Teoría de números algebraicos
Tarea 5

Alexey Beshenov (alexey.beshenov@cimat.mx)

23 de septiembre de 2020

Fecha límite: viernes, 2 de octubre.

Ejercicio 5.1. Sea X una matriz de $n \times n$ e Y una matriz de $n' \times n'$. El **producto de Kronecker** $X \otimes Y$ es la matriz de $nn' \times nn'$ que consiste en bloques

$$\begin{pmatrix} x_{11}Y & \cdots & x_{1n}Y \\ \vdots & \ddots & \vdots \\ x_{n1}Y & \cdots & x_{nn}Y \end{pmatrix}.$$

Demuestre que

$$\det(X \otimes Y) = \det(X)^{n'} \cdot \det(Y)^n.$$

Solución. Hay varios modos de verlo. Por ejemplo, si se trata de matrices complejas, recordamos que X es diagonalizable si y solamente si el polinomio característico p_X no tiene raíces múltiples. Esta condición corresponde a $\Delta(p_X) \neq 0$, donde $\Delta(p_X)$ es el discriminante, que será un polinomio en los coeficientes de p_X (ocupando la fórmula $\Delta(f) = \pm \operatorname{Res}(f, f') = \det(\cdots)$), y entonces un polinomio en los coeficientes de x_{ij}. Entonces, el conjunto de matrices diagonalizables en $M_n(\mathbb{C})$ corresponde a la condición $\Delta(p_x) \neq 0$, y este conjunto es denso en $M_n(\mathbb{C})$. Entonces, bastaría probar la identidad $\det(X \otimes Y) = \det(X)^{n'} \cdot \det(Y)^n$ para las matrices diagonalizables.

Ahora recordemos que los valores propios de $X \otimes Y$ son de la forma $\alpha\beta$, donde α es un valor propio de X y β es un valor propio de Y. De hecho, para los vectores propios correspondientes se tiene $Xu = \alpha u$ e $Yv = \beta v$. Luego, $(X \otimes Y)(u \otimes v) = \alpha\beta\, u \otimes v$.

Una vez sabemos esto, no hay que probar mucho. Al diagonalizar X e Y, vemos que

$$\det(X \otimes Y) = \prod_{i,j} \alpha_i \beta_j,$$

donde α_i son los valores propios de X y β_j son los valores propios de Y. Ahora el último producto es precisamente

$$\Big(\prod_i \alpha_i\Big)^{n'} \cdot \Big(\prod_j \beta_j\Big)^n = \det(X)^{n'} \cdot \det(Y)^n.$$

En general, la identidad se cumplirá para matrices con coeficientes en cualquier anillo conmutativo R por la siguiente razón. Acabamos de probar que es cierta para $R = \mathbb{C}$, pero luego es cierta para $R = \mathbb{Z}$, y podemos tratarla como una identidad de polinomios con coeficientes enteros en las variables x_{ij} e $y_{k\ell}$. Tomando el cambio de base de $\mathbb{Z}$ a R, se concluye que la misma identidad se cumple para los polinomios con coeficientes en R.

También podemos ocupar un cálculo directo. Notamos que la matriz $X \otimes Y$ es igual al producto $(X \otimes I_{n'})\,(I_n \otimes Y)$. Aquí la matriz $(I_n \otimes Y)$ tiene forma

$$\begin{pmatrix} Y & & \\ & \ddots & \\ & & Y \end{pmatrix}$$

Además, después de un cambio de base, $X \otimes I_{n'}$ tiene la misma forma: si $e_1, \ldots, e_n$ es la base estándar de R^n y $f_1, \ldots, f_{n'}$ es la base estándar de $R^{n'}$, entonces basta escribir $X \otimes I_{n'}$ en la base

$$e_1 \otimes f_1,\ e_1 \otimes f_2, \ldots, e_1 \otimes f_{n'},\ e_2 \otimes f_1,\ e_2 \otimes f_2, \ldots$$

Entonces,

$$\det(X \otimes Y) = \det(I_{n'} \otimes X) \cdot \det(I_n \otimes Y) = \det(X)^{n'} \cdot \det(Y)^n. \qquad \square$$

Ejercicio 5.2. Para el campo de números $K = \mathbb{Q}(\sqrt{3}, \zeta_5)$ calcule $\mathcal{O}_K$ y Δ_K. ¿Cuáles primos racionales se ramifican en K?

Solución. Tenemos $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ y $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$. Notamos que $\sqrt{3} \notin \mathbb{Q}(\zeta_5)$: por ejemplo, si esto sería cierto, entonces 3 (y también 2) se ramificaría en $\mathbb{Q}(\zeta_5)$, pero sabemos que allí se ramifica solo 5. Estas consideraciones nos llevan a la conclusión que

$$[\mathbb{Q}(\sqrt{3}, \zeta_5) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 8,$$

y los campos son linealmente disjuntos. Ya sabemos cómo calcular los discriminantes:

$$\Delta_{\mathbb{Q}(\sqrt{3})} = 4 \cdot 3, \quad \Delta_{\mathbb{Q}(\zeta_5)} = 5^3.$$

Los discriminantes son coprimos, así que una base de $\mathcal{O}_K$ es el producto de las bases:

$$1,\ \zeta_5,\ \zeta_5^2,\ \zeta_5^3,\ \sqrt{3},\ \sqrt{3}\zeta_5,\ \sqrt{3}\zeta_5^2,\ \sqrt{3}\zeta_5^3.$$

En fin, el discriminante será

$$\Delta_K = (2^2 \cdot 3)^4 \cdot (5^3)^2 = 2^8 \cdot 3^4 \cdot 5^6.$$

Solo para confirmarlo, preguntémoslo a PARI/GP:

```
? K=nfinit(t^2-3);
? L=rnfinit(K,polcyclo(5));
? nfinit(L).disc
% = 324000000
? factor (%)
% =
[2 8]

[3 4]

[5 6]
```

□

Ejercicio 5.3. Consideremos los campos cuadráticos $K = \mathbb{Q}(\sqrt{3})$ y $K' = \mathbb{Q}(\sqrt{-5})$ y su compositum $KK' = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$. Sea $\mathcal{O} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \sqrt{-5}\mathbb{Z} \oplus \sqrt{-15}\mathbb{Z}$.

Calcule $\mathcal{O}_{KK'}$, $\Delta_{KK'}$ y el índice $[\mathcal{O}_{KK'} : \mathcal{O}]$.

Solución. Tenemos $\Delta_K = 4 \cdot 3$ y $\Delta_{K'} = 4 \cdot 5$. De aquí sabemos que

$$\Delta(\mathcal{O}) = (2^2 \cdot 3)^2 \cdot (2^2 \cdot 5)^2 = 2^8 \cdot 3^2 \cdot 5^2.$$

Sin embargo, los discriminantes no son coprimos, así que no podemos afirmar que $\mathcal{O} = \mathcal{O}_K$.

De hecho, desde el principio se puede observar que se nos escapó un elemento entero bastante obvio: $3 \equiv -5 \equiv 3 \pmod 4$, pero luego $-15 \equiv 1 \pmod 4$, y el elemento $\frac{1+\sqrt{-15}}{2}$ es entero. Lo que no es tan obvio es que $\frac{\sqrt{3}+\sqrt{-5}}{2}$ es entero, pero lo podemos comprobar calculando directamente el polinomio mínimo. Primero, el polinomio mínimo de $\sqrt{3} + \sqrt{-5}$ es

$$x^4 + 4x^2 + 64.$$

Este es un caso particular del cálculo general: dados dos campos cuadráticos linealmente disjuntos $\mathbb{Q}(\sqrt{d_1})$ y $\mathbb{Q}(\sqrt{d_2})$, el polinomio mínimo de $\sqrt{d_1} + \sqrt{d_2}$ sobre $\mathbb{Q}$ es su polinomio característico que viene dado por

$$x^4 - 2\,(d_1 + d_2)\,x^2 + (d_1 - d_2)^2.$$

Ahora si $\sqrt{3} + \sqrt{-5}$ es una raíz de $x^4 + 4x^2 + 64$, entonces $\frac{\sqrt{3}+\sqrt{-5}}{2}$ es una raíz de $x^4 + x^2 + 4$. Esto demuestra la integralidad. Tiene sentido entonces considerar el anillo más grande

$$\mathcal{O}' = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \frac{\sqrt{3} + \sqrt{-5}}{2}\mathbb{Z} \oplus \frac{1 + \sqrt{-15}}{2}\mathbb{Z}.$$

Para no equivocarnos y calcular bien el índice $[\mathcal{O}' : \mathcal{O}]$, notamos que la base de $\mathcal{O}$ se expresa en términos de la base de $\mathcal{O}'$ como

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

El determinante de esta matriz es 4, así que $[\mathcal{O}' : \mathcal{O}] = 4$ y luego $\Delta(\mathcal{O}') = \Delta(\mathcal{O})/4^2 = 2^4 \cdot 3^2 \cdot 5^2$. Ahora

$$2^4 \cdot 3^2 \cdot 5^2 = \Delta(\mathcal{O}') = [\mathcal{O}_{KK'} : \mathcal{O}']^2 \cdot \Delta_{KK'}.$$

Sabemos que $2, 3$ se ramifican en $\mathbb{Q}(\sqrt{3})$ y $2, 5$ se ramifican en $\mathbb{Q}(\sqrt{-5})$, así que necesariamente $2, 3, 5$ dividen a Δ_K. Esto nos deja muy pocas posibilidades:

$$[\mathcal{O}_{KK'} : \mathcal{O}'] = 1, 2.$$

Entonces, bastaría considerar el cociente $\frac{1}{2}\mathcal{O}'/\mathcal{O}'$; es decir, ver cuáles elementos entre

$$\frac{a_1}{2}\,\alpha_1 + \frac{a_2}{2}\,\alpha_2 + \frac{a_3}{2}\,\alpha_3 + \frac{a_4}{2}\,\alpha_4,$$
$$\alpha_1 = 1,\ \alpha_2 = \sqrt{3},\ \alpha_3 = \frac{\sqrt{3}+\sqrt{-5}}{2},\ \alpha_4 = \frac{1+\sqrt{-15}}{2}.$$

son enteros para $a_i = 0, 1$.

```
? K = nfinit(t^2-3);
? L = rnfinit(K,x^2+5);
? alpha2 = rnfeltreltoabs(L,t);
? alpha3 = rnfeltreltoabs(L,(t+x)/2);
? alpha4 = rnfeltreltoabs(L,(1+t*x)/2);

? { for(a1=0,1, for(a2=0,1, for(a3=0,1, for(a4=0,1,
        print([[a1,a2,a3,a4],
               minpoly((a1+a2*alpha2+a3*alpha3+a4*alpha4)/2)])
)))) };
[[0, 0, 0, 0], x]
[[0, 0, 0, 1], x^2 - 1/2*x + 1]
[[0, 0, 1, 0], x^4 + 1/4*x^2 + 1/4]
[[0, 0, 1, 1], x^4 - x^3 + 5/2*x^2 + 3/4*x + 9/16]
[[0, 1, 0, 0], x^2 - 3/4]
[[0, 1, 0, 1], x^4 - x^3 + 3/4*x^2 - 1/4*x + 23/8]
[[0, 1, 1, 0], x^4 - 11/4*x^2 + 4]
[[0, 1, 1, 1], x^4 - x^3 - 1/2*x^2 + 6*x + 6]
[[1, 0, 0, 0], x - 1/2]
[[1, 0, 0, 1], x^2 - 3/2*x + 3/2]
```

```
[[1, 0, 1, 0], x^4 - 2*x^3 + 7/4*x^2 - 3/4*x + 3/8]
[[1, 0, 1, 1], x^4 - 3*x^3 + 11/2*x^2 - 3*x + 1]
[[1, 1, 0, 0], x^2 - x - 1/2]
[[1, 1, 0, 1], x^4 - 3*x^3 + 15/4*x^2 - 9/4*x + 27/8]
[[1, 1, 1, 0], x^4 - 2*x^3 - 5/4*x^2 + 9/4*x + 27/8]
[[1, 1, 1, 1], x^4 - 3*x^3 + 5/2*x^2 + 21/4*x + 49/16]
```

No hay elementos enteros adicionales, y entonces podemos concluir que $\mathcal{O}_{KK'} = \mathcal{O}'$, $\Delta_{KK'} = 2^4 \cdot 3^2 \cdot 5^2$, $[\mathcal{O}_{KK'} : \mathcal{O}] = 4$. □

Ejercicio 5.4. Calcule que

$$\Delta(\mathbb{Z}[\zeta_{p^e}]) = \Delta(\Phi_{p^e}) = \pm p^s, \quad \text{donde } s = p^{e-1}\,(pe - e - 1).$$

¿Cuál es el signo?

Solución. Tenemos

$$\Delta(1, \zeta, \ldots, \zeta^{d-1}) = \Delta(\Phi_{p^e}) = \pm N_{K/\mathbb{Q}}(\Phi'_{p^e}(\zeta)).$$

Ahora

$$x^{p^e} - 1 = (x^{p^{e-1}} - 1)\,\Phi_{p^e}(x),$$

Tomando las derivadas,

$$p^e\, x^{p^e-1} = p^{e-1}\, x^{p^{e-1}-1}\,\Phi_{p^e}(x) + (x^{p^{e-1}} - 1)\,\Phi'_{p^e}(x).$$

Al sustituir ζ en lugar de x, nos queda

$$p^e\, \zeta^{p^e-1} = (\zeta_p - 1)\,\Phi'_{p^e}(\zeta).$$

Dado que ζ es invertible, tenemos $N_{K/\mathbb{Q}}(\zeta) = \pm 1$. Ahora para calcular la norma de $\zeta_p - 1$, notamos que

$$[\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}(\zeta_p)] = \frac{[\mathbb{Q}(\zeta_{p^e}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_p) : \mathbb{Q}]} = \frac{\phi(p^e)}{\phi(p)} = p^{e-1}.$$

(Recordamos que $\phi(p^e) = (p-1)\,p^{e-1}$.) Entonces,

$$N_{K/\mathbb{Q}}(\zeta_p - 1) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{p^{e-1}} = p^{p^{e-1}}.$$

Esto nos lleva a la fórmula

$$N_{K/\mathbb{Q}}(\Phi'_{p^e}(\zeta)) = \pm\frac{(p^e)^{\phi(p^e)}}{p^{p^{e-1}}} = \pm p^s,$$

donde

$$s = e\,\phi(p^e) - p^{e-1} = p^{e-1}\,(pe - e - 1).$$

El signo del discriminante sale del teorema de Brill: este es $(-1)^{\phi(p^e)/2}$. □

Ejercicio 5.5. Demuestre que si $n = mp^e$, donde $p \nmid m$, entonces se cumple la congruencia

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^e)} \pmod{p}.$$

Solución. Se trata de polinomios con coeficientes enteros, así que en teoría podríamos resolver el ejercicio ocupando fórmulas como $x^n - 1 = \prod_{d|n} \Phi_d(x)$ que definen los polinomios ciclotómicos. Procedamos por inducción sobre m y e. Por ejemplo, si $m = 1$, entonces la fórmula sí se cumple:

$$\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}}) = \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} \equiv (x-1)^{p^e - p^{e-1}} = (x-1)^{\phi(p^e)} \pmod{p}.$$

De la misma manera, si $e = 0$, entonces la fórmula se vuelve trivial.

Para el paso inductivo, escribamos

$$\Phi_n(x) = (x^n - 1) \Big/ \prod_{\substack{d|n \\ d<n}} \Phi_d(x) = (x^n - 1) \Big/ \Big(\prod_{\substack{d|m \\ d<m}} \prod_{0 \le k \le e} \Phi_{dp^k}(x) \prod_{0 \le k \le e-1} \Phi_{mp^k}(x) \Big)$$

Reduciendo módulo p, y usando la identidad $\sum_{0 \le k \le e} \phi(p^k) = p^e$,

$$\Phi_n(x) \equiv \frac{\left((x^m - 1) \Big/ \prod_{\substack{d|m \\ d<m}} \Phi_d(x) \right)^{p^e}}{\Phi_m(x)^{p^{e-1}}} = \Phi_m(x)^{\phi(p^e)} \pmod{p}. \qquad \square$$