Teoría de números algebraicos
Tarea 4

Alexey Beshenov (alexey.beshenov@cimat.mx)

15 de septiembre de 2020

Fecha límite: viernes, 25 de septiembre.

Ejercicio 4.1. Encuentre la fórmula para el discriminante del polinomio

$$x^n + ax + b.$$

Solución. Este cálculo es bien conocido, pero espero que no hayan *googleado* la respuesta inmediatamente :–) Daré una prueba que tiene sentido en el contexto de nuestra clase. Hemos visto la fórmula

$$\Delta(f) = (-1)^{\binom{n}{2}} \operatorname{Res}(f, f') = (-1)^{\binom{n}{2}} \prod_{1\le i\le n} f'(\alpha_i),$$

donde $\alpha_1, \ldots, \alpha_n$ son las raíces de f. En nuestro caso $f = x^n + ax + b$ y su derivada es $f' = nx^{n-1} + a$. Para una raíz α de f calculamos

$$\alpha f'(\alpha) = n\,\alpha^n + a\,\alpha = n\,(-a\alpha - b) + a\,\alpha = -nb - (n-1)\,a\,\alpha.$$

Entonces,

$$\frac{\alpha}{(n-1)\,a}\,f'(\alpha) = -\frac{nb}{(n-1)\,a} - \alpha.$$

Ahora

$$\prod_i f'(\alpha_i) = \frac{(n-1)^n\,a^n}{\prod_i \alpha} \prod_i \left(-\frac{nb}{(n-1)\,a} - \alpha_i\right) = \frac{(n-1)^n\,a^n}{(-1)^n b}\,f\left(-\frac{nb}{(n-1)\,a}\right).$$

Calculamos que

$$f\left(-\frac{nb}{(n-1)\,a}\right) = (-1)^n\,\frac{n^n\,b^n}{(n-1)^n\,a^n} - \frac{nb}{(n-1)} + b.$$

De aquí

$$\prod_i f'(\alpha_i) = n^n\,b^{n-1} - (-1)^n\,(n-1)^{n-1}\,a^n.$$

Entonces, podemos escribir la fórmula del discriminante como

$$\Delta(f) = (-1)^{\binom{n}{2}}\,((-1)^{n+1}\,(n-1)^{n-1}\,a^n + n^n\,b^{n-1}).$$

Técnicamente hablando, en algún momento hemos ocupado la división por α_i y por a, asumiendo de manera implícita que $a, b \neq 0$. Sin embargo, de todos modos, el resultante puede ser escrito como el determinante de alguna matriz formada por los coeficientes de f y f', y entonces este es un polinomio en los coeficientes de f. Como consecuencia, si nuestra fórmula es válida para $a, b \neq 0$, esta debe ser válida para $a = 0$ o $b = 0$. (Les doy esta justificación tramposa para no considerar diferentes casos por separado :–) □

Ejercicio 4.2. Sea $K/\mathbb{Q}$ un campo de números y $\alpha \in \mathcal{O}_K$ un elemento entero tal que $\alpha \notin m\mathcal{O}_K$ para $m > 1$. Demuestre que en este caso existe una base de $\mathcal{O}_K$ sobre $\mathbb{Z}$ que contiene α. En particular, demuestre que $\mathcal{O}_K$ siempre admite una base que contiene 1.

Solución. Esta pregunta es sobre álgebra lineal. Dado que $\mathcal{O}_K \cong \mathbb{Z}^n$, estamos simplemente afirmando que si $\vec{a} = (a_1, \ldots, a_n)$ es un vector que cumple la condición $\operatorname{mcd}(a_1, \ldots, a_n) = 1$, entonces $\vec{a}$ está contenido en alguna base de $\mathbb{Z}^n$. Esto equivale a decir que existe una matriz entera invertible de $n \times n$ que contiene el vector $\vec{a}$ como una de sus columnas (o filas). Está claro que esto es imposible si $a_1, \ldots, a_n$ no son coprimos: el determinante de la matriz será divisible por $d = \operatorname{mcd}(a_1, \ldots, a_n)$. Para $n = 2$ la afirmación está clara:

$$\operatorname{mcd}(a_1, a_2) = 1 \iff \det \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} = \pm 1 \text{ para algunos } b_1, b_2 \in \mathbb{Z}.$$

Se puede dar una prueba por inducción que a partir de $\vec{a}$ construye una matriz en $\mathrm{GL}_n(\mathbb{Z})$ que contiene $\vec{a}$. A saber, si $\operatorname{mcd}(a_1, \ldots, a_n) = 1$, consideremos los números $\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}$, donde $d = \operatorname{mcd}(a_1, \ldots, a_{n-1})$. En este caso por la hipótesis de inducción habrá una matriz de determinante ± 1

$$\begin{pmatrix} a_1/d & b_{11} & \cdots & b_{1,n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1}/d & b_{n-1,1} & \cdots & b_{n-1,n-2} \end{pmatrix}.$$

Ahora $\operatorname{mcd}(a_1, \ldots, a_n) = \operatorname{mcd}(d, a_n) = 1$, así que se tiene $xd + ya_n = 1$ para algunos $x, y \in \mathbb{Z}$. Se puede verificar que

$$\det \begin{pmatrix} a_1 & b_{11} & \cdots & b_{1,n-2} & y\,a_1/d \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & b_{n-1,1} & \cdots & b_{n-1,n-2} & y\,a_{n-1}/d \\ a_n & 0 & \cdots & 0 & x \end{pmatrix} = \pm 1.$$

(Despeje el determinante respecto a la última fila.)

Propongo ver un argumento un poco distinto y más natural.

Consideremos el cociente de $\mathbb{Z}$-módulos $M = \mathbb{Z}^n/\mathbb{Z}\vec{a}$. Afirmamos que este es un $\mathbb{Z}$-módulo libre (de rango $n-1$). Dado que M es un grupo abeliano finitamente generado (siendo un cociente de $\mathbb{Z}^n$), es suficiente probar que M es libre de torsión. La torsión significa en este caso que existe un vector $\vec{b} \notin \mathbb{Z}\vec{a}$, tal que para algún $c \neq 0$ se cumple $c\vec{b} \in \mathbb{Z}\vec{a}$. Pero no es difícil ver que esto es imposible bajo nuestra hipótesis sobre $\vec{a}$.

Ahora tenemos $\mathbb{Z}^n/\mathbb{Z}\vec{a} \cong \mathbb{Z}^{n-1}$. Esto significa que existen algunos vectores $\vec{e}_1, \ldots, \vec{e}_{n-1} \in \mathbb{Z}^n$ tales que sus imágenes en el cociente $\mathbb{Z}^n/\mathbb{Z}\vec{a}$ forman una base. Pero luego $\vec{e}_1, \ldots, \vec{e}_{n-1}, \vec{a}$ es una base de $\mathbb{Z}^n$. □

Ejercicio 4.3. Sea d un entero libre de cuadrados. Consideremos el campo cúbico $K = \mathbb{Q}(\sqrt[3]{d})$. Denotemos $\alpha = \sqrt[3]{d}$ y consideremos un elemento

$$\beta = a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q}.$$

a) Calcule las trazas $T_{K/\mathbb{Q}}(\beta)$, $T_{K/\mathbb{Q}}(\alpha\beta)$, $T_{K/\mathbb{Q}}(\alpha^2\beta)$ y la norma $N_{K/\mathbb{Q}}(\beta)$.

b) Si $\beta \in \mathcal{O}_K$, entonces las trazas y normas de arriba son números enteros. Use esto para concluir que $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha]$.

c) Use estas consideraciones para calcular el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K (¡la respuesta depende de d!).

Solución. Las trazas son

$$T_{K/\mathbb{Q}}(\beta) = 3a, \quad T_{K/\mathbb{Q}}(\alpha\beta) = 3cd, \quad T_{K/\mathbb{Q}}(\alpha^2\beta) = 3bd,$$

y la norma es

$$N_{K/\mathbb{Q}}(\beta) = a^3 - 3abcd + b^3 d + c^3 d^2.$$

Ahora si $\beta \in \mathcal{O}_K$, entonces las trazas y normas de arriba son números enteros. Las condiciones para las trazas quieren decir que existen $a', b', c' \in \mathbb{Z}$ tales que

$$a = \frac{a'}{3}, \quad b = \frac{b'}{3d}, \quad c = \frac{c'}{3d}.$$

Lo que queremos ver es que $d \mid b'$ y $d \mid c'$, y para esto vamos a revisar la norma de 3β que resulta ser igual a

$$a'^3 - \frac{3a'b'c'}{d} + \frac{b'^3}{d^2} + \frac{c'^3}{d} \in \mathbb{Z}.$$

Entonces,

$$-\frac{3a'b'c' + c'^3}{d} + \frac{b'^3}{d^2} \in \mathbb{Z}.$$

Supongamos que para algún $p \mid d$ se tiene $p \nmid b'$. En este caso tomando las valuaciones p-ádicas de la expresión de arriba llegamos a una contradicción.

Entonces, $d \mid b'$. Ahora sustituyendo $b = \frac{b'}{3}$, de la misma manera se ve que $d \mid c'$. Esto demuestra que $\beta \in \frac{1}{3}\mathbb{Z}[\alpha]$. Entonces,

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha].$$

Podemos analizar el cociente $\frac{1}{3}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$ para ver cuáles elementos enteros faltan a $\mathbb{Z}[\alpha]$; es decir, cuáles elementos entre

$$\beta = \frac{1}{3}\left(a + b\alpha + c\alpha^2\right)$$

son enteros, donde $0 \le a, b, c < 3$. Escribamos el polinomio característico de β (lo calculé en PARI/GP):

$$x^3 - ax^2 + \frac{a^2 - bcd}{3}\,x - \frac{a^3 + b^3 d + d^2 c^3 - 3abcd}{27}.$$

Si $b = 0$ o $c = 0$, entonces el coeficiente de x no será entero, y si $a = 0$, el término constante no es entero. Esto nos dice que $abc \neq 0$, y tenemos que analizar ocho diferentes casos. Además, notamos que β es entero si y solamente si $-\beta$ lo es. Módulo 3, esto corresponde a pasar de (a, b, c) a $(2a, 2b, 2c)$. Entonces, en realidad no son ocho casos diferentes, sino solamente cuatro.

En cada caso la condición sobre el coeficiente de x nos dice cuál es el resto de d módulo 3, mientras que la condición sobre el término constante quiere decir algo sobre d módulo 3^3.

a	b	c	$d\ (3)$	$27 \times$ term. const.	$d\ (3^3)$
1	1	1	1	$d^2 - 2d + 1$	$1, 10, 19$
1	1	2	2	$8d^2 - 5d + 1$	—
1	2	1	2	$d^2 + 2d + 1$	$8, 17, 26$
1	2	2	1	$8d^2 - 4d + 1$	—

Al final, la respuesta depende de $d \pmod 9$. Nos salió lo siguiente:

- Si $d \equiv 1 \pmod 9$, entonces el elemento

  $$\beta = \frac{1}{3} + \frac{1}{3}\alpha + \frac{1}{3}\alpha^2$$

  es entero (el otro que nos saldrá es 2β). Tenemos

  $$\mathcal{O}_K = \mathbb{Z}[\alpha, \beta] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z}.$$

  Para verificar el resultado, calculamos que el discriminante correspondiente será

  $$\Delta_K = \det \begin{pmatrix} T(1) & T(\alpha) & T(\beta) \\ T(\alpha) & T(\alpha^2) & T(\alpha\beta) \\ T(\beta) & T(\alpha\beta) & T(\beta^2) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 1 \\ 0 & 0 & d \\ 1 & d & (2d+1)/3 \end{pmatrix} = -3d^2.$$

Por otra parte, $\Delta(\mathbb{Z}[\alpha]) = -27d^2$, y luego $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$. Podemos también escribir la expresión para $\Delta(\mathbb{Z}[\beta])$ y concluir que $[\mathcal{O}_K : \mathbb{Z}[\beta]] = \frac{d-1}{9}$.

- Si $d \equiv 8 \pmod 9$, entonces el elemento

$$\beta = \frac{1}{3} + \frac{2}{3}\alpha + \frac{1}{3}\alpha^2$$

  es entero. En este caso también se tiene $\Delta_K = -3d^2$ y $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$. Además, es posible ver que $[\mathcal{O}_K : \mathbb{Z}[\beta]] = \frac{d-8}{9}$.

- En el resto de los casos cuando $d \not\equiv \pm 1 \pmod 9$, no habrá elementos enteros adicionales.

Cuando $d \equiv \pm 1 \pmod 9$, entonces $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$, y en el caso contrario, $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

Ejercicio 4.4. Encuentre el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K para los campos cúbicos $\mathbb{Q}(\sqrt[3]{6})$ y $\mathbb{Q}(\sqrt[3]{12})$.

Solución. En el caso de $\mathbb{Q}(\sqrt[3]{6})$, el ejercicio anterior nos dice que $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{6}]$, y el discriminante correspondiente será $\Delta_K = \Delta(x^3 - 6) = -27 \cdot 6^2 = -2^2 \cdot 3^5$.

Ahora para $\mathbb{Q}(\sqrt[3]{12})$, el número 12 no es libre de cuadrados, así que no podemos aplicar el mismo argumento. Denotemos $\alpha = \sqrt[3]{12}$. No es difícil notar otro elemento entero: $\beta = \alpha^2/2 = \sqrt[3]{18}$. Calculamos que

$$\Delta(\mathbb{Z}[\alpha]) = -2^4 \cdot 3^5, \quad \Delta(\mathbb{Z}[\beta]) = -2^2 \cdot 3^7.$$

Ahora consideremos

$$\mathbb{Z}[\alpha, \beta] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$$

(note que $\alpha\beta = 6$, $\alpha^2 = 2\beta$, $\beta^2 = 6\alpha$). Calculamos

$$\Delta(\mathbb{Z}[\alpha,\beta]) = \det \begin{pmatrix} T(1) & T(\alpha) & T(\beta) \\ T(\alpha) & T(\alpha^2) & T(\alpha\beta) \\ T(\beta) & T(\alpha\beta) & T(\beta^2) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 18 \\ 0 & 18 & 0 \end{pmatrix} = -2^2 \cdot 3^5.$$

Esto implica que

$$[\mathcal{O}_K : \mathbb{Z}[\alpha,\beta]] = m = 1, 2, 3, 6, 9, 18.$$

Podemos analizar la integridad de los elementos en el cociente $\frac{1}{m}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$. Para esto consideremos los elementos

$$\gamma = \frac{a}{m} + \frac{b}{m}\alpha + \frac{c}{m}\beta,$$

donde $0 \le a, b, c < m$. Basta considerar $m = 18$. En teoría, todo esto se puede hacer a mano, hasta cierto punto. Por ejemplo, calculamos

$$T_{K/\mathbb{Q}}(\gamma) = \frac{3a}{m} = \frac{a}{6},$$

de donde $a = 0, 6, 12$, lo que quita una parte del trabajo. Podemos sustituir estos valores de a y, por ejemplo, analizar $N_{K/\mathbb{Q}}(\gamma)$, pero mejor hacerlo con la computadora.

```
? m = 18;
? nrm = norm (1/m*Mod(a + b*x + c*x^2/2, x^3-12))
% = 1/5832*a^3 - 1/324*c*b*a + (1/486*b^3 + 1/324*c^3)

{ for (a=0,m-1, for (b=0,m-1, for (c=0,m-1,
        if (denominator(eval(nrm)) == 1,
          print ([a,b,c])
        )
  )))
};

[0, 0, 0]
/* ¡y nada más! */
```

Esto implica que $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$. Ya calculamos Δ_K. Notamos que para $\mathbb{Q}(\sqrt[3]{6})$ y $\mathbb{Q}(\sqrt[3]{12})$ nos salió el mismo discriminante. $\square$

Ejercicio 4.5. Consideremos el campo cúbico $K = \mathbb{Q}(\sqrt[3]{17})$.

a) Calcule el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K.

b) Describa las factorizaciones de primos racionales $p \in \mathbb{Z}$ en $\mathcal{O}_K$.

c) Describa los ideales primos $\mathfrak{p} \subset \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(\mathfrak{p}) \le 10$.

d) Describa todos los ideales $I \subseteq \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(I) \le 10$.

Solución. Denotando $\sqrt[3]{17}$ por α, el ejercicio 3 nos dice que

$$\mathcal{O}_K = \mathbb{Z}[\alpha, \beta], \quad \beta = \frac{1}{3} + \frac{2}{3}\,\alpha + \frac{1}{3}\,\alpha^2.$$

Además, allí escribimos la fórmula curiosa $[\mathcal{O}_K : \mathbb{Z}[\beta]] = \frac{d-8}{9}$, y para $d = 17$ tenemos suerte y $\mathcal{O}_K = \mathbb{Z}[\beta]$. Por otra parte, $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 3$. Esto significa que podemos aplicar el Kummer–Dedekind al polinomio mínimo de β:

$$x^3 - x^2 - 11x - 12.$$

Sin embargo, será más fácil considerar el polinomio $x^3 - 17$ para todos los primos excepto $p = 3$. En ese caso excepcional tenemos

$$x^3 - x^2 - 11x - 12 \equiv x\,(x+1)^2 \pmod{3},$$

lo que nos da la factorización

$$3\mathcal{O}_K = \mathfrak{p}_3\,\mathfrak{p}_3'^2 = (3,\beta)\,(3,1+\beta)^2,$$

donde $N_{K/\mathbb{Q}}(\mathfrak{p}_3) = N_{K/\mathbb{Q}}(\mathfrak{p}_3') = 3$. Para los primos distintos de 3, las factorizaciones son las siguientes.

- $17\mathcal{O}_K = \mathfrak{p}^3$, donde $\mathfrak{p} = \sqrt[3]{17}\mathcal{O}_K$. Tenemos $N_{K/\mathbb{Q}}(\mathfrak{p}) = 17$.
- Si $p \equiv 2 \pmod 3$ y $p \ne 17$, entonces $p\mathcal{O}_K = \mathfrak{p}\,\mathfrak{p}'$, lo que viene de la factorización

  $$x^3 - 17 \equiv (x-a) \times \text{polinomio cuadrático} \pmod p.$$

  Aquí $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ y $N_{K/\mathbb{Q}}(\mathfrak{p}') = p^2$.
- Para $p \equiv 1 \pmod 3$ hay dos opciones. Si 17 no es un cubo módulo p, entonces $\mathfrak{p} = p\mathcal{O}_K$ es un ideal primo y $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^3$. Si 17 es un cubo módulo p, entonces $p\mathcal{O}_K = \mathfrak{p}\,\mathfrak{p}'\,\mathfrak{p}''$, lo que viene de la factorización

  $$x^3 - 17 \equiv (x-a_1)\,(x-a_2)\,(x-a_3) \pmod p.$$

Ahora si nos interesan los ideales primos de norma $N_{K/\mathbb{Q}}(\mathfrak{p}) \le 10$, esto en particular implica que $\mathfrak{p} \mid p$, donde $p < 10$. Para obtener todos los ideales de norma $N_{K/\mathbb{Q}}(I) \le 10$, hay que multiplicar los ideales primos correspondientes (usando la unicidad de descomposición de ideales en ideales primos).

Los primos $p \equiv 2 \pmod 3$ que nos interesan son $p = 2, 5$, y las factorizaciones de $x^3 - 17$ son

$$\begin{aligned} p = 2&\colon (x+1)\,(x^2+x+1),\\ p = 5&\colon (x+2)\,(x^2+3x+4). \end{aligned}$$

El primo $p = 7$ es inerte, y el ideal primo correspondiente $\mathfrak{p} = 7\mathcal{O}_K$ tiene norma 7^3 y no nos interesa. Ahora los ideales primos de norma < 10 que salen de la lista de arriba son nada más los siguientes:

$$\begin{aligned} N = 2&\colon \mathfrak{p}_2 = (2, 1+\alpha),\\ N = 3&\colon \mathfrak{p}_3 = (3,\beta),\ \mathfrak{p}_3' = (3, 1+\beta),\\ N = 4&\colon \mathfrak{p}_2' = (2, 1+\alpha+\alpha^2),\\ N = 5&\colon \mathfrak{p}_5 = (5, 2+\alpha). \end{aligned}$$

Si nos interesan todos los ideales de norma ≤ 10, hay que considerar los productos:

$$\begin{aligned} N = 1 &\colon \mathcal{O}_K, \\ N = 2 &\colon \mathfrak{p}_2, \\ N = 3 &\colon \mathfrak{p}_3,\ \mathfrak{p}_3', \\ N = 4 &\colon \mathfrak{p}_2^2,\ \mathfrak{p}_2', \\ N = 5 &\colon \mathfrak{p}_5, \\ N = 6 &\colon \mathfrak{p}_2\,\mathfrak{p}_3,\ \mathfrak{p}_2\,\mathfrak{p}_3', \\ N = 8 &\colon \mathfrak{p}_2^3,\ \mathfrak{p}_2\,\mathfrak{p}_2', \\ N = 9 &\colon \mathfrak{p}_3^2,\ \mathfrak{p}_3\,\mathfrak{p}_3',\ \mathfrak{p}_3'^2, \\ N = 10 &\colon \mathfrak{p}_2\,\mathfrak{p}_5, \end{aligned}$$

En total, nos salieron 15 ideales. Podemos comprobarlo con PARI/GP. Allí la función `ideallist(`K`,`N`)` devuelve los ideales en $\mathcal{O}_K$ de norma $\le N$ como una lista separada por normas

```
? L = ideallist (nfinit(x^3-17),10);
? vector (#L, i, #L[i])
% = [1, 1, 2, 2, 1, 2, 0, 2, 3, 1]
? vecsum(%)
% = 15
```

Las consideraciones similares demuestran que para cualquier campo de números $K/\mathbb{Q}$ y N fijo hay un número finito de ideales $I \subseteq \mathcal{O}_K$ con la norma $N_{K/\mathbb{Q}}(I) \le N$. $\square$