Introducción a los Números Algebraicos
Lista 3 - entrega 26/4

35. (2p.) Sea $K = \mathbb{Q}[\sqrt{m}]$. Mostrar que dado $M > 0$ hay un número finito de enteros $\alpha \in \mathcal{O}_K$ tales que $\max(|\alpha|, |\alpha'|) \leq N$. (Sugerencia: considerar el polinomio minimal.)

36. Una forma (constructiva) de mostrar la existencia de soluciones de la ecuación de Pell es mediante el uso de fracciones continuas (ver ejercicio 5.8 del curso de TN de 2006). Veremos aquí otra forma utilizando el siguiente lema de aproximación diofántica debido a Dirichlet (que también puede demostrarse utilizando fracciones continuas, o directamente utilizando el principio del palomar de Dirichlet):

    Lema. Si $\xi \in \mathbb{R}$ es irracional, existen infinitos números racionales x/y con $\mathrm{mcd}(x, y) = 1$ tal que $|x/y - \xi| < 1/y^2$.

    (a) Mostrar que dado $n > 0$ entero existe una constante $M > 0$ tal que $\left|x^2 - ny^2\right| < M$ tiene infinitas soluciones racionales. (Sugerencia: aproximar $\sqrt{n}$ por infinitos racionales x/y, mostrando que para tales aproximaciones $\left|x^2 - ny^2\right|$ está acotado).

    (b) Concluir que existe un entero $m \in \mathbb{Z}$ y pares de enteros (x_1, y_1) y (x_2, y_2) tales que $x_i^2 - ny_i^2 = m$, con $x_1 \neq x_2$, $x_1 \equiv x_2 \pmod{|m|}$, $y_1 \equiv y_2 \pmod{|m|}$.

    (c) Mostrar que $(x_1 + y_1\sqrt{n})/(x_2 + y_2\sqrt{n}) = (x + y\sqrt{n})$ con $x, y \in \mathbb{Z}$, $y \neq 0$, concluyendo que existe una solución no trivial en $\mathbb{Z}$ a la ecuación de Pell $x^2 - ny^2 = 1$.

37. Demostrar el lema de aproximación diofántica del ejercicio anterior usando el principio del palomar de Dirichlet. Recordar que la *parte fracional* de un real x es $x - [x] \in [0, 1)$.

    (a) Sea $n > 0$ un entero arbitrario. Mostrar que entre las partes fracionales de los números $0, \xi, 2\xi, \ldots, n\xi$ hay al menos dos que caen en el mismo intervalo en la partición de $[0, 1)$ dada por

    $$[0, 1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \cdots \cup \left[\frac{n-1}{n}, 1\right).$$

    (b) Concluir que existen $x, y \in \mathbb{Z}$ con $0 < y < n$ tales que $|x/y - \xi| < 1/ny < 1/y^2$.

    (c) Usar que $x/y \neq \xi$ (pues ξ es irracional) para construir una sucesión infinita de aproximaciones diofánticas, y terminar de probar el lema.

38. Sea m un entero libre de cuadrados.

    (a) Asumir $m \equiv 2, 3 \pmod 4$. Sea $y > 0$ el menor entero positivo tal que $my^2 \pm 1$ es un cuadrado, digamos x^2, con $x > 0$. Entonces $x + y\sqrt{m}$ es una unidad en $\mathbb{Z}[\sqrt{m}]$. Probar que es la unidad fundamental.

    (b) Establecer un procedimiento similar para el caso en que $m \equiv 1 \pmod 4$. (Sugerencia: $my^2 \pm 4$.)

39. (2p.) Determinar la unidad fundamental en $\mathbb{Q}[\sqrt{m}]$ para $2 \leq m \leq 30$ 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 $x^2 - 7y^2 = 1$.)

40. Sean K y L dos cuerpos de números de grado m y n, respectivamente, y supongamos que KL tiene grado mn.

    (a) Mostrar que $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL}$.

    (b) Sea $d = \mathrm{mcd}(\Delta(\mathcal{O}_K), \Delta(\mathcal{O}_L))$. Entonces $\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.

41. El anillo de enteros de $\mathbb{Q}[\sqrt{3}]$ es $\mathbb{Z}[\sqrt{3}]$ ($\Delta = 12$) y el de $\mathbb{Q}[\sqrt{7}]$ es $\mathbb{Z}[\sqrt{7}]$ ($\Delta = 28$).

    (a) ¿Qué puede decirse a priori sobre el anillo de enteros del cuerpo compuesto $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$?

    (b) Considerar $\frac{\sqrt{3}+\sqrt{7}}{2}$ y volver a contestar la parte (a). (Puede ser importante conocer algo sobre la descomposición del 2.)

42. Sea $\zeta_m = e^{\frac{2\pi i}{m}}$, con $m \geq 3$. Como ζ_m es una unidad, se tiene $N(\zeta_m) = \pm 1$. Probar que el signo es $+$.

43. Sea $\zeta_m = e^{\frac{2\pi i}{m}}$, con m entero positivo.

    (a) Mostrar que $1 + \zeta_m + \zeta_m^2 + \cdots + \zeta_m^{k-1}$ es una unidad en $\mathbb{Z}[\zeta_m]$ siempre que k sea relativamente primo con m.

    (b) Sea $m = p^r$, con p primo. Mostrar que $p = u(1 - \zeta_m)^n$, donde $n = \varphi(p^r)$ y u es una unidad en $\mathbb{Z}[\zeta_m]$.

44. Sea $\theta = \zeta_m + \zeta_m^{-1}$ donde $\zeta_m = e^{\frac{2\pi i}{m}}$, con $m \geq 3$.

    (a) Mostrar que $\mathbb{Q}[\zeta_m]/\mathbb{Q}[\theta]$ es una extensión de cuerpos de grado 2, que $\mathbb{Q}[\theta] \subseteq \mathbb{R}$, y que $\mathbb{Q}[\theta]$ es el cuerpo fijo por la conjugación compleja. Concluir que el anillo de enteros de $\mathbb{Q}[\theta]$ es $\mathbb{R} \cap \mathbb{Z}[\zeta_m]$.

    (b) Mostrar que $\{1, \zeta_m, \theta, \theta\zeta_m, \theta^2, \theta^2\zeta_m, \ldots, \theta^{n-1}, \theta^{n-1}\zeta_m\}$, con $n = \varphi(m)/2$, es una base entera de $\mathbb{Z}[\zeta_m]$. Concluir que el anillo de enteros de $\mathbb{Q}[\theta]$ es $\mathbb{Z}[\theta]$.

    (c) Si $m = p$, puede probarse que $\Delta(\theta) = \pm p^{(p-3)/2}$. Mostrar que de hecho el signo debe ser $+$. (Sugerencia: ver que $\sqrt{\Delta(\theta)} \in \mathbb{Z}[\theta]$)

45. 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 $k = mn/\,\mathrm{mcd}(m,n)^2$.

    (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).

    (c) 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 $\Delta(\mathcal{O}_K)$.

46. (2p.) Supongamos que $K/\mathbb{Q}$ es una extensión normal con grupo de Galois simple pero no cíclico. Mostrar que no hay ningún primo racional p que siga siendo primo en K.