Introducción a los Números Algebraicos
Lista 2 - entrega 24/3

19. Sea $\omega = e^{\frac{2\pi i}{p}}$ con p primo impar, y sea $f(X) = 1 + X + X^2 + \ldots + X^{p-1}$ su polinomio minimal.

    (a) Mostrar que $f'(\omega) = \frac{p}{\omega(\omega-1)}$.

    (b) Calcular $N(f'(\omega))$ y concluir que $\Delta(\omega) = \pm p^{p-2}$ donde el signo es $+$ si $p \equiv 1 \pmod 4$ y $-$ si $p \equiv 3 \pmod 4$.

20. Sea $\omega = e^{\frac{2\pi i}{p}}$ con p primo impar.

    (a) Mostrar que $\mathbb{Q}[\omega]$ contiene a $\sqrt{p}$ si $p \equiv 1 \pmod 4$ y a $\sqrt{-p}$ si $p \equiv 3 \pmod 4$. (Sugerencia: usar la fórmula para $\Delta(\omega)$ del ejercicio anterior). Expresar $\sqrt{-3}$ y $\sqrt{5}$ como polinomios en ω correspondiente.

    (b) Mostrar que el octavo cuerpo ciclotómico contiene $\sqrt{2}$.

    (c) Mostrar que todo cuerpo cuadrático está contenido en algún cuerpo ciclotómico. En efecto, $K = \mathbb{Q}[\sqrt{m}]$ está contenido en el d-ésimo cuerpo ciclotómico, donde $d = \Delta(\mathcal{O}_K)$. (Más generalmente, el Teorema de Kronecker-Weber muestra que cualquier extensión abeliana de $\mathbb{Q}$ — normal con grupo de Galois abeliano — está contenida en un cuerpo ciclotómico.)

21. (a) Mostrar, usando la norma, que $9 + \sqrt{10}$ es irreducible en $\mathbb{Z}[\sqrt{10}]$.

    (b) Mostrar, usando la traza, que $\sqrt{3} \notin \mathbb{Q}[\sqrt[4]{2}]$.

22. (2p.) Otra forma de definir traza y norma es la siguiente. Sea K un cuerpo de números y sea $\alpha \in K$. La multiplicación por α es una transformación $\mathbb{Q}$-lineal de K en K. Mostrar que $T_K(\alpha)$ y $N_K(\alpha)$ son, respectivamente, la traza y el determinante de dicha transforamción lineal.

23. Sea K un cuerpo de números de grado n sobre $\mathbb{Q}$, y sean $\alpha_1, \ldots, \alpha_n \in K$ enteros algebraicos. Mostraremos que $d = \Delta(\alpha_1, \ldots, \alpha_n) \equiv 0, 1 \pmod 4$ (criterio de Stickelberger).

    (a) El determinante de $(\sigma_i(\alpha_j))$ es suma de $n!$ términos, uno para cada permutación de $\{1, \ldots, n\}$. Sea P la suma de los términos correspondientes a permutaciones pares, y sea N la suma de los términos correspondientes a permutaciones impares. Mostrar que
    $$d = (P + N)^2 - 4PN.$$

    (b) Mostrar que $P + N$ y PN están en $\mathbb{Z}$ y concluir la demostración.

24. (2p.) Mostrar que para cualquier número algebraico α, existe $m \in \mathbb{Z}$, $m \neq 0$ tal que $m\alpha$ es un entero algebraico. (Sugerencia: usar una potencia del coeficiente principal de $f \in \mathbb{Z}[X]$ que anule α).

25. (2p.) Sean $a_0, a_1, \ldots, a_{n-1}$ enteros algebraicos, y sea $\alpha \in \mathbb{C}$ tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Mostrar que $\mathbb{Z}[a_0, \ldots, a_{n-1}, \alpha]$ es finitamente generado, y concluir que α es un entero algebraico.

26. Sea $R = \mathbb{Z}[\sqrt{-5}]$.

(a) Mostrar que

$$(2) = (2, 1 + \sqrt{-5})^2,$$
$$(3) = (3, 1 + \sqrt{-5})\,(3, 1 - \sqrt{-5}).$$

(b) Probar que todos los ideales que aparecen a la derecha son primos. Sugerencia: observar que $R/(2)$ tiene 4 elementos; ¿qué estructura tiene $R/(2, 1 + \sqrt{-5})$?

27. Sea $R = \mathbb{Z}[\alpha]$ con $\alpha = \sqrt[3]{2}$.

(a) Verificar que $(5) = (5, \alpha + 2)\,(5, \alpha^2 + 3\alpha - 1)$

(b) Mostrar que existe un isomorfismo de anillos

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \to (\mathbb{Z}/5)[x]/(x^2 + 3x - 1),$$

y un homomorfismo sobreyectivo

$$\mathbb{Z}[x]/(5, x^2 + 3x - 1) \to R/(x^2 + 3x - 1).$$

(c) Concluir que $R/(5, \alpha^2+3\alpha-1)$ es un cuerpo de 25 elementos o $R = (5, \alpha^2+3\alpha-1)$. Usar la parte (a) para ver que $R \neq (5, \alpha^2 + 3\alpha - 1)$.

28. Sea $R = \mathbb{Z}[\alpha]$ con $\alpha^3 = \alpha + 1$.

(a) Verificar que $(23) = (23, \alpha - 10)^2\,(23, \alpha - 3)$.

(b) Mostrar que $(23, \alpha - 10, \alpha - 3) = R$, y concluir que $(23, \alpha - 10)$ y $(23, \alpha - 3)$ son ideales relativamente primos entre sí.

29. Sea $K = \mathbb{Q}[\sqrt{m}]$, con m libre de cuadrados, y sea p un primo en $\mathbb{Z}$. Verificar que las siguientes son factorizaciones en ideales primos de (p):

(a) Si $p \mid m$, entonces $(p) = (p, \sqrt{m})^2$.

(b) Si m es impar, entonces

$$(2) = \begin{cases} (2, 1 + \sqrt{m})^2 & \text{si } m \equiv 3 \pmod 4, \\ (2, \frac{1+\sqrt{m}}{2})\,(2, \frac{1-\sqrt{m}}{2}) & \text{si } m \equiv 1 \pmod 8, \\ \text{primo} & \text{si } m \equiv 5 \pmod 8. \end{cases}$$

(c) Si p es impar, $p \nmid m$, entonces

$$(p) = \begin{cases} (p, n + \sqrt{m})\,(p, n - \sqrt{m}) & \text{si } m \equiv n^2 \pmod p, \\ \text{primo} & \text{si } m \text{ no es un cuadrado módulo } p. \end{cases}$$

30. Los polinomios $F(X) = X^3+10X+1$ y $G(X) = X^3-8X+15$ tienen ambos discriminante -4027, primo, y son ambos irreducibles (pues no tienen raíces racionales). Consideremos $K = \mathbb{Q}[\alpha]$ y $L = \mathbb{Q}[\beta]$ con $F(\alpha) = 0$ y $G(\beta) = 0$.

    (a) Explicar por qué $\mathcal{O}_K = \mathbb{Z}[\alpha]$ y $\mathcal{O}_L = \mathbb{Z}[\beta]$.

    (b) Determinar la factorización de 2, 17, 4027 en ideales primos de $\mathcal{O}_K$ y de $\mathcal{O}_L$.

    (c) ¿Son K y L isomorfos?

31. Sea $F(X) = X^3 - X^2 - 2X - 8$. Observar que $F(X)$ es irreducible en $\mathbb{Q}[X]$ (no tiene raíces racionales). Sea $K = \mathbb{Q}[\alpha]$ con $F(\alpha) = 0$, y sea $\beta = (\alpha^2 - \alpha)/2$. Entonces β es raíz de $G(X) = X^3-2X^2+3X-10$ así que es un entero algebraico. Los dos polinomios $F(X)$ y $G(X)$ tienen el mismo discriminante $-2012 = -4 \cdot 503$ (con 503 primo).

    (a) Mostrar que $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta$ y verificar la tabla de multiplicar

    $$\alpha^2 = \alpha + 2\beta, \qquad \alpha\beta = \alpha + 4, \qquad \beta^2 = -2 + 2\alpha + \beta.$$

    (b) Mostrar que $(2) = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ donde $\mathfrak{p}$, $\mathfrak{p}'$ y $\mathfrak{p}''$ son ideales primos de $\mathcal{O}_K$ tales que

    $$(\alpha, \beta) \equiv (0, 0) \pmod{\mathfrak{p}}, \quad (\alpha, \beta) \equiv (0, 1) \pmod{\mathfrak{p}'}, \quad (\alpha, \beta) \equiv (1, 1) \pmod{\mathfrak{p}''}.$$

    (c) Mostrar que no existe ningún $\gamma \in \mathcal{O}_K$ tal que $\mathcal{O}_K = \mathbb{Z}[\gamma]$ (¿cómo podría factorizar $2\mathcal{O}_K$ en $\mathbb{Z}[\gamma]$?)

32. 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 $(m - \alpha)$.

33. Sea α una raíz de $F(X) = X^2 + X + 6$.

    (a) 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 $\mathfrak{p}' = (2, \alpha)$.

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

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

34. Hacer una conjetura sobre la estadística de cómo se descomponen los primos racionales en el cuerpo cúbico K del problema 30. En la tabla siguiente (calculada con `gp`), la línea `[`m`,[`a`,`b`,`c`]]` indica que de todos los primos menores que $1000m$, la fracción de ellos que son inertes es a, la fracción que descompone como producto de dos primos es b y la fracción que descompone totalmente (producto de tres primos) es c.

```
? n=vector(3,j,0.);for(m=1,40,forprime(p=m*1000-1000,m*1000,\
    n[matsize(factormod(X^3+10*X+1,p,1))[1]]++);print([m,n/(n[1]+n[2]+n[3])]))

   [1, [0.38690476, 0.48214286, 0.13095238]]
   [2, [0.35643564, 0.48844884, 0.15511551]]
   [3, [0.34883721, 0.49069767, 0.16046512]]
   [4, [0.34181818, 0.49454545, 0.16363636]]
   [5, [0.33931241, 0.49476831, 0.16591928]]
   [6, [0.34099617, 0.49553001, 0.16347382]]
   [7, [0.33222222, 0.51000000, 0.15777778]]
   [8, [0.33167825, 0.51142006, 0.15690169]]
   [9, [0.33124440, 0.51029543, 0.15846016]]
   [10, [0.32872254, 0.50772986, 0.16354760]]
   [11, [0.32958801, 0.50262172, 0.16779026]]
   [12, [0.32892907, 0.50347705, 0.16759388]]
   [13, [0.32967033, 0.50355527, 0.16677440]]
   [14, [0.33777240, 0.49757869, 0.16464891]]
   [15, [0.33352338, 0.50114025, 0.16533637]]
   [16, [0.33243824, 0.50375940, 0.16380236]]
   [17, [0.33061224, 0.50510204, 0.16428571]]
   [18, [0.33187984, 0.50339147, 0.16472868]]
   [19, [0.33039852, 0.50278035, 0.16682113]]
   [20, [0.33244916, 0.50265252, 0.16489832]]
   [21, [0.33135593, 0.50466102, 0.16398305]]
   [22, [0.33116883, 0.50365260, 0.16517857]]
   [23, [0.32917317, 0.50507020, 0.16575663]]
   [24, [0.32946027, 0.50524738, 0.16529235]]
   [25, [0.32910934, 0.50615496, 0.16473570]]
   [26, [0.32972028, 0.50419580, 0.16608392]]
   [27, [0.33130699, 0.50422155, 0.16447146]]
   [28, [0.33224223, 0.50114566, 0.16661211]]
   [29, [0.33523628, 0.49730415, 0.16745956]]
   [30, [0.33436055, 0.49892142, 0.16671803]]
   [31, [0.33502994, 0.49850299, 0.16646707]]
   [32, [0.33595571, 0.49825175, 0.16579254]]
   [33, [0.33436970, 0.49886942, 0.16676088]]
   [34, [0.33397471, 0.49890049, 0.16712479]]
   [35, [0.33413719, 0.49785638, 0.16800643]]
   [36, [0.33525105, 0.49764644, 0.16710251]]
   [37, [0.33545756, 0.49757838, 0.16696406]]
   [38, [0.33656958, 0.49639034, 0.16704008]]
   [39, [0.33625517, 0.49817385, 0.16557098]]
   [40, [0.33404711, 0.50011896, 0.16583393]]
```