Teoría de números algebraicos
Tarea 8

Alexey Beshenov (alexey.beshenov@cimat.mx)

28 de octubre de 2020

Ejercicio 8.1. Demuestre que si X es un conjunto convexo simétrico compacto tal que $\operatorname{vol} X = 2^n \cdot \operatorname{covol} \Lambda$, entonces $X \cap \Lambda \neq \{0\}$.

Solución. Para $k = 1, 2, 3, \ldots$ definamos

$$X_k = (1 + 1/k)\, X.$$

Esto nos da una cadena de conjuntos convexos simétricos compactos

$$X_1 \supset X_2 \supset X_3 \supset \cdots \supset X$$

Además, es fácil ver que

$$\bigcap_{k \geq 1} X_k = X.$$

Notamos que $\operatorname{vol} X_k > \operatorname{vol} X$, así que para todo k se cumple la condición del teorema de Minkowski, y existe un punto no nulo $\omega_k \in X_k \cap \Lambda$. Todos estos puntos están en X_1 que es compacto, y por la compacidad la sucesión (ω_k) tiene una subsucesión convergente (ω_{n_k}). Pongamos

$$\omega = \lim_{k \to \infty} \omega_{n_k}.$$

Primero, los ω_{n_k} son elementos de $\Lambda \setminus \{0\}$ que es un conjunto discreto, así que el mismo ω debe ser un elemento de $\Lambda \setminus \{0\}$.

Afirmamos que $\omega \in X \cap \Lambda$. En efecto, usando que Λ es un conjunto discreto, podemos concluir que para k suficientemente grande

$$\omega_{n_k} = \omega_{n_{k+1}} = \omega_{n_{k+2}} = \cdots = \omega.$$

Efectivamente, existe $\epsilon > 0$ suficientemente pequeño tal que $B_\epsilon(\omega) \cap \Lambda = \{\omega\}$. Luego existe k tal que todos los ω_{n_ℓ} para $\ell \geq k$ están en la bola $B_\epsilon(\omega)$, y por esto coinciden con ω. Tenemos $\omega = \omega_{n_\ell} \in X_{n_\ell}$ para todo $\ell \geq k$, y luego

$$\omega \in \bigcap_{\ell \geq k} X_{n_\ell} = \bigcap_{k \geq 1} X_k = X. \qquad \square$$

Ejercicio 8.2. 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

$$\operatorname{vol}(X_t) = 2^{r_1}\,(2\pi)^{r_2}\,t^n.$$

Solución. Este cálculo es muy sencillo. Si x_τ es una coordenada real, entonces esta contribuye $2t$. Por otra parte, si x_σ y $x_{\overline{\sigma}}$ es un par de coordenadas complejas, entonces nos interesa la condición $u^2 + v^2 < t^2$. Este es un círculo de radio t, y su área es πt^2. Tenemos entonces

$$\operatorname{vol}(X) = 2^{r_2}\,\operatorname{vol}_{Leb.}(X) = 2^{r_2}\cdot(2t)^{r_1}\cdot(\pi t^2)^{r_2} = 2^{r_1}\,(2\pi)^{r_2}\,t^n. \qquad \square$$

Ejercicio 8.3. 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 $\operatorname{Cl}(K)$ isomorfo a $(\mathbb{Z}/2\mathbb{Z})^{s-1}$.

Solución. Tenemos $d \ne 1,3$ y $\mathcal{O}_K^\times = \{\pm 1\}$. Todo primo $p_i \mid d$ se ramifica: se tiene $p_i\mathcal{O}_K = \mathfrak{p}_i^2$ para algún ideal primo $\mathfrak{p}_i \subset \mathcal{O}_K$. Este ideal no es principal: en el caso contrario $\alpha^2 = \pm p_i$ para algún $\alpha \in \mathcal{O}_K$, pero luego $\sqrt{\pm p_i} \in K$, y este no es el caso.

Consideremos el homomorfismo de grupos $\phi\colon (\mathbb{Z}/2\mathbb{Z})^s \to \operatorname{Cl}(K)$ que envía $(0,\ldots,1,\ldots,0)$ a $[\mathfrak{p}_i]$. Ocupando el mismo argumento de arriba, se calcula que

$$\ker\phi = \{(0,\ldots,0),\ (1,\ldots,1)\}.$$

Entonces, $\operatorname{Cl}(K)$ contiene como un subgrupo

$$\operatorname{im}\phi \cong (\mathbb{Z}/2\mathbb{Z})^s/\ker\phi \cong (\mathbb{Z}/2\mathbb{Z})^{s-1}. \qquad \square$$

Ejercicio 8.4. Calcule los grupos de clases de campos

$$\mathbb{Q}(\sqrt{-110}),\quad \mathbb{Q}(\sqrt{-127}),\quad \mathbb{Q}(\sqrt{33}),\quad \mathbb{Q}(\sqrt[3]{19}),\quad \mathbb{Q}(\sqrt{-3},\sqrt{-5}).$$

Solución. Todos estos cálculos son bastante trabajosos, pero escogí los ejemplos de arriba precisamente para tener algo no trivial. Tal vez este ejercicio tenía que ser una tarea separada.

- Para $K = \mathbb{Q}(\sqrt{-110})$ tenemos $\Delta_K = -2^3\cdot 5\cdot 11$, y la cota de Minkowski es $M_K \approx 13{,}35$. Las factorizaciones de primos relevantes son las siguientes:

$$\begin{aligned}
2\mathcal{O}_K &= \mathfrak{p}_2^2,\\
3\mathcal{O}_K &= \mathfrak{p}_3\,\mathfrak{p}_3',\\
5\mathcal{O}_K &= \mathfrak{p}_5^2,\\
7\mathcal{O}_K &= \mathfrak{p}_7\,\mathfrak{p}_7',\\
11\mathcal{O}_K &= \mathfrak{p}_{11}^2,\\
13\mathcal{O}_K &= \mathfrak{p}_{13}\quad \text{(inerte)},
\end{aligned}$$

donde

$$\begin{aligned}
\mathfrak{p}_2 &= (2, \alpha), \\
\mathfrak{p}_3 &= (3, 1 + \alpha), \\
\mathfrak{p}_5 &= (5, \alpha), \\
\mathfrak{p}_7 &= (7, 3 + \alpha), \\
\mathfrak{p}_{11} &= (11, \alpha).
\end{aligned}$$

Aquí los ideales primos arriba de $p = 2, 3, 5, 7, 11$ no son principales porque en $\mathcal{O}_K = \mathbb{Z}[\sqrt{-110}]$ no hay elementos de norma p: la norma viene dada por $N_{K/\mathbb{Q}}(a + b\,\alpha) = a^2 + 110\, b^2$. Otros ideales de norma $< M_K$ son

$$\mathfrak{p}_2\, \mathfrak{p}_3, \quad \mathfrak{p}_2\, \mathfrak{p}_3', \quad \mathfrak{p}_3^2, \quad \mathfrak{p}_3'^2, \quad \mathfrak{p}_2\, \mathfrak{p}_5.$$

Estos tampoco son principales: en $\mathcal{O}_K$ no hay elementos de norma 6 y 10, y los elementos de norma 9 son ± 3, y es fácil ver que $\mathfrak{p}_3^2 \neq 3\mathcal{O}_K$. Calculamos que $\mathfrak{p}_{11}\,(\alpha/11) = \mathfrak{p}_2\, \mathfrak{p}_5$, así que en el grupo de clases se tiene $[\mathfrak{p}_{11}] = [\mathfrak{p}_2\, \mathfrak{p}_5]$.

Esto nos dice que

$$\mathrm{Cl}(K) = \{[\mathcal{O}_K], [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_3'], [\mathfrak{p}_5], [\mathfrak{p}_2\, \mathfrak{p}_3], [\mathfrak{p}_2\, \mathfrak{p}_3'], [\mathfrak{p}_7], [\mathfrak{p}_7'], [\mathfrak{p}_3^2], [\mathfrak{p}_3'^2], [\mathfrak{p}_2\, \mathfrak{p}_5]\} \tag{*}$$

(todavía no estoy afirmando que todos estos elementos son distintos; lo veremos un poco más adelante).

Podemos calcular que

$$\mathfrak{p}_3^2 = (9, 4 + \alpha), \quad \mathfrak{p}_3^3 = (27, 22 + \alpha), \quad \mathfrak{p}_3^6 = (17 + 2\alpha).$$

El ideal $\mathfrak{p}_3^3$ tampoco es principal porque en $\mathcal{O}_K$ no hay elementos de norma 27. Esto demuestra que $[\mathfrak{p}_3]$ es un elemento de orden 6 en el grupo de clases. Calculamos sus potencias

$$[\mathfrak{p}_3]^3 = [\mathfrak{p}_5], \quad [\mathfrak{p}_3]^4 = [\mathfrak{p}_3]^{-2} = [\mathfrak{p}_3'^2], \quad [\mathfrak{p}_3]^5 = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3'].$$

Dado que $\mathrm{Cl}(K)$ tiene un elemento $[\mathfrak{p}_3]$ de orden 6 y otro elemento $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]^3 = [\mathfrak{p}_5]$ de orden 2, podemos concluir que $\mathrm{Cl}(K)$ es un grupo abeliano de orden 12. En particular, todos los elementos en (*) son distintos. Hay solamente dos posibilidades: $\mathbb{Z}/12\mathbb{Z}$ y $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^2$.

Se puede probar la relación

$$[\mathfrak{p}_7] = [\mathfrak{p}_3']\, [\mathfrak{p}_2]\, [\mathfrak{p}_5],$$

que nos dice en particular que $[\mathfrak{p}_7]$ tiene orden 6 en el grupo de clases. De aquí y nuestra lista de elementos de $\mathrm{Cl}(K)$ se ve que no hay elementos de orden 12. La única opción que nos queda es entonces $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

- Para $K = \mathbb{Q}(\sqrt{-127})$ tenemos $\mathcal{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{-127}}{2}\Big] \cong \mathbb{Z}[x]/(x^2 - x + 32)$, $\Delta_K = -127$, y la cota de Minkowski es $M_K \approx 7{,}17$.

  Denotemos $\alpha = \frac{1+\sqrt{-127}}{2}$.

  El primo $p = 2$ se escinde: tenemos

  $$2\mathcal{O}_K = \mathfrak{p}_2\,\mathfrak{p}_2', \quad \mathfrak{p}_2 = (2, \alpha), \quad \mathfrak{p}_2' = (2, 1 + \alpha).$$

  Por otra parte, los primos $p = 3, 5, 7$ son inertes. Como consecuencia, el grupo de clases está generado por $[\mathfrak{p}_2]$.

  El ideal $\mathfrak{p}_2$ no es principal: la norma sobre $\mathcal{O}_K$ viene dada por

  $$N(a + b\alpha) = a^2 + ab + 32\, b^2 = \frac{1}{4}\Big((2a + b)^2 + 127\, b^2\Big),$$

  y esta no puede ser igual a 2. Además,

  $$\mathfrak{p}_2^2 = (4, 2\alpha, \alpha^2) = (4, \alpha)$$

  tampoco será principal: para esto basta notar que el único elemento en $\mathcal{O}_K$ de norma 4 es ± 2 y $\mathfrak{p}_2^2 \neq 2\mathcal{O}_K$. De manera similar, se verifica que $\mathfrak{p}_2^3$ y

  $$\mathfrak{p}_2^4 = (16, 4\alpha, \alpha^2) = (16, \alpha)$$

  no son principales. Por otra parte,

  $$\mathfrak{p}_2^5 = (16, \alpha)\,(2, \alpha) = (32, 2\alpha, \alpha^2) = (\alpha)$$

  sí es principal (para la última igualdad, use que $32 = N_{K/\mathbb{Q}}(\alpha)$, y por otra parte, $\alpha^2 - \alpha + 32 = 0$).

  Esto demuestra que $[\mathfrak{p}_2]$ tiene orden 5 en el grupo de clases. Podemos concluir que $\mathrm{Cl}(K) \cong \mathbb{Z}/5\mathbb{Z}$.

- Para $K = \mathbb{Q}(\sqrt{33})$ tenemos $\Delta_K = 33$, y la cota de Minkowski es $M_K \approx 2{,}87$. Bastaría entonces revisar qué sucede con el primo $p = 2$. Escribamos $\mathcal{O}_K = \mathbb{Z}[\alpha]$, donde $\alpha = \frac{1+\sqrt{33}}{2}$. Factorizando el polinomio mínimo $f = f_{\mathbb{Q}}^{\alpha} = x^2 - x - 8$ mód 2, se obtiene

  $$2\mathcal{O}_K = \mathfrak{p}_2\,\mathfrak{p}_2', \quad \mathfrak{p}_2 = (2, \alpha), \quad \mathfrak{p}_2' = (2, 1 + \alpha).$$

  Estos ideales resultan ser principales. Por ejemplo, se tiene $\mathfrak{p}_2 = (2 + \alpha)$. Una de las inclusiones está clara, y para la otra podemos observar que $N_{K/\mathbb{Q}}(2 + \alpha) = -2$, así que 2 (y luego α) pertenece al ideal generado por $2 + \alpha$.

  Podemos concluir que el grupo de clases es trivial. Notamos que según el ejercicio anterior, el grupo de clases del campo *imaginario* $\mathbb{Q}(\sqrt{-33})$ será no trivial, con por lo menos un elemento no trivial de 2-torsión (en realidad, $\mathrm{Cl}(\mathbb{Q}(\sqrt{-33})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Como acabamos de ver, el mismo resultado no funciona para los campos cuadráticos reales.

- Para $K = \mathbb{Q}(\sqrt[3]{19})$ tenemos $\Delta_K = -3\cdot 19^2$ y la cota de Minkowski es $M_K \approx 9{,}31$. Los primos relevantes se descomponen de la siguiente manera:

$$\begin{aligned} 2\mathcal{O}_K &= \mathfrak{p}_2\,\mathfrak{p}_2', \\ 3\mathcal{O}_K &= \mathfrak{p}_3\,\mathfrak{p}_3'^2, \\ 5\mathcal{O}_K &= \mathfrak{p}_5\,\mathfrak{p}_5', \\ 7\mathcal{O}_K &= \mathfrak{p}_7 \quad \text{(inerte)}. \end{aligned}$$

Aquí

$$\begin{gathered} N(\mathfrak{p}_2) = 2,\ N(\mathfrak{p}_2') = 2^2, \\ N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3, \\ N(\mathfrak{p}_5) = 5,\ N(\mathfrak{p}_5') = 5^2, \\ N(\mathfrak{p}_7) = 3^3. \end{gathered}$$

De manera explícita, denotando $\alpha = \sqrt[3]{19}$, los ideales primos que están sobre 2 y 5 se obtienen factorizando el polinomio $f = x^3 - 19$:

$$\mathfrak{p}_2 = (2, 1{+}\alpha), \quad \mathfrak{p}_2' = (2, 1{+}\alpha{+}\alpha^2), \quad \mathfrak{p}_5 = (5, 1{+}\alpha), \quad \mathfrak{p}_5' = (5, 1{+}4\alpha{+}\alpha^2).$$

Los ideales primos arriba de 3 se obtiene factorizando $g = x^3 - x^2 - 6x - 12$ que es el polinomio mínimo de $\beta = \frac{1}{3}\,(1 + \alpha + \alpha^2)$ (véase el capítulo 3 de los apuntes donde se considera el ejemplo de $\mathbb{Q}(\sqrt[3]{19})$). El resultado es

$$\mathfrak{p}_3 = (3, 2+\beta), \quad \mathfrak{p}_3' = (3, \beta).$$

Primero afirmo que en $\mathcal{O}_K$ no hay elementos de norma 2 y 4, y por lo tanto los ideales $\mathfrak{p}_2$ y $\mathfrak{p}_2'$ no son principales. Recordemos que

$$\mathcal{O}_K = \mathbb{Z}[\alpha, \beta] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta.$$

Calculamos

$$N_{K/\mathbb{Q}}(a + b\alpha + c\beta) = a^3 + a^2c - 19\,abc - 6\,ac^2 + 19\,b^3 + 19\,b^2c + 12c^3.$$

Las ecuaciones

$$N_{K/\mathbb{Q}}(a + b\alpha + c\beta) \equiv 2, 4 \pmod{19}$$

no tienen solución, y por lo tanto podemos concluir que $N_{K/\mathbb{Q}}(a + b\alpha + c\beta) = 2, 4$ tampoco tienen solución.

Ahora se puede calcular que

$$(3)\,\mathfrak{p}_2^3 = (4 + \alpha + \alpha^2),$$

así que $[\mathfrak{p}_2]$ es un elemento de orden 3 en el grupo de clases. Por otra parte, $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]^2$.

Luego con ayuda de computadora se verifican las relaciones

$$\begin{aligned} 3\,\mathfrak{p}_3 &= \mathfrak{p}_3'\,(2+\alpha),\\ 3\,\mathfrak{p}_2 &= \mathfrak{p}_3'\,(1-\alpha),\\ 3\,\mathfrak{p}_5 &= \mathfrak{p}_3'\,(4-\alpha), \end{aligned}$$

de donde

$$[\mathfrak{p}_3] = [\mathfrak{p}_3'] = [\mathfrak{p}_2], \quad [\mathfrak{p}_5] = [\mathfrak{p}_2].$$

De aquí podemos concluir que $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$.

- Para $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-5})$ tenemos $\mathcal{O}_K = \mathbb{Z}\Big[\frac{1+\sqrt{-3}}{2}, \sqrt{-5}\Big]$, $\Delta_K = 2^4 \cdot 3^2 \cdot 5^2$, y la cota de Minkowski es $M_K \approx 9{,}11$. Nos interesa cómo los primos $p = 2, 3, 5, 7$ se factorizan en $\mathcal{O}_K$. El tipo de descomposición puede ser deducido de la descomposición de p en los subcampos $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{15})$, usando que $K/\mathbb{Q}$ es una extensión de Galois.

$$\begin{aligned} 2\mathcal{O}_K &= \mathfrak{p}_2^2, & N &= 4,\\ 3\mathcal{O}_K &= \mathfrak{p}_3^2\,\mathfrak{p}_3'^2, & N &= 3,\\ 5\mathcal{O}_K &= \mathfrak{p}_5^2, & N &= 25,\\ 7\mathcal{O}_K &= \mathfrak{p}_7\,\mathfrak{p}_7'\,\mathfrak{p}_7''\,\mathfrak{p}_7''', & N &= 7. \end{aligned}$$

El ideal primo arriba de $p = 5$ será irrelevante porque su norma excede la cota de Minkowski.

Para ocupar el teorema de Kummer–Dedekind, podemos, por ejemplo, tomar $\alpha = \frac{1+\sqrt{-3}}{2} + \sqrt{-5}$. El polinomio mínimo correspondiente es $f = x^4 - 2x^3 + 13x^2 - 12x + 21$. Calculamos $\Delta(f) = \Delta(\mathbb{Z}[\alpha]) = 2^4 \cdot 3^2 \cdot 5^2 \cdot 17^2$. Entonces, $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 17$, y las factorizaciones de $p \neq 17$ corresponden a las factorizaciones de f mód p. Calculamos

$$\begin{aligned} f &\equiv (x^2+x+1)^2 \pmod 2,\\ f &\equiv x^2\,(x+2)^2 \pmod 3,\\ f &\equiv x\,(x+1)\,(x+5)\,(x+6) \pmod 7. \end{aligned}$$

Entonces,

$$\mathfrak{p}_2 = (2, \alpha^2+\alpha+1),$$
$$\mathfrak{p}_3 = (3, \alpha), \quad \mathfrak{p}_3' = (3, \alpha+2),$$
$$\mathfrak{p}_7 = (7, \alpha), \quad \mathfrak{p}_7' = (7, \alpha+1), \quad \mathfrak{p}_7'' = (7, \alpha+5), \quad \mathfrak{p}_7'' = (7, \alpha+6).$$

No es difícil verificar que el ideal $\mathfrak{p}_2$ es principal: podemos tomar como su generador $\sqrt{-3} + \sqrt{-5}$. Para el resto de ideales, nos conviene escribirlos ocupando los automorfismos que generan el grupo de Galois:

$$\sigma\colon \sqrt{-3} \mapsto -\sqrt{-3}, \quad \tau\colon \sqrt{-5} \mapsto -\sqrt{-5}.$$

Primero, tenemos

$$\mathfrak{p}_3 = \Big(3, \frac{1+\sqrt{-3}}{2} + \sqrt{-5}\Big), \quad \mathfrak{p}_3' = \tau(\mathfrak{p}_3),$$

donde $D(\mathfrak{p}_3|3) = D(\mathfrak{p}_3'|3) = \{1, \sigma\}$. Para los ideales arriba de $p = 7$, tenemos

$$\mathfrak{p}_7 = \Big(7, \frac{1+\sqrt{-3}}{2} + \sqrt{-5}\Big), \quad \mathfrak{p}_7' = \tau(\mathfrak{p}_7), \quad \mathfrak{p}_7'' = \sigma(\mathfrak{p}_7), \quad \mathfrak{p}_7'' = \sigma\tau(\mathfrak{p}_7).$$

Calculamos

$$\mathfrak{p}_3^2 = \Big(\frac{1+3\sqrt{-3}}{2} + \sqrt{-5}\Big), \quad \mathfrak{p}_3'^2 = \tau(\mathfrak{p}_3^2),$$

y además

$$\mathfrak{p}_3\,\mathfrak{p}_3' = (\sqrt{-3}).$$

Afirmo que los ideales $\mathfrak{p}_3$ y $\mathfrak{p}_3'$ no son principales. Para esto bastaría ver que en $\mathcal{O}_K$ no hay elementos de norma 3. Lo haré en PARI/GP, reduciendo la norma mód 5.

```
? K = nfinit(t^2 + 3);
? L = nfinit(rnfinit(K,x^2 + 5));
? nrm = norm (Mod(L.zk*[a,b,c,d]~,L.pol))
% = ...
? test (N) = {
  for (a=0,N-1,
    for (b=0,N-1,
      for (c=0,N-1,
        for (d=0,N-1,
          if (Mod (eval(nrm), N) == Mod (3,N),
            return (1)
        )
      )
    )
  )
);
0 };

? test(5)
% = 0
```

Todo esto quiere decir que $[\mathfrak{p}_3] = [\mathfrak{p}_3']$ es un elemento de orden 2 en el grupo de clases.

Calculamos que

$$\mathfrak{p}_3\,\mathfrak{p}_7 = \Bigl(\frac{1+\sqrt{-3}}{2} + \sqrt{-5}\Bigr).$$

De manera similar,

$$\mathfrak{p}_3\,\sigma\mathfrak{p}_7 = \sigma\mathfrak{p}_3\,\sigma\mathfrak{p}_7 = \sigma(\mathfrak{p}_3\,\mathfrak{p}_7) = \Bigl(\frac{1-\sqrt{-3}}{2} + \sqrt{-5}\Bigr),$$

y

$$\mathfrak{p}_3'\,\tau\mathfrak{p}_7 = \tau(\mathfrak{p}_3\,\mathfrak{p}_7) = \Bigl(\frac{1+\sqrt{-3}}{2} - \sqrt{-5}\Bigr),$$

y en fin,

$$\mathfrak{p}_3'\,\sigma\tau\mathfrak{p}_7 = \sigma\tau(\mathfrak{p}_3\,\mathfrak{p}_7) = \Bigl(\frac{1-\sqrt{-3}}{2} - \sqrt{-5}\Bigr).$$

Estos cálculos demuestran que

$$[\mathfrak{p}_7] = [\mathfrak{p}_7'] = [\mathfrak{p}_7''] = [\mathfrak{p}_7'''] = [\mathfrak{p}_3] = [\mathfrak{p}_3'].$$

Podemos concluir que $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. □

Ejercicio 8.5. 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.

Solución. Gracias a la finitud del grupo de clases, sabemos que el ideal I^n es principal para algún $n = 1, 2, 3, \ldots$ (por ejemplo, basta tomar $n = h_K$). Tenemos $I^n = (\alpha)$ para algún $\alpha \in \mathcal{O}_K$. Ahora $\sqrt[n]{\alpha}$ es también un entero algebraico, y en la extensión $L = K(\sqrt[n]{\alpha})$ se tiene $I\mathcal{O}_L = (\sqrt[n]{\alpha})$. □

Ejercicio 8.6. 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 $M' \oplus M'' \cong M$.

Solución. Si $(e_i)_{i\in I}$ es una base de M'' como R-módulo, escojamos elementos $(m_i)_{i\in I}$ tales que $p(m_i) = e_i$. Luego $s\colon e_i \mapsto m_i$ define una sección.

En la parte 2), definamos la aplicación R-lineal

$$\phi\colon M' \oplus M'' \to M, \quad (m', m'') \mapsto i(m') + s(m'').$$

Tenemos un diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{m' \mapsto (m',0)} & M' \oplus M'' & \xrightarrow{(m',m'')\mapsto m''} & M'' & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle id} & & \big\downarrow{\scriptstyle \phi} & & \big\downarrow{\scriptstyle id} & & \\
0 & \longrightarrow & M' & \xrightarrow{\quad i \quad} & M & \xrightarrow{\quad p \quad} & M'' & \longrightarrow & 0
\end{array}$$

Por el lema del tres (o del cinco, lema de la serpiente, etc.) podemos concluir que ϕ es un isomorfismo. □