Teoría de números algebraicos
Tarea 3

Alexey Beshenov (alexey.beshenov@cimat.mx)

2 de septiembre de 2020

Fecha límite: ~~viernes, 11 de septiembre~~ miércoles, 15 de septiembre.

Consideremos el campo ciclotómico $K = \mathbb{Q}(\zeta_8)$. Más adelante veremos un modo adecuado para probar que $\mathcal{O}_K = \mathbb{Z}[\zeta_8]$, pero por el momento se puede aceptar este resultado.

Ejercicio 3.1. Usando el teorema de Kummer–Dedekind, describa las factorizaciones de $p\mathcal{O}_K$ en ideales primos para diferentes primos racionales p.
(La respuesta depende de p mód 8.)

Solución. Para ocupar el Kummer–Dedekind, nos interesa cómo el octavo polinomio ciclotómico $\Phi_8 = x^4 + 1$ se factoriza módulo diferentes primos p.

Primero, módulo 2 se obtiene $(x+1)^4$. Si p es un primo impar, se ve que el polinomio $f = x^8 - 1$ es separable en $\mathbb{F}_p[x]$: tenemos $\gcd(f, f') = 1$. Esto implica que Φ_8 es también separable.

Notamos que si x^4+1 tiene raíz ζ en $\mathbb{F}_p$, entonces ζ es un elemento de orden 8 en el grupo cíclico $\mathbb{F}_p^\times$. Esto es posible si y solamente si $p \equiv 1 \pmod{8}$. En este caso ζ^3, ζ^5, ζ^7 son otras raíces de $x^4 + 1$ en $\mathbb{F}_p$:

$$\overline{\Phi_8} = (x - \zeta)\,(x - \zeta^3)\,(x - \zeta^5)\,(x - \zeta^7).$$

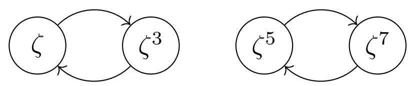
Supongamos ahora que $p \equiv 3, 5, 7 \pmod{8}$. En cada uno de estos casos $p^2 \equiv 1 \pmod{8}$, así que las raíces octavas primitivas $\zeta, \zeta^3, \zeta^5, \zeta^8$ existen en $\mathbb{F}_{p^2}^\times$. Recordemos que $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \{1, \sigma\}$, donde $\sigma\colon x \mapsto x^p$ es el automorfismo de Frobenius, y la teoría de Galois nos dice que

$$\mathbb{F}_p = \{a \in \mathbb{F}_{p^2} \mid \sigma(a) = a\}.$$

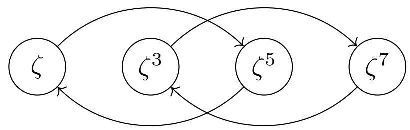
Para $p \not\equiv 1 \pmod{8}$ el polinomio Φ_8 no puede tener un factor lineal, así que este será irreducible o producto de dos polinomios cuadráticos. Curiosamente, Φ_8 no será irreducible módulo ningún primo p.

Para verlo, consideremos cómo el Frobenius permuta las raíces octavas primitivas par $p \equiv 3, 5, 7$.

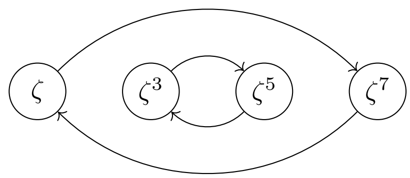
$p \equiv 3 \pmod 8$



$p \equiv 5 \pmod 8$



$p \equiv 7 \pmod 8$



Ahora si $\{\alpha_1, \alpha_2\}$ y $\{\alpha_3, \alpha_4\}$ forman órbitas respecto a la acción del Frobenius, entonces el último dejo fijo a

$$\alpha_1 + \alpha_2,\ \alpha_1\alpha_2,\ \alpha_3 + \alpha_4,\ \alpha_3\alpha_4,$$

así que estos elementos están en $\mathbb{F}_p$, y por lo tanto tenemos factorización en $\mathbb{F}_p[x]$

$$(x-\alpha_1)\,(x-\alpha_2)\,(x-\alpha_3)\,(x-\alpha_4) = (x^2-(\alpha_1+\alpha_2)\,x+\alpha_1\alpha_2)\cdot(x^2-(\alpha_3+\alpha_4)\,x+\alpha_3\alpha_4).$$

En particular,

- Si $p \equiv 3 \pmod 8$, entonces

  $$\Phi_8(x) = (x^2 - (\zeta + \zeta^3)\,x - 1)\,(x^2 - (\zeta^5 + \zeta^7)\,x - 1).$$

  También podemos calcular que

  $$(\zeta + \zeta^3)^2 = (\zeta^5 + \zeta^7)^2 = -2,$$

  así que los coeficientes de x que nos salen son las dos raíces cuadradas de -2 módulo p.

- Si $p \equiv 5 \pmod p$, entonces

  $$\Phi_8(x) = (x^2 - \zeta^2)\,(x^2 + \zeta^2).$$

  Aquí $\pm\zeta^2$ son las raíces cuadradas de -1 módulo p.

- Si $p \equiv 7 \pmod p$, entonces

  $$\Phi_8(x) = (x^2 - (\zeta + \zeta^7)\,x + 1)\,(x^2 - (\zeta^3 + \zeta^5)\,x + 1).$$

  Notamos que

  $$(\zeta + \zeta^7)^2 = (\zeta^3 + \zeta^5) = 2,$$

  así que los coeficientes de x son las raíces cuadradas de 2 módulo p.

Resumiendo todo esto y ocupando el teorema de Kummer–Dedekind, podemos concluir que los primos racionales se factorizan en $\mathbb{Z}[\zeta_8] = \mathcal{O}_K$ de la siguiente manera.

- $2\mathcal{O}_K = \mathfrak{p}^4$.
- Si $p \equiv 1 \pmod 8$, entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.
- Si $p \equiv 3, 5, 7 \pmod 8$, entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$.

Esto es algo curioso: ningún primo racional $p \in \mathbb{Z}$ es inerte en $\mathbb{Z}[\zeta_8]$, lo que equivale al hecho de que $\Phi_8 = x^4 + 1$ es un polinomio irreducible en $\mathbb{Z}[x]$ que se vuelve reducible en $\mathbb{F}_p[x]$ para cualquier p.

Recordemos que uno de los criterios de irreducibilidad más sencillos nos dice que *si $f \in \mathbb{Z}[x]$ es un polinomio mónico que se vuelve irreducible módulo algún p, entonces f es irreducible en $\mathbb{Z}[x]$*. Como acabamos de ver, hay polinomios irreducibles para cuales este criterio no sirve. $\square$

Ejercicio 3.2. Encuentre las subextensiones $\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta_8)$ y las factorizaciones de $p\mathcal{O}_F$ para cada una de estas.
(Para encontrar las subextensiones, use la teoría de Galois.)

Solución. Primero, el grupo de Galois de $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ consiste en los automorfismos

$$\sigma_a \colon \zeta_8 \mapsto \zeta_8^a, \quad a = 1, 3, 5, 7$$

Este grupo es isomorfo a $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. Hay tres subgrupos propios no triviales, cada uno cíclico de orden 2. Por la teoría de Galois, habrá tres suextensiones que corresponden a los subcampos fijos por $\sigma_3, \sigma_5, \sigma_7$ respectivamente.

Tenemos

$$\begin{aligned} K^{\langle\sigma_3\rangle} &= \mathbb{Q}(\zeta_8 + \zeta_8^3) = \mathbb{Q}(\sqrt{-2}), \\ K^{\langle\sigma_5\rangle} &= \mathbb{Q}(\zeta_8^2) = \mathbb{Q}(i), \\ K^{\langle\sigma_7\rangle} &= \mathbb{Q}(\zeta_8 - \zeta_8^3) = \mathbb{Q}(\sqrt{2}). \end{aligned}$$

$$\begin{tikzcd}[arrows=dash] & \mathbb{Q}(\zeta_8) \arrow[dl] \arrow[d] \arrow[dr] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr] & \mathbb{Q}(i) \arrow[d] & \mathbb{Q}(\sqrt{-2}) \arrow[dl] \\ & \mathbb{Q} & \end{tikzcd}$$

Ya sabemos cómo se factorizan primos racionales en campos cuadráticos. En todos los casos de arriba el único primo que se ramifica es 2. Ahora para $K = \mathbb{Q}(\sqrt{d})$ con $d = 2, -2, -1$ y p primo impar tenemos dos casos:

- si $\left(\frac{d}{p}\right) = +1$, entonces $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$,
- si $\left(\frac{d}{p}\right) = -1$, entonces $p\mathcal{O}_K$ es primo.

También vale la pena notar que este ejercicio junto con el anterior nos dan una prueba de las leyes suplementarias de reprocidad cuadrática.

- $\left(\frac{2}{p}\right) = +1$ si y solamente si p se escinde en $\mathbb{Q}(\sqrt{2})$. Por otra parte, las consideraciones del ejercicio anterior demuestran que esto sucede si y solamente si $p \equiv 1, 7 \pmod{8}$.
- De la misma manera, $\left(\frac{-2}{p}\right) = +1$ si y solamente si $p \equiv 1, 3 \pmod{8}$.
- $\left(\frac{-1}{p}\right) = +1$ si y solamente si $p \equiv 1, 5 \pmod{8}$; es decir, $p \equiv 1 \pmod{4}$.

Otra observación interesante: ningún primo racional p queda inerte en $\mathbb{Q}(\zeta_8)$ porque este se descompone en uno de los subcampos cuadráticos. La siguiente página contiene una tabla de descomposiciones.

p	$p\mathbb{Z}[\sqrt{2}]$	$p\mathbb{Z}[\sqrt{-1}]$	$p\mathbb{Z}[\sqrt{-2}]$	$p\mathbb{Z}[\zeta_8]$	$p\ (8)$
2	$\mathfrak{p}^2$	$\mathfrak{p}^2$	$\mathfrak{p}^2$	$\mathfrak{q}^4$	2
3	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
5	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
7	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
11	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
13	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
17	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
19	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
23	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
29	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
31	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
37	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
41	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
43	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
47	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
53	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
59	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
61	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
67	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
71	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
73	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
79	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
83	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
89	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
97	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1
101	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
103	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	7
107	$\mathfrak{p}$	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2$	3
109	$\mathfrak{p}$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{q}_1\,\mathfrak{q}_2$	5
113	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{p}_1\,\mathfrak{p}_2$	$\mathfrak{q}_1\,\mathfrak{q}_2\,\mathfrak{q}_3\,\mathfrak{q}_4$	1

$\square$

Ejercicio 3.3. Considerando la descomposición de primos racionales en $\mathcal{O}_K$, demuestre que $\zeta_p \notin \mathbb{Q}(\zeta_q)$ para diferentes primos impares $p \neq q$.

Solución. Si $\zeta_p \in \mathbb{Q}(\zeta_q)$, entonces tenemos la inclusión de anillos de enteros $\mathbb{Z}[\zeta_p] \subset \mathbb{Z}[\zeta_q]$. Ahora p se ramifica en $\mathbb{Z}[\zeta_p]$:

$$p\mathbb{Z}[\zeta_p] = (1-\zeta_p)^{p-1}.$$

Al pasar a $\mathbb{Z}[\zeta_q]$, vemos que allí p debe también ramificarse. Sin embargo, el único primo que se ramifica en $\mathbb{Z}[\zeta_q]$ es q, así que $p = q$.

Notamos que a priori no es completamente obvio qué $\zeta_p \notin \mathbb{Q}(\zeta_q)$. Una condición necesaria sería

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] \mid [\mathbb{Q}(\zeta_q) : \mathbb{Q}] \iff (p-1) \mid (q-1),$$

pero esto puede pasar para varios p y q. La teoría de Galois tampoco ayuda mucho: los grupos de Galois son cíclicos y C_{p-1} sí se obtiene como un cociente de C_{q-1}... $\square$

Ejercicio 3.4. Para el campo ciclotómico $K = \mathbb{Q}(\zeta_p)$ el grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ es cíclico, así que la teoría de Galois implica que existe un subcampo cuadrático único $F \subset K$. Considerando la factorización de primos racionales en $\mathcal{O}_F$ y $\mathcal{O}_K$, demuestre que $F = \mathbb{Q}(\sqrt{p^*})$, donde $p^* = (-1)^{(p-1)/2}p$.
(Sugerencia: si q se ramifica en $\mathcal{O}_F$, entonces q se ramifica en $\mathcal{O}_K$.)

Solución. Primero, el grupo de Galois es isomorfo a $(\mathbb{Z}/p\mathbb{Z})^\times$, y allí hay un solo subgrupo de orden $\frac{p-1}{2}$ que corresponde a una subextensión cuadrática.

$$\begin{tikzcd} \mathbb{Q}(\zeta_p) \arrow[d, dash, "\frac{p-1}{2}"] \\ F \arrow[d, dash, "2"] \\ \mathbb{Q} \end{tikzcd}$$

Por ejemplo, si $p = 7$, el subgrupo de $(\mathbb{Z}/7\mathbb{Z})^\times$ generado por 2 tiene 3 elementos, y entonces F es el subcampo fijo por el automorfismo $\sigma\colon \zeta_7 \mapsto \zeta_7^2$, y se puede calcular que este es $\mathbb{Q}(\sqrt{-7})$.

Tenemos la siguiente situación:

$$\begin{tikzcd} \mathbb{Z}[\zeta_p] \arrow[d, dash] & \subset & \mathbb{Q}(\zeta_p) \arrow[d, dash] \\ \mathcal{O}_F \arrow[d, dash] & \subset & F \arrow[d, dash] \\ \mathbb{Z} & \subset & \mathbb{Q} \end{tikzcd}$$

Si un primo racional $q \in \mathbb{Z}$ se ramifica en $\mathcal{O}_F$, esto significa que (dado que se trata de un campo cuadrático)

$$q\mathcal{O}_F = \mathfrak{p}^2.$$

Ahora

$$q\mathcal{O}_K = \mathfrak{p}^2\mathcal{O}_K.$$

El ideal $\mathfrak{p} \subset \mathcal{O}_L$ puede factorizarse en $\mathcal{O}_K$, pero de todas maneras, habrá ramificación.

Ahora $K = \mathbb{Q}(\zeta_p)$, así que el único primo que puede ramificarse en K es p. Por otra parte, si $F = \mathbb{Q}(\sqrt{d})$, entonces todos los divisores $q \mid d$ se ramifican en F. Esto nos dice que $d = \pm p$, falta solo determinar el signo. Como vimos, si $d \equiv 2, 3 \pmod{4}$, entonces 2 también se ramifica, y luego necesariamente

$$d = \pm p \equiv 1 \pmod{4}.$$

Esto nos dice que $d = (-1)^{(p-1)/2}\, p$.

Por ejemplo, si $p = 7$, entonces hay ramificación

$$\begin{aligned} 7\mathbb{Z}\Big[\frac{1+\sqrt{-7}}{2}\Big] &= (\sqrt{-7})^2, \\ 7\mathbb{Z}[\zeta_7] &= (1-\zeta_7)^6. \end{aligned}$$

El ideal $(\sqrt{-7})$ no es primo en $\mathbb{Z}[\zeta_7]$: tenemos la factorización $\sqrt{-7}\mathbb{Z}[\zeta_7] = (1-\zeta_7)^3$. Usando las sumas de Gauss, se puede obtener la expresión

$$\sqrt{-7} = \sum_{1 \le a \le 6} \left(\frac{a}{7}\right) \zeta_7^a = 1 + 2\zeta_7 + 2\zeta_7^2 + 2\zeta_7^4,$$

pero ¡el punto de este ejercicio es evitar las sumas de Gauss! $\square$