La vez pasada: para $0 \neq I \subseteq \mathcal{O}_K$ existe $0 \neq \alpha \in I$

tal que $|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N_{K/\mathbb{Q}}(I)$,

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\Delta_K|}$$ (cota de Minkowski)

Lema 2. Para todo $[I] \in Cl(K)$ existe $J \subseteq \mathcal{O}_K$ tal que $[I] = [J]$ y $N_{K/\mathbb{Q}}(J) \leq M_K$

Demostración. I — ideal fraccionario no nulo.

Existe $0 \neq \beta \in \mathcal{O}_K$ tal que $\beta I^{-1} \subseteq \mathcal{O}_K$.

$\Longrightarrow$ Existe $0 \neq \alpha \in \beta I^{-1}$ tal que

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K \cdot N_{K/\mathbb{Q}}(\beta I^{-1})$$

$\underbrace{\alpha \beta^{-1} I}_{\text{ideal entero}} \subseteq (\beta I^{-1}) \cdot (\beta^{-1} I) \subseteq \mathcal{O}_K$ $\qquad [\alpha \beta^{-1} I] = [I]$.

$$N_{K/\mathbb{Q}}(\alpha \beta^{-1} I) \leq M_K.$$

$\square$

Teorema. $Cl(K)$ es finito.

Demostración. Lema 2 $\Rightarrow$ todo $[I] \in Cl(K)$ se representa por $I \subseteq \mathcal{O}_K$ con $N_{K/\mathbb{Q}}(I) \leq M_K$. Lema 1 $\Rightarrow$ hay un número finito de estos I. $\square$

Definición. $h_K = \# Cl(K)$ se llama el **número de clases**.

§ 2. CAMPOS CUADRÁTICOS IMAGINARIOS.

$$\mathbb{Q}(\sqrt{-d})$$

Consideremos los campos cuadráticos imaginarios

$K = \mathbb{Q}(\sqrt{-d})$

$r_1 = 0, \; r_2 = 1, \; n = 2$

$$\Delta_K = \begin{cases} -4d, & d \equiv 1,2 \ (4) \\ -d, & d \equiv 3 \ (4) \end{cases}$$

$$M_K = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot \sqrt{|\Delta_K|}$$

$$= \frac{2}{\pi} \sqrt{|\Delta_K|}$$

Las cotas de Minkowski:

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

Nota: si $M_K < 2$, entonces $cl(K) = 0$.

Para $K = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$

$\mathcal{O}_K = \mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$

son dominios euclidianos

($\Rightarrow$ DFU $\Rightarrow cl(K) = 0$)

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

$K = \mathbb{Q}(\sqrt{-5})$.

$$2\mathcal{O}_K = \mathfrak{p}^2, \qquad \mathfrak{p} = (2, 1+\sqrt{-5})$$

$$N_{K/\mathbb{Q}}(\mathfrak{p}) = 2.$$

Si $\mathfrak{p} = (\alpha)$ es principal $\Rightarrow N(\alpha) = 2$.

Norma: $N_{K/\mathbb{Q}}(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 2$

Entonces, $\mathfrak{p}$ no es principal.

$[\mathfrak{p}]$ es el único elemento no trivial en $Cl(K) \Rightarrow Cl(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

$K = \mathbb{Q}(\sqrt{-6})$. 2 y 3 se ramifican

$$2\mathcal{O}_K = \mathfrak{p}_2^2, \qquad \mathfrak{p}_2 = (2, \sqrt{-6})$$

$$3\mathcal{O}_K = \mathfrak{p}_3^2, \qquad \mathfrak{p}_3 = (3, \sqrt{-6})$$

$$N_{K/\mathbb{Q}}(a + b\sqrt{-6}) = a^2 + 6b^2 \neq 2, 3$$

$\Rightarrow$ $\mathfrak{p}_2$ y $\mathfrak{p}_3$ no son principales

$$[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = [\mathcal{O}_K].$$

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (\sqrt{-6}) \Rightarrow [\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$$

Conclusión: $Cl(K) \simeq \mathbb{Z}/2\mathbb{Z}$

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

• $K = \mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-13})$

$Cl(K) \simeq \mathbb{Z}/2\mathbb{Z}$ (¡ejercicio!)

• $K = \mathbb{Q}(\sqrt{-11})$: 2 es <u>inerte</u> en K.

$\Rightarrow$ no hay primos de norma 2

$\Rightarrow Cl(K) = 0$.

De hecho, $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$

es euclidiano

d:	1	2	3	5	6	7	10	11	13	14
M_K:	1,27	1,80	1,10	2,85	3,12	1,68	4,03	2,11	4,55	4,76

$K = \mathbb{Q}(\sqrt{-14})$

$$2\mathcal{O}_K = \mathfrak{p}_2^2 \qquad \mathfrak{p}_2 = (2, \sqrt{-14})$$

$$3\mathcal{O}_K = \mathfrak{p}_3 \overline{\mathfrak{p}_3} \qquad \mathfrak{p}_3 = (3, 1 - \sqrt{-14}).$$

No hay $\alpha \in \mathbb{Z}[\sqrt{-14}]$ de norma 2, 3

$$\Longrightarrow [\mathfrak{p}_2], [\mathfrak{p}_3] \neq [\mathcal{O}_K].$$

$[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$ (¡ejercicio!)

$[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = [\mathcal{O}_K]$

$[\mathfrak{p}_3]^{-1} = [\overline{\mathfrak{p}_3}] = [\mathfrak{p}_3]^3$

$Cl(K) \simeq \mathbb{Z}/4\mathbb{Z}$

K	$Cl(K)$	K	$Cl(K)$	K	$Cl(K)$
$\mathbb{Q}(i)$	0	$\mathbb{Q}(\sqrt{-17})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-2})$	0	$\mathbb{Q}(\sqrt{-19})$	0	$\mathbb{Q}(\sqrt{-38})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-3})$	0	$\mathbb{Q}(\sqrt{-21})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-39})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-5})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-23})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-41})$	$\mathbb{Z}/8$
$\mathbb{Q}(\sqrt{-6})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-26})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-42})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-7})$	0	$\mathbb{Q}(\sqrt{-29})$	$\mathbb{Z}/6$	$\mathbb{Q}(\sqrt{-43})$	0
$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-30})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-46})$	$\mathbb{Z}/4$
$\mathbb{Q}(\sqrt{-11})$	0	$\mathbb{Q}(\sqrt{-31})$	$\mathbb{Z}/3$	$\mathbb{Q}(\sqrt{-47})$	$\mathbb{Z}/5$
$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-33})$	$\mathbb{Z}/2 \oplus \mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-51})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{-14})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-34})$	$\mathbb{Z}/4$	$\mathbb{Q}(\sqrt{-53})$	$\mathbb{Z}/6$
$\mathbb{Q}(\sqrt{-15})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{-55})$	$\mathbb{Z}/4$

Observaciones:

- $Cl(\mathbb{Q}(\sqrt{-d}))$ no suelen ser triviales.

- Muchos elementos de 2-torsión.

¿Por qué?

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}], & d \equiv 1, 2 \ (4) \\ \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right], & d \equiv 3 \ (4) \end{cases} \quad \text{para} \quad K = \mathbb{Q}(\sqrt{-d}).$$

•) $N_{K/\mathbb{Q}}(a + b\sqrt{-d}) = a^2 + db^2$

•) $N_{K/\mathbb{Q}}\left(a + b\,\frac{1+\sqrt{-d}}{2}\right) = a^2 + ab + \frac{1+d}{4}\, b^2$

$$= \frac{1}{4}\left((2a+b)^2 + db^2\right)$$

Si $d \neq 1, 2, 7 \Rightarrow$ no hay elementos de norma 2.

$$\left.\begin{array}{l} 2\mathcal{O}_K = \mathfrak{p}_2^2 \\ \text{ó} \\ 2\mathcal{O}_K = \mathfrak{p}_2 \cdot \overline{\mathfrak{p}}_2 \end{array}\right\} \quad \begin{array}{l} \mathfrak{p}_2 \text{ no es principal} \\ \Rightarrow \text{elemento de orden } 2 \\ \qquad \text{en } Cl(K) \end{array}$$

Proposición 1. Supongamos $d \neq 1, 2, 7$.

$d \equiv 1, 2 \ (4)$ o $d \equiv 7 \ (8)$ $\Rightarrow$ $\mathfrak{P}_2 \mid 2$, $[\mathfrak{P}_2] \neq [\mathcal{O}_K]$

(2 se ramifica) (2 se escinde)

Proposición 2. Si d es compuesto, $p \mid d$,

entonces $\mathfrak{P} \mid p$ tiene orden 2 en $Cl(\mathbb{Q}(\sqrt{-d}))$

Demostración. $p\mathcal{O}_K = \mathfrak{P}^2$

$\mathfrak{P}$ principal $\Longrightarrow$ $\mathfrak{P} = (\sqrt{\pm p})$ $\boxed{\text{usando que } \mathcal{O}_K^\times = \{\pm 1\}}$

$\sqrt{\pm p} \in K \Rightarrow K = \mathbb{Q}(\sqrt{\pm p})$ pero $p \neq d$ $\square$

Conclusión: Si $Cl(\mathbb{Q}(\sqrt{-d})) = 0$, entonces

$d = p$ es primo, $p \equiv 3 \ (8)$ (con única excepción de $d = 1, 2, 7$)

Teorema (Dirichlet) Para $p \equiv 3\ (4)$, $p > 3$,

$$h\,\mathbb{Q}(\sqrt{-p}) = \begin{cases} \frac{1}{3} \sum'_{1 \le a < p/2} \left(\frac{a}{p}\right), & p \equiv 3\ (8) \\ \sum'_{1 \le a < p/2} \left(\frac{a}{p}\right), & p \equiv 7\ (8) \end{cases}$$

(número de clases)

Demostración: ¡al final del curso!

Significado: Si $p \equiv 3\ (4)$, el intervalo $\left[1, \frac{p-1}{2}\right]$ contiene más residuos que no-residuos cuadráticos. El "defecto" $\leftrightarrow$ $Cl(K)$.

Ejemplo: $\left(\frac{1}{7}\right) + \left(\frac{2}{7}\right) + \left(\frac{3}{7}\right) = 1 + 1 - 1 = 1$

$3^2 \equiv 2$

$Cl(\mathbb{Q}(\sqrt{-7})) = 0$

Ejemplo: $\left(\frac{1}{11}\right) + \left(\frac{2}{11}\right) + \left(\frac{3}{11}\right) + \left(\frac{4}{11}\right) + \left(\frac{5}{11}\right) = 1 - 1 + 1 + 1 + 1 = 3$

$5^2 \equiv 3$ $\quad 4^2 \equiv 5$

$Cl(\mathbb{Q}(\sqrt{-11})) = 0$

$h_{\mathbb{Q}(\sqrt{-p})}$ para $p \equiv 3\ (8)$

p	h	p	h	p	h	p	h
11	1	179	5	443	5	643	3
19	1	211	3	467	7	659	11
43	1	227	5	491	9	683	5
59	3	251	7	499	3	691	5
67	1	283	3	523	5	739	5
83	3	307	3	547	3	787	5
107	3	331	3	563	9	811	7
131	5	347	5	571	5	827	7
139	3	379	3	587	7	859	7
163	1	419	9	619	5	883	3

Una explicación.

Consideremos el primer primo <u>no</u> inerte en $\mathbb{Q}(\sqrt{-p})$ $\left(\Leftarrow \left(\frac{-p}{q}\right) = +1\right)$.

$\mathbb{Q}(\sqrt{-p})$:	$\mathbb{Q}(\sqrt{-11})$	$\mathbb{Q}(\sqrt{-19})$	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Q}(\sqrt{-163})$
M_K:	2,11	2,77	4,17	5,21	8,13
q:	3	5	11	17	41

Si $q > M_K \Rightarrow$ todos los $I \subseteq \mathcal{O}_K$ con $N_{K/\mathbb{Q}}(I) \leq M_K$ son principales

$$\Rightarrow Cl(K) = 0.$$

Conjetura (Gauss):

$Cl(\mathbb{Q}(\sqrt{-d})) = 0 \iff d = 1, 2, 3, 7, 11, 19, 43, 67, 163$

- Heilbronn, Linfoot, 1936: a lo sumo hay otro d más, pero $d > 10^9$
- Heegner, 1952: este d no existe (prueba con pequeñas omisiones)
- Baker, 1966: diferente prueba
- Stark, 1967: otra prueba, confirmación del argumento de Heegner.

"Números de Heegner":

1, 2, 3, 7, 11, 19, 43, 67, 163.

Otras conjeturas de Gauss

•) $h_{\mathbb{Q}(\sqrt{-d})} \xrightarrow{d \to \infty} \infty$ Heilbronn 1934

•) Generalización de la $1^{\underline{ra}}$ conjetura:
para cualquier h un número finito de $K = \mathbb{Q}(\sqrt{-d})$ con $h_K = h$.

•) Baker, Stark, 1971: 18 campos con $h_K = 2$.

•) Oesterlé, 1985: 16 campos con $h_K = 3$

Goldfield, Oesterlé, Gross, Zagier
$\Longrightarrow$ Cota para d en términos de h_K.

§3. NÚMEROS DE LA SUERTE DE EULER

Euler descubrió que $f(x) = x^2 + x + 41$ toma valores primos para $x = 0, 1, \ldots, 39$ $\left(f(40) = 41^2 \right)$

$f(0) = 41$	$f(10) = 151$	$f(20) = 461$	$f(30) = 971$
$f(1) = 43$	$f(11) = 173$	$f(21) = 503$	$f(31) = 1033$
$f(2) = 47$	$f(12) = 197$	$f(22) = 547$	$f(32) = 1097$
$f(3) = 53$	$f(13) = 223$	$f(23) = 593$	$f(33) = 1163$
$f(4) = 61$	$f(14) = 251$	$f(24) = 641$	$f(34) = 1231$
$f(5) = 71$	$f(15) = 281$	$f(25) = 691$	$f(35) = 1301$
$f(6) = 83$	$f(16) = 313$	$f(26) = 743$	$f(36) = 1373$
$f(7) = 97$	$f(17) = 347$	$f(27) = 797$	$f(37) = 1447$
$f(8) = 113$	$f(18) = 383$	$f(28) = 853$	$f(38) = 1523$
$f(9) = 131$	$f(19) = 421$	$f(29) = 911$	$f(39) = 1601$

Teorema (Rabinowitsch, 1912)

Sean p un primo impar y $K = \mathbb{Q}(\sqrt{-p})$.

Si $Cl(K) = 0$, entonces

$$f(x) = x^2 + x + \frac{p+1}{4}$$

* Recordemos que $Cl(K) = 0 \Rightarrow p \equiv 3\ (4)$

toma valores primos para

$$0 \leq x < \frac{p-3}{4}$$

Objetivo: una prueba elemental (sin usar la lista de campos con $Cl(\mathbb{Q}(\sqrt{-d})) = 0$)

Lema 1. Si $Cl(K)=0$ y q es un primo $< \frac{p+1}{4}$, entonces $\left(\frac{q}{p}\right) = -1$

Demostración. $Cl(K)=0 \implies p \equiv 3 \ (4)$

$\implies \left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$. Si $\left(\frac{q}{p}\right) = +1 \implies q$ se escinde:

$$q\mathcal{O}_K = \mathfrak{q}\cdot\bar{\mathfrak{q}}.$$

$\mathfrak{q}, \bar{\mathfrak{q}}$ principales por la hipótesis.

$$\mathfrak{q} = \left(a + \underbrace{b}_{\neq 0}\, \frac{1+\sqrt{-p}}{2}\right)$$

$$q = N_{K/\mathbb{Q}}\left(a + b\,\frac{1+\sqrt{-p}}{2}\right) = \frac{1}{4}\left((2a+b)^2 + pb^2\right)$$

$$\geq \frac{p+1}{4},$$ ya que $b \neq 0$.

$\square$

Lema 2. Si $Cl(K) = 0$, entonces $f(0) = \frac{p+1}{4}$ es primo.

Demostración. Si $q \mid \frac{p+1}{4}$ y $q < \frac{p+1}{4}$, entonces...

$Cl(K) = 0 \Rightarrow \mathcal{O}_K$ es un DFU

Lema 1 $\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right) = -1. \Rightarrow$ q es inerte en K
(= elto primo en $\mathcal{O}_K$)

$$q \mid \frac{p+1}{4} \Rightarrow q \mid \left(\frac{1+\sqrt{-p}}{2}\right)\left(\frac{1-\sqrt{-p}}{2}\right)$$

$$\Rightarrow q \mid \frac{1 \pm \sqrt{-p}}{2} \quad \text{¡imposible!}$$

$\square$

Teorema. $Cl(K) = 0 \Rightarrow f(x) = x^2 + x + \frac{p+1}{4}$

es primo para $0 \leq x < \frac{p-3}{4}$

Demostración. Si $f(x)$ no es primo,

habrá q primo impar, $q \mid f(x)$, $q^2 \leq f(x)$.

$$4q^2 \leq 4x^2 + 4x + (p+1)$$

$$= (2x+1)^2 + p < \left(\frac{p+1}{2}\right)^2$$

$$q < \frac{p+1}{2} \underset{\text{Lema 1}}{\Longrightarrow} \left(\frac{q}{p}\right) = -1$$

Pero $\quad x^2 + x + \frac{p+1}{4} = aq \qquad a \in \mathbb{Z}$

$$(2x+1)^2 + p = 4aq \Longrightarrow \left(\frac{-p}{q}\right) = +1.$$

Tenemos necesariamente $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$ $\square$

Ejemplo $Cl(\mathbb{Q}(\sqrt{-163})) = 0 \Rightarrow f(x) = x^2 + x + 41.$

Ejemplo $Cl(\mathbb{Q}(\sqrt{-67})) = 0 \Rightarrow f(x) = x^2 + x + 17.$

toma valores primos para

$x = 0, 1, \ldots, 15.$

$f(1) = 19$	$f(6) = 59$	$f(11) = 149$
$f(2) = 23$	$f(7) = 73$	$f(12) = 173$
$f(3) = 29$	$f(8) = 89$	$f(13) = 199$
$f(4) = 37$	$f(9) = 107$	$f(14) = 227$
$f(5) = 47$	$f(10) = 127$	$f(15) = 257.$

Ejemplo $Cl(\mathbb{Q}(\sqrt{-43})) = 0 \Rightarrow f(x) = x^2 + x + 11,$

toma valores primos para

$x = 0, 1, \ldots, 9.$

La otra implicación. Finitud de la suerte.

Si para q el polinomio $f(x) = x^2 + x + q$ toma valores primos en $x = 0, 1, \ldots, q-2$, se dice que q es un **número de la suerte de Euler.**

Hay una prueba elemental de que en este caso $Cl(\mathbb{Q}(\sqrt{1-4q})) = 0$.

Baker-Heegner-Stark: Los únicos números de la suerte son

$$2, \quad 3, \quad 5, \quad 11, \quad 17, \quad 41.$$

7   11   15   43   67   163

§4. CAMPOS CUADRÁTICOS REALES.

$$\mathbb{Q}(\sqrt{d})$$

$K = \mathbb{Q}(\sqrt{d})$

$r_1 = 2, \; r_2 = 0.$

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}$$

$$= \frac{1}{2}\sqrt{\Delta_K}.$$

Algunos cálculos.

d:	2	3	5	6	7	10	11	13	14	15
M_K:	1,41	1,73	1,12	2,45	2,65	3,16	3,32	1,80	3,74	3,87

$Cl(K) = 0$ si $M_K < 2$.

•) $K = \mathbb{Q}(\sqrt{6})$, $\quad M_K \approx 2{,}45$

$2\mathcal{O}_K = \mathfrak{p}_2^2 \qquad \mathfrak{p}_2 = (2, \sqrt{6})$.

De hecho (!) $\mathfrak{p}_2 = (2 + \sqrt{6})$ es principal.

$N_{K/\mathbb{Q}}(2 + \sqrt{6}) = 2^2 - 6 \cdot 1^2 = -2$.

Conclusión: $Cl(K) = 0$.

•) $K = \mathbb{Q}(\sqrt{7})$, $\quad M_K \approx 2{,}65$

Lo mismo: $2\mathcal{O}_K = \mathfrak{p}_2^2$, $\quad \mathfrak{p}_2 = (2, 1 + \sqrt{7})$

$Cl(K) = 0$. $\qquad = (3 + \sqrt{7})$.

•) $K = \mathbb{Q}(\sqrt{11})$, $\mathbb{Q}(\sqrt{14})$

Ejercicio: $Cl(K) = 0$.

.) $K = \mathbb{Q}(\sqrt{10})$, $M_K \simeq 3{,}16$

$$2\mathcal{O}_K = \mathfrak{p}_2^2 \qquad \mathfrak{p}_2 = (2, \sqrt{10})$$

$$3\mathcal{O}_K = \mathfrak{p}_3 \overline{\mathfrak{p}_3}, \qquad \mathfrak{p}_3 = (3, 1+\sqrt{10})$$

Norma: $N_{K/\mathbb{Q}}(a + b\sqrt{10}) = a^2 - 10b^2$

$$\not\equiv 2, 3 \pmod{5}$$

No hay elementos de norma 2 y 3

$\Longrightarrow$ $\mathfrak{p}_2$ y $\mathfrak{p}_3$ no son principales.

$$\left(1 - \sqrt{10}/2\right) \mathfrak{p}_2 = \mathfrak{p}_3 \Longrightarrow [\mathfrak{p}_2] = [\mathfrak{p}_3].$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \Longrightarrow [\mathfrak{p}_2] = [\overline{\mathfrak{p}_3}]$$

Conclusión: $Cl(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

•) $K = \mathbb{Q}(\sqrt{15})$, $M_K \approx 3,87$.

$$2\mathcal{O}_K = \mathfrak{p}_2^2, \quad \mathfrak{p}_2 = (2, 1+\sqrt{15})$$

$$3\mathcal{O}_K = \mathfrak{p}_3^2, \quad \mathfrak{p}_3 = (3, \sqrt{15}).$$

$$N(a+b\sqrt{15}) = a^2 - 15b^2 \not\equiv 2, 3 \pmod 5$$

$$\Rightarrow [\mathfrak{p}_2], [\mathfrak{p}_3] \neq [\mathcal{O}_K]$$

De hecho, $[\mathfrak{p}_2] = [\mathfrak{p}_3]$,

$$Cl(K) = \mathbb{Z}/2\mathbb{Z}.$$

Hay <u>muchos</u> $K = \mathbb{Q}(\sqrt{d})$ con $cl(K) = 0$.

K	cl	K		K	cl
$\mathbb{Q}(\sqrt{2})$	0	$\mathbb{Q}(\sqrt{17})$	0	$\mathbb{Q}(\sqrt{33})$	0
$\mathbb{Q}(\sqrt{3})$	0	$\mathbb{Q}(\sqrt{15})$	0	$\mathbb{Q}(\sqrt{34})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{5})$	0	$\mathbb{Q}(\sqrt{21})$	0	$\mathbb{Q}(\sqrt{35})$	$\mathbb{Z}/2$
$\mathbb{Q}(\sqrt{7})$	0	$\mathbb{Q}(\sqrt{22})$	0	$\mathbb{Q}(\sqrt{37})$	0
$\mathbb{Q}(\sqrt{10})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{23})$	0	$\mathbb{Q}(\sqrt{38})$	0
$\mathbb{Q}(\sqrt{11})$	0	$\mathbb{Q}(\sqrt{26})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{35})$	0
$\mathbb{Q}(\sqrt{13})$	0	$\mathbb{Q}(\sqrt{29})$	0	. . . .	
$\mathbb{Q}(\sqrt{14})$	0	$\mathbb{Q}(\sqrt{30})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{79})$	$\mathbb{Z}/3$
$\mathbb{Q}(\sqrt{15})$	$\mathbb{Z}/2$	$\mathbb{Q}(\sqrt{31})$	0	$\mathbb{Q}(\sqrt{82})$	$\mathbb{Z}/4$

Para N primos, ¿cuántos campos $K = \mathbb{Q}(\sqrt{p})$ tienen $\mathrm{cl}(K) = 0$? ¡Muchísimos!

Cálculo en PARI/GP:

$N = 100$: 91

$N = 1000$: 845

$N = 10000$: 7570

$N = 100000$: 77962

$N = 1000000$: 769230

Conjetura (Gauss) un número infinito de $K = \mathbb{Q}(\sqrt{p})$ con $cl(K) = 0$.

Conjetura (Cohen, Lenstra, 1984)
El porcentaje debe ser

$$\frac{1}{2 C_\infty \cdot \eta_\infty(2)} \approx 75{,}445\ \%$$

$$C_\infty := \prod_{n \geq 2} \zeta(n), \quad \eta_\infty(p) = \prod_{n \geq 1} \frac{1}{1 - p^{-n}}$$

Para ninguna familia infinita de $K/\mathbb{Q}$ ha sido probado que $cl(K) = 0$.

§5. CAMPOS CICLOTÓMICOS

$$\mathbb{Q}(\zeta_n)$$

Ejemplo calculable con nuestros métodos

$K = \mathbb{Q}(\zeta_7)$. $n = \varphi(7) = 6$, $r_1 = 0$, $r_2 = 3$

$$M_K = \frac{6!}{6^6}\left(\frac{4}{\pi}\right)^3 7^{5/2} \approx 4{,}12.$$

$$2\mathcal{O}_K = (2, 1+\zeta_7+\zeta_7^3)(2, 1+\zeta_7^2+\zeta_7^3).$$

3 es un generador de $\mathbb{F}_7^\times \Rightarrow$ inerte.

$$(1+\zeta_7+\zeta_7^3)(1+\zeta_7^2+\zeta_7^3) = 2\zeta_7^3 \sim 2$$

$\Rightarrow$ los ideales sobre 2

son principales

$\Rightarrow$ $Cl(K) = 0$.

Kummer: el primer campo ciclotómico con $Cl(K) \neq 0$ es $\mathbb{Q}(\zeta_{23})$

$$Cl(\mathbb{Q}(\zeta_{23})) \simeq \mathbb{Z}/3.$$

$* \ M_K = 9\,324\,406,48$ ¡oops!

Teorema: Los únicos $\mathbb{Q}(\zeta_n)$ con $Cl = 0$ son

$n = 1, 3, 4, 5, 7, 8, 9, 11,$
$12, 13, 15, 16, 17, 19, 20, 21,$
$24, 25, 27, 28, 32, 33, 35, 36,$
$40, 44, 45, 48, 60, 84.$

$(n \not\equiv 2 \ (4)$: si $n \equiv 2 \ (4) \Rightarrow \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2}))$

Estudio de $Cl(\mathbb{Q}(\zeta_n)) \rightsquigarrow$ "teoría de Iwasawa"

Conclusiones.

— $Cl(K)$ es finito.

— $Cl(K)$ es calculable para $K/\mathbb{Q}$ fijo.

— No se sabe mucho de las propiedades generales.

— $\mathbb{Q}(\sqrt{-d})$ y $\mathbb{Q}(\sqrt{d})$ se comportan de manera muy diferente.

La razón: $\mathcal{O}_K^\times$ finito vs. infinito.
(próxima sesión)