Introducción a los Números Algebraicos
Lista de ejercicios final - entrega 28/6

Instrucciones. Justificar todas las respuestas. *No está permitido discutir los problemas con nadie.* Se puede usar material como libros, notas de curso, páginas web, dando referencias precisas a cualquier resultado que se use. Se puede usar una computadora, en cuyo caso tiene que quedar claro qué programa se usa, y qué cuentas hace la computadora.

Calificación. Hay que entregar *exactamente* 3 problemas de los 5. Todos los problemas valen lo mismo. El puntaje obtenido se considerará como nota de práctico.

Entrega. La fecha límite para la entrega es el jueves 28 de junio *sin excepciones.*

Página del curso. `http://www.cmat.edu.uy/~tornaria/2007/TNA/`

F1. Sea $F(X) \in \mathbb{Z}[X]$ mónico irreducible, sea $K = \mathbb{Q}[\alpha]$ con $F(\alpha) = 0$, y supongamos que $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(a) Sea $\mathfrak{p}$ un ideal primo de grado 1 en $\mathcal{O}_K$. Mostrar que $\mathfrak{p} = (p, m-\alpha)$ donde $\mathfrak{p} \mid p$, y m es un entero racional tal que $\alpha \equiv m \pmod{\mathfrak{p}}$.

(b) Mostrar que para $m \in \mathbb{Z}$ se tiene $F(m) = N_K(m - \alpha)$.

(c) Mostrar que si $m \in \mathbb{Z}$ y $F(m) = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ es la factorización de $F(m)$ entonces

$$(m - \alpha) = \prod_i (p_i, m - \alpha)^{a_i}$$

es la factorización de $(m - \alpha)$.

De aquí en más sea α una raíz de $F(X) = X^2 + X + 6$.

(d) Mostrar que $\mathbb{Z}[\alpha]$ es el anillo de enteros en $\mathbb{Q}[\sqrt{-23}]$, y ver que $(2) = \mathfrak{p}\mathfrak{p}'$, donde $\mathfrak{p} = (2, 1 - \alpha)$ y $\mathfrak{p}' = (2, \alpha)$.

(e) Mostrar que no hay elementos de norma 2 en $\mathbb{Z}[\alpha]$, y concluir que $\mathfrak{p}$ no es principal.

(f) Usar $F(1) = 2^3$ y las ideas del ejercicio anterior para mostrar que $\mathfrak{p}^3$ es principal.

F2. Determinar la unidad fundamental en $\mathbb{Q}[\sqrt{m}]$ para $2 \le m \le 30$ libre de cuadrados, con excepción de $m = 19, 22$ (en estos dos casos las unidades fundamentales son $170 + 39\sqrt{19}$ y $197 + 42\sqrt{22}$ respectivamente). ¿Cuál es la solución fundamental de la ecuación de Pell $x^2 - 28y^2 = 1$? (Sugerencia: usar la solución fundamental de $x^2 - 7y^2 = 1$.)

F3. Sea $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ con m y n enteros distintos libres de cuadrados, $m \neq 1$, $n \neq 1$. Un tal K se llama *cuerpo bicuadrático*. Observar que K contiene también $\mathbb{Q}[\sqrt{k}]$, donde $k = mn/\operatorname{mcd}(m,n)^2$.

(a) Si $\alpha \in K$, mostrar que $\alpha \in \mathcal{O}_K$ sii las normas y trazas relativas $N^K_{\mathbb{Q}[\sqrt{m}]}$ y $T^K_{\mathbb{Q}[\sqrt{m}]}$ son enteros algebraicos.

(b) Suponer $m \equiv 3, n \equiv k \equiv 2 \pmod 4$. Mostrar que todo $\alpha \in \mathcal{O}_K$ puede escribirse como

$$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2},$$

con $a, b, c, d \in \mathbb{Z}$. (Sugerencia: escribir α como combinación lineal de 1, $\sqrt{m}$, $\sqrt{n}$, $\sqrt{k}$, y considerar las tres trazas relativas). Mostrar que a y b deben ser pares y que $c \equiv d \pmod 2$ considerando $N^K_{\mathbb{Q}[\sqrt{m}]}(\alpha)$. Concluir que

$$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}\right\}$$

es una base entera de $\mathcal{O}_K$, y calcular $\Delta(\mathcal{O}_K)$.

(c) Suponer $m \equiv 1, n \equiv k \equiv 2 \pmod 4$. Mostrar que nuevamente todo $\alpha \in \mathcal{O}_K$ puede escribirse como

$$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2},$$

con $a, b, c, d \in \mathbb{Z}$. Mostrar que $a \equiv b \pmod 2$ y que $c \equiv d \pmod 2$ Concluir que

$$\left\{1, \frac{1 + \sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{k}}{2}\right\}$$

es una base entera de $\mathcal{O}_K$, y calcular $\Delta(\mathcal{O}_K)$.

F4. Sea $F(X) \in \mathbb{Z}[X]$ un polinomio mónico irreducible de grado 5.

(a) Para cada uno de los cinco posibles grupos de Galois, calcular la densidad del conjunto $P(F, i)$ de primos racionales p tales que F tiene exactamente i raíces módulo p. Hacer una tabla con los resultados.

(b) Se consideran los polinomios quínticos $A(X) = X^5 - X^3 - 2X^2 - 2X - 1$, $B(X) = X^5 - X + 3$, $C(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$, $D(X) = X^5 - 5$, $E(X) = X^5 + 10X^3 - 10X^2 + 35X - 18$. Todos son irreducibles, y sus discriminantes son $\Delta_A = 47^2$, $\Delta_B = 252869$ (primo), $\Delta_C = 11^4$, $\Delta_D = 5^9$, $\Delta_E = 2^6 \cdot 5^8 \cdot 11^2$.

La tabla siguiente muestra para cada uno de los polinomios, la cantidad de primos p entre los primeros 1000 según el número de sus raíces módulo p.

raíces	0	1	2	3	5
A	399	510	0	1	90
B	366	386	174	68	6
C	799	1	0	0	200
D	201	755	0	0	44
E	410	251	326	0	13

Con esta información, y el resultado de la parte (a) hacer una conjetura sobre los grupos de Galois de cada uno de los polinomios.

F5. Sea m un entero negativo libre de cuadrados.

(a) Mostrar que el anillo de enteros en $\mathbb{Q}[\sqrt{m}]$ es principal cuando

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Supongamos ahora que el anillo de enteros en $\mathbb{Q}[\sqrt{m}]$ es principal.

(b) Mostrar que $m \equiv 5 \pmod 8$ excepto cuando $m = -1, -2, -7$. (Sugerencia: considerar un primo arriba de 2).

(c) Si p es un primo impar tal que $4p < |m|$, entonces m es no residuo cuadrático módulo p.

(d) Concluir que si $m < -19$, entonces m es congruente a alguno de

$$-43, -67, -163, -403, -547, -667$$

módulo 840.

(e) Mostrar que los valores de m dados en la parte (a) son los únicos con $0 > m > -1000$ para los cuales el anillo de enteros en $\mathbb{Q}[\sqrt{m}]$ es principal.

Es un teorema (difícil) de Heegner, Stark, Baker que los m dados en la parte (a) son todos los enteros negativos para los cuales el anillo de enteros en $\mathbb{Q}[\sqrt{m}]$ es principal