Q}}(\mathfrak{p})^{-s}).$$

Luego, $\zeta_K(s) = \zeta_{K'}(s)$, $Z_K(s) = Z_{K'}(s)$, $[K : \mathbb{Q}] = [K' : \mathbb{Q}]$, $r_1 = r_1'$, $r_2 = r_2'$, $\Delta_K = \Delta_{K'}$.

Demostración. Sea S el conjunto finito de primos racionales para cuales no se cumple la hipótesis de arriba. Podemos aplicar el lema anterior a las funciones

$$f(s) = \prod_{\substack{\mathfrak{p} \mid p\mathcal{O}_K \\ p \in S}} (1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}), \quad g(s) = \prod_{\substack{\mathfrak{p} \mid p\mathcal{O}_{K'} \\ p \in S}} (1 - N_{K'/\mathbb{Q}}(\mathfrak{p})^{-s}), \quad \phi(s) = \frac{Z_K(s)\, Z_{K'}(1-s)\, \zeta_{K'}(s)\, \zeta_K(1-s)}{Z_{K'}(s)\, Z_K(1-s)\, \zeta_K(s)\, \zeta_{K'}(1-s)}.$$

De hecho, los ceros y polos de $Z_K(s)$ y $\zeta_K(s)$ están en $s = 0$ y $s = 1$, y estos no coinciden con los ceros de $f(s)$ y $f(g)$. Además, calculamos que $\phi(s)\, h(1-s) = h(s)$ usando

$$\zeta_K(1-s)\, f(1-s) = \zeta_{K'}(1-s)\, g(1-s)$$

—por la definición, $f(s)$ y $g(s)$ precisamente corresponden a los factores de Euler de $\zeta_K(s)$ y $\zeta_{K'}(s)$ que no coinciden.

Luego, el lema nos da $f(s) = g(s)$, lo que significa que $\zeta_K(s) = \zeta_{K'}(s)$. Recordemos que los ordenes de ceros de $\zeta_K(s)$ en enteros negativos $s = -n$ son r_2 o $r_1 + r_2$, dependiendo de la paridad de n. Entonces, la igualdad $\zeta_K(s) = \zeta_{K'}(s)$ implica que $r_1 = r_1'$ y $r_2 = r_2'$. Como consecuencia, $[K : \mathbb{Q}] = r_1 + 2r_2 = r_1' + 2r_2' = [K' : \mathbb{Q}]$.

Por el mismo lema anterior, se tiene $\phi(s) = 1$, de donde se deduce

$$Z_K(s)^2 = Z_K(s)\, Z_K(1-s) = Z_{K'}(s)\, Z_{K'}(1-s) = Z_{K'}(s)^2.$$

Calculamos el residuo

$$\lim_{s \to 1^+} (1-s)\, Z_K(s)^2 = |\Delta_K| \left(\pi^{-1/2}\, \Gamma\Big(\frac{1}{2}\Big)\right)^{2r_1} \left(2\,(2\pi)^{-1}\, \Gamma(1)\right)^{2r_2} \zeta_K^*(1)^2 = |\Delta_K|\, \pi^{-2r_2}\, \zeta_K^*(1)^2.$$

Aquí usamos que $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$[*]. Entonces, nuestra identidad nos da

$$|\Delta_K|\, \pi^{-2r_2} = |\Delta_{K'}|\, \pi^{-2r_2'},$$

de donde $|\Delta_K| = |\Delta_K'|$. Recordemos que el signo del discriminante es $(-1)^{r_2}$, así que $\Delta_K = \Delta_{K'}$. ■

Ahora si $p \in \mathbb{Z}$ es un primo racional que no se ramifica en K (es decir, $p \nmid \Delta_K$), entonces se tiene factorización $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, donde los grados de campos residuales $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$ satisfacen $f_1 + \cdots + f_s = [K : \mathbb{Q}]$. De esta manera a cada primo no ramificado corresponde una partición de $[K : \mathbb{Q}]$, y esta se llama el **tipo de descomposición** de p. El siguiente resultado explica el término «equivalencia aritmética».

[*] Este es un caso particular de la ecuación funcional $\Gamma(s)\, \Gamma(1-s) = \frac{\pi}{\operatorname{sen} \pi s}$.

6.10.5. Teorema. *Las siguientes condiciones son equivalentes.*

1) $\zeta_K(s) = \zeta_{K'}(s)$*,*

2) los tipos de descomposición de p en K y K′ coinciden para todo p no ramificado,

3) los tipos de descomposición de p en K y K′ coinciden para todo p, salvo un número finito.

En particular, dos campos aritméticamente equivalentes necesariamente comparten el grado $[K:\mathbb{Q}]$*, el número de encajes reales* r_1 *y complejos* r_2*, y el discriminante* Δ_K*.*

Demostración. Para $n \geq 1$ denotemos por a_n el número de ideales en $\mathcal{O}_K$ de norma n. Tenemos $\zeta_K(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$, y si $\zeta_K(s) = \zeta_{K'}(s)$, entonces $a_n = a'_n$ para todo $n \geq 1$ porque para una serie de Dirichlet los coeficientes a_n están definidos de modo único.

Ahora si $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, entonces $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$. Se sigue que a_p es el número de ideales primos sobre p con el grado del campo residual $f = 1$. Luego, el número de ideales primos con $f = 2$ será $a_{p^2} - \binom{a_p}{2} - a_p$. De la misma manera, el número de ideales primos con el grado del campo residual f se expresa mediante $a_p, a_{p^2}, \ldots, a_{p^{f-1}}$. Entonces, los coeficientes a_n determinan los tipos de descomposición de primos racionales en K. Dado que $a_n = a'_n$, los tipos de descomposición serán los mismos en K y K'. Esto establece la implicación 1)⇒2), y la implicación 2)⇒3) es trivial.

Para la implicación 3)⇒1), notamos que si los tipos de descomposición coinciden, posiblemente salvo un número finito de primos p, entonces los factores de Euler

$$\prod_{\mathfrak{p}\mid p\mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}) = \prod_{\mathfrak{p}\mid p\mathcal{O}_{K'}} (1 - N_{K'/\mathbb{Q}}(\mathfrak{p})^{-s}).$$

coinciden, salvo un número finito de p. La proposición de arriba implica que $\zeta_K(s) = \zeta_{K'}(s)$. ■

6.10.1 Ternas de Gassmann

El matemático suizo Fritz Gassmann (1899–1990) encontró en 1926 una caracterización elemental de la equivalencia aritmética, que da una manera eficaz de verificarla y construir ejemplos no triviales con K y K' no isomorfos.

6.10.6. Definición. Sean G un grupo finito y H, H' sus subrupos. Se dice que (G, H, H') es una **terna de Gassmann** si existe una biyección entre H y H' que preserva las clases de conjugación en G. En otras palabras, si para todo $g \in G$ se tiene

$$\#(H \cap g^G) = \#(H' \cap g^G),$$

donde g^G denota la clase de conjugación de g.

Gassmann probó el siguiente resultado.

6.10.7. Teorema. *Sean K y K′ dos campos de números y* $L/\mathbb{Q}$ *una extensión de Galois tal que* $K, K' \subseteq L$ *(por ejemplo, la cerradura de Galois del compositum KK′). Entonces, K y K′ son aritméticamente equivalentes si y solamente si*

$$(\mathrm{Gal}(L/\mathbb{Q}),\ \mathrm{Gal}(L/K),\ \mathrm{Gal}(L/K'))$$

es una terna de Gassmann.

El teorema de Gassmann nos permite construir ejemplos de campos no isomorfos aritméticamente equivalentes. Para esto basta encontrar una terna de Gassmann (G, H, H') con H y H' subgrupos no conjugados en G y saber realizar G como el grupo de Galois de alguna extensión $L/\mathbb{Q}$[*]. Luego basta tomar $K = L^H$ y $K' = L^{H'}$, y puesto que H y H' no son conjugados, tendremos $K \ncong K'$.

Una manera fácil de construir ternas de Gassmann no triviales es la siguiente.

[*]Recordemos que el **problema inverso** de la teoría de Galois afirma que cualquier grupo finito G se realiza como un grupo de Galois de $L/\mathbb{Q}$. Esta es una gran conjetura, pero la solución existe para muchos G y varias familias infinitas.

6.10.8. Proposición. *Para un grupo finito H definamos la **estadística de ordenes** como la función*

$$\phi_H \colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \#\{h \in H \mid \operatorname{ord} h = n\}.$$

Para dos grupos finitos H y H' existe una terna de Gassmann (G, H, H') si y solamente si $\phi_H = \phi_{H'}$.

Demostración. En una dirección, si (G, H, H') es una terna de Gassmann, entonces por la definición existe una biyección $H \leftrightarrow H'$ que preserva las clases de conjugación en G, y los elementos cada clase de conjugación tienen el mismo orden, así que $\phi_H = \phi_{H'}$.

En la otra dirección, supongamos que $\phi_H = \phi_{H'}$. Pongamos $n = \#H = \#H'$ y sea G el grupo simétrico S_n. La acción de H sobre sí mismo mediante la multiplicación por la izquierda nos da encajes $H, H' \hookrightarrow G$. Todo $h \in H$ da lugar a una permutación que consiste en $\frac{n}{\operatorname{ord} h}$ ciclos de longitud $\operatorname{ord} h$. Ahora $h \in H$ y $h' \in H'$ serán conjugados en G si y solamente si $\operatorname{ord} h = \operatorname{ord} h'$. Dado que $\phi_H = \phi_{H'}$, podemos escoger una biyección $H \leftrightarrow H'$ que preserva los ordenes de elementos, y luego las clases de conjugación en G. Esto nos da una terna de Gassmann (G, H, H'). ■

Todo grupo simétrico se realiza como un grupo de Galois de alguna extensión $L/\mathbb{Q}$, así que el último argumento nos permite construir ejemplos de equivalencia aritmética. Sin embargo, la extensión $L/\mathbb{Q}$ tendrá grado $n!$, así que este método no será muy eficaz.

6.10.9. Ejemplo. Con ayuda de computadora, ocupando el programa GAP[*], se pueden buscar grupos no isomorfos H y H' de pequeño orden $\#H = \#H'$ tales que $\phi_H = \phi_{H'}$. Resulta que el ejemplo más pequeño se realiza por grupos de orden 16. Por ejemplo, podemos tomar $H = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ y el producto semidirecto no trivial $H' = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.[**]

Las clases de conjugación en H son triviales. Hay tres elementos de orden 2: estos son $(0,2)$, $(2,0)$, $(2,2)$. El resto de elementos no triviales tienen orden 4, en total son $16 - 3 - 1 = 12$. Por otra parte, en H' las clases de conjugación son las siguientes.

orden de elementos:	1	2	4
tamaño de clase:	1	1	2
número de clases:	1	3	6

La estadística de ordenes es la misma. ▲

6.10.10. Ejemplo. Por otra parte, la búsqueda en GAP nos dice que el grupo más pequeño G que admite una terna de Gassmann (G, H, H') con H y H' no conjugados tiene orden 32 (en la notación de GAP, este es `[32,43]`).

```
isGassmannTripple := function (H,Hp,cc)
  local c;

  for c in cc do
    if Size(Intersection(H,c)) <> Size(Intersection(Hp,c)) then
      return false;
    fi;
  od;

  return true;
end;;
```

[*] https://gap-system.org/

[**] Estos dos grupos están tabulados en *Small Groups Library* de GAP como `[16,2]` y `[16,4]`.

Para obtener campos K y K' de grado menor posible, vamos a minimizar el índice $[G : H]$ / maximizar el orden $\#H$.

```
findGassmannTriple := function (G)
  local cc, ccSubgr, i, j, H, Hp, hSize, triple;

  triple := [];
  hSize := 0;
  triple := [];

  cc := ConjugacyClasses(G);
  ccSubgr := ConjugacyClassesSubgroups(G);

  for i in [1..Size(ccSubgr)] do
    for j in [i+1..Size(ccSubgr)] do
      # H and H' must have the same size
      if (Size(Representative(ccSubgr[i])) <>
            Size(Representative(ccSubgr[j]))) then
        continue;
      fi;

      for H in Elements (ccSubgr[i]) do
        for Hp in Elements (ccSubgr[j]) do
          if isGassmannTripple (H,Hp,cc) and Size(H) > hSize then
            triple := [G,H,Hp];
            hSize := Size(H);
          fi;
        od;
      od;

    od;
  od;

  return triple;
end;;
```

```
gap> findGassmannTriple (SmallGroup(32,43));
[ <pc group of size 32 with 5 generators>, Group([ f2, f3 ]),
  Group([ f2*f4, f3 ]) ]
gap> Size(last[2]);
4
```

En este caso $[G : H] = 8$, y G puede ser realizado como un grupo de Galois de alguna extensión $L/\mathbb{Q}$, lo que nos da un ejemplo de dos campos no isomorfos aritméticamente equivalentes de grado 8. Con ayuda de PARI/GP o LMFDB, encontramos dos campos específicos definidos por polinomios irreducibles

$$f = x^8 - x^4 - 1, \quad f' = x^8 - 4x^6 + 5x^4 - 2x^2 - 1.$$

En este caso $r_1 = 2$, $r_2 = 3$, y el discriminante correspondiente es $-2^{16} \cdot 5^4 = -40960000$.

Para verificar la equivalencia aritmética de manera indirecta, sin ocupar los grupos de Galois, podemos recurrir a las siguientes consideraciones. El teorema de Kummer–Dedekind nos dice que que salvo un número finito de primos, el tipo de descomposición de p en $\mathcal{O}_K$ es el mismo que el tipo de descomposición del polinomio f mód p. Podemos entonces escribir un código que compara los tipos de descomposición de f y f' para una cantidad suficientemente grande de primos.

```
dectype (f,p) = {
  local (dec = factor(f*Mod(1,p)));
  vecsort (vector (matsize(dec)[1], i, poldegree(dec[i,1])))
};

N = 10^6;

compare (f1,f2) = {
  local (badprimes = List());

  forprime (p=2,N,
    if (dectype(f1,p) != dectype(f2,p),
      listput (badprimes,p)
    )
  );

  Vec(badprimes)
};
```

Aquí esencialmente estamos comparando los factores de Euler de las funciones zeta $\zeta_K(s)$ y $\zeta_{K'}(s)$, salvo un número finito, que como ya sabemos, no afectan el resultado. Por otra parte, el cálculo de los valores de las funciones zeta con una buena precisión requiere bastante memoria, y por esto lo evitamos.

```
? f1 = x^8 - x^4 - 1;
? f2 = x^8 - 4*x^6 + 5*x^4 - 2*x^2 - 1;
? compare (f1,f2)
? = []
? K1 = nfinit(f1);
? K2 = nfinit(f2);
? nfisisom(K1,K2)
% = 0
? K1.disc
% = -40960000
? K2.disc
% = -40960000
? K1.sign
% = [2, 3]
? K2.sign
% = [2, 3]
```

▲

6.10.11. Ejemplo. El artículo de Perlis [Per1977] contiene un argumento sencillo de la teoría de grupos que demuestra que para una terna de Gassmann no trivial (G, H, H') necesariamente se tiene $[G : H] \geq 7$. Esto

significa que los campos no isomorfos de grado ≤ 6 no pueden ser aritméticamente equivalentes. Perlis dice que un campo K es **solitario** si todo campo aritméticamente equivalente a K debe ser isomorfo a K.

De nuevo, usando GAP, se puede verificar que el grupo más pequeño que nos da una terna con $[G : H] = 7$ es $G = \mathrm{GL}_3(\mathbb{F}_2)$.

```
gap> findGassmannTriple(GL(3,2));
[ SL(3,2), <matrix group of size 24 with 4 generators>,
  <matrix group of size 24 with 4 generators> ]
gap> Size(last[1])/Size(last[2]);
7
```

De hecho, hay una manera geométrica de obtener la terna de Gassmann en cuestión. El grupo $\mathrm{GL}_3(\mathbb{F}_2) \cong \mathrm{SL}_3(\mathbb{F}_2) \cong \mathrm{PSL}_3(\mathbb{F}_2)$ actúa sobre los 7 puntos de $\mathbb{A}^3(\mathbb{F}_2) \setminus \{0\}$, y por otra parte sobre los 7 hiperplanos en este espacio que corresponden a los puntos del plano proyectivo $\mathbb{P}^2(\mathbb{F}_2)$. Estas acciones son 2-transitivas[*]. Ahora sean P un punto no nulo en $\mathbb{A}^3(\mathbb{F}_2)$ y L el hiperplano ortogonal correspondiente. Una matriz $A \in \mathrm{GL}_3(\mathbb{F}_2)$ fija L si y solamente si la matriz traspuesta A^t fija P. Sean H el grupo estabilizador de P y H' el estabilizador de L. Se puede ver que H y H' no son conjugados, y para toda matriz $A \in \mathrm{GL}_3(\mathbb{F}_2)$ existe una biyección

$$(H \cap A^G) \leftrightarrow (H' \cap A^G).$$

Especificamente, esta biyección viene dada por $B \mapsto B^t$, ya que toda matriz es conjugada con su traspuesta.

Realizando $\mathrm{GL}_3(\mathbb{F}_2)$ como un grupo de Galois, a partir de esta terna de Gassmann se pueden encontrar polinomios específicos

$$f = x^7 - 7x - 3, \quad f' = x^7 - 7x^4 - 21x^3 + 21x^2 + 42x - 9.$$

En este caso $r_1 = 3$, $r_2 = 2$, $\Delta = 3^6 \cdot 7^8 = 4202539929$.

```
? f1 = x^7 - 7*x - 3;
? f2 = x^7 - 7*x^4 - 21*x^3 + 21*x^2 + 42*x - 9;
? compare (f1,f2);
% = [3]
? K1 = nfinit(f1);
? K2 = nfinit(f2);
? nfisisom(K1,K2)
% = 0
? K1.disc
% = 4202539929
? K2.disc
% = 4202539929
? K1.sign
% = [3, 2]
? K2.sign
% = [3, 2]
```

▲

Más ejemplos particulares de campos aritméticamente equivalentes de grado pequeño se encuentran en el artículo [BdS2002]. Antes de discutir la prueba del teorema de Gassmann, notamos su consecuencia importante.

[*] Para cualesquiera (x, y), (x', y') con $x \neq y$, $x' \neq y'$ existe $g \in G$ tal que $(g \cdot x, g \cdot y) = (x', y')$

6.10.12. Corolario. *Si K y K' son aritméticamente equivalentes, entonces $\mathcal{O}_K^\times \cong \mathcal{O}_{K'}^\times$.*

Demostración. Primero, $r_1 = r_1'$ y $r_2 = r_2'$ implica que

$$\operatorname{rk} \mathcal{O}_K^\times = r_1 + r_2 - 1 = r_1' + r_2' - 1 = \operatorname{rk} \mathcal{O}_{K'}^\times.$$

Nos falta ver que las partes de torsión de los grupos de unidades también coinciden; es decir, que $\mu_K = \mu_{K'}$.

Por la definición, el **corazón normal**[*] de K es el subcampo más grande $F \subseteq K$ tal que la extensión $F/\mathbb{Q}$ es normal. Este será precisamente el subcampo de L fijo por el subgrupo generado por todos los subgrupos conjugados H^g para $g \in G$. Por la definición de ternas de Gassmann, para todo $h \in H$ tenemos $\#(H \cap h^G) = \#(H' \cap H^G) \neq 0$. En particular, algún conjugado h^g está en H'. De aquí se sigue fácilmente que $\langle H^g \mid g \in G\rangle = \langle H'^g \mid g \in G\rangle$, así que K y K' comparten el mismo corazón normal.

Las extensiones ciclotómicas $\mathbb{Q}(\mu_K)/\mathbb{Q}$ y $\mathbb{Q}(\mu_{K'})/\mathbb{Q}$ son normales, así que ambas están en el corazón normal de K y K', y por ende $\mu_K = \mu_{K'}$. ■

6.10.13. Corolario. *Si K y K' son aritméticamente equivalentes, entonces*

$$\operatorname{Reg}_K \, h_K = \operatorname{Reg}_{K'} \, h_{K'}.$$

Demostración. Dado que $\zeta_K(s) = \zeta_{K'}(s)$, las funciones zeta tienen el mismo residuo en $s = 1$ que nos da la fórmula del número de clases:

$$\frac{2^{r_1}\,(2\pi)^{r_2}\,\operatorname{Reg}_K\, h_K}{\#\mu_K\,\sqrt{|\Delta_K|}} = \frac{2^{r_1'}\,(2\pi)^{r_2'}\,\operatorname{Reg}_{K'}\, h_{K'}}{\#\mu_{K'}\,\sqrt{|\Delta_{K'}|}}.$$

Aquí $r_1 = r_1'$, $r_2 = r_2'$, $\Delta_K = \Delta_{K'}$. ■

Esto nos deja con la siguiente pregunta: ¿será también cierto que la equivalencia aritmética implica que $\operatorname{Reg}_K = \operatorname{Reg}_{K'}$ y $h_K = h_{K'}$? La respuesta es *negativa*.

6.10.14. Ejemplo. En [dSP1994] de Smit y Perlis construyen una familia de ejemplos, entre cuales está

$$K = \mathbb{Q}(\sqrt[8]{-15}), \quad K' = \mathbb{Q}(\sqrt[8]{-240}).$$

Estos dos campos son aritméticamente equivalentes, pero

$$\operatorname{Reg}_K = 66{,}316448\ldots, \quad h_K = 16, \quad \operatorname{Reg}_{K'} = 132{,}632896\ldots, \quad h_{K'} = 8.$$

```
? f1 = x^8 + 15;
? f2 = x^8 + 240;
? compare (f1,f2);
% = []
? K1 = bnfinit(f1);
? K2 = bnfinit(f2);
? nfisisom(K1,K2)
% = 0
? K1.disc
% = 174960000000
? K2.disc
% = 174960000000
? K1.sign
% = [0, 4]
```

[*] *normal core* en inglés y *cœur* en francés

```
? K2.sign
% = [0, 4]
? K1.no
% = 16
? K2.no
% = 8
? K1.reg
% = 66.316448148870962189601403176835356992
? K2.reg
% = 132.63289629774192437920280635367071398
```

▲

Entonces, la función zeta $\zeta_K(s)$ sabe mucho del campo de números K, ¡pero no todo! En algún sentido, esto pasa porque, aunque los invariantes aritméticos de K aparecen en las fórmulas para los valores especiales de $\zeta_K(s)$, estos invariantes están «entrelazados» entre sí.

6.10.2 Demostración del teorema de Gassmann

Para probar el teorema de Gassmann 6.10.7, necesitamos revisar cómo el automorfismo de Frobenius determina el tipo de descomposición de primos racionales. Sea $L/\mathbb{Q}$ una extensión de Galois y $K \subseteq L$ un subcampo. Denotemos $G = \mathrm{Gal}(L/\mathbb{Q})$ y $H = \mathrm{Gal}(L/K)$.

1. A todo primo racional p que no se ramifica en L corresponde el automorfismo de Frobenius $\mathrm{Frob}_p \in G$. El teorema de densidad de Chebotarëv (véase 4.4.5) nos dice que para cada $\sigma \in G$ existe un número infinito de p tales que Frob_p tiene la misma clase de conjugación que σ.

2. El teorema 4.5.1 nos dice que para p no ramificado en L el tipo de descomposición $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ se determina por la acción de Frob_p sobre las clases laterales

   $$H\backslash G = \{H\tau \mid \tau \in G\}$$

   por la multiplicación por la derecha. Específicamente, los grados de campos residuales $f_1, \ldots, f_s$ corresponden exactamente al tipo de ciclo de Frob_p visto como una permutación del conjunto $H\backslash G$.

3. En general, dada una representación por permutaciones $G \to \mathrm{Sym}(X)$, la traza correspondiente cuenta los puntos fijos y da lugar a un carácter $\chi\colon G \to \mathbb{Z}$ que es una función constante sobre las clases laterales.

   $$\chi(\sigma) = \#\{x \in X \mid \sigma(x) = x\}.$$

   El tipo de ciclo de cada $\sigma \in G$ se determina por el carácter χ, específicamente por los valores de $\chi(\sigma^n)$ para $n = 1, 2, 3, \ldots$

4. En nuestro caso particular, nos interesa la representación $G \to \mathrm{Sym}(H\backslash G)$ y el carácter correspondiente

   $$\chi_H(\sigma) = \#\{H\tau \in H\backslash G \mid H\tau\sigma = H\tau\}.$$

Ahora supongamos que $K, K' \subseteq L$ son dos subcampos y $H = \mathrm{Gal}(L/K)$, $H' = \mathrm{Gal}(L/K')$.

6.10.15. Lema. *Los campos K y K' son aritméticamente equivalentes si y solamente si $\chi_H = \chi_{H'}$.*

Demostración. Si K y K' son aritméticamente equivalentes, entonces salvo un número finito, todo primo p tiene el mismo tipo de descomposición en K y K'. Entonces, el tipo de ciclo de la acción de Frob_p sobre $H\backslash G$

y $H'\backslash G$ coincide. Puesto que cada clase de conjugación σ^G se realiza por Frob_p por un número infinito de p, esto implica que $\chi_H = \chi_{H'}$.

Viceversa, si $\chi_H = \chi_{H'}$, entonces para todo p no ramificado en L el tipo de ciclo de Frob_p actuando sobre $H\backslash G$ y $H'\backslash G$ coincide. Esto implica que el tipo de descomposición de p en K y K' es el mismo. Entonces, K y K' son aritméticamente equivalentes. ■

Para probar el teorema de Gassmann, nos falta relacionar la condición $\chi_H = \chi_{H'}$ con las ternas de Gassmann.

6.10.16. Lema. *Para un grupo finito G, dos subgrupos $H, H' \subset G$ dan lugar a una terna de Gassmann (G, H, H') si y solamente si $\chi_H = \chi_{H'}$.*

Demostración. Definamos

$$\psi_H \colon G \to \mathbb{Z}, \quad \sigma \mapsto \#(H \cap \sigma^G).$$

Esta es una función constante sobre las clases de conjugación, y por la definición, (G, H, H') es una terna de Gassmann si y solamente si $\psi_H = \psi_{H'}$.

Para $\sigma \in G$ consideremos el centralizador correspondiente

$$C_G(\sigma) = \{\tau \in G \mid \tau\sigma = \sigma\tau\}.$$

Este es el estabilizador de la acción de G sobre la clase de conjugación σ^G mediante la conjugación. Tenemos

$$\psi_H(\sigma) \cdot \#C_G(\sigma) = \#\{\tau \in G \mid \tau\sigma\tau^{-1} \in H\} = \#\{\tau \in G \mid H\tau\sigma = H\tau\} = \chi_H(\sigma) \cdot \#H.$$

Podemos definir entonces la función $\phi_H \colon G \to \mathbb{Q}$ mediante $\phi_H(\sigma) = \#C_G(\sigma)/\#H$. El cálculo de arriba nos dice que $\chi_H = \psi_H \phi_H$.

Ahora si (G, H, H') es una terna de Gassmann, entonces $\phi_H = \psi_{H'}$ y $\phi_H = \phi_{H'}$ (dado que $\#H = \#H'$). Esto implica que $\chi_H = \chi_{H'}$. Viceversa, si $\chi_H = \chi_{H'}$, entonces $\phi_H = \phi_{H'}$, dado que $\#(H\backslash G) = \chi_H(1) = \chi_{H'}(1) = \#(H'\backslash G)$. Esto implica que $\psi_H = \psi_{H'}$, así que (G, H, H') es una terna de Gassmann. ■

Juntando todas las observaciones, se obtiene una prueba del teorema de Gassmann 6.10.7.

Ejercicios

Ejercicio 6.1. Dado un número natural n, calcule el número de representaciones $n = x^2 - xy + y^2$ con $x, y \in \mathbb{Z}$.
(Considere la función zeta de $\mathbb{Q}(\zeta_3)$.)

Ejercicio 6.2 (Símbolo de Kronecker)**.** Para $a \in \mathbb{Z}$ libre de cuadrados, $a \equiv 0 \pmod 4$, definamos el **símbolo de Kronecker** χ_a de la siguiente manera.

- Si $p \mid a$, entonces $\chi_a(p) = 0$.
- Si $p \nmid a$ es un primo impar, entonces $\chi_a(p) = \left(\frac{a}{p}\right)$ es el símbolo de Legendre.
- $\chi_a(2) = +1$ si $a \equiv 1 \pmod 8$ y $\chi_a(2) = -1$ si $a \equiv 5 \pmod 8$.
- En geleral, si $\pm b = p_1 \cdots p_s$, entonces $\chi_a(n) = \chi_a(p_1) \cdots \chi_a(p_s)$.

Demuestre las siguientes propiedades.

1) $\chi_d(n) = \left(\frac{n}{d}\right)$ es el símbolo de Jacobi para n impar.
2) Si $n > 0$, $\mathrm{mcd}(a, n) = 1$, $a = 2^t c$ con c impar, entonces
$$\chi_a(n) = (-1)^{\frac{c-1}{2}\,\frac{n-1}{2}}\, \chi_2(n)^t\, \chi_n(c).$$
3) $\chi_a(m) = \chi_a(n)$ si $m \equiv n \pmod a$.

Ejercicio 6.3. Para un campo cuadrático $K = \mathbb{Q}(\sqrt{d})$ consideremos el símbolo de Kronecker $\chi = \chi_{\Delta_K}$.

1) Demuestre que χ es un carácter de Dirichlet mód $|\Delta_K|$.
2) Demuestre que χ determina la factorización de primos racionales en $\mathcal{O}_K$:
$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}\,\overline{\mathfrak{p}}, & \text{si } \chi(p) = +1, \\ \mathfrak{p}, & \text{si } \chi(p) = -1, \\ \mathfrak{p}^2, & \text{si } \chi(p) = 0. \end{cases}$$
3) Demuestre que $\zeta_K(s) = \zeta(s)\, L(s, \chi)$.

Ejercicio 6.4. Sea p un número primo y χ el carácter de Dirichlet de orden 2 mód p, definido por el símbolo de Legendre $\chi(n) = \left(\frac{n}{p}\right)$.

1) Demuestre que
$$\exp(g(\chi)\, L(1, \chi)) = \prod_n (1 - \zeta_p^n) \prod_r (1 - \zeta_p^r)^{-1},$$
donde $g(\chi) = \sum_{1 \le a \le p-1} \chi(a)\, \zeta_p^a$, y los productos son sobre los no-residuos y residuos cuadráticos mód p respectivamente.
2) Use la parte anterior para calcular $L(1, \chi)$, donde χ es el carácter de orden 2 mód 5. (Para el valor numérico en PARI/GP, basta digitar `lfun(5,1)`)

Ejercicio 6.5. Sean X un grupo de caracteres de Dirichlet y K un subcampo de $\mathbb{Q}(\zeta_m)$ correspondiente. Demuestre que K es un campo real si y solamente si todos los caracteres $\chi \in X$ son pares (satisfacen $\chi(-1) = +1$).

Ejercicio 6.6. Los números y polinomios de Bernoulli tienen parientes muy cercanos: los **números y polinomios de Euler**. Estos se definen por las funciones generatrices

$$\frac{2}{e^t + e^{-t}} = \sum_{k\geq 0} \frac{E_k}{k!}\, t^k, \quad \frac{2e^{xt}}{e^t + 1} = \sum_{k\geq 0} E_k(x)\, \frac{t^k}{k!}.$$

Demuestre las identidades.

$$E_k = 2^k E_k\left(\frac{1}{2}\right), \quad E_k(x+1) + E_k(x) = 2\,x^k, \quad E_k(1-x) = (-1)^k E_k(x), \quad E_k'(x) = k\,E_{k-1}(x).$$

Ejercicio 6.7 (Continuación)**.** Consideremos la función periódica $f(x) = E_k(x - \lfloor x \rfloor)$.

a) Demuestre que la serie de Fourier para $f(x)$ viene dada por

$$f(x) = \frac{2 \cdot k!}{(\pi i)^{k+1}} \sum_{n\in\mathbb{Z}} \frac{e^{(2n+1)\pi i x}}{(2n+1)^{k+1}}.$$

b) Deduzca que para la **función beta** $\beta(s) = \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)^s}$ se tiene

$$\beta(2k+1) = (-1)^k \frac{E_{2k}}{4^{k+1}\,(2k)!}\, \pi^{2k+1}.$$

Ejercicio 6.8 (Continuación)**.** Sea χ el carácter de Dirichlet no trivial mód 4.

a) Demuestre que $\beta(s) = L(s,\chi)$.

b) Exprese los valores especiales $\beta(2k+1)$ en términos de $B_{2k+1,\chi}$.

c) Demuestre que $E_k = -\frac{2B_{k+1,\chi}}{k+1}$.

Apéndice A

Campos y la teoría de Galois básica

El propósito de este apéndice es resumir la teoría campos y teoría de Galois necesaria para nuestros propósitos. Será suficiente considerar extensiones finitas K/F, y de hecho nos interesará más que todo el caso de $F = \mathbb{Q}$. Otras fuentes recomendadas son [Mor1996] y el pequeño libro de Artin [Artin-Galois] (¡el primer tratamiento moderno y conciso de la teoría de Galois!).

A.1 Extensiones de campos

A.1.1. Definición. Si K es un campo y $F \subseteq K$ es un subcampo, se dice que K es una **extensión** de F y se escribe «K/F» o se dibuja el diagrama

$$\begin{array}{c} K \\ | \\ F \end{array}$$

La dimensión de K como un espacio vectorial sobre F se llama el **grado** de la extensión y se denota por $[K : F] = \dim_F(K)$. Si el grado es finito, se dice que K/F es una **extensión finita**.

A.1.2. Proposición. *Para una torre de extensiones finitas $F \subseteq K \subseteq L$ se tiene*

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

Específicamente, si $\alpha_1, \ldots, \alpha_m \in K$ es una base de K sobre F y $\beta_1, \ldots, \beta_n \in L$ es una base de L sobre K, entonces los productos $\alpha_i\beta_j$ forman una base de L sobre F.

$$\begin{array}{rl} L & \beta_1, \ldots, \beta_n \\ {\scriptstyle [L:K]=n}\,\big| & \\ K & \alpha_1, \ldots, \alpha_m \\ {\scriptstyle [K:F]=m}\,\big| & \\ F & \end{array}$$

Demostración. Ejercicio para el lector. ■

A.1.3. Teorema. *Sea F un campo y $f \in F[x]$ un polinomio irreducible de grado n.*

1) *El anillo cociente $K = F[x]/(f)$ es un campo.*
2) *el homomorfismo canónico $F \hookrightarrow F[x] \twoheadrightarrow F[x]/(f)$ identifica F con un subcampo de K y entonces $F[x]$ con un subanillo de $K[x]$. Considerando f como un elemento de $K[x]$, se tiene $f(\alpha) = 0$.*

3) si $\alpha \in K$ es la imagen de la variable x en el cociente, entonces $[K : F] = n$, y los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forman una base de K sobre F.

Demostración. El anillo de polinomios $F[x]$ es un dominio de ideales principales, y entonces si f es irreducible, el ideal $(f) \subset F[x]$ es maximal. Esto significa que $F[x]/(f)$ es un campo.

Todo elemento de $F[x]/(f)$ puede ser representado por algún polinomio $g \in F[x]$ considerado módulo f. La división con resto en $F[x]$ nos permite concluir que podemos asumir que $\deg(g) < \deg(f)$, así que

$$\overline{g} = a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} \in K.$$

Entonces, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ generan a K como un espacio vectorial sobre F. Ahora si se cumple $\overline{g} = 0$, esto significa que $f \mid g$, pero luego $g = 0$ y $a_0 = a_1 = \cdots = a_{n-1} = 0$. Esto significa que $1, \alpha, \ldots, \alpha^{n-1}$ son linealmente independientes sobre F. ■

Hemos visto cómo añadir a un campo F una raíz de un polinomio irreducible $f \in F[x]$ de manera formal: hay que pasar al cociente $F[x]/(f)$. En muchos casos estas raíces ya están en una extensión específica de F y pueden ser añadidas en el siguiente sentido.

A.1.4. Definición. Para una extensión de campos K/F y elementos $\alpha_1, \alpha_2, \ldots \in K$ el subcampo mínimo de K que contiene a $\alpha_1, \alpha_2, \ldots$ y todos los elementos de F se llama el subcampo **generado** por $\alpha_1, \alpha_2, \ldots$ sobre F y se denota por

$$F(\alpha_1, \alpha_2, \ldots) = \bigcap_{\substack{F \subseteq F' \subseteq K \\ \alpha_1, \alpha_2, \ldots \in F'}} F'.$$

Las extensiones de la forma $F(\alpha)/F$ para un solo elemento $\alpha \in K$ se llaman las **extensiones simples** de F. En este caso α se llama un **elemento primitivo** de $F(\alpha)$. En general, las extensiones de la forma $F(\alpha_1, \ldots, \alpha_n)/F$ se llaman las **extensiones finitamente generadas** de F.

No es difícil verificar que $F(\alpha, \beta) = (F(\alpha))(\beta)$.

A.1.5. Definición. Para una extensión K/F se dice que un elemento $\alpha \in K$ es **algebraico** sobre F si $f(\alpha) = 0$ para algún polinomio no nulo $f \in F[x]$.

Se dice que K/F es una extensión algebraica si todo elemento de K es algebraico sobre F.

A.1.6. Proposición. *Para una cadena de extensiones $F \subseteq K \subseteq L$, si $\alpha \in L$ es algebraico sobre F, entonces es algebraico sobre K.*

Demostración. Si $f(\alpha) = 0$ para algún polinomio no nulo $f \in F[x]$, en particular $f \in K[x]$. ■

A.1.7. Proposición. *Toda extensión finita es algebraica.*

Demostración. Si K/F es una extensión de grado $[K : F] = n$, entonces para cualquier elemento $\alpha \in K$ hay una dependencia F-lineal entre $1, \alpha, \alpha^2, \ldots, \alpha^n$, pero esto nos da un polinomio no nulo $f \in F[x]$ tal que $f(\alpha) = 0$. ■

A.2 Polinomio mínimo

A.2.1. Teorema (Polinomio mínimo). *Sean K/F una extensión de campos y $\alpha \in K$ un elemento.*

1) α es algebraico sobre F si y solamente si el homomorfismo de evaluación

$$ev_\alpha : F[x] \to F(\alpha), \quad f \mapsto f(\alpha)$$

tiene núcleo no trivial.

2) *En este caso* $\ker ev_\alpha = (f_F^\alpha)$*, donde* $f_F^\alpha \in F[x]$ *es un polinomio mónico irreducible definido de modo único; a saber,* f_F^α *es el polinomio mónico de grado mínimo posible que tiene* α *como su raíz.*

3) *Hay un isomorfismo natural* $F[x]/(f_F^\alpha) \cong F(\alpha)$*, y* $[F(\alpha) : F] = \deg(f_F^\alpha)$.

4) *Un polinomio* $g \in F[x]$ *tiene al elemento* α *como su raíz si y solamente si* $f_F^\alpha \mid g$*. Si* g *es irreducible, entonces* $F[x]/(g) \cong F(\alpha)$.

Demostración. Puesto que $F[x]$ es un dominio de ideales principales, se tiene necesariamente $\ker ev_\alpha = (f)$ para algún polinomio $f \in F[x]$. Si α no es algebraico, entonces $f = 0$. En el caso contrario, al revisar la prueba de que $F[x]$ es un DIP, se ve que f es un polinomio del mínimo grado posible tal que $f(\alpha) = 0$. Esto en particular implica que f es irreducible, y luego $F[x]/(f)$ es un campo (véase A.1.3).

Como siempre, un generador de un ideal principal está bien definido salvo elementos invertibles, en este caso salvo $F[x]^\times = F^\times$. Entonces, la condición de que f sea mónico lo define de modo único. Denotemos este polinomio mónico por f_F^α.

Se ve que el homomorfismo ev_α induce un isomorfismo de campos $F[x]/(f_F^\alpha) \cong F(\alpha)$, y como ya notamos en A.1.3, $[F(\alpha) : F] = \deg(f_F^\alpha)$.

Ahora para cualquier otro polinomio $g \in F[x]$ tenemos

$$g(\alpha) = 0 \iff g \in \ker ev_\alpha = (f_F^\alpha) \iff f_F^\alpha \mid f.$$

Si g es también irreducible, entonces $(f) = (f_F^\alpha)$, y luego $F[x]/(g) = F[x]/(f_F^\alpha) \cong F(\alpha)$. ■

A.2.2. Definición. Para una extensión K/F y un elemento $\alpha \in K$ algebraico sobre F, el polinomio mónico $f_F^\alpha \in F[x]$ de arriba se llama el **polinomio mínimo** de α sobre K.

A.2.3. Proposición. *Sea* $F \subseteq K \subseteq L$ *una cadena de extensiones y* $\alpha \in L$ *un elemento algebraico sobre* F*. Entonces, en el anillo de polinomios* $K[x]$ *se cumple* $f_K^\alpha \mid f_F^\alpha$*. En particular,* $[K(\alpha) : K] \leq [F(\alpha) : F]$.

Demostración. Tenemos $f_F^\alpha(\alpha) = 0$. Puesto que $f_F^\alpha \in F[x] \subseteq K[x]$, se cumple $f_K^\alpha \mid f_F^\alpha$. ■

He aquí una caracterización de los elementos algebraicos.

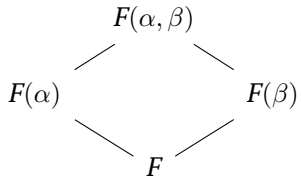
A.2.4. Proposición. *Un elemento* $\alpha \in K$ *es algebraico sobre* F *si y solo si* $[F(\alpha) : F] < \infty$.

Demostración. Ya hemos visto que si α es algebraico, entonces existe un polinomio mínimo y $[F(\alpha) : F] = \deg f_K^\alpha < \infty$. Viceversa, si $[F(\alpha) : F] < \infty$, entonces la extensión $F(\alpha)/F$ es algebraica, como notamos en A.1.7. ■

A.2.5. Proposición. *Para elementos* $\alpha, \beta \in K$ *algebraicos sobre* F *se cumple*

$$[F(\alpha, \beta) : F] \leq [F(\alpha) : F] \cdot [F(\beta) : F].$$

Demostración. Consideremos las extensiones



La desigualdad de A.2.3 aplicada a las extensiones $F \subseteq F(\alpha) \subseteq F(\alpha, \beta)$ y $\beta \in F(\alpha, \beta)$ nos da

$$[(F(\alpha))(\beta) : F(\alpha)] \leq [F(\beta) : F],$$

de donde

$$[F(\alpha, \beta) : F] = [(F(\alpha))(\beta) : F(\alpha)] \cdot [F(\alpha) : F] \leq [F(\beta) : F] \cdot [F(\alpha) : F].$$ ■

Por inducción se sigue que en general,

$$[F(\alpha_1,\ldots,\alpha_n):F] \leq [F(\alpha_1):F]\cdots[F(\alpha_n):F].$$

Tenemos la siguiente caracterización de extensiones finitas.

A.2.6. Proposición. *Una extensión K/F es finita si y solo si $K = F(\alpha_1,\ldots,\alpha_n)$, donde $\alpha_1,\ldots,\alpha_n \in F$ es un número finito de elementos algebraicos sobre F.*

Demostración. Si K/F es una extensión finita de grado n, sea $\alpha_1,\ldots,\alpha_n$ una base de K sobre F. Tenemos $[F(\alpha_i):F] \leq n$, así que $\alpha_1,\ldots,\alpha_n$ son algebraicos. Está claro que $K = F(\alpha_1,\ldots,\alpha_n)$.

Viceversa, si $K = F(\alpha_1,\ldots,\alpha_n)$ donde $\alpha_1,\ldots,\alpha_n$ son algebraicos sobre F, entonces

$$[K:F] \leq [F(\alpha_1):F]\cdots[F(\alpha_n):F],$$

así que la extensión es finita. ■

Hay otra noción relacionada con el polinomio mínimo que es el **polinomio característico**.

A.2.7. Definición. Para una extensión K/F y $\alpha \in K$, el **polinomio característico** $f^{\alpha}_{K/F}$ es el polinomio característico de la aplicación F-lineal

$$\mu_\alpha : K \to K, \quad x \mapsto \alpha x.$$

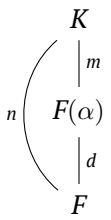
En otras palabras, si A es una matriz que representa a μ_A en alguna base de K sobre F, entonces $f^{\alpha}_{K/F} = \det(x\,I_n - A) \in F[x]$.

Según el teorema de Cayley–Hamilton, tenemos $f^{\alpha}_{K/F}(\alpha) = 0$, y en particular, el polinomio mínimo f^{α}_{F} siempre divide al polinomio característico $f^{\alpha}_{K/F}$. Ahora si $K = F(\alpha)$, entonces los grados de los dos polinomios coinciden y entonces $f^{\alpha}_{K/F} = f^{\alpha}_{K/F}$. En general, la relación es la siguiente.

A.2.8. Proposición. *Sean K/F una extensión finita y $\alpha \in K$. Luego,*

$$f^{\alpha}_{K/F} = (f^{\alpha}_{F})^{[K:F(\alpha)]}.$$

Demostración. Pongamos $n = [K:F]$ y $d = [F(\alpha):F]$. Consideremos las extensiones



Como una base de $F(\alpha)$ sobre F podemos tomar las potencias de α:

$$1, \alpha, \alpha^2, \ldots, \alpha^{d-1}.$$

Sea

$$\beta_1, \beta_2, \ldots, \beta_m$$

una base de K sobre $F(\alpha)$. Entonces, se pueden tomar como una base de K sobre F los productos

$$\alpha^i\,\beta_j. \quad (0 \leq i \leq d-1,\ 1 \leq j \leq m)$$

Sean c_{ij} los coeficientes de la matriz que representa el endomorfismo $\mu_\alpha : F(\alpha) \to F(\alpha)$:

$$\alpha \cdot \alpha^j = \sum_{0 \le i \le d-1} c_{ij}\, \alpha^i.$$

Tenemos entonces

$$f_F^\alpha = f_{F(\alpha)/F}^\alpha = \det(x \cdot I_d - A),$$

donde

$$A = \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,d-1} \\ c_{10} & c_{11} & \cdots & c_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{d-1,0} & c_{d-1,1} & \cdots & c_{d-1,d-1} \end{pmatrix}.$$

Luego,

$$\alpha \cdot \alpha^j \beta_k = \sum_{0 \le i \le d-1} c_{ij}\, \alpha^j \beta_k,$$

de donde se ve que la multiplicación por α sobre K se representa en la base $\alpha^j \beta_k$ por la matriz diagonal por bloques

$$I_m \otimes A = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}.$$

Su polinomio característico viene dado por

$$\det \begin{pmatrix} x I_d - A & & & \\ & x I_d - A & & \\ & & \ddots & \\ & & & x I_d - A \end{pmatrix} = \det(x I_d - A)^m = (f_F^\alpha)^{n/d}. \qquad \blacksquare$$

A.3 Campos de descomposición

A.3.1. Definición. Para un polinomio $f \in F[x]$ se dice que una extensión K/F es un **campo de descomposición** de fx si se cumplen las siguientes condiciones

1) f se descompone en factores lineales en $K[x]$; es decir, $f = (x - \alpha_1) \cdots (x - \alpha_n)$, donde $\alpha_i \in K$,
2) ningún subcampo propio $F \subseteq K' \subsetneq K$ cumple con esta propiedad o de manera equivalente, $K = F(\alpha_1, \ldots, \alpha_n)$.

A.3.2. Proposición. *Para un polinomio $f \in F[x]$ existe un campo de descomposición K/F. Además, $[K : F] \le n!$ donde $n = \deg(f)$.*

Demostración. Bastaría probar que existe una extensión K/F de grado $\le n!$ tal que f se descompone en factores lineales en $K[x]$.

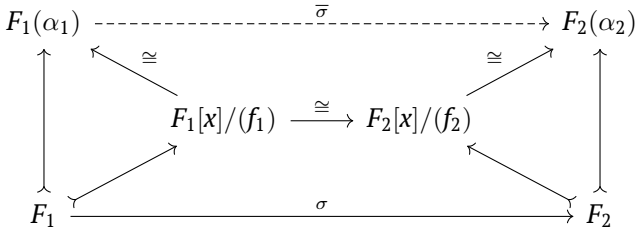
Procedamos por inducción sobre n, tomando como base el caso trivial $n = 1$. Para $n > 1$, sea $g \mid f$ algún factor irreducible de f. Consideremos el campo $K' = F[x]/(g)$. Denotemos por α la imagen de x en el cociente. Tenemos $[K' : F] = \deg(g) \le n$. Además, $g(\alpha) = 0$ y por ende $f(\alpha) = 0$. Se sigue que en $K'[x]$ tenemos una factorización $f = (x - \alpha)\, h$ para algún polinomio $h \in K'[x]$. Ahora $\deg(h) = n - 1$, así que por la hipótesis de inducción, existe una extensión K/K' de grado $\le (n-1)!$ tal que h (y entonces f) se descompone en factores lineales en $K[x]$. En fin,

$$[K : F] = [K : K'] \cdot [K' : F] \le (n-1)! \cdot n \le n! \qquad \blacksquare$$

A.3.3. Comentario. De manera similar se define un campo de descomposición para una familia de polinomios $\{f_i\}$. Para una familia finita $\{f_1, \ldots, f_s\}$ el campo de descomposición coincide con el campo de descomposición del producto $f_1 \cdots f_s$.

A.3.4. Lema. *Sean $\sigma\colon F_1 \to F_2$ un isomorfismo de campos, $f_1 \in F_1[x]$ un polinomio irreducible, α_1 una raíz de f_1 en alguna extensión K_1/F_1 y α_2 una raíz de $\sigma(f_1) \in F_2[x]$ en alguna extensión K_2/F_2. Luego σ se extiende a un isomorfismo $\overline{\sigma}\colon F_1(\alpha_1) \to F_2(\alpha_2)$ tal que $\overline{\sigma}(\alpha_1) = \alpha_2$.*

Demostración. Por la hipótesis sobre f_1, la evaluación de polinomios en α_1 induce un F_1-isomorfismo $F_1[x]/(f_1) \cong F_1(\alpha_1)$. El polinomio $f_2 = \sigma(f_1) \in F_2[x]$ será también irreducible y de manera similar tenemos un F_2-isomorfismo $F_2[x]/(f_2) \cong F_2(\alpha_2)$. Está claro que σ se extiende a un isomorfismo $F_1[x]/(f_1) \cong F_2[x]/(f_2)$.



■

A.3.5. Lema (Extensión de isomorfismos). *Sea $\sigma\colon F_1 \xrightarrow{\cong} F_2$ un isomorfismo de campos. Sean $f_1 \in F_1[x]$ un polinomio irreducible y $f_2 \in F_2[x]$ el polinomio que corresponde a f_1 bajo el isomorfismo $F_1[x] \xrightarrow{\cong} F_2[x]$ inducido por σ. Sean K_1/F_1 y K_2/F_2 campos de descomposición de f_1 y f_2 respectivamente. Entonces, el isomorfismo entre F_1 y F_2 se extiende a un isomorfismo entre K_1 y K_2:*

$$\begin{array}{ccc} K_1 & \overset{\cong}{\dashrightarrow} & K_2 \\ | & & | \\ F_1 & \xrightarrow{\cong} & F_2 \end{array}$$

Demostración. Procedamos por inducción sobre $n = \deg(f_1)$. Notamos que los factores irreducibles de f_1 en $F_1[x]$ corresponden a los factores irreducibles de f_2 en $F_2[x]$.

Si $n = 1$, o en general si f_1 se descompone en factores lineales en $F_1[x]$, se tiene $K_1 = F_1$, $K_2 = F_2$ y no hay que probar nada.

Si $n > 1$, sea $g_1 \in F_1[x]$ un factor irreducible de f y $g_2 \in F_2[x]$ el factor irreducible correspondiente de f_2. Si $\alpha_1 \in K_1$ es una raíz de g_1 y $\alpha_2 \in K_2$ es una raíz de g_2, entonces el lema anterior nos permite extender el isomorfismo $F_1 \xrightarrow{\cong} F_2$ a un isomorfismo $F_1(\alpha_1) \xrightarrow{\cong} F_2(\alpha_2)$. Ahora

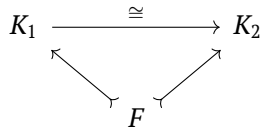
$$f_1 = (x - \alpha_1)\, h_1 \text{ en } F_1(\alpha_1)[x], \quad f_2 = (x - \alpha_2)\, h_2 \text{ en } F_2(\alpha_2)[x].$$

Notamos que K_1 y K_2 son campos de descomposición para h_1 y h_2 sobre $F_1(\alpha_1)$ y $F_2(\alpha_2)$ respectivamente. Puesto que $\deg(h_1) = \deg(h_2) = n - 1$, por la hipótesis de inducción, el isomorfismo $F_1(\alpha_1) \xrightarrow{\cong} F_2(\alpha_2)$ se extiende a un isomorfismo $K_1 \xrightarrow{\cong} K_2$.

$$\begin{array}{ccc} K_1 & \overset{\cong}{\dashrightarrow} & F_2 \\ | & & | \\ F_1(\alpha_1) & \xrightarrow{\cong} & F_2(\alpha_2) \\ | & & | \\ F_1 & \xrightarrow{\cong} & F_2 \end{array}$$

■

A.3.6. Corolario (Unicidad de campos de descomposición). *Para un polinomio $f \in F[x]$, si K_1/F y K_2/F son dos campos de descomposición, entonces existe un isomorfismo*



A.4 Cerradura algebraica

A.4.1. Proposición-definición. *Sea K un campo. Se dice que K es* ***algebraicamente cerrado*** *si este satisface las siguientes condiciones equivalentes:*

1) *todo polinomio no constante en $K[x]$ tiene una raíz en K;*
2) *todo polinomio de grado $n > 0$ en $K[x]$ tiene n raíces en K, contándolas con multiplicidades; es decir,*

$$f = c\,(x-\alpha_1)\cdots(x-\alpha_n)$$

   para $\alpha_1, \ldots, \alpha_n \in K$;

3) *todo polinomio irreducible en $K[x]$ es lineal;*
4) *K no tiene extensiones algebraicas propias: si L/K es una extensión algebraica, entonces $L = K$.*
5) *K no tiene extensiones finitas propias.*

Demostración. 1) $\Rightarrow$ 2): si f es un polinomio de grado $n > 0$ y f tiene una raíz $\alpha \in K$, entonces $f = (x-\alpha)\,g$, donde $\deg(g) = n-1$. Luego, g también debe tener una raíz, etcétera. Continuando de esta manera, se obtiene una descomposición $f = c\,(x-\alpha_1)\cdots(x-\alpha_n)$.

2) $\Rightarrow$ 3): está claro.

3) $\Rightarrow$ 4): si L/K es una extensión algebraica, entonces para todo $\alpha \in L$ el polinomio mínimo f_K^α debe ser lineal según 3), lo que significa que $\alpha \in K$.

4) $\Rightarrow$ 5): toda extensión finita es algebraica.

5) $\Rightarrow$ 1): para un polinomio no constante f, escribamos $f = g\,h$ donde g es irreducible. Luego, $L = K[x]/(g)$ es una extensión finita de grado $[L : K] = \deg(g)$, pero según 5), tenemos $L = K$, así que $\deg(g) = 1$. ■

A.4.2. Definición. Para un campo K, se dice que una extensión $\overline{K}/K$ es una **cerradura algebraica** de K si

1) $\overline{K}/K$ es una extensión algebraica;
2) el campo $\overline{K}$ es algebraicamente cerrado.

A.4.3. Teorema. *Para todo campo K existe una cerradura algebraica $\overline{K}$.*

Emil Artin. Consideremos el anillo de polinomios $K[x_f]$, donde cada variable x_f corresponde a un polinomio mónico no constante $f \in K[x]$. (Este anillo es muy grande.)

Sea I el ideal en $K[x_f]$ generado por los polinomios $f(x_f)$ para todo polinomio mónico irreducible $f \in K[x]$. Este ideal es propio. En efecto, en el caso contrario existen algunos polinomios $g_1, \ldots, g_n \in K[x_f]$ y $f_1, \ldots, f_n \in K[x]$ tales que

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}).$$

Sea L/K una extensión finita donde cada uno de los polinomios f_i tiene una raíz $\alpha_i \in L$. Consideremos el homomorfismo de evaluación

$$\begin{aligned}\phi\colon K[x_f] &\to L,\\ x_{f_i} &\mapsto \alpha_i, \text{ para } i = 1,\dots,n,\\ x_f &\mapsto 0, \text{ si } f \neq f_i \text{ para } i = 1,\dots,n.\end{aligned}$$

Luego,

$$\phi\Big(g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n})\Big) = 0,$$

pero esto significa que

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) \neq 1.$$

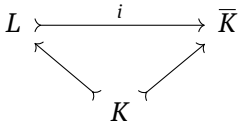
Siendo un ideal propio, I está contenido en un ideal maximal $\mathfrak{m} \subset K[x_f]$. Consideremos el campo $K_1 = K[x_f]/\mathfrak{m}$. Por la construcción, todo polinomio no constante $f \in K[x]$ tiene una raíz en K_1. En efecto, bastaría considerar el caso cuando f es mónico. Denotemos por $\alpha_f \in K_1$ la imagen de x_f en el cociente. Entonces, $f(\alpha_f) = 0$. Notamos que los elementos α_f son algebraicos sobre K, y entonces el campo K_1, siendo generado por los α_f, es una extensión algebraica de K.

De la misma manera, se puede construir una extensión K_2/K_1 tal que todo polinomio no constante $f \in K_1[x]$ tiene una raíz en K_2, etcétera. Esto nos da una torre de extensiones algebraicas

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$$

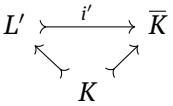
Pongamos $\overline{K} = \bigcup_{i\geq 1} K_i$. Esta es una extensión algebraica de K. Además, para cualquier polinomio no constante $f \in \overline{K}[x]$ sus coeficientes pertenecen a algún K_n para n suficientemente grande, así que f tiene una raíz en K_{n+1}. Entonces, $\overline{K}$ es un campo algebraicamente cerrado. ■

A.4.4. Lema. *Sean $\overline{K}/K$ una cerradura algebraica de K y L/K una extensión algebraica. Entonces, existe un encaje*



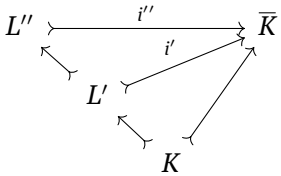
La prueba es una aplicación típica del lema de Zorn[*].

Demostración. Sea $\mathcal{P}$ el conjunto que consiste en pares de elementos (L', i') donde $K \subseteq L' \subseteq L$ es una subextensión e i' es un encaje de L' en $\overline{K}$:



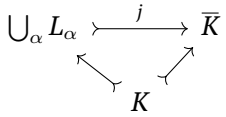
Este conjunto no es vacío: $(K, i) \in \mathcal{P}$. Este conjunto es parcialmente ordenado por la relación

$$(L', i') \preceq (L'', i'') \iff L' \subseteq L'' \text{ y } i''|_{L'} = i'.$$



[*] Nuestra construcción de una cerradura algebraica también usa el lema de Zorn, pero escondido en el resultado sobre la existencia de ideales maximales.

Es fácil comprobar que toda cadena ascendente en $\mathcal{P}$ tiene una cota superior: para una cadena $\{(L_\alpha, i_\alpha)\}_\alpha$ podemos tomar



donde $j(\alpha) = i_\alpha(\alpha)$ si $\alpha \in L_\alpha$. Entonces, el lema de Zorn nos dice que $\mathcal{P}$ tiene un elemento maximal (F, i). Para concluir la prueba, vamos a ver que $F = L$. Todo elemento $x \in L$ es algebraico sobre K, y entonces es algebraico sobre F. Sea $f = f_F^x \in F[x]$ el polinomio mínimo de x sobre F. Tenemos

$$F(x) \cong F[x]/(f).$$

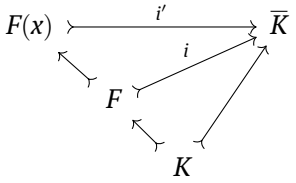
El polinomio f tiene una raíz $\alpha \in \overline{K}$. Consideremos el homomorfismo

$$\begin{aligned} &ev_\alpha : F[x] \to \overline{K}, \\ &\sum_{k\geq 0} a_k x^k \mapsto \sum_{k\geq 0} i(a_k)\, \alpha^k. \end{aligned}$$

Tenemos $f \in \ker ev_\alpha$, así que este homomorfismo induce un homomorfismo

$$i' : F(x) \cong F[x]/(f) \to \overline{K}$$

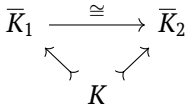
que es necesariamente inyectivo, dado que $F(x)$ es un campo, y que extiende a i:



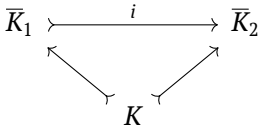
Entonces, $(F, i) \preceq (F(x), i')$. Sin embargo, la maximalidad de (F, i) implica que $F = F(x)$. Esto se cumple para cualquier $x \in L$, así que $F = L$. ■

De este lema se deduce que las cerraduras algebraicas son isomorfas entre sí.

A.4.5. Teorema. *Sean $K \hookrightarrow \overline{K}_1$ y $K \hookrightarrow \overline{K}_2$ dos cerraduras algebraicas. Entonces, existe un isomorfismo*



Demostración. Aplicando el lema anterior a $L = \overline{K}_1$ y $\overline{K} = \overline{K}_2$, se obtiene un encaje



Sin embargo, i es necesariamente sobreyectivo. En efecto, un elemento $y \in \overline{K}_2$ es una raíz de algún polinomio mónico irreducible $f \in K[x]$. Luego, f se factoriza como $(x - x_1) \cdots (x - x_n)$ en $\overline{K}_1[x]$, así que $y = i(x_k)$ para algún $k = 1, \ldots, n$. ■

A.5 Extensiones normales

A.5.1. Proposición-definición. *Para una extensión finita K/F las siguientes condiciones son equivalentes.*

1) *K es un campo de descomposición de algún polinomio $f \in F[x]$.*
2) *Para una cerradura algebraica $\overline{K}/K$ y F-homomorfismo $\sigma\colon K \to \overline{K}$ se tiene $\sigma(K) = K$.*
3) *Para un polinomio irreducible $f \in F[x]$, si f tiene una raíz en K, entonces f se descompone en factores lineales en $K[x]$.*

*En este caso se dice que K/F es una extensión **normal**.*

Demostración. 1)⇒2): si K es un campo de descomposición de f, entonces $\sigma(K)$ es también un campo de descomposición de f, y luego $K = \sigma(K)$.

2)⇒3): si α es una raíz de f, consideremos el campo $F(\alpha) \cong F[x]/(f)$. Ahora si β es otra raíz, entonces tenemos un encaje $\sigma\colon F(\alpha) \to \overline{K}$ que envía α a β. Argumentando como en A.4.4, podemos extenderlo a un encaje $\sigma\colon K \to \overline{K}$ que envía α a β, pero luego la condición 2) implica que $\beta \in K = \sigma(K)$.

3)⇒1): bajo la condición 3), K es un campo de descomposición de la familia de polinomios $\{f_F^\alpha \mid \alpha \in K\}$. Dado que nos interesan extensiones finitas K/F, podemos escribir $K = F(\alpha_1, \ldots, \alpha_n)$, y luego K es un campo de descomposición de $f = f_F^{\alpha_1} \cdots f_F^{\alpha_n}$. ■

Un típico ejemplo de extensión que *no es* normal es $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Por ejemplo, hay tres diferentes encajes $\mathbb{Q}(\sqrt[3]{2}) \to \overline{\mathbb{Q}}$: uno real definido por $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ y dos complejos conjugados definidos por $\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$ y $\sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2}$. Estos encajes tienen diferente imagen, lo cual no pasa para una entensión normal. El campo de descomposición de $x^3 - 2$ es $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

A.6 Extensiones separables

A.6.1. Definición. Sea F un campo y $f \in F[x]$ un polinomio. En un campo de descomposición K/F tenemos

$$f = c\,(x-\alpha_1)^{e_1} \cdots (x-\alpha_s)^{e_s},$$

donde $\alpha_1, \ldots, \alpha_s \in K$ son diferentes elementos y $e_i \geq 1$. Si $e_i = 1$, se dice que α_i es una **raíz simple** de f y si $e_i > 1$, se dice que α_i es una **raíz múltiple** de **multiplicidad** e_i. Si todas las raíces de f son simples, se dice que f es un **polinomio separable**.

Para un polinomio $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ su **derivada (formal)** viene dada por $f' = n\,a_n\,x^{n-1} + (n-1)\,a_{n-1}\,x^{n-2} + \cdots + a_1$. Es fácil comprobar que se cumplen las reglas habituales, como por ejemplo $(fg)' = f'g + fg'$.

A.6.2. Proposición. *Un polinomio $f \in F[x]$ tiene una raíz múltiple $\alpha \in F$ si y solo si $f(\alpha) = f'(\alpha) = 0$.*

Demostración. Si α es una raíz múltiple, entonces $f = (x-\alpha)^2 g$ para algún polinomio $g \in F[x]$. Luego, tomando las derivadas, se obtiene $f' = 2\,(x-\alpha)\,g + (x-\alpha)^2\,g'$, de donde $f'(\alpha) = 0$.

Viceversa, si $\alpha \in F$ es una raíz común de f y f', entonces tenemos $f = (x-\alpha)\,g$ para algún $g \in F[x]$, y luego $f' = g + (x-\alpha)\,g'$. De aquí se sigue que $g = f' - (x-\alpha)\,g'$ tiene α como su raíz; es decir, $(x-\alpha) \mid g$. Entonces, $f = (x-\alpha)^2\,h$ para algún $h \in F[x]$. ■

A.6.3. Corolario. *Un polinomio $f \in F[x]$ es separable si y solo si* $\operatorname{mcd}(f, f') = 1$.

Demostración. Sea K/F un campo de descomposición de f.

Si $\operatorname{mcd}(f, f') \neq 1$, entonces existe un polinomio no constante $g \in F[x]$ tal que $g \mid f$ y $g \mid f'$. El polinomio g tiene una raíz $\alpha \in K$, y luego $f(\alpha) = f'(\alpha) = 0$, lo que significa que α es una raíz múltiple de f en K.

Viceversa. si f no es separable, entonces existe $\alpha \in K$ tal que $f(\alpha) = f'(\alpha) = 0$. Esto implica que el polinomio mínimo f_F^α divide a f y f', y por ende $\operatorname{mcd}(f, f') \neq 1$. ■

A.6.4. Corolario. *Sea $f \in F[x]$ un polinomio irreducible. Si $f' \neq 0$, entonces f es separable.*

Demostración. Si $g \mid f$ y $g \mid f'$ y f es irreducible, entonces $g \in F^\times$ o $g \sim f$. Sin embargo, en el segundo caso tenemos $\deg(f') < \deg(f)$, así que $g \nmid f'$. Se sigue que $\mathrm{mcd}(f, f') = 1$, y por lo tanto f es separable. ■

A.6.5. Definición. Para una extensión algebraica K/F se dice que un elemento $\alpha \in K$ es **separable** sobre F si el polinomio mínimo de α sobre F es separable. Si todo elemento de K es separable sobre F, se dice que K/F es una **extensión separable**.

Un ejemplo típico de extensión que *no es* separable es $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$. En este caso el polinomio mínimo de t sobre $\mathbb{F}_p(t^p)$ es $x^p - t^p = (x-t)^p$, y no es separable.

Para ciertos campos todas las extensiones algebraicas son automáticamente separables.

A.6.6. Definición. Se dice que un campo F es **perfecto** si se cumple una de las siguientes condiciones:

1) $\mathrm{char}\, F = 0$,

2) $\mathrm{char}\, F = p$ y todo elemento de F es una p-ésima potencia.

A.6.7. Ejemplo. Todo campo finito es perfecto. En efecto, si F es finito y $\mathrm{char}\, F = p$, entonces la aplicación $x \mapsto x^p$ es un automorfismo de F. ▲

A.6.8. Proposición. *Si F es un campo perfecto, entonces todo polinomio irreducible $f \in F[x]$ es separable. En particular, toda extensión algebraica (y en particular toda extensión finita) K/F es separable.*

Demostración. Gracias a A.6.4, sería suficiente probar que para todo polinomio irreducible

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

donde $a_n \neq 0$ se tiene

$$f' = n\, a_n x^{n-1} + (n-1)\, a_{n-1} x^{n-2} + \cdots + a_1 \neq 0.$$

Si $\mathrm{char}\, F = 0$, entonces $n\, a_n \neq 0$ y por ende $f' \neq 0$. Asumamos que $\mathrm{char}\, F = p$ y todo elemento de F es una p-ésima potencia. Notamos que si $f' = 0$, entonces $i \cdot a_i = 0$ para todo $i = 1, \ldots, n$; es decir, $a_i = 0$ o $p \mid i$. Esto significa que el polinomio tiene forma

$$f = b_m x^{mp} + b_{m-1} x^{(m-1)\,p} + \cdots + b_1 x^p + b_0$$

para algunos $b_0, b_1, \ldots, b_m \in F$. Por nuestra hipótesis, todo b_i es una potencia p-ésima en F, así que

$$f = c_m^p x^{mp} + c_{m-1}^p x^{(m-1)\,p} + \cdots + c_1^p x^p + c_0^p = (c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0)^p$$

(usando que $\mathrm{char}\, F = p$). Pero esto contradice la irreducibilidad de f. Entonces, $f' \neq 0$. ■

A.7 Teorema del elemento primitivo

A.7.1. Teorema. *Sea K/F una extensión finita de campos tal que $K = F(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_2, \ldots, \alpha_n \in K$ son separables*[*]*. Luego, existe un elemento $\theta \in K$ tal que $K = F(\theta)$.*

Demostración. Consideremos primero el caso de $n = 2$. Sea entonces $K = F(\alpha, \beta)$, donde β es separable sobre F. Sea $f = f_F^\alpha$ el polinomio mínimo de α sobre F y $g = f_F^\beta$ el polinomio mínimo de β sobre F. Sea L/K una extensión donde f y g se descomponen en factores lineales y sean

$$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r \in L$$

[*] Sic. La separabilidad de α_1 no será necesaria en la prueba.

las raíces diferentes de f en L y sean

$$\beta_1 = \beta, \beta_2, \ldots, \beta_s \in L$$

las raíces de g (son todas diferentes, dado que β es separable).

Notamos que sin pérdida de generalidad, se puede asumir que F es un campo infinito. En el caso contrario, K también sería un campo finito, y luego $K = F(\theta)$ donde θ es un generador del grupo cíclico $K^\times$.

Notamos que $\beta_j \neq \beta_1$ para $j \neq 1$, así que la ecuación

$$\alpha_i + x\,\beta_j = \alpha_1 + x\,\beta_1$$

tiene a lo sumo una raíz $x \in F$ para cualesquiera $i = 1, \ldots, r$ y $j = 2, \ldots, s$. Gracias a nuestra hipótesis de que F sea infinito, existe un elemento $c \in F$ que es distinto de las raíces de las ecuaciones de arriba:

$$\alpha_i + c\,\beta_j \neq \alpha_1 + c\,\beta_1 \quad \text{para } i = 1, \ldots, r,\ j = 2, \ldots, s.$$

Pongamos

$$\theta = \alpha_1 + c\,\beta_1 = \alpha + c\,\beta.$$

Tenemos $\theta = F(\alpha, \beta)$. Si logramos probar que $\beta \in F(\theta)$, entonces también $\alpha = \theta - c\,\beta \in F(\theta)$ y $F(\alpha, \beta) = F(\theta)$. Notamos que

$$g(\beta) = 0, \quad f(\alpha) = f(\theta - c\,\beta) = 0$$

y los polinomios $g \in F[x]$ y $f(\theta - c\,x) \in F(\theta)[x]$ no pueden tener más de una raíz común por nuestra elección de c: se tiene

$$\theta - c\,\beta_j \neq \alpha_i \quad \text{para } i = 1, \ldots, r,\ j = 2, \ldots, s,$$

así que $f(\theta - c\,\beta_j) \neq 0$ para $j \neq 1$. Calculamos

$$\operatorname{mcd}(g, f(\theta - c\,x)) = h \quad \text{en } F(\theta)[x]$$

para algún polinomio mónico $h \in F(\theta)[x]$. Notamos que $\deg(h) > 0$: dado que $g(\beta) = f(\theta - c\,\beta) = 0$, ambos polinomios g y $f(\theta - c\,x)$ deben ser divisibles por el polinomio mínimo $f^{\beta}_{F(\theta)}$. En $L[x]$ el polinomio h se descompone en factores lineales y toda raíz de h es una raíz de g y $f(\theta - c\,x)$. Pero β es la única raíz común de g y $f(\theta - c\,x)$ y g no tiene raíces múltiples, así que necesariamente $h = x - \beta$. Esto nos permite concluir que $\beta \in F(\theta)$.

Esto termina la prueba en el caso de $n = 2$. En el caso general, podemos proceder por inducción sobre n. Asumamos que el resultado es válido para $n - 1$ y se tiene

$$F(\alpha_1, \ldots, \alpha_{n-1}) = F(\eta)$$

para algún $\eta \in K$. Luego,

$$F(\alpha_1, \ldots, \alpha_n) = F(\eta, \alpha_n) = F(\theta)$$

por el caso de dos generadores. ■

A.8 Lema de Dedekind

Para un grupo G y un campo K un **carácter** (multiplicativo) es un homomorfismo $\chi\colon G \to K^\times$. El siguiente resultado es bastante fácil de probar, pero es de mucha importancia, así que merece una sección separada.

A.8.1. Lema (Dedekind; independencia lineal de caracteres). *Dado un grupo G y un campo K, consideremos diferentes caracteres multiplicativos $\chi_1, \ldots, \chi_n\colon G \to K^\times$. Estos son necesariamente linealmente independientes sobre K: si para algunos $c_1, \ldots, c_n \in K$ se cumple*

$$c_1\chi_1(g) + \cdots + c_n\chi_n(g) = 0 \quad \textit{para todo } g \in G,$$

entonces $c_1 = \cdots = c_n = 0$.

Demostración. Inducción sobre n, el caso base siendo $n = 1$. Supongamos que el resultado es válido para $n-1$ caracteres. Consideremos una dependencia lineal

$$c_1\chi_1(g) + \cdots + c_{n-1}\chi_{n-1}(g) + c_n\chi_n(g) = 0 \quad \text{para todo } g \in G. \tag{*}$$

Dado que los caracteres son diferentes, existe $g_0 \in G$ tal que $\chi_1(g_0) \neq \chi_n(g_0)$. Sustituyendo $g_0 g$ en lugar de g, se obtiene

$$c_1\chi_1(g_0)\chi_1(g) + \cdots + c_{n-1}\chi_{n-1}(g_0)\chi_{n-1}(g) + c_n\chi_n(g_0)\chi_n(g) = 0. \tag{**}$$

Ahora si multiplicamos (*) por $\chi_n(g_0)$ y luego restamos el resultado de (**), nos queda

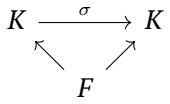
$$c_1(\chi_1(g_0) - \chi_n(g_0))\chi_1(g) + \cdots + c_{n-1}(\chi_{n-1}(g_0) - \chi_n(g_0))\chi_{n-1}(g) = 0.$$

Entonces, por la hipótesis de inducción, $c_1(\chi_1(g_0) - \chi_n(g_0)) = 0$, pero dado que $\chi_1(g_0) \neq \chi_n(g_0)$, tenemos que concluir que $c_1 = 0$. El mismo razonamiento nos dice que $c_2 = \cdots = c_{n-1} = 0$, pero luego también $c_n = 0$. ■

El lema de Dedekind será útil para caracteres $\sigma\colon K^\times \to K^\times$ que vienen de automorfismos $\sigma\colon K \to K$.

A.9 Automorfismos de campos

Para una extensión de campos K/F denotaremos por $\mathrm{Aut}(K/F)$ el grupo de automorfismos $\sigma\colon K \to K$ tales que $\sigma|_F = id$. Estos se llaman F-**automorfismos** de K.



Todos los automorfismos de K serán denotados por $\mathrm{Aut}(K)$.

A.9.1. Proposición. *Sean K/F una extensión finita de campos y $\sigma\colon K \to K$ un F-automorfismo.*

1) *Si $K = F(\alpha_1, \ldots, \alpha_n)$, entonces σ está definido por las imágenes de los generadores α_i.*
2) *Para $\alpha \in K$ sea $f = f_F^\alpha$ el polinomio mínimo correspondiente. En este caso $f(\sigma(\alpha)) = 0$ y f es también el polinomio mínimo de $\sigma(\alpha)$.*
3) *$\mathrm{Aut}(K/F)$ es un grupo finito.*

Demostración. Las partes 1) y 2) se siguen del hecho de que σ, siendo un automorfismo, preserva sumas y productos, y entonces todos los polinomios: $\sigma(f(\alpha)) = f(\sigma(\alpha))$.
En particular, la parte 2) implica que hay solamente un número finito de F-automorfismos $\sigma\colon K \to K$. ■

El siguiente resultado relaciona subcampos de K y subgrupos de $\mathrm{Aut}(K)$.

A.9.2. Proposición. *Sea K un campo.*

1) *Dado un subgrupo $H \subseteq \mathrm{Aut}(K)$, el conjunto*

$$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in H\}$$

*es un subcampo de K, llamado el **subcampo fijo** de H.*

2) *Para un subcampo $F \subseteq K$ se tiene $F \subseteq K^{\mathrm{Aut}(K/F)}$.*
3) *Para un subgrupo $H \subseteq \mathrm{Aut}(K)$ se tiene $H \subseteq \mathrm{Aut}(K/K^H)$.*

4) Para subcampos $F_1 \subseteq F_2 \subseteq K$ se tiene $\mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$.

5) Para subgrupos $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K)$ se tiene $K^{H_2} \subseteq K^{H_1}$.

6) Si $F = K^H$ para algún subgrupo $H \subseteq \mathrm{Aut}(K)$, entonces $F = K^{\mathrm{Aut}(K/F)}$.

7) Si $H = \mathrm{Gal}(K/F)$ para algún subcampo $F \subseteq K$, entonces $H = \mathrm{Aut}(K/K^H)$.

Demostración. 1)–5) se deja al lector. En la parte 6), notamos que $H \subseteq \mathrm{Aut}(K/F)$ por la parte 3), y luego $K^{\mathrm{Aut}(K/F)} \subseteq K^H = F$. Por otra parte, $F \subseteq K^{\mathrm{Aut}(K/F)}$ según la parte 2).

De manera similar, en 7) tenemos $F \subseteq K^{\mathrm{Aut}(K/F)}$, y luego $\mathrm{Aut}(K/K^H) = \mathrm{Aut}(K/K^{\mathrm{Aut}(K/F)}) \subseteq \mathrm{Aut}(K/F) = H$. Por otra parte, $H \subseteq \mathrm{Aut}(K/K^H)$ según 3). ■

A.9.3. Proposición. *Para una extensión finita K/F se tiene* $|\mathrm{Aut}(K/F)| \leq [K : F]$.

Demostración. Sean $\sigma_1, \ldots, \sigma_m$ los elementos de $\mathrm{Aut}(K/F)$ y $\alpha_1, \ldots, \alpha_n$ una base de K sobre F. Supongamos que $n < m$. En este caso habrá dependencia K-lineal entre las filas de la siguiente matriz de $m \times n$ con entradas en K:

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_n) \end{pmatrix}$$

Esto significa que existen $c_i \in K$, no todos nulos, tales que

$$c_1\sigma_1(\alpha_j) + \cdots + c_n\sigma_n(\alpha_j) = 0$$

para todo $j = 1, \ldots, n$. Ahora para cualquier elemento $\alpha \in K$ podemos escribir $\alpha = \sum_j a_j\alpha_j$, y luego

$$\sum_i c_i\sigma_i(\alpha) = \sum_j a_j \sum_i c_i\sigma_i(\alpha_j) = 0.$$

Pero esto significa que los caracteres $\sigma_i \colon K^\times \to K^\times$ son linealmente dependientes, lo cual contradice el lema de Dedekind. ■

A.9.4. Lema. *Sean K/F una extensión finita y $G \subseteq \mathrm{Aut}(K)$ tal que $F = K^G$. En este caso $|G| = [K : F]$ y $G = \mathrm{Aut}(K/F)$.*

Demostración. Sea $G = \{\sigma_1, \ldots, \sigma_m\}$ y $\alpha_1, \ldots, \alpha_n \in K$ una base de K sobre F. La proposición anterior nos dice que $n \leq m$. Supongamos que $n < m$ y consideremos la matriz

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_n) \end{pmatrix}$$

Hay una dependencia K-lineal entre las columnas. Sea k el mínimo posible tal que algunas k columnas son linealmente dependientes. Después de renumerar los α_j, podemos suponer que la dependencia lineal es entre las primeras k columnas:

$$c_1\,\sigma_i(\alpha_1) + \cdots + c_k\,\sigma_i(\alpha_k) = 0 \qquad (*)$$

para todo $i = 1, \ldots, m$, donde $c_1, \ldots, c_k \in K^\times$. Además, podemos normalizar los coeficientes y asumir que $c_k = 1$.

Para cualquier elemento $\sigma \in G$ tenemos $\{\sigma\sigma_j \mid i = 1, \ldots, m\} = G$, así que la aplicación de σ a la ecuación (*) nos permite concluir que

$$\sigma(c_1)\,\sigma_i(\alpha_1) + \cdots + \sigma(c_k)\,\sigma_i(\alpha_k) = 0 \qquad (**)$$

para todo i. Ahora restando (**) de (*) y tomando en cuenta que $c_k = 1$, se obtiene

$$(c_1 - \sigma(c_1))\,\sigma_i(\alpha_1) + \cdots + (c_{k-1} - \sigma(c_{k-1}))\,\sigma_i(\alpha_k) = 0,$$

y luego por la minimalidad de k tenemos $c_j = \sigma(c_j)$ para todo j.

Este argumento es válido para todo $\sigma \in G$ y demuestra que $c_1, \ldots, c_k \in K^G$. Pero por nuestra hipótesis, $K^G = F$. Entonces, usando que los automorfismos σ_j son F-lineales, (*) nos da

$$\sigma_j(c_1\,\alpha_1 + \cdots + c_k\,\alpha_k) = 0,$$

y luego $c_1\,\alpha_1 + \cdots + c_k\,\alpha_k = 0$, pero esto contradice la independencia lineal de los α_i. ■

A.10 Extensiones de Galois

La correspondencia entre los subgrupos y subcampos funciona bien para las extensiones de Galois.

A.10.1. Proposición-definición. *Se dice que una extensión finita K/F es una **extensión de Galois** si se cumple una de las siguientes condiciones equivalentes:*

1) $|\operatorname{Aut}(K/F)| = [K : F]$,
2) $F = K^{\operatorname{Aut}(K/F)}$,
3) *K/F es normal y separable,*
4) *K es el campo de descomposición de un polinomio separable $f \in F[x]$.*

Demostración. Para la implicación 1)⇒2) supongamos que se cumple $|\operatorname{Aut}(K/F)| = [K : F]$. En este caso el lema A.9.4 implica que $|\operatorname{Aut}(K/K^{\operatorname{Aut}(K/F)})| = [K : K^{\operatorname{Aut}(K/F)}]$. Entonces, $F \subseteq K^{\operatorname{Aut}(K/F)} \subseteq K$ y $[K : F] = [K : K^{\operatorname{Aut}(K/F)}]$, así que $F = K^{\operatorname{Aut}(K/F)}$.

Para probar 2)⇒3), para un elemento $\alpha \in K$, sean $\alpha_1, \ldots, \alpha_n$ diferentes elementos del conjunto finito $\{\sigma(\alpha) \mid \sigma \in \operatorname{Aut}(K/F)\}$. Consideremos el polinomio

$$f(x) = (x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n)) \in K[x].$$

Se tiene $\sigma(f) = f$, para todo $\sigma \in \operatorname{Aut}(K/F)$, así que los coeficientes de f están en $K^{\operatorname{Aut}(K/F)} = F$. Notamos que para todo $\sigma \in \operatorname{Aut}(K/F)$ el elemento $\sigma(\alpha)$ es una raíz del polinomio mínimo f_F^α, y en particular $f_F^\alpha \mid f$. Se sigue que f_F^α se descompone en diferentes factores lineales en $K[x]$, así que f_F^α es separable.

Esto establece la separabilidad de K/F. Por otra parte, si $K = F(\alpha_1, \ldots, \alpha_n)$, entonces nuestro argumento demuestra que K es el campo de descomposición del polinomio $f = f_F^{\alpha_1} \cdots f_F^{\alpha_n}$, así que K es normal.

Para la implicación 3)⇒4), escribamos $K = F(\alpha_1, \ldots, \alpha_n)$. Por la normalidad, todo polinomio mínimo $f_F^{\alpha_i}$ se descompone en factores lineales en $K[x]$. Por otra parte, la separabilidad significa que cada $f_F^{\alpha_i}$ no tiene raíces múltiples. Podemos tomar $f = f_F^{\alpha_1} \cdots f_F^{\alpha_n}$. Puede ser que $f_F^{\alpha_i}$ y $f_F^{\alpha_j}$ tienen una raíz común, pero en este caso $f_F^{\alpha_i} = f_F^{\alpha_j}$. Quitando los factores repetidos, podemos asegurarnos que f es separable.

Para la implicación 4)⇒1), sea K un campo de descomposición de $f \in F[x]$. Consideremos el grupo de automorfismos $G = \operatorname{Aut}(K/F)$. Vamos a probar que $|G| = [K : F]$ por inducción sobre $[K : F]$. El caso base es cuando $K = F$. Para el paso inductivo, si $[K : F] > 1$, existe una raíz $\alpha \in K$ de f tal que $\alpha \notin F$. En este caso $[K : F(\alpha)] < [K : F]$, así que por la hipótesis de inducción el grupo de automorfismos $H = \operatorname{Aut}(K/F(\alpha)) \subset G$ satisface $|H| = [K : F(\alpha)]$.

Sean $\alpha_1, \ldots, \alpha_s$ las raíces del polinomio mínimo f_F^α. Estas son distintas y $s = \deg(f_F^\alpha) = [F(\alpha) : F]$. Notamos que para toda raíz α_i, usando A.3.4 y A.3.5, se obtiene un automorfismo $\sigma_i \in G$ tal que $\sigma_i(\alpha) = \alpha_i$:

$$\begin{array}{ccc} K & \overset{\sigma_i}{\dashrightarrow} & K \\ | & & | \\ F(\alpha) & \overset{\cong}{\longrightarrow} & F(\alpha_i) \\ | & & | \\ F & = & F \end{array}$$

Notamos que $\sigma_i H \neq \sigma_j H$ para $i \neq j$. En efecto, si $\sigma_i H = \sigma_j H$, entonces, dado que $H = \mathrm{Aut}(K/F(\alpha))$, esto implicaría $\sigma_i(\alpha) = \sigma_j(\alpha)$. De esta manera hemos encontrado $s = [F(\alpha) : F]$ diferentes elementos en el cociente G/H. Ahora

$$|G| = [G : H] \cdot |H| \geq [F(\alpha) : F] \cdot [K : F(\alpha)] = [K : F].$$

La otra desigualdad $|G| \leq [K : F]$ se cumple en cualquier caso (véase A.9.3). ■

A.10.2. Definición. Para una extensión de Galois K/F el grupo de automorfismos $\mathrm{Aut}(K/F)$ se conoce como el **grupo de Galois** y se denota por $\mathrm{Gal}(K/F)$.

Notamos que según lema A.9.4, se tiene $|\mathrm{Gal}(K/F)| = [K : F]$.

A.10.3. Lema. *Si K/F es una extensión de Galois, entonces para cualquier subextensión $F \subseteq L \subseteq K$, la extensión K/L es también de Galois.*

Demostración. Si K/F es separable, esto significa que para todo $\alpha \in K$ el polinomio mínimo f_F^α es separable. Pero ahora $f_L^\alpha \mid f_F^\alpha$, así que f_L^α es también separable.

Ahora la normalidad de K/F significa que K es un campo de descomposición para algún polinomio $f \in F[x]$. En particular, $f \in L[x]$, así que la extensión K/L es también normal. ■

A.11 Teorema fundamental de la teoría de Galois

A.11.1. Lema (Extensión de automorfismos). *Sea K/F una extensión de Galois y $F \subseteq L \subseteq K$ una subextensión. En este caso todo F-automorfismo $\tau : L \to L$ es de la forma $\sigma|_L$ para algún $\sigma \in \mathrm{Gal}(K/F)$.*

Demostración. Para simplificar el asunto, podemos invocar el teorema del elemento primitivo y escribir $K = F(\alpha)$ para algún $\alpha \in K$. Dado que $\tau|_F = id$, los polinomios mínimos de α y $\tau(\alpha)$ sobre F coinciden, y K es un campo de descomposición de estos. Podemos entonces ocupar el lema A.3.5. ■

A.11.2. Teorema (Correspondencia de Galois). *Dada una extensión finita de Galois K/F, consideremos el grupo de Galois $G = \mathrm{Gal}(K/F)$. A una subextensión $F \subset L \subset K$ se puede asociar un subgrupo $H = \mathrm{Gal}(K/L) \subseteq G$. Viceversa, dado un subgrupo $H \subseteq G$, se obtiene una subextensión*

$$L = K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ para } \sigma \in H\}.$$

Esto nos da una biyección

$$\{ \text{subcampos } F \subseteq L \subseteq G\} \underset{K^H \hookleftarrow H}{\overset{L \mapsto \mathrm{Gal}(K/L)}{\rightleftarrows}} \{ \text{subgrupos } H \subseteq G\}$$

Esta correspondencia satisface las siguientes propiedades.

1) *La correspondencia invierte las inclusiones. Si $L_1 \subseteq L_2$, entonces $\mathrm{Gal}(K/L_2) \subseteq \mathrm{Gal}(K/L_1)$. Si $H_1 \subseteq H_2 \subseteq G$, entonces $K^{H_2} \subseteq K^{H_1}$.*

2) $[K:L] = |H|$ y $[L:F] = [G:H]$.

3) *La extensión L/F es normal (y entonces Galois) si y solamente si el subgrupo $H \subseteq G$ es normal. En este caso la restricción de automorfismos* $\mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$ *es sobreyectiva y tiene H como su núcleo, así que* $\mathrm{Gal}(L/F) \cong G/H$.

4) *Para dos subextensiones L_1 y L_2 hay un F-isomorfismo $L_1 \cong L_2$ si y solamente si los subgrupos correspondientes $H, H' \subseteq G$ son conjugados por un elemento de G.*

Demostración. La proposición A.9.2 nos da la biyección deseada para las subextensiones de la forma $L = K^H$ para $H \subseteq \mathrm{Gal}(K/F)$ y subgrupos $H = \mathrm{Gal}(K/L) \subseteq \mathrm{Gal}(K/F)$. Entonces, tenemos que probar que en el caso de extensión de Galois todas las subextensiones surgen de campos fijos por un subgrupo H y que todo subgrupo de $\mathrm{Gal}(K/F)$ tiene forma $\mathrm{Gal}(K/L)$.

Dada una subextensión $F \subseteq L \subseteq K$, puesto que K/F es una extensión de Galois, K/L también lo es. Entonces, $L = K^{\mathrm{Gal}(K/L)}$. Esto demuestra que todas las subextensiones vienen de subcampos fijos. Por otra parte, para un subgrupo $H \subseteq \mathrm{Gal}(K/F)$, según A.9.4 se cumple $H = \mathrm{Gal}(K/K^H)$.

Esto establece la biyección deseada. La propiedad 1) se verifica fácilmente. Para la parte 2), dado que K/F y K/L son extensiones de Galois, tenemos $|G| = |\mathrm{Gal}(K/F)| = [K:F]$ y $|H| = |\mathrm{Gal}(K/L)| = [K:L]$. Luego,

$$[L:F] = \frac{[K:F]}{[K:L]} = \frac{|G|}{|H|} = [G:H].$$

Supongamos ahora que $H \subseteq G$ es un subgrupo normal y consideremos el subcampo $L = K^H$. Para un elemento $\alpha \in L$ consideremos el polinomio mínimo f_F^α. Si β es cualquier otra raíz de f_F^α, entonces existe un automorfismo $\sigma \in G$ tal que $\sigma(\alpha) = \beta$. Notamos que para cualquier automorfismo $\tau \in H$ se tiene $\tau(\beta) = \sigma(\sigma^{-1}\tau\sigma(\alpha))$, donde $\sigma^{-1}\tau\sigma \in H$ por la normalidad, y entonces $\tau(\beta) = \sigma(\alpha) = \beta$. Esto demuestra que toda raíz de f_F^α está en $K^H = L$. Entonces, si un polinomio irreducible $f \in F[x]$ se descompone en factores lineales en $K[x]$, entonces este ya se descompone en factores lineales en $L[x]$. Esto establece la normalidad de la extensión L/F. Por otra parte, L/F es separable, puesto que K/F lo es.

Viceversa, si L/F es una extensión de Galois, consideremos el homomorfismo

$$\phi\colon\ \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F), \quad \sigma \mapsto \sigma|_L\,.$$

Gracias a la normalidad de L/F, la restricción $\sigma|_L$ tiene imagen en L (véase A.5.1). Ahora

$$\ker\phi = \{\sigma \in \mathrm{Gal}(K/F) \mid \sigma|_L = id\} = \mathrm{Gal}(K/L).$$

En particular, $H = \mathrm{Gal}(K/L)$ es un subgrupo normal de $G = \mathrm{Gal}(K/F)$. El homomorfismo ϕ es sobreyectivo: todo F-homomorfismo $\tau\colon L \to L$ se extiende a $\sigma\colon K \to K$ gracias al lema de extensión de isomorfismos A.3.5. Entonces, ϕ induce un isomorfismo $\mathrm{Gal}(L/F) \cong G/H$.

En fin, para la parte 4), notamos que dos subcampos L_1 y L_2 son isomorfos si y solamente si $L_2 = \sigma(L_1)$ para algún automorfismo $\sigma \in \mathrm{Gal}(K/F)$. En una dirección esto está claro: la restricción de $\sigma\colon K \to K$ a L_1 induce un isomorfismo $L_1 \cong \sigma(L_1)$. En la otra dirección, un F-isomorfismo $\tau\colon L_1 \to L_2$ se extiende a $\sigma\colon K \to K$, y luego $L_2 = \sigma(L_1)$. Un pequeño cálculo demuestra que $\mathrm{Gal}(K/\sigma(L_1)) = \sigma\,\mathrm{Gal}(K/L_1)\sigma^{-1}$. ■

A.12 Campos finitos

Todo campo finito F necesariamente tiene característica p, y entonces es una extensión del campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Siendo un $\mathbb{F}_p$-espacio vectorial, F debe tener p^n elementos.

A.12.1. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un campo finito $\mathbb{F}$ de p^n elementos; específicamente, este es un campo de descomposición del polinomio separable $x^{p^n} - x \in \mathbb{F}_p[x]$.*

En particular, $\mathbb{F}$ es único salvo isomorfismo, y $\mathbb{F}/\mathbb{F}_p$ es una extensión de Galois.

Demostración. Consideremos una extensión $\mathbb{F}/\mathbb{F}_p$. Notamos que el polinomio $f = x^{p^n} - x \in \mathbb{F}_p[x]$ es separable, dado que tenemos $f' = -1$, y luego $\operatorname{mcd}(f, f') = 1$.

1) Sea $\mathbb{F}/\mathbb{F}_p$ un campo de descomposición de f. En este caso $\mathbb{F}$ contiene p^n raíces distintas de f. Usando que $\operatorname{char}\mathbb{F} = p$, no es difícil verificar que las raíces de f forman un subcampo de $\mathbb{F}$. Por la minimalidad de campos de descomposición, esto significa que $\mathbb{F}$ consiste precisamente en las raíces de f y $|\mathbb{F}| = p^n$.

2) Viceversa, notamos que si $\mathbb{F}$ es un campo de p^n elementos, entonces $\mathbb{F}$ tiene característica p y $\mathbb{F}_p \subseteq \mathbb{F}$. El grupo multiplicativo $\mathbb{F}^\times$ tiene orden $p^n - 1$, así que todo elemento $\alpha \in \mathbb{F}^\times$ satisface $\alpha^{p^n-1} = 1$ según el teorema de Lagrange, así que $\alpha^{p^n} = \alpha$. Para $\alpha = 0$ esto también trivialmente se cumple. Luego, todos los p^n elementos de $\mathbb{F}$ son raíces del polinomio $f = x^{p^n} - x \in \mathbb{F}_p[x]$ de grado p^n, así que $\mathbb{F}$ es un campo de descomposición de f. Este es único salvo isomorfismo. ■

En vista del último resultado, normalmente un campo finito de p^n elementos se denota por $\mathbb{F}_{p^n}$, siempre tomando en cuenta que este está bien definido salvo isomorfismo.

El grupo multiplicativo de un campo finito es cíclico, lo que puede ser deducido de la siguiente observación general de la teoría de grupos.

A.12.2. Lema. *Sea G un grupo de orden finito n. Supongamos que para todo $d \mid n$ se cumple*

$$\#\{x \in G \mid x^d = 1\} \leq d. \tag{*}$$

Entonces G es cíclico.

Demostración. Si G tiene un elemento g de orden d, entonces por el teorema de Lagrange tenemos necesariamente $d \mid n$. Ahora g genera el subgrupo $\langle g \rangle$ que es cíclico de orden d. Todo elemento $h \in G$ tal que $h^d = 1$ pertenece a este subgrupo gracias a la hipótesis (*), y si h tiene orden d, entonces es otro generador de $\langle g \rangle$. En total este subgrupo tiene $\phi(d)$ generadores. Entonces, el número de elementos de orden d, donde $d \mid n$, es igual a 0 o $\phi(d)$. De hecho, el primer caso no es posible: la fórmula $\sum_{d|n} \phi(d) = n$ demuestra que si para algún $d \mid n$ el grupo G no tiene elementos de orden d, entonces $|G| < n$. En particular, G debe tener un elemento de orden n y por lo tanto es cíclico. ■

A.12.3. Corolario. *Si K es cualquier campo y G un subgrupo finito del grupo multiplicativo $K^\times$, entonces G es cíclico. En particular, para un campo finito $\mathbb{F}_{p^n}$ el grupo $\mathbb{F}_{p^n}^\times$ es cíclico.*

Demostración. Para un campo, la ecuación polinomial $x^d - 1 = 0$ tiene como máximo d soluciones. Entonces, se cumple la hipótesis del lema anterior. ■

En particular, si $K = \mathbb{F}_{p^n}$ es un campo finito de p^n elementos y α es un generador multiplicativo de $K^\times$, tenemos $K = \mathbb{F}_p(\alpha)$. El polinomio mínimo de α sobre $\mathbb{F}_p$ es algún polinomio irreducible $f \in \mathbb{F}_p[x]$ de grado n. Entonces, para construir un campo finito $\mathbb{F}_{p^n}$, hay que encontrar ese polinomio y tomar el cociente $\mathbb{F}_p[x]/(f)$. El campo $\mathbb{F}_{p^n}$ está bien definido solo salvo isomorfismo no único. No es difícil describir los automorfismos de campos finitos.

A.12.4. Teorema. *Sea $q = p^\ell$ para p primo y $\ell = 1, 2, 3, \ldots$ Para un campo finito $\mathbb{F}_{q^n}$ el grupo* $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *es cíclico de orden n, generado por el* ***automorfismo de Frobenius*** *$F\colon x \mapsto x^q$.*

Demostración. Notamos primero que F es un automorfismo. Para cualesquiera $x, y \in \mathbb{F}_{q^n}$ tenemos obviamente $(xy)^q = x^q y^q$, y para las sumas se tiene $(x + y)^q = x^q + y^q$, usando que estamos en característica p. Esto demuestra que $F\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ es un homomorfismo. Ahora F es automáticamente inyectivo, pero ya que $\mathbb{F}_{q^n}$ es finito, F es también sobreyectivo.

El grupo multiplicativo $\mathbb{F}_{q^n}^\times$ es cíclico y podemos escoger un generador $\alpha \in \mathbb{F}_{q^n}^\times$. Todo automorfismo $\sigma \in \operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ está definido por la imagen de α, y de allí es fácil ver que las potencias del automorfismo de Frobenius $F^k\colon x \mapsto x^{q^k}$ son distintas para $k = 0, \ldots, n-1$. Esto nos da n diferentes automorfismos de $\mathbb{F}_{q^n}$, pero sabemos que en general $|\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, así que acabamos de describir todos los automorfismos. ■

La teoría de Galois nos da la siguiente descripción de las subextensiones de $\mathbb{F}_{q^n}/\mathbb{F}_q$.

A.12.5. Corolario. *Los subcampos de un campo finito $\mathbb{F}_{q^n}/\mathbb{F}_q$ corresponden a los divisores de n: son precisamente*

$$\mathbb{F}_{q^d} = \{x \in \mathbb{F}_{q^n} \mid x^{q^d} = x\}.$$

A.12.6. Comentario. Respecto a las inclusiones $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$, podemos tomar

$$\mathbb{F}_{p^\infty} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

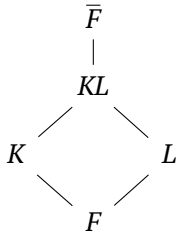
A saber, los elementos de $\mathbb{F}_{p^\infty}$ son $x \in \mathbb{F}_{p^m}$ e $y \in \mathbb{F}_{p^n}$, y para calcular $x\,y$ o $x \pm y$, hay que encajar x e y en $\mathbb{F}_{p^{\mathrm{mcm}(m,n)}}$. Esto nos da una extensión infinita de $\mathbb{F}_p$. Todo polinomio $f \in \mathbb{F}_{p^\infty}[x]$ tendrá sus coeficientes en algún campo finito $\mathbb{F}_{p^n}$ para n suficientemente grande, y el campo de descomposición de f, siendo una extensión finita de $\mathbb{F}_{p^n}$, también será de la forma $\mathbb{F}_{p^N}$ y será un subcampo de $\mathbb{F}_{p^\infty}$. Esto demuestra que $\mathbb{F}_{p^\infty}$ es un campo algebraicamente cerrado. Siendo la unión de extensiones finitas de $\mathbb{F}_p$, es una extensión algebraica de $\mathbb{F}_p$. Entonces, $\mathbb{F}_{p^\infty}$ es una cerradura algebraica de $\mathbb{F}_p$.

No es difícil calcular que el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^\infty})$ es isomorfo al grupo de enteros profinitos $\widehat{\mathbb{Z}}$.

A.13 Campos linealmente disjuntos

En esta sección vamos a revisar la noción de campos linealmente disjuntos. Para nuestros propósitos, será suficiente asumir que las extensiones son finitas.

A.13.1. Definición. Para dos extensiones finitas K/F y L/F adentro de un campo común (por ejemplo, adentro de una cerradura algebraica fija $\overline{F}$), el subcampo más pequeño que contiene a K y L se llama el **compositum** de K y L y se denota por KL.



Si $K = F(\alpha_1, \ldots, \alpha_m)$ y $L = F(\beta_1, \ldots, \beta_n)$, está claro que $KL = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$. En términos de bases sobre F, tenemos el siguiente resultado.

A.13.2. Lema. *Sean K/F y L/F extensiones finitas, $\alpha_1, \ldots, \alpha_n$ una base de K sobre F y $\beta_1, \ldots, \beta_m$ una base de L sobre F. Entonces, los productos $\alpha_i\beta_j$ generan KL como un espacio vectorial sobre F. En particular,*

$$[KL : F] \leq [K : F] \cdot [L : F].$$

Demostración. Denotemos por A el espacio F-lineal generado por los $\alpha_i\beta_j$. Está claro que A está cerrado respecto a sumas y productos. Además, A tiene dimensión finita sobre F, así que para cualquier elemento no nulo $x \in A$ tenemos $F[x] = F(x)$. En particular, $x^{-1} \in F[x] \subseteq A$, lo que demuestra que A está cerrado respecto a inversos y es un campo. Está claro que $A = KL$. ■

Note que no estamos afirmando que los $\alpha_i\beta_j$ forman una *base* de KL. Esto es falso en general. Por ejemplo, si $K = L$, entonces obviamente $KL = K$ tiene dimensión menor que $[K : F] \cdot [L : F]$. Otro ejemplo más interesante: para los campos $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ el compositum $KL = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ tiene dimensión 8 sobre $\mathbb{Q}$. En el caso cuando $[KL : F] = [K : F] \cdot [L : F]$, se dice que los campos son linealmente disjuntos.

A.13.3. Proposición-definición. *Se dice que K y L son **linealmente disjuntos** si se cumple una de las siguientes condiciones equivalentes:*

a) el homomorfismo de F-álgebras

$$K \otimes_F L \to KL, \quad x \otimes y \mapsto xy$$

es un isomorfismo;

a′) el mismo homomorfismo de F-álgebras es inyectivo;

b) si $\alpha_1, \ldots, \alpha_m$ es una base de K sobre F, esta es linealmente independiente sobre L;

b′) si $\beta_1, \ldots, \beta_n$ es una base de L sobre F, esta es linealmente independiente sobre K;

c) si α_i y β_j son bases de K y L respectivamente, entonces $\alpha_i\beta_j$ es una base de KL;

d) $[KL : F] = [K : F] \cdot [L : F]$.

Demostración. El lema anterior implica que la aplicación $K \otimes_F L \to KL$ es siempre sobreyectiva. Esto demuestra la equivalencia entre a) y a′).

Ahora supongamos que se cumple la condición b) y $\alpha_1, \ldots, \alpha_m$ es una base de K sobre F y $\beta_1, \ldots, \beta_n$ es una base de L sobre F. En este caso $\alpha_i \otimes \beta_j$ es una base de $L \otimes_F K$ sobre F. Si un elemento $\sum_{i,j} a_{ij}\alpha_i \otimes \beta_j \in K \otimes_F L$ está en el núcleo de la aplicación $K \otimes_F L \to KL$, entonces $\sum_{i,j} a_{ij}\alpha_i\beta_j = 0$, pero luego $a_{ij}\beta_j = 0$ para todo j por la hipótesis b). Esto significa que el núcleo es nulo.

Viceversa, supongamos que la aplicación $K \otimes_F L \to KL$ es inyectiva. Sea $\alpha_1, \ldots, \alpha_m$ una base de K sobre L. Si tenemos $\sum_i c_i\alpha_i = 0$ para algunos $c_i \in L$, entonces el elemento $\sum_i \alpha_i \otimes c_i$ está en el núcleo de $K \otimes_F L \to KL$, así que $\sum_i \alpha_i \otimes c_i = 0$. Esto implica que $c_i = 0$ para todo i, así que no hay L-dependencia no trivial entre los α_i.

Esto establece la equivalencia entre a) y b), pero luego $K \otimes_F L \cong L \otimes_F K$ y $KL = LK$, así que b) es equivalente a b′).

La condición a) es visiblemente equivalente a c). Además, el lema anterior establece la equivalencia entre c) y d). ■

A.13.4. Proposición (≈ teorema de irracionalidades naturales). *Si K/F y L/F son extensiones finitas de Galois, entonces son linealmente disjuntas si y solamente si $K \cap L = F$.*

Demostración. El resultado se sigue de la fórmula

$$[KL : F] = [L : F] \cdot [K : K \cap L]. \tag{*}$$

Primero notamos que KL/L es una extensión de Galois. De hecho, si K es un campo de descomposición de un polinomio separable $f \in F[x]$, entonces KL es un campo de descomposición del mismo polinomio considerado como elemento de $L[x]$.

Consideremos el homomorfismo de grupos

$$\phi\colon \operatorname{Gal}(KL/L) \to \operatorname{Gal}(K/F), \quad \sigma \mapsto \sigma|_K.$$

Por la normalidad de K/F, la restricción $\sigma|_K$ toma valores en K, así que este homomorfismo tiene sentido. Notamos que el núcleo de ϕ consiste en los automorfismos $\sigma \in \operatorname{Gal}(KL/L)$ tales que $\sigma|_K = id$. Entonces, para $\sigma \in \ker\phi$ el subcampo fijo $(KL)^\sigma$ contiene K y L, y por lo tanto contiene el compositum KL, así que $\sigma = id$. Esto significa que el núcleo de ϕ es trivial.

La imagen de ϕ es un subgrupo $H \subseteq \operatorname{Gal}(K/F)$, y por la correspondencia de Galois $H = \operatorname{Gal}(K/K^H)$. Vamos a probar que $K^H = K \cap L$. Primero, si $\alpha \in K \cap L$, entonces $\alpha \in K^H$ por la definición de ϕ. Viceversa, si $\alpha \in K^H$, entonces $\sigma(\alpha) = \alpha$ para todo $\sigma \in \operatorname{Gal}(KL/L)$. Esto implica que $\alpha \in KL^{\operatorname{Gal}(KL/L)} = L$.

Hemos probado entonces que la imagen de ϕ es $\operatorname{Gal}(KL/K \cap L)$, así que ϕ induce un isomorfismo de grupos de Galois $\operatorname{Gal}(KL/L) \cong \operatorname{Gal}(KL/K \cap L)$. Entonces, $[KL : L] = [K : K \cap L]$, y se sigue (*). ■

Apéndice B

Polinomios y campos ciclotómicos

En este apéndice vamos a revisar brevemente los polinomios ciclotómicos Φ_n y probar su irreducibilidad.

B.1 Definición y propiedades básicas

B.1.1. Definición. Consideremos las raíces n-ésimas de la unidad

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \in \mathbb{C},$$

donde $\zeta_n = \exp(2\pi i/n)$. Se dice que ζ_n^a es una raíz **primitiva** si $\mathrm{mcd}(a, n) = 1$.

El número de las raíces n-ésimas primitivas coincide entonces con la función de Euler $\phi(n)$.

B.1.2. Lema. *Para todo $a = 0, 1, \ldots, n-1$ el número ζ_n^a es una raíz d-ésima primitiva para algún $d \mid n$. Este d está definido de modo único.*

Si ζ es una raíz d-ésima primitiva, entonces, todas las raíces d-ésimas primitivas son de la forma ζ^a para $\mathrm{mcd}(a, d) = 1$.

Demostración. Teoría de números elemental. Si denotamos por $\mathcal{S}_d$ el conjunto de las raíces primitivas de orden d, entonces

$$\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} = \bigcup_{d|n} \mathcal{S}_d$$

es una partición gracias a la identidad $\sum_{d|n} \phi(n) = n$. La última afirmación también está clara. ■

B.1.3. Definición. El n-ésimo **polinomio ciclotómico**[*] es el polinomio mónico que tiene como sus raíces las raíces n-ésimas primitivas de la unidad:

$$\Phi_n = \prod_{\substack{0 \le a < n \\ \mathrm{mcd}(a,n)=1}} (x - \zeta_n^a).$$

Esta claro que Φ_n es un poliomio mónico de grado $\phi(n)$.

[*] La palabra «ciclotomia» significa «división del círculo» en griego y se refiere al hecho de que las n-ésimas raíces de la unidad son vértices de un n-ágono regular inscrito en el circulo unitario.

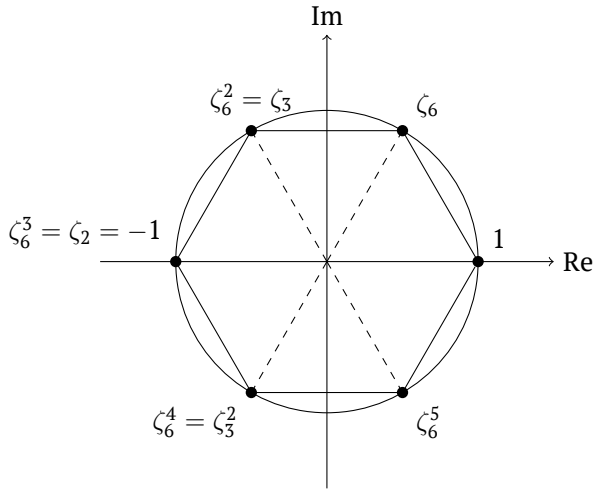


Figura B.1: Raíces sextas de la unidad

B.1.4. Ejemplo. Los primeros polinomios ciclotómicos son

$$\begin{aligned}
\Phi_1 &= x - 1,\\
\Phi_2 &= x + 1,\\
\Phi_3 &= (x - \zeta_3)\,(x - \zeta_3^2) = x^2 + x + 1,\\
\Phi_4 &= (x - \zeta_4)\,(x - \zeta_4^3) = x^2 + 1.
\end{aligned}$$

▲

Lo que no está tan claro de la definición es que los coeficientes de Φ_n son números enteros.

B.1.5. Proposición.

1) Para todo primo p se tiene

$$\Phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

2) Para todo primo p y $k \geq 1$ se tiene

$$\Phi_{p^k} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \Phi_p(x^{p^{k-1}}) = x^{(p-1)\,p^{k-1}} + x^{(p-2)\,p^{k-1}} + \cdots + x^{2p^{k-1}} + x^{p^{k-1}} + 1.$$

3) Para todo n se tiene

$$\prod_{d|n} \Phi_d = x^n - 1.$$

4) Todos los polinomios Φ_n tienen coeficientes enteros.

Demostración. Observamos que

$$\prod_{0 \leq a < n} (x - \zeta_n^a) = x^n - 1.$$

En la parte 1), basta notar que entre las raíces p-ésimas, todas son primitivas, salvo la raíz trivial 1, así que

$$\Phi_p = \prod_{1 \leq a < p} (x - \zeta_p^a) = \prod_{0 \leq a < p} (x - \zeta_p^a) \Big/ (x - 1) = \frac{x^p - 1}{x - 1}.$$

De la misma manera, en 2) notamos que un número $0 \leq a < p^k$ tal que $\operatorname{mcd}(a, p^k) \neq 1$ es necesariamente divisible por p, así que las raíces de orden p^k que no son primitivas tienen forma $\zeta_{p^k}^{pb} = \zeta_{p^{k-1}}^{b}$ y son precisamente todas las raíces de orden p^{k-1}:

$$\Phi_{p^k} = \prod_{\substack{0\leq a<p^k \\ \operatorname{mcd}(a,p^k)=1}} (x - \zeta_{p^k}^a) = \prod_{0\leq a<p^k} (x - \zeta_{p^k}^a) \Big/ \prod_{0\leq b<p^{k-1}} (x - \zeta_{p^{k-1}}^b) = \frac{x^{p^k}-1}{x^{p^{k-1}}-1}.$$

En la parte 3), basta notar que

$$x^n - 1 = \prod_{0\leq a<n} (x - \zeta_n^a) = \prod_{d|n} \prod_{\substack{0\leq a<n \\ \operatorname{mcd}(a,d)=1}} (x - \zeta_n^a) = \prod_{d|n} \Phi_d,$$

usando la observación que hicimos en B.1.2.

La parte 4) se demuestra por inducción sobre n. Esto es cierto, por ejemplo, para $\Phi_1 = x - 1$. Luego, si $\Phi_m \in \mathbb{Z}[x]$ para todo $m < n$, entonces podemos considerar el polinomio

$$g = \prod_{\substack{d|n \\ d\neq n}} \Phi_d \in \mathbb{Z}[x].$$

Este es mónico, siendo un producto de polinomios mónicos. La división con resto en el anillo $\mathbb{Z}[x]$ nos da

$$x^n - 1 = q\,g + r, \quad \deg(r) < \deg(g)$$

para algunos $q, r \in \mathbb{Z}[x]$, mientras que en el anillo más grande $\mathbb{Q}[x] \supset \mathbb{Z}[x]$ se cumple

$$x^n - 1 = \Phi_n\, g.$$

Pero para la división con resto en $\mathbb{Q}[x]$ el cociente y el resto están definidos de modo único, así que $r = 0$ y $\Phi_n = q \in \mathbb{Z}[x]$. ■

B.1.6. Ejemplo. Tenemos

$$\begin{aligned}
\Phi_4 &= \Phi_2(x^2) = x^2 + 1,\\
\Phi_5 &= x^4 + x^3 + x^2 + x + 1,\\
\Phi_6 &= \frac{x^6-1}{\Phi_1\,\Phi_2\,\Phi_3} = \frac{(x^3-1)\,(x^3+1)}{\Phi_1\,\Phi_2\,\Phi_3} = \frac{x^3+1}{\Phi_2} = \frac{x^3+1}{x+1} = x^2 - x + 1,\\
\Phi_7 &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
\Phi_8 &= \Phi_2(x^4) = x^4 + 1,\\
\Phi_9 &= \Phi_3(x^2) = x^6 + x^3 + 1,\\
\Phi_{10} &= \frac{x^{10}-1}{\Phi_1\,\Phi_2\,\Phi_5} = \frac{(x^5+1)\,(x^5-1)}{(x^5-1)\,\Phi_2} = \frac{x^5+1}{x+1} = x^4 - x^3 + x^2 - x + 1.
\end{aligned}$$

Notamos que

$$\begin{aligned}
\Phi_3 = x^2 + x + 1, \quad \Phi_6 = x^2 - x + 1 = \Phi_3(-x),\\
\Phi_5 = x^4 + x^3 + x^2 + x + 1, \quad \Phi_{10} = x^4 - x^3 + x^2 - x + 1 = \Phi_5(-x).
\end{aligned}$$

Esta no es una coincidencia: en general, $\Phi_{2m} = \Phi_m(-x)$ para todo $m > 1$ impar (este es un buen ejercicio para el lector). ▲

El resultado de arriba nos permite calcular de manera bastante eficaz los polinomios ciclotómicos. En PARI/GP la función `polcylo(n)` devuelve Φ_n.

```
? polcyclo(105)
% = x^48 + x^47 + x^46 - x^43 - x^42 - 2*x^41 - x^40 - x^39 + x^36
    + x^35 + x^34 + x^33 + x^32 + x^31 - x^28 - x^26 - x^24 - x^22
    - x^20 + x^17 + x^16 + x^15 + x^14 + x^13 + x^12 - x^9 - x^8 - 2*x^7
    - x^6 - x^5 + x^2 + x + 1

? polcyclo(1)*polcyclo(3)*polcyclo(5)*polcyclo(15)
% = x^15 - 1
```

B.1.7. Comentario. Una prueba mucho más lista de que $\Phi_n \in \mathbb{Z}[x]$ es la siguiente. El grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times$ y consiste en automorfismos $\sigma\colon \zeta_n \mapsto \zeta_n^a$ con $\mathrm{mcd}(a,n)=1$. Se ve que cada σ deja fijos los coeficientes de Φ_n, y la teoría de Galois nos dice entonces que los coeficientes están en $\mathbb{Q}\cap\mathbb{Z}[\zeta_n]=\mathbb{Z}$.

Sin embargo, este argumento me parece un poco tramposo: uno que sabe calcular $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ normalmente también sabrá manejar los polinomios ciclotómicos...

B.2 Irreducibilidad

El objetivo de esta sección es probar que los polinomios ciclotómicos Φ_n son irreducibles en $\mathbb{Z}[x]$ (y luego en $\mathbb{Q}[x]$ gracias al lema de Gauss). Para tratar primero el caso de $n=p^k$ donde p es primo, recordemos el siguiente criterio de irreducibilidad.

B.2.1. Proposición (Eisenstein). *Sea*

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

un polinomio mónico con coeficientes enteros. Supongamos que existe un primo p tal que $p \mid a_i$ para todo $i = 0,1,\ldots,n-1$, pero $p^2 \nmid a_0$. Entonces, f es irreducible.

La prueba es muy breve, así que será más fácil recordarla por completo que citar un libro de texto.

Demostración. Si f es reducible, entonces $f=gh$, donde $1 \le \deg(g), \deg(h) < n$. Reduciendo módulo p, se obtiene la identidad

$$\overline{x^n} = \bar f = \bar g\,\bar h \quad \text{en } \mathbb{F}_p[x]$$

por la hipótesis sobre los coeficientes de f. Esto implica que

$$\bar g = c\,x^k, \quad \bar h = c^{-1}\,x^\ell,$$

para algún $c \in \mathbb{F}_p^\times$ y $k+\ell=n$, donde $k \le \deg(g)$ y $\ell \le \deg(h)$, así que $k,\ell>0$.

Sin embargo, si ambos g y h se reducen a un polinomio sin término constante, esto significa que los términos constantes de g y h son divisibles por p. Esto implicaría que el término constante de f es divisible por p^2, pero no es el caso por nuestra hipótesis. ■

Una aplicación típica del criterio de Eisenstein es la irreducibilidad de los polinomios ciclotómicos Φ_{p^k}. Notamos que el término constante de cualquier polinomio ciclotómico viene dado por

$$\Phi_n(0) = (-1)^{\phi(n)} \prod_{\substack{0\le a<n \\ \mathrm{mcd}(a,n)=1}} \zeta_n^a. \tag{B.1}$$

Excluyendo el caso excepcional de $\Phi_1 = x - 1$ y $\Phi_2 = x + 1$, notamos que para $n > 2$ el número $\phi(n)$ es par y cada ζ_n^a en el producto se cancela con su inverso ζ_n^{-a}, así que $\Phi_n(0) = 1$.

Esto significa que el criterio de Eisenstein nunca se aplica directamente a Φ_n, pero para $n = p^k$ funciona la sustitución de $x + 1$ en lugar de x. Por ejemplo,

$$\Phi_8(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2,$$

y el criterio de Eisenstein sí funciona para $p = 2$.

Notamos que un polinomio no constante $f \in \mathbb{Z}[x]$ es irreducible si y solo si $f(x+a)$ es irreducible para algún $a \in \mathbb{Z}$: esta sustitución no cambia el grado y una factorización no trivial $f(x+a) = g(x)\,h(x)$ corresponde a una factorización no trivial $f(x) = g(x-a)\,h(x-a)$.

B.2.2. Proposición. *Para todo primo p el polinomio Φ_p es irreducible.*

Demostración. Al sustituir $x+1$ en lugar de x, nos salen los coeficientes $a_i = \binom{p}{i}$, y a estos se aplica el criterio de Eisenstein:

$$\begin{aligned}\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{1}{x} \sum_{1 \le i \le p} \binom{p}{i} x^i \\ &= \binom{p}{p} x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{3} x^2 + \binom{p}{2} x + \binom{p}{1}. \quad \blacksquare\end{aligned}$$

B.2.3. Proposición. *Para todo primo p y $k \ge 1$ el polinomio Φ_{p^k} es irreducible.*

Demostración. Ya vimos el caso de $k = 1$. Podemos asumir entonces que $k \ge 2$. De nuevo, consideremos la sustitución

$$\Phi_{p^k}(x+1) = \frac{(x+1)^{p^k} - 1}{(x+1)^{p^{k-1}} - 1} = \sum_{0 \le i \le p-1} (x+1)^{i\,p^{k-1}}.$$

Tenemos para todo $k \ge 2$

$$(x+1)^{p^{k-1}} \equiv x^{p^{k-1}} + 1 \pmod{p},$$

y luego

$$\begin{aligned}\Phi_{p^k}(x+1) \equiv \sum_{0 \le i \le p-1} (x^{p^{k-1}} + 1)^i = \frac{(x^{p^{k-1}} + 1)^p - 1}{(x^{p^{k-1}} + 1) - 1} \\ = \frac{(x^{p^{k-1}} + 1)^p - 1}{x^{p^{k-1}}} \equiv \frac{x^{p^k}}{x^{p^{k-1}}} = x^{p^{k-1}(p-1)} \pmod{p}.\end{aligned}$$

Esto significa que todos los coeficientes menores de $\Phi_{p^k}(x+1)$ son divisibles por p. El coeficiente constante es igual a

$$\Phi_{p^k}(1) = \Phi_p(1^{p^{k-1}}) = \Phi_p(1) = p,$$

y de nuevo podemos aplicar el criterio de Eisenstein. $\blacksquare$

La irreducibilidad de Φ_n para todo n es un resultado más difícil.

B.2.4. Teorema (Gauss). *Para cualquier $n = 1, 2, 3, \ldots$ el polinomio ciclotómico Φ_n es irreducible.*

Un poco de la historia: el 1808 Gauss anotó en su diario matemático que había establecido la irreducibilidad de Φ_n para cualquier n. Su argumento original se considera perdido, pero ya que se trata de Gauss, es muy probable que él disponía de una prueba correcta y completa. Sin embargo, la primera demostración publicada pertenece a Kronecker (1854).

Empecemos por un pequeño lema.

B.2.5. Lema. *Si $p \nmid n$, entonces en la factorización del polinomio ciclotómico Φ_n en $\mathbb{F}_p[x]$ no hay factores repetidos.*

Demostración. Gracias a la fórmula $x^n - 1 = \prod_{d|n} \Phi_n$, sería suficiente probar que en la factorización de $f = x^n - 1$ en $\mathbb{F}_p[x]$ no hay factores repetidos. Para esto basta calcular que $\operatorname{mcd}(f, f') = \operatorname{mcd}(x^n - 1, nx^{n-1}) = 1$. Por ejemplo, usando $p \nmid n$, podemos escribir laa identidad de Bézout

$$\frac{x}{n} \cdot (n\, x^{n-1}) - (x^n - 1) = 1. \qquad \blacksquare$$

Demostración del teorema. Escribamos

$$\Phi_n = fg$$

para algunos polinomios $f, g \in \mathbb{Z}[x]$, donde f es irreducible. Dado que Φ_n es mónico, el coeficiente mayor de f y g es ± 1, y podemos asumir que son también mónicos. Sea ζ una raíz n-ésima primitiva. Tenemos entonces

$$\Phi_n(\zeta) = f(\zeta)\, g(\zeta) = 0.$$

Esto implica que $f(\zeta) = 0$ o $g(\zeta) = 0$. Puesto que f no es constante, alguna raíz n-ésima primitiva ζ debe ser una raíz de f, y nuestro objetivo es probar que todas las raíces primitivas

$$\zeta^a, \quad \operatorname{mcd}(a, n) = 1$$

son raíces de f.

Asumamos entonces que $f(\zeta) = 0$. Por la irreducibilidad de f, esto significa que f es el polinomio mínimo de ζ. Sea p un número primo tal que $p \nmid n$. Entonces, ζ^p es también una raíz n-ésima primitiva y

$$\Phi_n(\zeta^p) = f(\zeta^p)\, g(\zeta^p) = 0.$$

Asumamos que $g(\zeta^p) = 0$. En este caso $f \mid g(x^p)$ en $\mathbb{Z}[x]$, ya que f es el polinomio mínimo de ζ. Reduciendo módulo p, se obtiene[*] $\bar{f} \mid \bar{g}(x^p) = \bar{g}^p$ en $\mathbb{F}_p[x]$. Pero esto implica que $\overline{\Phi_n} = \bar{f}\bar{g}$ tiene un factor repetido en su factorización en $\mathbb{F}_p[x]$, lo que contradice el lema B.2.5. Entonces, $f(\zeta^p) = 0$.

Esto demuestra que para cualquier primo p tal que $p \nmid n$ se tiene

$$f(\zeta) = 0 \Longrightarrow f(\zeta^p) = 0.$$

Ahora todas las raíces n-ésimas primitivas son de la forma ζ^a donde $\operatorname{mcd}(a, n) = 1$. Podemos factorizar entonces $a = p_1 \cdots p_s$ donde p_i son primos (no necesariamente diferentes) tales que $p_i \nmid n$, y luego

$$\zeta^a = (((\zeta^{p_1})^{p_2})^{\cdots})^{p_s}.$$

El argumento de arriba nos dice que $f(\zeta^{p_1}) = 0$. Luego, el mismo argumento aplicado a ζ^{p_1} demuestra que $f((\zeta^{p_1})^{p_2}) = 0$, etcétera, y en fin $f(\zeta^a) = 0$. Entonces, todas las raíces n-ésimas primitivas son raíces de f y por ende $g = 1$. $\blacksquare$

Para una prueba alternativa, basada en el teorema de Dirichlet sobre primos en progresiones aritméticas, véase §D.6.

[*] Usando el teorema del binomio en característica p y $a^p = a$ en $\mathbb{F}_p$, notamos que

$$g(x)^p = (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0)^p = a_n (x^p)^n + a_{n-1} (x^p)^{n-1} + \cdots + a_1 x^p + a_0 = g(x^p).$$

B.3 Campos ciclotómicos

B.3.1. Definición. El n-ésimo campo ciclotómico es el campo $\mathbb{Q}(\zeta_n)$.

De la irreducibilidad de Φ_n se sigue que Φ_n es el polinomo mínimo de ζ_n sobre $\mathbb{Q}$, y por ende $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n)$, y en particular $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$. El campo ciclotómico es el campo de descomposición de Φ_n, así que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois.

B.3.2. Proposición. *El grupo* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *consiste en automorfismos* $\sigma_k \colon \zeta_n \mapsto \zeta_n^k$*, donde* $\mathrm{mcd}(k,n) = 1$*. Hay isomorfismo* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Demostración. Un automorfismo $\sigma \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ debe mandar ζ_n a otra raíz de Φ_n, y de allí surgen todos los automorfismos σ_k. La aplicación $\sigma_k \mapsto k \mod n$ establece el isomorfismo $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. ■

Notamos que si $m \mid n$, entonces $\zeta_m = \zeta_n^{n/m} \in \mathbb{Q}(\zeta_n)$, y luego $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Ahora si m es un número impar, entonces $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. De hecho, tenemos la inclusión obvia $\zeta_m \in \mathbb{Q}(\zeta_{2m})$, y por otro lado, escribiendo $m = 2k+1$,

$$\zeta_{2m} = \zeta_{2m}^{(2k+1)-2k} = \zeta_{2m}^m \, (\zeta_{2m}^2)^{-k} = \zeta_2 \, \zeta_m^{-k} = -\zeta_m^{-k} \in \mathbb{Q}(\zeta_m).$$

Esta propiedad se cumle por la razón banal de que $\zeta_2 = -1 \in \mathbb{Q}$. Resulta que en otras situaciones los campos ciclotómicos no coinciden. Para probarlo, podemos investigar cuáles raíces de la unidad están en $\mathbb{Q}(\zeta_m)$.

B.3.3. Lema. *Si* m *es par y* $m \mid r$*, entonces* $\phi(r) \leq \phi(m)$ *implica* $r = m$.

Demostración. Primero, notamos que para cualesquiera $a, m \geq 1$ se cumple

$$\phi(am) = \frac{\phi(a)\,\phi(m)\,\mathrm{mcd}(a,m)}{\phi(\mathrm{mcd}(a,m))}$$

—esto se sigue de las fórmulas

$$\begin{aligned}
\phi(a) &= a \prod_{p \mid a} \left(1 - \frac{1}{p}\right), \\
\phi(m) &= m \prod_{p \mid m} \left(1 - \frac{1}{p}\right), \\
\phi(am) &= am \prod_{p \mid am} \left(1 - \frac{1}{p}\right), \\
\phi(\mathrm{mcd}(a,m)) &= \mathrm{mcd}(a,m) \prod_{p \mid a, p \mid m} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

(Notamos que cuando a y m son coprimos, se tiene $\mathrm{mcd}(a,m) = \phi(\mathrm{mcd}(a,m)) = 1$ y se recupera la fórmula conocida.) Ahora para m par y $m \mid r$, asumamos que $m < r$, así que $r = am$ para algún $a > 1$. Tenemos

$$\phi(r) = \phi(am) = \frac{\phi(a)\,\phi(m)\,\mathrm{mcd}(a,m)}{\phi(\mathrm{mcd}(a,m))}.$$

Si $a = 2$, entonces $\phi(a) = \phi(2) = 1$ y $\mathrm{mcd}(a,m) = 2$. Luego,

$$\frac{\phi(a)\,\phi(m)\,\mathrm{mcd}(a,m)}{\phi(\mathrm{mcd}(a,m))} = 2\,\phi(m) > \phi(m).$$

Si $a > 2$, entonces $\phi(a) \geq 2$, y luego

$$\frac{\phi(a)\,\phi(m)\,\operatorname{mcd}(a,m)}{\phi(\operatorname{mcd}(a,m))} \geq \phi(a)\,\phi(m) > \phi(m).$$

En ambos casos, $m < r$ implica $\phi(m) < \phi(r)$. ■

B.3.4. Proposición. *Las raíces de la unidad en el campo $\mathbb{Q}(\zeta_m)$ son precisamente*

$$\mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times = \begin{cases} \mu_m(\mathbb{C}), & \text{si } m \text{ es par}, \\ \mu_{2m}(\mathbb{C}), & \text{si } m \text{ es impar}. \end{cases}$$

Demostración. Si $m = 2k+1$ es un número impar, entonces ya notamos que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. Por esto sería suficiente considerar el caso cuando m es un número par. Tenemos $\zeta_m \in \mathbb{Q}(\zeta_m)$, y por ende todas las raíces m-ésimas de la unidad, siendo potencias de ζ_m, están en $\mathbb{Q}(\zeta_m)$:

$$\mu_m(\mathbb{C}) \subseteq \mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times.$$

Hay que ver que en $\mathbb{Q}(\zeta_m)$ no hay raíces de la unidad de orden $k \nmid m$. Bastaría considerar las raíces k-ésimas primitivas. Supongamos que $\zeta_k^\ell \in \mathbb{Q}(\zeta_m)$ donde ζ_k^ℓ es una raíz k-ésima primitiva; es decir, $\operatorname{mcd}(k,\ell) = 1$. Pongamos

$$r = \operatorname{mcm}(k,m) = \frac{km}{d}, \quad d = \operatorname{mcd}(k,m).$$

Luego,

$$\operatorname{mcd}(k,\ell m) = \operatorname{mcd}(k,m) = d,$$

lo que significa que existen $a, b \in \mathbb{Z}$ tales que

$$d = ak + b\ell m.$$

Ahora,

$$\zeta_r = \zeta_{km}^d = \zeta_{km}^{ak+b\ell m} = \zeta_{km}^{ak}\,\zeta_{km}^{b\ell m} = \zeta_m^a\,(\zeta_k^\ell)^b \in \mathbb{Q}(\zeta_m)$$

y

$$\phi(r) \leq \phi(m), \quad m \text{ es par}, \quad m \mid r,$$

así que el lema B.3.3 nos permite concluir que

$$r = \operatorname{mcd}(k,m) = m,$$

lo que significa que $k \mid m$. ■

B.3.5. Corolario. *Si $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ para $m < n$, entonces m es impar y $n = 2m$.*

Demostración. Si m es par, entonces las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m, mientras que las raíces de la unidad en $\mathbb{Q}(\zeta_n)$ son de orden n o $2n$, dependiendo de la paridad de n. Pero en ambos casos la hipótesis $m < n$ nos lleva a una contradicción. Entonces, m es impar y las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m. La única posibilidad es $n = 2m$. ■

Entonces, para enumerar los campos ciclotómicos sin redundancias, basta considerar $\mathbb{Q}(\zeta_n)$ donde $n \not\equiv 2 \pmod 4$.

Apéndice C

Algunos grupos de clases

C.1 Campos cuadráticos imaginarios

K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$
$\mathbb{Q}(\sqrt{-1})$	0	$\mathbb{Q}(\sqrt{-34})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-69})$	$\mathbb{Z}/4 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-2})$	0	$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-70})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-3})$	0	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-71})$	$\mathbb{Z}/7$
$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-38})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-73})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-6})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-39})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-74})$	$\mathbb{Z}/10$
$\mathbb{Q}(\sqrt{-7})$	0	$\mathbb{Q}(\sqrt{-41})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-77})$	$\mathbb{Z}/4 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-42})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-78})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-11})$	0	$\mathbb{Q}(\sqrt{-43})$	0	$\mathbb{Q}(\sqrt{-79})$	$\mathbb{Z}/5$
$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-46})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-82})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-14})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-47})$	$\mathbb{Z}/5$	$\mathbb{Q}(\sqrt{-83})$	$\mathbb{Z}/3$
$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-51})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-85})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-17})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-53})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-86})$	$\mathbb{Z}/10$
$\mathbb{Q}(\sqrt{-19})$	0	$\mathbb{Q}(\sqrt{-55})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-87})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-21})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-57})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-89})$	$\mathbb{Z}/12$
$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-91})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-23})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-59})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-93})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-26})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-61})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-94})$	$\mathbb{Z}/8$
$\mathbb{Q}(\sqrt{-29})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-62})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-95})$	$\mathbb{Z}/8$
$\mathbb{Q}(\sqrt{-30})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-65})$	$\mathbb{Z}/4 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-97})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-31})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-66})$	$\mathbb{Z}/4 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-101})$	$\mathbb{Z}/14$
$\mathbb{Q}(\sqrt{-33})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-67})$	0	$\mathbb{Q}(\sqrt{-102})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$

K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$
$\mathbb{Q}(\sqrt{-103})$	$\mathbb{Z}/5$	$\mathbb{Q}(\sqrt{-158})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-211})$	$\mathbb{Z}/3$
$\mathbb{Q}(\sqrt{-105})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-159})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-213})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-106})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-161})$	$\mathbb{Z}/8\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-214})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-107})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-163})$	0	$\mathbb{Q}(\sqrt{-215})$	$\mathbb{Z}/14$
$\mathbb{Q}(\sqrt{-109})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-165})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-217})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-110})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-166})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-218})$	$\mathbb{Z}/10$
$\mathbb{Q}(\sqrt{-111})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-167})$	$\mathbb{Z}/11$	$\mathbb{Q}(\sqrt{-219})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-113})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-170})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-221})$	$\mathbb{Z}/8\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-114})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-173})$	$\mathbb{Z}/14$	$\mathbb{Q}(\sqrt{-222})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-115})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-174})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-223})$	$\mathbb{Z}/7$
$\mathbb{Q}(\sqrt{-118})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-177})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-226})$	$\mathbb{Z}/8$
$\mathbb{Q}(\sqrt{-119})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-178})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-227})$	$\mathbb{Z}/5$
$\mathbb{Q}(\sqrt{-122})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-179})$	$\mathbb{Z}/5$	$\mathbb{Q}(\sqrt{-229})$	$\mathbb{Z}/10$
$\mathbb{Q}(\sqrt{-123})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-181})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-230})$	$\mathbb{Z}/10\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-127})$	$\mathbb{Z}/5$	$\mathbb{Q}(\sqrt{-182})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-231})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-129})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-183})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-233})$	$\mathbb{Z}/12$
$\mathbb{Q}(\sqrt{-130})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-185})$	$\mathbb{Z}/8\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-235})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-131})$	$\mathbb{Z}/5$	$\mathbb{Q}(\sqrt{-186})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-237})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-133})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-187})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-238})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-134})$	$\mathbb{Z}/14$	$\mathbb{Q}(\sqrt{-190})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-239})$	$\mathbb{Z}/15$
$\mathbb{Q}(\sqrt{-137})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{-191})$	$\mathbb{Z}/13$	$\mathbb{Q}(\sqrt{-241})$	$\mathbb{Z}/12$
$\mathbb{Q}(\sqrt{-138})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-193})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-246})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-139})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-194})$	$\mathbb{Z}/20$	$\mathbb{Q}(\sqrt{-247})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-141})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-195})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-249})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-142})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-197})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-251})$	$\mathbb{Z}/7$
$\mathbb{Q}(\sqrt{-143})$	$\mathbb{Z}/10$	$\mathbb{Q}(\sqrt{-199})$	$\mathbb{Z}/9$	$\mathbb{Q}(\sqrt{-253})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-145})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-201})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-254})$	$\mathbb{Z}/16$
$\mathbb{Q}(\sqrt{-146})$	$\mathbb{Z}/16$	$\mathbb{Q}(\sqrt{-202})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-255})$	$\mathbb{Z}/6\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-149})$	$\mathbb{Z}/14$	$\mathbb{Q}(\sqrt{-203})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-257})$	$\mathbb{Z}/16$
$\mathbb{Q}(\sqrt{-151})$	$\mathbb{Z}/7$	$\mathbb{Q}(\sqrt{-205})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-258})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-154})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-206})$	$\mathbb{Z}/20$	$\mathbb{Q}(\sqrt{-259})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-155})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-209})$	$\mathbb{Z}/10\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-262})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-157})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-210})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-263})$	$\mathbb{Z}/13$

C.2 Campos cuadráticos reales

K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$
$\mathbb{Q}(\sqrt{2})$	0	$\mathbb{Q}(\sqrt{53})$	0	$\mathbb{Q}(\sqrt{103})$	0	$\mathbb{Q}(\sqrt{155})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{3})$	0	$\mathbb{Q}(\sqrt{55})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{105})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{157})$	0
$\mathbb{Q}(\sqrt{5})$	0	$\mathbb{Q}(\sqrt{57})$	0	$\mathbb{Q}(\sqrt{106})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{158})$	0
$\mathbb{Q}(\sqrt{6})$	0	$\mathbb{Q}(\sqrt{58})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{107})$	0	$\mathbb{Q}(\sqrt{159})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{7})$	0	$\mathbb{Q}(\sqrt{59})$	0	$\mathbb{Q}(\sqrt{109})$	0	$\mathbb{Q}(\sqrt{161})$	0
$\mathbb{Q}(\sqrt{10})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{61})$	0	$\mathbb{Q}(\sqrt{110})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{163})$	0
$\mathbb{Q}(\sqrt{11})$	0	$\mathbb{Q}(\sqrt{62})$	0	$\mathbb{Q}(\sqrt{111})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{165})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{13})$	0	$\mathbb{Q}(\sqrt{65})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{113})$	0	$\mathbb{Q}(\sqrt{166})$	0
$\mathbb{Q}(\sqrt{14})$	0	$\mathbb{Q}(\sqrt{66})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{114})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{167})$	0
$\mathbb{Q}(\sqrt{15})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{67})$	0	$\mathbb{Q}(\sqrt{115})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{170})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{17})$	0	$\mathbb{Q}(\sqrt{69})$	0	$\mathbb{Q}(\sqrt{118})$	0	$\mathbb{Q}(\sqrt{173})$	0
$\mathbb{Q}(\sqrt{19})$	0	$\mathbb{Q}(\sqrt{70})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{119})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{174})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{21})$	0	$\mathbb{Q}(\sqrt{71})$	0	$\mathbb{Q}(\sqrt{122})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{177})$	0
$\mathbb{Q}(\sqrt{22})$	0	$\mathbb{Q}(\sqrt{73})$	0	$\mathbb{Q}(\sqrt{123})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{178})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{23})$	0	$\mathbb{Q}(\sqrt{74})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{127})$	0	$\mathbb{Q}(\sqrt{179})$	0
$\mathbb{Q}(\sqrt{26})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{77})$	0	$\mathbb{Q}(\sqrt{129})$	0	$\mathbb{Q}(\sqrt{181})$	0
$\mathbb{Q}(\sqrt{29})$	0	$\mathbb{Q}(\sqrt{78})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{130})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{182})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{30})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{79})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{131})$	0	$\mathbb{Q}(\sqrt{183})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{31})$	0	$\mathbb{Q}(\sqrt{82})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{133})$	0	$\mathbb{Q}(\sqrt{185})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{33})$	0	$\mathbb{Q}(\sqrt{83})$	0	$\mathbb{Q}(\sqrt{134})$	0	$\mathbb{Q}(\sqrt{186})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{34})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{85})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{137})$	0	$\mathbb{Q}(\sqrt{187})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{35})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{86})$	0	$\mathbb{Q}(\sqrt{138})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{190})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{37})$	0	$\mathbb{Q}(\sqrt{87})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{139})$	0	$\mathbb{Q}(\sqrt{191})$	0
$\mathbb{Q}(\sqrt{38})$	0	$\mathbb{Q}(\sqrt{89})$	0	$\mathbb{Q}(\sqrt{141})$	0	$\mathbb{Q}(\sqrt{193})$	0
$\mathbb{Q}(\sqrt{39})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{91})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{142})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{194})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{41})$	0	$\mathbb{Q}(\sqrt{93})$	0	$\mathbb{Q}(\sqrt{143})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{195})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{42})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{94})$	0	$\mathbb{Q}(\sqrt{145})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{197})$	0
$\mathbb{Q}(\sqrt{43})$	0	$\mathbb{Q}(\sqrt{95})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{146})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{199})$	0
$\mathbb{Q}(\sqrt{46})$	0	$\mathbb{Q}(\sqrt{97})$	0	$\mathbb{Q}(\sqrt{149})$	0	$\mathbb{Q}(\sqrt{201})$	0
$\mathbb{Q}(\sqrt{47})$	0	$\mathbb{Q}(\sqrt{101})$	0	$\mathbb{Q}(\sqrt{151})$	0	$\mathbb{Q}(\sqrt{202})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{51})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{102})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{154})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{203})$	$\mathbb{Z}/2$

K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$
$\mathbb{Q}(\sqrt{205})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{258})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{313})$	0	$\mathbb{Q}(\sqrt{371})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{206})$	0	$\mathbb{Q}(\sqrt{259})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{314})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{373})$	0
$\mathbb{Q}(\sqrt{209})$	0	$\mathbb{Q}(\sqrt{262})$	0	$\mathbb{Q}(\sqrt{317})$	0	$\mathbb{Q}(\sqrt{374})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{210})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{263})$	0	$\mathbb{Q}(\sqrt{318})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{377})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{211})$	0	$\mathbb{Q}(\sqrt{265})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{319})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{379})$	0
$\mathbb{Q}(\sqrt{213})$	0	$\mathbb{Q}(\sqrt{266})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{321})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{381})$	0
$\mathbb{Q}(\sqrt{214})$	0	$\mathbb{Q}(\sqrt{267})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{322})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{382})$	0
$\mathbb{Q}(\sqrt{215})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{269})$	0	$\mathbb{Q}(\sqrt{323})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{383})$	0
$\mathbb{Q}(\sqrt{217})$	0	$\mathbb{Q}(\sqrt{271})$	0	$\mathbb{Q}(\sqrt{326})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{385})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{218})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{273})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{327})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{386})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{219})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{274})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{329})$	0	$\mathbb{Q}(\sqrt{389})$	0
$\mathbb{Q}(\sqrt{221})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{277})$	0	$\mathbb{Q}(\sqrt{330})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{390})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{222})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{278})$	0	$\mathbb{Q}(\sqrt{331})$	0	$\mathbb{Q}(\sqrt{391})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{223})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{281})$	0	$\mathbb{Q}(\sqrt{334})$	0	$\mathbb{Q}(\sqrt{393})$	0
$\mathbb{Q}(\sqrt{226})$	$\mathbb{Z}/8$	$\mathbb{Q}(\sqrt{282})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{335})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{394})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{227})$	0	$\mathbb{Q}(\sqrt{283})$	0	$\mathbb{Q}(\sqrt{337})$	0	$\mathbb{Q}(\sqrt{395})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{229})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{285})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{339})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{397})$	0
$\mathbb{Q}(\sqrt{230})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{286})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{341})$	0	$\mathbb{Q}(\sqrt{398})$	0
$\mathbb{Q}(\sqrt{231})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{287})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{345})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{399})$	$\mathbb{Z}/4\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{233})$	0	$\mathbb{Q}(\sqrt{290})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{346})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{401})$	$\mathbb{Z}/5$
$\mathbb{Q}(\sqrt{235})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{291})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{347})$	0	$\mathbb{Q}(\sqrt{402})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{237})$	0	$\mathbb{Q}(\sqrt{293})$	0	$\mathbb{Q}(\sqrt{349})$	0	$\mathbb{Q}(\sqrt{403})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{238})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{295})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{353})$	0	$\mathbb{Q}(\sqrt{406})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{239})$	0	$\mathbb{Q}(\sqrt{298})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{354})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{407})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{241})$	0	$\mathbb{Q}(\sqrt{299})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{355})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{409})$	0
$\mathbb{Q}(\sqrt{246})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{301})$	0	$\mathbb{Q}(\sqrt{357})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{410})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{247})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{302})$	0	$\mathbb{Q}(\sqrt{358})$	0	$\mathbb{Q}(\sqrt{411})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{249})$	0	$\mathbb{Q}(\sqrt{303})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{359})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{413})$	0
$\mathbb{Q}(\sqrt{251})$	0	$\mathbb{Q}(\sqrt{305})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{362})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{415})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{253})$	0	$\mathbb{Q}(\sqrt{307})$	0	$\mathbb{Q}(\sqrt{365})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{417})$	0
$\mathbb{Q}(\sqrt{254})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{309})$	0	$\mathbb{Q}(\sqrt{366})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{418})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{255})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{310})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{367})$	0	$\mathbb{Q}(\sqrt{419})$	0
$\mathbb{Q}(\sqrt{257})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{311})$	0	$\mathbb{Q}(\sqrt{370})$	$\mathbb{Z}/2\oplus\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{421})$	0

C.3 Campos ciclotómicos

Si $n \equiv 2 \pmod 4$, entonces $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$. Estos casos están excluidos para evitar redundancias.

K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$	K	$\mathrm{Cl}(K)$
$\mathbb{Q}(\zeta_3)$	0	$\mathbb{Q}(\zeta_{36})$	0	$\mathbb{Q}(\zeta_{69})$	$\mathbb{Z}/69$
$\mathbb{Q}(\zeta_4)$	0	$\mathbb{Q}(\zeta_{37})$	$\mathbb{Z}/37$	$\mathbb{Q}(\zeta_{71})$	$\mathbb{Z}/3882809$
$\mathbb{Q}(\zeta_5)$	0	$\mathbb{Q}(\zeta_{39})$	$\mathbb{Z}/2$	$\mathbb{Q}(\zeta_{72})$	$\mathbb{Z}/3$
$\mathbb{Q}(\zeta_7)$	0	$\mathbb{Q}(\zeta_{40})$	0	$\mathbb{Q}(\zeta_{73})$	$\mathbb{Z}/11957417$
$\mathbb{Q}(\zeta_8)$	0	$\mathbb{Q}(\zeta_{41})$	$\mathbb{Z}/11 \oplus \mathbb{Z}/11$	$\mathbb{Q}(\zeta_{75})$	$\mathbb{Z}/11$
$\mathbb{Q}(\zeta_9)$	0	$\mathbb{Q}(\zeta_{43})$	$\mathbb{Z}/211$	$\mathbb{Q}(\zeta_{76})$	$\mathbb{Z}/19$
$\mathbb{Q}(\zeta_{11})$	0	$\mathbb{Q}(\zeta_{44})$	0	$\mathbb{Q}(\zeta_{77})$	$\mathbb{Z}/20 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/4$
$\mathbb{Q}(\zeta_{12})$	0	$\mathbb{Q}(\zeta_{45})$	0	$\mathbb{Q}(\zeta_{79})$	$\mathbb{Z}/100146415$
$\mathbb{Q}(\zeta_{13})$	0	$\mathbb{Q}(\zeta_{47})$	$\mathbb{Z}/695$	$\mathbb{Q}(\zeta_{80})$	$\mathbb{Z}/5$
$\mathbb{Q}(\zeta_{15})$	0	$\mathbb{Q}(\zeta_{48})$	0	$\mathbb{Q}(\zeta_{81})$	$\mathbb{Z}/2593$
$\mathbb{Q}(\zeta_{16})$	0	$\mathbb{Q}(\zeta_{49})$	$\mathbb{Z}/43$	$\mathbb{Q}(\zeta_{83})$	$\mathbb{Z}/838216959$
$\mathbb{Q}(\zeta_{17})$	0	$\mathbb{Q}(\zeta_{51})$	$\mathbb{Z}/5$	$\mathbb{Q}(\zeta_{84})$	0
$\mathbb{Q}(\zeta_{19})$	0	$\mathbb{Q}(\zeta_{52})$	$\mathbb{Z}/3$	$\mathbb{Q}(\zeta_{85})$	$\mathbb{Z}/6205$
$\mathbb{Q}(\zeta_{20})$	0	$\mathbb{Q}(\zeta_{53})$	$\mathbb{Z}/4889$	$\mathbb{Q}(\zeta_{87})$	$\mathbb{Z}/24 \oplus \mathbb{Z}/8 \oplus \mathbb{Z}/8$
$\mathbb{Q}(\zeta_{21})$	0	$\mathbb{Q}(\zeta_{55})$	$\mathbb{Z}/10$	$\mathbb{Q}(\zeta_{88})$	$\mathbb{Z}/55$
$\mathbb{Q}(\zeta_{23})$	$\mathbb{Z}/3$	$\mathbb{Q}(\zeta_{56})$	$\mathbb{Z}/2$	$\mathbb{Q}(\zeta_{89})$	$\mathbb{Z}/13379363737$
$\mathbb{Q}(\zeta_{24})$	0	$\mathbb{Q}(\zeta_{57})$	$\mathbb{Z}/9$	$\mathbb{Q}(\zeta_{91})$	$\mathbb{Z}/13468 \oplus \mathbb{Z}/4$
$\mathbb{Q}(\zeta_{25})$	0	$\mathbb{Q}(\zeta_{59})$	$\mathbb{Z}/41241$	$\mathbb{Q}(\zeta_{92})$	$\mathbb{Z}/201$
$\mathbb{Q}(\zeta_{27})$	0	$\mathbb{Q}(\zeta_{60})$	0	$\mathbb{Q}(\zeta_{93})$	$\mathbb{Z}/6795$
$\mathbb{Q}(\zeta_{28})$	0	$\mathbb{Q}(\zeta_{61})$	$\mathbb{Z}/76301$	$\mathbb{Q}(\zeta_{95})$	$\mathbb{Z}/107692$
$\mathbb{Q}(\zeta_{29})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\zeta_{63})$	$\mathbb{Z}/7$	$\mathbb{Q}(\zeta_{96})$	$\mathbb{Z}/3 \oplus \mathbb{Z}/3$
$\mathbb{Q}(\zeta_{31})$	$\mathbb{Z}/9$	$\mathbb{Q}(\zeta_{64})$	$\mathbb{Z}/17$	$\mathbb{Q}(\zeta_{97})$	$\mathbb{Z}/411322824001$
$\mathbb{Q}(\zeta_{32})$	0	$\mathbb{Q}(\zeta_{65})$	$\mathbb{Z}/4 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\zeta_{99})$	$\mathbb{Z}/93 \oplus \mathbb{Z}/31$
$\mathbb{Q}(\zeta_{33})$	0	$\mathbb{Q}(\zeta_{67})$	$\mathbb{Z}/853513$	$\mathbb{Q}(\zeta_{100})$	$\mathbb{Z}/55$
$\mathbb{Q}(\zeta_{35})$	0	$\mathbb{Q}(\zeta_{68})$	$\mathbb{Z}/8$	...	...

Apéndice D

Teorema de Dirichlet sobre primos en progresiones aritméticas

Clase 16
07/10/20

Uno de los temas principales de nuestro curso es la descomposición de primos racionales $p \in \mathbb{Z}$ en ideales primos en el anillo de enteros $\mathcal{O}_K$ de un campo de números $K/\mathbb{Q}$. Cuando el grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ es abeliano, el tipo de descomposición depende del resto de p módulo m para cierto m. En particular, lo observamos en el caso cuando $K = \mathbb{Q}(\zeta_m)$ es un campo ciclotómico (véase 3.10.6). Esto hace particularmente interesante el **teorema de Dirichlet sobre primos en progresiones aritméticas** que afirma que si $\mathrm{mcd}(a, m) = 1$, entonces hay un número infinito de primos tales que $p \equiv a \pmod{m}$. Además, en cierto sentido técnico, hay precisamente $1/\phi(m)$ primos con esta propiedad. Este apéndice está dedicado a un bosquejo de la prueba que usa ideas importantes de la teoría analítica de números.

D.1 Caso de p = 1 (m)

Primero veremos un resultado particular cuando $a = 1$. En este caso existe una prueba elemental basada en las propiedades de polinomios ciclotómicos.

D.1.1. Lema. *Si p es un primo tal que $p \nmid m$ y $p \mid \Phi_m(N)$ para algún $N \in \mathbb{Z}$, entonces $p \equiv 1 \pmod{m}$.*

Demostración. Las raíces de $\Phi_m(x)$ en $\mathbb{F}_p$ corresponden a los elementos de orden m en $\mathbb{F}_p^\times$. Entonces, si $\Phi_m(N) \equiv 0 \pmod{p}$, esto significa que N tiene orden m en $\mathbb{F}_p^\times$, y luego $p \equiv 1 \pmod{m}$. ■

D.1.2. Ejemplo. Tenemos $\Phi_5(3) = \frac{3^5-1}{3-1} = 242/2 = 121 = 11^2$. Ahora $11 \equiv 1 \pmod{5}$. ▲

D.1.3. Teorema. *Para m fijo, existe un número infinito de primos $p \equiv 1 \pmod{m}$.*

Demostración. Supongamos que $p_1, \ldots, p_s$ son los únicos primos tales que $p_i \equiv 1 \pmod{m}$. Pongamos

$$N = Cmp_1 \cdots p_s,$$

donde $C \gg 1$ se escoge de tal manera que $\Phi_m(N) > 1$. El término constante de cualquier polinomio ciclotómico es igual a ± 1 (véase (B.1)), así que

$$\Phi_m(N) \equiv \pm 1 \pmod{m}, \quad \Phi_m(N) \equiv \pm 1 \pmod{p_i}.$$

Ahora si p es un factor primo de $\Phi_m(N)$, entonces las congruencias de arriba demuestran que $p \nmid m$ y $p \notin \{p_1, \ldots, p_s\}$. Pero luego el lema de arriba implica que $p \equiv 1 \pmod{m}$. Contradicción. ■

Notamos que aunque el argumento de arriba está formulado como una prueba por contradicción, en realidad este nos da una manera de obtener a partir de un primo $p \equiv 1 \pmod m$ un número infinito de p con la misma propiedad, aunque estos p serán bastante grandes y muy pronto el número $\Phi_m(N)$ se volverá demasiado grande para buscar sus factores primos en práctica.

D.1.4. Ejemplo. Consideremos $m = 3$. El primo $p_1 = 7$ claramente cumple la condición $p_1 \equiv 1 \pmod 3$. Luego

$$p_2 = \Phi_3(3 \cdot p_1) = 463$$

casualmente es también primo. Luego

$$p_3 = \Phi_3(3 \cdot p_1 p_2) = 94546453$$

es también primo. En fin,

$$\Phi_3(3 \cdot p_1 p_2 p_3) = 845066824425253137587881 = 2059573 \cdot 410311663837724197$$

tiene dos factores primos p_4 y p_5. Todos los primos p_i de arriba cumplen la condición $p_i \equiv 1 \pmod 3$. ▲

El argumento con polinomios ciclotómicos funciona para $a = 1$. Nos interesa el caso general de $\mathrm{mcd}(a, m) = 1$, y allí ya no existe una prueba elemental; todas las pruebas conocidas tienen origen analítico.

D.2 Series de Dirichlet

A partir de ahora vamos a ocupar varios resultados de la teoría analítica de números. Como referencia, recomiendo los apuntes [ES2016]. Otro texto útil es [HTS1991]. Allí se encuentran demostraciones de todas las afirmaciones de abajo.

D.2.1. Definición. Para una función $f\colon \mathbb{Z}_{>0} \to \mathbb{C}$ la **serie de Dirichlet** correspondiente viene dada por

$$F(s) = \sum_{n \geq 1} \frac{f(n)}{n^s},$$

donde s es una variable compleja.

Un caso muy particular de las series de Dirichlet es la **función zeta de Riemann**

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

Las series de Dirichlet cumplen las siguientes propiedades generales.

1. Existe un número $-\infty \leq \sigma_0 \leq +\infty$, llamado la **abscisa de convergencia**, tal que $F(s)$ converge para $\operatorname{Re} s > \sigma_0$. Este es un análogo del radio de convergencia que se tiene para las series de potencias habituales.
2. De la misma manera, existe la **abscisa de convergencia absoluta** σ_a tal que $F(s)$ converge absolutamente para $\operatorname{Re} s > \sigma_a$. Siempre se tiene $\sigma_0 \leq \sigma_a \leq \sigma_0 + 1$.
3. Si existe una constante C tal que $\left|\sum_{1 \leq n \leq N}\right| \leq C$ para todo N, entonces $F(s)$ converge para $\operatorname{Re} s > 0$.
4. Si f es una función multiplicativa en el sentido fuerte, es decir, $f(ab) = f(a)f(b)$ para cualesquiera $a, b \in \mathbb{Z}_{>0}$, entonces para $\operatorname{Re} s > \sigma_a$ se cumple la **fórmula del producto de Euler**

$$F(s) = \prod_p \frac{1}{1 - f(p)\, p^{-s}},$$

donde el producto es sobre todos los primos.

Esta fórmula tiene sus orígenes en el teorema fundamental de la aritmética. De hecho, manipulando con las series de manera formal[*] y ocupando la multiplicatividad de f,

$$\prod_p \frac{1}{1-f(p)\,p^{-s}} = \prod_p \sum_{e\geq 0} \frac{f(p^e)}{p^{es}} = \sum_{n\geq 1} \frac{f(n)}{n^s}.$$

Un homomorfismo $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ se llama un **carácter de Dirichlet** mód m. Notamos que los valores de χ son las raíces m-ésimas de la unidad. Un carácter χ se levanta a una función $\widetilde{\chi}\colon \mathbb{Z}\to\mathbb{C}$ mediante

$$\widetilde{\chi}(a) = \begin{cases} \chi(a), & \text{si } \operatorname{mcd}(a,m)=1,\\ 0, & \text{si } \operatorname{mcd}(a,m)\neq 1.\end{cases}$$

A continuación vamos a escribir simplemente «χ» en lugar de «$\widetilde{\chi}$».

Los caracteres de Dirichlet mód m forman un grupo abeliano respecto a la multiplicación punto por punto. El elemento neutro en este grupo es el **carácter principal** (o **trivial**) χ_0 definido mediante

$$\chi_0(a) = \begin{cases} 1, & \text{si } \operatorname{mcd}(a,m)=1,\\ 0, & \text{si } \operatorname{mcd}(a,m)\neq 1.\end{cases}$$

En general, para cualquier grupo abeliano finito G podemos considerar su grupo de caracteres $\widehat{G} = \operatorname{Hom}(G,\mathbb{C}^\times)$, y este cumple la **relación de ortogonalidad**

$$\sum_{\chi\in\widehat{G}} \chi(g)\,\chi^{-1}(h) = \begin{cases} |G|, & \text{si } g=h,\\ 0, & \text{si } g\neq h.\end{cases}$$

(Este cálculo se ve en la teoría de representación de grupos finitos; véase por ejemplo [Ser1978, §2.3].) En particular, para $G=(\mathbb{Z}/m\mathbb{Z})^\times$ y $\operatorname{mcd}(a,m)=\operatorname{mcd}(b,m)=1$ se cumple

$$\sum_{\chi} \chi(a)\,\chi^{-1}(b) = \begin{cases} \phi(m), & \text{si } a\equiv b \pmod m,\\ 0, & \text{si } a\not\equiv b \pmod m.\end{cases} \tag{D.1}$$

D.2.2. Definición. Dado un carácter de Dirichlet χ, la **serie L** correspondiente se define mediante

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

La función zeta de Riemann converge para $\operatorname{Re} s > 1$ y también cumple la fórmula del producto (descubierta por Euler)

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}. \quad (\operatorname{Re} s > 1)$$

Notamos que $L(s,\chi)$ también converge absolutamente para $\operatorname{Re} s > 1$ (los coeficientes $\chi(n)$ son nulos o cumplen con $|\chi(n)|=1$), así que gracias a la multiplicatividad de χ,

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)\,p^{-s}}. \quad (\operatorname{Re} s > 1)$$

Por otra parte, para $s=1$ se obtiene la **serie armónica** $\sum_{n\geq 1}\frac{1}{n}$ que es divergente. No es difícil calcular que (véase 6.0.1)

$$\lim_{s\to 1^+} (s-1)\,\zeta(s) = 1. \tag{D.2}$$

[*] ¿O informal? :-)

Para las series L, si $\chi = \chi_0$ es el carácter principal mód m, entonces se obtiene

$$L(s,\chi_0) = \prod_{p\nmid m} \frac{1}{1-p^{-s}} = \prod_{p\mid m}(1-p^{-s})\,\zeta(s).$$

En particular, $L(s,\chi_0)$ es divergente en $s=1$, y se tiene

$$\lim_{s\to 1^+}(s-1)\,L(s,\chi_0) = \prod_{p\mid m}(1-p^{-1}) = \phi(m)/m.$$

Por otra parte, si $\chi \neq \chi_0$ no es un carácter principal, entonces $\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\chi(a)=0$, y de allí es fácil ver que para cualquier N se cumple $\left|\sum_{1\le n\le N}\chi(n)\right| < m$. Esto implica que $L(s,\chi)$ converge para $\operatorname{Re} s > 0$ en el caso cuando $\chi\neq\chi_0$. El resultado clave que contiene todas las dificultades técnicas de la prueba de Dirichlet es el siguiente.

D.2.3. Teorema. *Si χ no es un carácter principal, entonces $L(1,\chi)\neq 0$.*

Demostración. Una prueba mediante la teoría algebraica de números es 6.7.17. Para una prueba concisa y elemental, véase por ejemplo [IR1990, §16.5]. En general, $L(s,\chi)\neq 0$ para $\operatorname{Re} s = 1$. Esto se demuestra, por ejemplo, en [ES2016, Chapter 5] y [HTS1991, Chapter 6]. ■

D.2.4. Ejemplo. Sea χ el carácter no principal mód 3. Este viene dado por $\chi(1)=+1$ y $\chi(2)=-1$. Ahora

$$L(1,\chi) = \sum_{n\ge 1}\frac{\chi(n)}{n} = \sum_{n\ge 0}\left(\frac{1}{3n+1}-\frac{1}{3n+2}\right) = \sum_{n\ge 0}\frac{1}{(3n+1)\,(3n+2)}.$$

Para evaluar la suma, notamos que

$$\int_0^1 t^{3n}\,(1-t)\,dt = \frac{1}{(3n+1)\,(3n+2)}.$$

Ahora

$$\sum_{n\ge 0}\frac{1}{(3n+1)\,(3n+2)} = \sum_{n\ge 0}\int_0^1 t^{3n}\,(1-t)\,dt = \int_0^1\left(\sum_{n\ge 0}t^{3n}\,(1-t)\right)dt =$$
$$\int_0^1\frac{1-t}{1-t^3}\,dt = \int_0^1\frac{1}{1+t+t^2}\,dt = \frac{2}{\sqrt{3}}\left[\arctan\left(\frac{2t+1}{\sqrt{3}}\right)\right]_0^1 = \frac{2}{\sqrt{3}}\left(\frac{\pi}{3}-\frac{\pi}{6}\right) = \frac{\pi}{3\sqrt{3}}. \quad ▲$$

D.3 Densidad de primos

D.3.1. Lema. *Se tiene*

$$\lim_{s\to 1^+}\log\zeta(s)\Big/\log\frac{1}{s-1} = 1.$$

Demostración. Denotemos $\psi(s) = (s-1)\,\zeta(s)$. Tenemos entonces

$$\log\psi(s) = \log(s-1)+\log\zeta(s).$$

Luego,

$$\log\zeta(s)\Big/\log\frac{1}{s-1} = 1+\log\psi(s)\Big/\log\frac{1}{s-1}\,.$$

Pasando al límite $s\to 1^+$, notamos que $\psi(s)\to 1$ según (D.2). ■

D.3.2. Lema. *Se tiene*

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + R(s),$$

donde la suma es sobre todos los primos, y la función $R(s)$ es acotada para $s \to 1^+$.

Demostración. La fórmula del producto nos dice que

$$\zeta(s) = \prod_{p \le N} \frac{1}{1-p^{-s}} R_N(s),$$

donde $\lim_{N\to\infty} R_N(s) = 1$. Tomando el logaritmo de ambas partes, se obtiene*

$$\log \zeta(s) = \sum_{p\le N} -\log(1-p^{-s}) + \log R_N(s) = \sum_{p\le N}\sum_{n\ge 1} \frac{p^{-ns}}{n} + \log R_N(s).$$

Al pasar al límite $N \to \infty$, nos queda

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + \sum_p \sum_{n\ge 2} \frac{p^{-ns}}{n}.$$

Usando la fórmula de progresión aritmética, escribamos el segundo término como

$$R(s) = \sum_p \sum_{n\ge 2} \frac{p^{-ns}}{n} = \sum_p p^{-2s} \frac{1}{1-p^{-s}}.$$

Ahora $\frac{1}{1-p^{-s}} \le 2$ para todo p y $s > 1$, así que

$$R(S) \le 2 \sum_p \frac{1}{p^{2s}} \le 2 \sum_{n\ge 1} \frac{1}{n^{2s}} \le 2\,\zeta(2). \qquad \blacksquare$$

Notamos que lo que acabamos de probar, junto con la divergencia de $\zeta(s)$ en $s = 1$, implica que la serie $\sum_p \frac{1}{p}$ es divergente. Esto nos da una prueba curiosa de la infinitud de números primos.

Las propiedades que acabamos de ver motivan la siguiente definición.

D.3.3. Definición. Sea X un conjunto que consiste en números primos. Su **densidad de Dirichlet** (o **densidad analítica**) viene dada por

$$d(X) = \lim_{s\to 1^+} \sum_{p\in X} \frac{1}{p^s} \Big/ \log \frac{1}{s-1},$$

si el límite correspondiente existe.

Los lemas de arriba nos dicen que la densidad es una especie de medida sobre los conjuntos de números primos. En partucular, se cumplen las siguientes propiedades.

1) Si X es un conjunto finito, entonces $d(X) = 0$.
2) Si X consiste en todos los primos, salvo un número finito de ellos, entonces $d(X) = 1$.
3) Si $X = Y \cup Z$ es una unión disjunta y las densidades $d(Y)$ y $d(Z)$ existen, entonces $d(X) = d(Y) + d(Z)$.

Dirichlet probó lo siguiente.

D.3.4. Teorema. *Para* $\operatorname{mcd}(a,m) = 1$ *la densidad de primos tales que* $p \equiv a \pmod m$ *es igual a* $1/\phi(m)$.

Notamos que puesto que la densidad no es nula, esto implica que hay un número infinito de primos con esta propiedad. Sin embargo, el resultado de Dirichlet es más fuerte: es *cuantitativo*.

Una generalización del teorema de Dirichlet en la teoría algebraica de números es el teorema de densidad de Chebotarëv, explicada en §4.4.

*Usando la serie del logaritmo $-\log(1-x) = \sum_{n\ge 1} \frac{x^n}{n}$ para $-1 < x < 1$.

D.4 Bosquejo de demostración del teorema de Dirichlet

Dado un carácter de Dirichlet χ mód m, consideremos la serie

$$G(s,\chi) = \sum_p \sum_{k\geq 1} \frac{(\chi(p)\,p^{-s})^k}{k}.$$

Aquí $\left|\frac{(\chi(p)\,p^{-s})^k}{k}\right| \leq \frac{1}{p^{ks}}$, y la serie $\zeta(s)$ converge para $s>1$ y converge uniformemente para $s \geq 1+\delta$, así que $G(s,\chi)$ define una función continua para $s>1$. Notamos que

$$\exp\left(\sum_{k\geq 1} \frac{(\chi(p)\,p^{-s})^k}{k}\right) = \exp(-\log(1-\chi(p)\,p^{-s})) = \frac{1}{1-\chi(p)\,p^{-s}}.$$

Entonces, la fórmula del producto para las series L nos dice que

$$\exp(G(s,\chi)) = L(s,\chi) \quad \text{para } s>1.$$

D.4.1. Proposición. *Tenemos*

$$\lim_{s\to 1^+} G(s,\chi) \Big/ \log\frac{1}{s-1} = \begin{cases} 1, & si\ \chi = \chi_0, \\ 0, & si\ \chi \neq \chi_0. \end{cases}$$

Demostración. Primero, si $\chi = \chi_0$, entonces para $s>1$ se tiene

$$G(s,\chi) = \log L(s,\chi) = \sum_{p\mid m} \log(1-p^{-s}) + \log\zeta(s),$$

y podemos concluir usando el lema D.3.1.

Por otra parte, si $\chi \neq \chi_0$, entonces, como fue mencionado en D.2.3, tenemos $L(1,\chi) \neq 0$, y luego $\lim_{s\to 1^+} G(s,\chi) = \log L(1,\chi)$. En este caso el valor $L(1,\chi)$ será un número complejo, y su logaritmo está bien definido solo módulo $2\pi i\mathbb{Z}$, pero de todas maneras, $G(s,\chi)$ es acotado para $s\to 1^+$. ■

Argumentando como en la prueba del lema D.3.2, llegamos a la conclusión que

$$G(s,\chi) = \sum_{p\nmid m} \chi(p)\,p^{-s} + R_\chi(s),$$

donde $R_\chi(s)$ es acotado para $s\to 1^+$. Dado un número a tal que $\mathrm{mcd}(a,m)=1$, multiplicamos ambas partes de la última ecuación por $\chi^{-1}(a)$ y sumamos sobre todos los caracteres de Dirichlet mód m:

$$\sum_\chi \chi^{-1}(a)\,G(s,\chi) = \sum_{p\nmid m} p^{-s} \sum_\chi \chi(p)\,\chi^{-1}(a) + \sum_\chi \chi^{-1}(a)\,R_\chi(s).$$

Usando la relación de ortogonalidad (D.1), podemos escribir esta expresión como

$$\sum_\chi \chi^{-1}(a)\,G(s,\chi) = \sum_{p\equiv a\ (m)} p^{-s} + \sum_\chi \chi^{-1}(a)\,R_\chi(s).$$

Al dividir esta expresión por $\log\frac{1}{s-1}$ y tomar el límite $s\to 1^+$, en la parte izquierda, gracias a la proposición de arriba, nos quedará 1. Por otra parte, en la parte derecha estará

$$\phi(m) \lim_{s\to 1^+} \sum_{p\equiv a\ (m)} \frac{1}{p} \Big/ \log\frac{1}{s-1} = \phi(m)\cdot d(\{p \mid p\equiv a\ (m)\}).$$

Esto establece el teorema de Dirichlet. ■

Voy a reiterar que la parte clave que no fue probada es el teorema D.2.3 que afirma que $L(1,\chi)\neq 0$ para $\chi\neq\chi_0$. Una posible prueba es 6.7.17.

D.5 Densidad natural

La definición de densidad $d(X)$ parece algo rara al principio, pero después de ver la prueba, se entiende cuál es su propósito. Hay otra noción de densidad, llamada la **densidad natural**:

$$d_{nat}(X) = \lim_{N\to\infty} \frac{\#\{p \mid p \in X,\ p \leq N\}}{\#\{p \mid p \leq N\}}.$$

Sería interesante investigar cuál es la densidad natural de los primos tales que $p \equiv a \pmod{m}$. Se puede probar que para la función

$$\pi(a, m, N) = \#\{p \mid p \equiv a\ (m),\ p \leq N\}$$

se tiene la asintótica

$$\pi(a, m, N) \sim \frac{1}{\phi(m)} \cdot \frac{N}{\log N}.$$

(Aquí la notación $f(N) \sim g(N)$ significa que $\lim_{N\to\infty} f(N)/g(N) = 1$.) Véase por ejemplo [ES2016, Chapter 7] o [HTS1991, Chapter 6]. Este resultado generaliza el célebre **teorema de los números primos** que nos dice que

$$\pi(N) \sim \frac{N}{\log N},$$

donde $\pi(N)$ denota el número de primos $\leq N$. Como consecuencia, la densidad natural de los primos $p \equiv a \pmod{m}$ es también igual a $1/\phi(m)$. En general, ocupando el teorema de los números primos, se puede probar que si un conjunto de primos X tiene densidad natural $d_{nat}(X)$, entonces este también tiene densidad de Dirichlet $d(X)$, y las dos coinciden. Esto no funciona en la otra dirección: existen conjuntos que tienen densidad de Dirichlet, pero no tienen densidad natural. En general, es más fácil trabajar con la densidad de Dirichlet.

También cabe mencionar que el teorema de los números primos es un resultado más complicado, que fue probado por Hadamard y de la Vallée Poussin en 1896, mientras que Dirichlet probó su teorema en 1837.

D.6 Aplicación: irreducibilidad de polinomios ciclotómicos

Como una aplicación curiosa del teorema de Dirichlet, podemos probar la irreducibilidad de polinomios ciclotómicos $\Phi_m \in \mathbb{Z}[x]$. El argumento es el siguiente.

Supongamos que $\Phi_m = fg$ para algunos polinomios $f, g \in \mathbb{Z}[x]$. Sin pérdida de generalidad, f y g son mónicos y f es irreducible. Entonces alguna raíz n-ésima primitiva ζ es una raíz de f. Nos gustaría probar que cualquier otra raíz primitiva ζ^a, donde $\mathrm{mcd}(a, m) = 1$ es una raíz de f, y por lo tanto $g = 1$.

Si p es un primo tal que $p \equiv a \pmod{m}$, entonces en el anillo $\mathbb{Z}[\zeta_m]$ se cumple

$$p \mid f(\zeta^p) = f(\zeta^a).$$

En efecto, la fórmula del binomio en característica p nos dice que $f(\zeta^p) \equiv f(\zeta)^p \pmod{p}$.

Ahora gracias al teorema de Dirichlet, existe un número infinito de primos tales que $p \equiv a \pmod{m}$, y que entonces dividen a $f(\zeta^a)$. Pero esto implica que $f(\zeta^a) = 0$: un elemento no nulo de $\mathbb{Z}[\zeta_m]$ tiene solo un número finito de divisores primos. ■

Bibliografía

[AC1981] Raymond G. Ayoub and Sarvadaman Chowla, *On Euler's polynomial*, J. Number Theory **13** (1981), no. 4, 443–445. MR642919
https://doi.org/10.1016/0022-314X(81)90035-4

[AM1969] Michael F. Atiyah and Ian G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802

[Apo1976] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York-Heidelberg, 1976, Undergraduate Texts in Mathematics. MR0434929
https://doi.org/10.1007/978-1-4757-5579-4

[Artin-Galois] Emil Artin, *Galois theory*, second ed., Dover Publications, Inc., Mineola, NY, 1998, Edited and with a supplemental chapter by Arthur N. Milgram. MR1616156

[AW2004] Şaban Alaca and Kenneth S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004. MR2031707

[Bak1990] Alan Baker, *Transcendental number theory*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990. MR1074572

[BBP2010] Karim Belabas, Manjul Bhargava, and Carl Pomerance, *Error estimates for the Davenport-Heilbronn theorems*, Duke Math. J. **153** (2010), no. 1, 173–210. MR2641942
https://doi.org/10.1215/00127094-2010-007

[BdS2002] Wieb Bosma and Bart de Smit, *On arithmetically equivalent number fields of small degree*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR2041074
https://doi.org/10.1007/3-540-45455-1_6

[Bel1997] Karim Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237. MR1415795
https://doi.org/10.1090/S0025-5718-97-00846-6

[Bha2005] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063. MR2183288
https://doi.org/10.4007/annals.2005.162.1031

[Bha2010] ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2) **172** (2010), no. 3, 1559–1591. MR2745272
https://doi.org/10.4007/annals.2010.172.1559

[BS1966] A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York-London, 1966. MR0195803

[BW1987] Johannes Buchmann and Hugh C. Williams, *On principal ideal testing in algebraic number fields*, J. Symbolic Comput. **4** (1987), no. 1, 11–19. MR908408
https://doi.org/10.1016/S0747-7171(87)80049-4

[Car1960] Leonhard Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392. MR111741
https://doi.org/10.1090/S0002-9939-1960-0111741-2

[CF2010] J. W. S. Cassels and Albrecht Fröhlich (eds.), *Algebraic number theory*, London Mathematical Society, London, 2010, Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata. MR3618860

[CL1984] Henri Cohen and Hendrik W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR756082
https://doi.org/10.1007/BFb0099440

[Cla1966] Luther Claborn, *Every abelian group is a class group*, Pacific J. Math. **18** (1966), 219–222. MR195889
http://projecteuclid.org/euclid.pjm/1102994263

[Clark-CA] Pete L. Clark, *Commutative algebra*.
http://math.uga.edu/~pete/integral2015.pdf

[Coh1993] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206
https://doi.org/10.1007/978-3-662-02945-9

[Coh2006] Henry Cohn, *A short proof of the simple continued fraction expansion of e*, Amer. Math. Monthly **113** (2006), no. 1, 57–62. MR2202921
https://arxiv.org/abs/math/0601660

[Coh2007] Henri Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007. MR2312337

[Cox2013] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR3236783
https://doi.org/10.1002/9781118400722

[CRSS2015] John Coates, A. Raghuram, Anupam Saikia, and R. Sujatha (eds.), *The Bloch-Kato conjecture for the Riemann zeta function*, London Mathematical Society Lecture Note Series, vol. 418, Cambridge University Press, Cambridge, 2015. MR3410209
https://doi.org/10.1017/CBO9781316163757

[Ţ2018] George C. Ţurcaş, *On Fermat's equation over some quadratic imaginary number fields*, Res. Number Theory **4** (2018), no. 2, Paper No. 24, 16. MR3798168
https://doi.org/10.1007/s40993-018-0117-y

[dSP1994] Bart de Smit and Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 2, 213–215. MR1260520
https://doi.org/10.1090/S0273-0979-1994-00520-8

[E461] Leonhard Euler, *Extrait d'un lettre de M. Euler le Pere à M. Bernoulli concernant le Mémoire imprimé parmi ceux de 1771, p. 318*, Nouveaux Mémoires de l'académie royale des sciences de Berlin (1774), 35–36.
https://scholarlycommons.pacific.edu/euler-works/461

[E792] _____, *Tractatus de numerorum doctrina capita XVI, quae supersunt*, 1849.
https://scholarlycommons.pacific.edu/euler-works/792

[Edw1975] Harold M. Edwards, *The background of Kummer's proof of Fermat's last theorem for regular primes*, Arch. History Exact Sci. **14** (1975), no. 3, 219–236. MR0472364
https://doi.org/10.1007/BF00327448

[Edw1977] _____, *Postscript to: "The background of Kummer's proof of Fermat's last theorem for regular primes" (Arch. History Exact Sci.* **14** *(1975), no. 3, 219–236)*, Arch. History Exact Sci. **17** (1977), no. 4, 381–394. MR0472365
https://doi.org/10.1007/BF00328877

[Edw1996] _____, *Fermat's last theorem*, Graduate Texts in Mathematics, vol. 50, Springer-Verlag, New York, 1996, A genetic introduction to algebraic number theory, Corrected reprint of the 1977 original. MR1416327

[EH2000] David Eisenbud and Joe Harris, *The geometry of schemes*, Graduate Texts in Mathematics, vol. 197, Springer-Verlag, 2000.
http://doi.org/10.1007/b97680

[Els2007] Jürgen Elstrodt, *The life and work of Gustav Lejeune Dirichlet (1805–1859)*, Analytic number theory, Clay Math. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 2007, pp. 1–37. MR2362192
https://doi.org/10.1070/rm1983v038n01abeh003384

[ES2016] Jan-Hendrik Evertse and Efthymios Sofos, *Analytic number theory*, 2016, Apuntes en línea.
http://www.math.leidenuniv.nl/~evertse/ant.shtml

[FT1993] Albrecht Fröhlich and Martin J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR1215934

[FV2020] Michael Fütterer and José Villanueva, *Torres infinitas sorprendentes. Una introducción a la teoría de Iwasawa*, 2020.
https://arxiv.org/abs/2008.13375

[Gol1985] Dorian Goldfeld, *Gauss's class number problem for imaginary quadratic fields*, Bull. Amer. Math. Soc. (N.S.) **13** (1985), no. 1, 23–37. MR788386
https://doi.org/10.1090/S0273-0979-1985-15352-2

[Gro1985] Emil Grosswald, *Representations of integers as sums of squares*, Springer-Verlag, New York, 1985. MR803155
https://doi.org/10.1007/978-1-4613-8566-0

[GW2010] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I: Schemes. With examples and exercises*, Vieweg+Teubner Verlag, 2010.
http://doi.org/10.1007/978-3-8348-9722-0

[HTS1991] Edmund Hlawka, Rudolf Taschner, and Johannes Schoißengeier, *Geometric and analytic number theory*, Universitext, Springer, Berlin Heidelberg, 1991, Translated from the 1986 German edition by Charles Thomas. MR1123023
https://doi.org/10.1007/978-3-642-75306-0

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[KCd-Selmer] Keith Conrad, *The galois group of* $x^n - x - 1$ *over* $\mathbb{Q}$, Apuntes en línea.
https://kconrad.math.uconn.edu/blurbs/

[Khi1997] A. Ya. Khinchin, *Continued fractions*, russian ed., Dover Publications, Inc., Mineola, NY, 1997, With a preface by B. V. Gnedenko, Reprint of the 1964 translation. MR1451873

[KKS2011] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito, *Number theory. 2*, Translations of Mathematical Monographs, vol. 240, American Mathematical Society, Providence, RI, 2011, Introduction to class field theory, Translated from the 1998 Japanese original by Masato Kuwata and Katsumi Nomizu, Iwanami Series in Modern Mathematics. MR2817199

[KZ2001] Maxim Kontsevich and Don Zagier, *Periods*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 771–808. MR1852188
https://doi.org/10.1007/978-3-642-56478-9_39

[Lan1994] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723
https://doi.org/10.1007/978-1-4612-0853-2

[Lan2002] ———, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
https://doi.org/10.1007/978-1-4613-0041-0

[Len1992] Hendrik W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244. MR1129315
https://doi.org/10.1090/S0273-0979-1992-00284-7

[Lor1996] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996. MR1376367
https://doi.org/10.1090/gsm/009

[Mar2018] Daniel A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018, Second edition of [MR0457396], With a foreword by Barry Mazur. MR3822326
https://doi.org/10.1007/978-3-319-90233-3

[Mor1996] Patrick Morandi, *Field and Galois theory*, Graduate Texts in Mathematics, vol. 167, Springer-Verlag, New York, 1996. MR1410264
https://doi.org/10.1007/978-1-4612-4040-2

[Mos1951] Leo Moser, *A theorem on quadratic residues*, Proc. Amer. Math. Soc. **2** (1951), 503–504. MR41159
https://doi.org/10.2307/2031783

[Motives-I] Uwe Jannsen, Steven Kleiman, and Jean-Pierre Serre (eds.), *Motives*, Proceedings of Symposia in Pure Mathematics, vol. 55, American Mathematical Society, Providence, RI, 1994. MR1265518
https://doi.org/10.1090/pspum/055.1

[Nag1964] Trygve Nagell, *Introduction to number theory*, Second edition, Chelsea Publishing Co., New York, 1964. MR0174513

[Neu1999] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859
https://doi.org/10.1007/978-3-662-03983-0

[Old1970] Carl D. Olds, *The Simple Continued Fraction Expansion of e*, Amer. Math. Monthly **77** (1970), no. 9, 968–974. MR1536091
https://www.maa.org/sites/default/files/pdf/upload_library/22/Chauvenet/Olds.pdf

[Osa1987] Hiroyuki Osada, *The Galois groups of the polynomials $X^n + aX^\ell + b$*, J. Number Theory **25** (1987), no. 2, 230–238. MR873881
https://doi.org/10.1016/0022-314X(87)90029-1

[Per1977] Robert Perlis, *On the equation $\zeta_K(s) = \zeta_{K'}(s)$*, J. Number Theory **9** (1977), no. 3, 342–360. MR447188
https://doi.org/10.1016/0022-314X(77)90070-1

[PZ1997] Michael Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1997, Revised reprint of the 1989 original. MR1483321

[Rei1995] Miles Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, vol. 29, Cambridge University Press, Cambridge, 1995. MR1458066
https://doi.org/10.1017/CBO9781139172721

[Rib1999] Paulo Ribenboim, *Fermat's last theorem for amateurs*, Springer-Verlag, New York, 1999. MR1719329
https://doi.org/10.1007/b97437

[Rib2000] ———, *My numbers, my friends*, Springer-Verlag, New York, 2000, Popular lectures on number theory. MR1761897
https://doi.org/10.1007/b98892

[Riv2000] Tanguy Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris Sér. I Math. **331** (2000), no. 4, 267–270. MR1787183
https://doi.org/10.1016/S0764-4442(00)01624-4

[RV2007] Fernando Rodriguez Villegas, *Experimental number theory*, Oxford Graduate Texts in Mathematics, vol. 13, Oxford University Press, Oxford, 2007. MR2317419

[Sam1966] Pierre Samuel, *à propos du théorème des unités*, Bull. Sci. Math. (2) **90** (1966), 89–96. MR204454

[Sam1967] ———, *Théorie algébrique des nombres*, Hermann, Paris, 1967. MR0215808

[San2006] Ed Sandifer, *How euler did it: Who proved e is irrational?*, 2006.
http://eulerarchive.maa.org/hedi/HEDI-2006-02.pdf

[Sch1980] Wolfgang M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer, Berlin, 1980. MR568710

[Sel1956] Ernst S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302. MR85223
https://doi.org/10.7146/math.scand.a-10478

[Ser1978] Jean-Pierre Serre, *Représentations linéaires des groupes finis*, 3 ed., Hermann, Paris, 1978. MR543841

[Sil2009] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094
https://doi.org/10.1007/978-0-387-09494-6

[SL1996] Peter Stevenhagen and Hendrik W. Lenstra, Jr., *Chebotarëv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37. MR1395088
https://doi.org/10.1007/BF03027290

[SO1985] Winfried Scharlau and Hans Opolka, *From Fermat to Minkowski*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1985, Lectures on the theory of numbers and its historical development, Translated from the German by Walter K. Bühler and Gary Cornell. MR770936
https://doi.org/10.1007/978-1-4757-1867-6

[Ste1992] John Steinig, *A proof of Lagrange's theorem on periodic continued fractions*, Arch. Math. (Basel) **59** (1992), no. 1, 21–23. MR1166013
https://doi.org/10.1007/BF01199010

[Ste2017] Peter Stevenhagen, *Number rings*, 2017.
http://websites.math.leidenuniv.nl/algebra/ant.pdf

[Sut2018] Andrew E. Sutherland, *Arithmetic equivalence and isospectrality*, 2018.
https://math.mit.edu/~drew/ArithmeticEquivalenceLectureNotes.pdf

[vdP1979] Alfred van der Poorten, *A proof that Euler missed. . .Apéry's proof of the irrationality of* $\zeta(3)$, Math. Intelligencer **1** (1979), no. 4, 195–203, An informal report. MR547748
http://dx.doi.org/10.1007/BF03028234

[Was1997] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575
https://doi.org/10.1007/978-1-4612-1934-7

[Wat2004] Mark Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), no. 246, 907–938. MR2031415
https://doi.org/10.1090/S0025-5718-03-01517-5

[Wei2006] André Weil, *Number theory, an approach through history from Hammurapi to Legendre*, Birkhäuser, 2006.

[Wil1970] Kenneth S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. **13** (1970), 519–526. MR279069
https://people.math.carleton.ca/~williams/papers/pdf/033.pdf

[Wil1977] ———, *On Eisenstein's supplement to the law of cubic reciprocity*, Bull. Calcutta Math. Soc. **69** (1977), no. 6, 311–314. MR558227
https://people.math.carleton.ca/~williams/papers/pdf/093.pdf

[Zud2004] Wadim Zudilin, *Arithmetic of linear forms involving odd zeta values*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 251–291. MR2145585
http://jtnb.cedram.org/item?id=JTNB_2004__16_1_251_0