TEORÍA DE NÚMEROS

Practicas SAGE $\mathbf{n^o\ 3}$

Utilizando las funciones ya implementadas en `SAGE` realizar los siguiente cálculos.

(1) Para $\alpha \in \left\{\sqrt{3}, \sqrt{5}, e^{\frac{2\pi i}{23}}, \sqrt{17}+\sqrt{19}, \frac{1+\sqrt{17}}{2\sqrt{-19}}, \sqrt{1+\sqrt{2}}+\sqrt{1-\sqrt{2}}\right\}$ construir en `SAGE` el cuerpo de números $K = \mathbb{Q}(\alpha)$. Para cada uno de los cuerpos de números anteriores calcular en `SAGE`:

- **(a)** Grado de K.
- **(b)** Anillo de enteros $\mathcal{O}_K$.
- **(c)** Una base entera de K.
- **(d)** Discriminante de K.
- **(e)** Inmersiones de K en $\overline{\mathbb{Q}}$.
- **(f)** Unidades de $\mathcal{O}_K$.
- **(g)** Grupo de clase de K.
- **(h)** Número de clase de K.
- **(i)** Factorizar los ideales $< 2 >, < 3 >, < 5 >$ dentro del anillo de enteros de K.

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

- **(a)** Demostrar con `SAGE` que $\mathbb{Z}[\zeta]$ tiene un número infinito de unidades.
- **(b)** Calcular $\mathrm{N}_K(\alpha)$ y $\mathrm{Tr}_K(\alpha)$ para $\alpha = \zeta+2, \zeta-2, \zeta+3, \zeta-3, \zeta+4, \zeta^2, \zeta+\zeta^2, 1+\zeta+\zeta^2+\zeta^3+\zeta^4$.
- **(c)** Demostrar con `SAGE` que $\zeta+2, \zeta-2, \zeta+3$ son irreducibles en $\mathbb{Z}[\zeta]$.
- **(d)** Demostrar con `SAGE` que todos los divisores propios de $\zeta+4$ tienen norma 5 ó 41, y, sabiendo que $\zeta-1$ es un factor de $\zeta+4$, encontrar en `SAGE` otro.

(3) Excluyendo el intercambio de números, demostrar con `SAGE` que 1729 es el menor entero positivo que se puede escribir como suma de dos cubos positivos de dos maneras distintas. ¿Cuál es el menor entero positivo que se puede escribir como suma de potencias n-ésimas positivos para $n = 2, 4, 5, 6, 7, 8, 9, 10$?

(4) Sea $\zeta_p = e^{2\pi i/p}$, p primo impar. Demostrar heurísticamente (para unos cuantos primos p) usando `SAGE` que $\mathbb{Z}[\zeta_p]$ contiene a $\sqrt{p}$ si $p \equiv 1 \pmod 4$, y contiene a $\sqrt{-p}$ si $p \equiv 3 \pmod 4$. Expresar $\sqrt{-3}$ y $\sqrt{5}$ como polinomios en el correspondiente ζ_p.

(5) Utilizar las siguientes igualdades para demostrar con `SAGE` que los anillos de enteros de los correspondientes cuerpos cuadráticos no son D.F.U.:

- **(a)** $\mathbb{Q}(\sqrt{-5}) \quad : \quad 6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$
- **(b)** $\mathbb{Q}(\sqrt{-6}) \quad : \quad 6 = 2\cdot 3 = \sqrt{-6}\sqrt{-6},$
- **(c)** $\mathbb{Q}(\sqrt{-10}) \quad : \quad 14 = 2\cdot 7 = (2+\sqrt{-10})(2-\sqrt{-10}),$
- **(d)** $\mathbb{Q}(\sqrt{-13}) \quad : \quad 14 = 2\cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13}),$
- **(e)** $\mathbb{Q}(\sqrt{-14}) \quad : \quad 15 = 3\cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14}),$
- **(f)** $\mathbb{Q}(\sqrt{-15}) \quad : \quad 4 = 2\cdot 2 = \left(\frac{1+\sqrt{-15}}{2}\right)\left(\frac{1-\sqrt{-15}}{2}\right),$
- **(g)** $\mathbb{Q}(\sqrt{-17}) \quad : \quad 18 = 2\cdot 3\cdot 3 = (1+\sqrt{-17})(1-\sqrt{-17}),$
- **(h)** $\mathbb{Q}(\sqrt{-21}) \quad : \quad 22 = 2\cdot 11 = (1+\sqrt{-21})(1-\sqrt{-21}).$

(6) Sea $K = \mathbb{Q}(\sqrt{-5})$ y $\mathcal{O} = \mathcal{O}_K$. Definimos los ideales

$$\mathfrak{p} =< 2, 1+\sqrt{-5} >, \qquad \mathfrak{q} =< 3, 1+\sqrt{-5} >, \qquad \mathfrak{r} =< 3, 1-\sqrt{-5} > .$$

- **(a)** Demostrar con `SAGE` que son ideales primos.
- **(b)** Demostrar con `SAGE`

$$\mathfrak{p}^2 =< 2 >, \quad \mathfrak{q}\cdot\mathfrak{r} =< 3 >, \quad \mathfrak{p}\cdot\mathfrak{q} =< 1+\sqrt{-5} >, \quad \mathfrak{p}\cdot\mathfrak{r} =< 1-\sqrt{-5} >, \quad \mathfrak{p}^2\mathfrak{q}\cdot\mathfrak{r} =< 6 > .$$

- **(c)** Calcular en `SAGE` las normas de los ideales $\mathfrak{p}, \mathfrak{q}$ y $\mathfrak{r}$.
- **(d)** Demostrar con `SAGE` que $\mathfrak{p}, \mathfrak{q}$ y $\mathfrak{r}$ no son principales.
- **(e)** Demostrar con `SAGE` que los ideales $< 2 >$ y $< 3 >$ están generados por elementos irreducibles pero que los ideales no son primos.
- **(f)** Encontrar en `SAGE` todos los ideales de $\mathcal{O}$ que contienen el elemento 6.
- **(g)** Demostrar en `SAGE` que en el grupo de clase $\mathcal{H}_K$ se tiene:

$$[\mathfrak{p}]^2 = [\mathcal{O}], \quad [\mathfrak{p}][\mathfrak{q}] = [\mathcal{O}], \quad [\mathfrak{p}][\mathfrak{r}] = [\mathcal{O}].$$

- **(h)** Demostrar en `SAGE` que el grupo de clase $\mathcal{H}_K$ $\mathfrak{p}, \mathfrak{q}$ y $\mathfrak{r}$ son equivalentes.

(8) Encontrar en `SAGE` todos los ideales de $\mathbb{Z}[\sqrt{2}]$ con norma 18.

(9) Sea $K = \mathbb{Q}(\sqrt{-29})$, $\mathcal{O} = \mathcal{O}_K$ y $\mathfrak{p} =< 2, 1+\sqrt{-29} >\subset \mathcal{O}$.

- **(a)** Demostrar en `SAGE` que $1-\sqrt{-29}, 30 \in \mathfrak{p}$ y que $30 \in \mathfrak{p}^2$.
- **(b)** Calcular en `SAGE` la descomposición en ideales primos de los ideales $< 2 >, < 3 >$, $< 5 >$, $< 1+\sqrt{-29} >$ y $< 1+\sqrt{-29} >$. Deducir la descomposición del ideal $< 30 >$.
- **(c)** Calcular en `SAGE` todos los ideales de $\mathcal{O}$ conteniendo al elemento 30.

(10) Crear una función en `SAGE` que haga lo siguiente:
INPUT: d entero libre de cuadrados.
OUPUT: $(\mathcal{H}_{\mathbb{Q}(\sqrt{d})}, h_{\mathbb{Q}(\sqrt{d})})$.
$-$ Crear una tabla en la que en la primera columna aparezca d, en la segunda la estructura de $\mathcal{H}_{\mathbb{Q}(\sqrt{d})}$ y en la tercera $h_{\mathbb{Q}(\sqrt{d})}$, para $|d| < 100$.