Práctica 1

Enteros algebraicos

1. Hallar *todas* las soluciones enteras de la ecuación $y^2 = x^3 - 2$.

Sobre esta ecuación: `https://www.lmfdb.org/EllipticCurve/Q/1728/o/3`.

2. Sea α una raíz de $X^3 + X^2 - 2X + 8$, y sea $K = \mathbb{Q}(\alpha)$. Sea $\beta = -\frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + 1$.

Probar que $\beta \in \mathcal{O}_K$.

3. *Un algoritmo para calcular el anillo de enteros.*

Sea K un cuerpo de números de grado n. Sea $R = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_K$ un $\mathbb{Z}$-módulo de rango n. Probar que si $R \neq \mathcal{O}_K$, entonces existen un primo p con $p^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$ y enteros $c_1, \ldots, c_n$ con $0 \le c_i < p$, no todos nulos, tales que

$$\alpha = \frac{1}{p} \sum_{i=1}^{n} c_i \alpha_i \quad \in \mathcal{O}_K.$$

4. *Para quien prefiera evitar hacer (muchas) cuentas en los ejercicios que siguen.*

Implementar el algoritmo anterior en `SAGE`.

Algunos comandos útiles:

```
sage: K.<a> = NumberField(x^3 + x^2 - 2*x + 8)
sage: K.discriminant([1,a,a^2]).factor()
-1 * 2^2 * 503
sage: b
-1/2*a^2 - 1/2*a + 1
sage: b.is_integral()
True
sage: K.discriminant([1,a,b]).factor()
-1 * 503
sage: K.ring_of_integers().basis() # ¡trampa!
[1, 1/2*a^2 + 1/2*a, a^2]
```

5. Sea $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{-1}\right)$. Probar que

$$\mathcal{O}_K = \left\langle 1, \sqrt{2}, \sqrt{-1}, \frac{1}{2}\sqrt{2}\left(1 + \sqrt{-1}\right) \right\rangle_{\mathbb{Z}}.$$

6. Hallar (una base del $\mathbb{Z}$-módulo) $\mathcal{O}_K$ para:
a) $K = \mathbb{Q}\left(\sqrt[3]{5}\right)$.
b) $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

7. Sean m, n enteros libres de cuadrados y coprimos, y sea $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

Hallar $\mathcal{O}_K$ en los casos:
a) $m, n \equiv 1 \bmod (4)$.
b) $m \equiv 1 \bmod (4),\ n \not\equiv 1 \bmod (4)$.

¿Qué se puede decir en los restantes casos?

8. Sea $K = \mathbb{Q}\left(\sqrt{7}, \sqrt{10}\right)$, y sea $\alpha \in \mathcal{O}_K$. El objetivo de este ejercicio es mostrar que $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$; esto es, que $\mathcal{O}_K$ no es *monógeno.*

a) Consideremos los enteros algebraicos

$$\begin{aligned}
\alpha_1 &= \left(1+\sqrt{7}\right)\left(1+\sqrt{10}\right),\\
\alpha_2 &= \left(1-\sqrt{7}\right)\left(1+\sqrt{10}\right),\\
\alpha_3 &= \left(1+\sqrt{7}\right)\left(1-\sqrt{10}\right),\\
\alpha_4 &= \left(1-\sqrt{7}\right)\left(1-\sqrt{10}\right).
\end{aligned}$$

i. Probar que si $i \neq j$ entonces $3 \mid \alpha_i\alpha_j$ en $\mathcal{O}_K$.

ii. Deducir que para todo $r \geq 1$

$$T_{K/\mathbb{Q}}(\alpha_i^r) \equiv \left(T_{K/\mathbb{Q}}(\alpha_i)\right)^r \mod(3).$$

iii. Probar que para todo $r \geq 1$ se tiene que $3 \nmid \alpha_i^r$ en $\mathcal{O}_K$.

b) Sea $g \in \mathbb{Z}[X]$. Probar que $3 \mid g(\alpha)$ en $\mathbb{Z}[\alpha]$ si y solo si $\overline{m_\alpha} \mid \overline{g}$ en $\mathbb{F}_3[X]$.

En adelante supongamos que $\mathcal{O}_K = \mathbb{Z}[\alpha]$. En particular, existen $f_i \in \mathbb{Z}[X]$ tales que $\alpha_i = f_i(\alpha)$.

c) Probar que $\overline{f_i} \neq \overline{f_j}$ para $i \neq j$.

d) Probar que para cada i se tiene que $\overline{m_\alpha} \in \mathbb{F}_3[X]$ tiene al menos un factor irreducible que *no* divide a $\overline{f_i}$ pero *sí* divide a $\overline{f_j}$ para $j \neq i$.

e) Concluir que $\overline{m_\alpha}$ tiene exactamente cuatro factores irreducibles distintos. *Lo cual es absurdo.*

9. Sea α una raíz de $X^3 + X^2 - 2X + 8$, y sea $K = \mathbb{Q}(\alpha)$.

a) Calcular $\Delta(1, \alpha, \alpha^2)$. *Sin hacer demasiadas cuentas.*

b) Sea $\beta = \frac{4}{\alpha}$. Probar que $\beta \in \mathcal{O}_K$.

c) Calcular $\Delta(1, \alpha, \beta)$. *Se puede aprovechar el discriminante anterior.*

d) Probar que $\mathcal{O}_K = \langle 1, \alpha, \beta\rangle_{\mathbb{Z}}$.

e) Consideremos a $\mathcal{O}_K/2\mathcal{O}_K$ como $\mathbb{F}_2$-espacio vectorial. Probar que no admite una base de la forma $\{1, t, t^2\}$.

f) Deducir que $\mathcal{O}_K$ no es monógeno.

10. *Teorema de Stickelberger.* Sea K un cuerpo de números, con $\operatorname{Hom}\left(K, \overline{K}\right) = \{\tau_1, ..., \tau_n\}$ y $\mathcal{O}_K = \langle \alpha_1, ..., \alpha_n\rangle_{\mathbb{Z}}$.

Sea $A = \left(\tau_i\left(\alpha_j\right)\right)$. Escribamos $\det(A) = P - I$, donde en P se suma sobre las permutaciones pares, y en I sobre las impares.

a) Probar que $P + I, PI$ son enteros algebraicos.

b) Probar que $P + I, PI \in \mathbb{Z}$.

Sugerencia: suponer que $K/\mathbb{Q}$ es de Galois.

c) Usando que $(P - I)^2 = (P + I)^2 - 4PI$, concluir que $\Delta_K \equiv 0, 1 \bmod(4)$.

11. Sea K un cuerpo de números, con clausura normal L.

a) Probar que $\mathbb{Q}\left(\sqrt{\Delta_K}\right) \subseteq L$.

b) Probar que si $[L:\mathbb{Q}]$ es impar, entonces Δ_K es un cuadrado en $\mathbb{Z}$. *En consonancia con el Teorema de Stickelberger.*

Unidades

12. Probar que $\mathbb{Z}\left[\sqrt{-2}\right]^\times = \{\pm 1\}$.

13. Dar infinitas soluciones enteras para las ecuaciones

$$x^2 - 8y^2 = 4, \quad x^2 - 8y^2 = -4.$$

14. Sea $K = \mathbb{Q}(\zeta)$, con $\zeta = e^{2\pi i/3}$.

a) Verificar que $N_{K/\mathbb{Q}}(x + y\zeta) = x^2 - xy + y^2$, para $x, y \in \mathbb{Q}$.

b) Probar que $\mathbb{Z}[\zeta]^\times = \{\pm 1, \pm\zeta, \pm\zeta^2\}$.

15. Sea $K = \mathbb{Q}(\zeta)$, con $\zeta = e^{2\pi i/5}$.

a) Probar $\zeta^2 + \zeta^3 \in \mathcal{O}_K^\times$.

b) Deducir que $\mathcal{O}_K^\times$ es infinito.