Teoría de números algebraicos
Tarea 6

Alexey Beshenov (alexey.beshenov@cimat.mx)

8 de octubre de 2020

Ejercicio 6.1. Para un campo cuadrático $\mathbb{Q}(\sqrt{d})$ encuentre n tal que $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_n)$.

Solución. Tenemos $\sqrt{-1} \in \mathbb{Q}(\zeta_4)$ y $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8)$. Si p es un primo impar, sabemos que $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$, donde $p^* = (-1)^{\frac{p-1}{2}} p$ (véase la tarea 3). Si $p \equiv 3 \pmod 4$, de todos modos $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$. Ahora si d es un entero libre de cuadrados, podemos factorizarlo como $\pm 2^e p_1 \cdots p_s$, donde $e = 0, 1$ y los p_i son impares, y las consideraciones de arriba nos dicen que $\mathbb{Q}(\sqrt{d})$ es un subcampo de $\mathbb{Q}(\zeta_{8p_1 \cdots p_s})$.

Este es un caso particular del teorema de Kronecker–Weber que afirma que cualquier campo abeliano $K/\mathbb{Q}$ se encaja en un campo ciclotómico. □

Ejercicio 6.2. Para $K = \mathbb{Q}(\sqrt[4]{2}, i)$ calcule el grupo $\mathrm{Gal}(K/\mathbb{Q})$ y describa los subcampos de K.

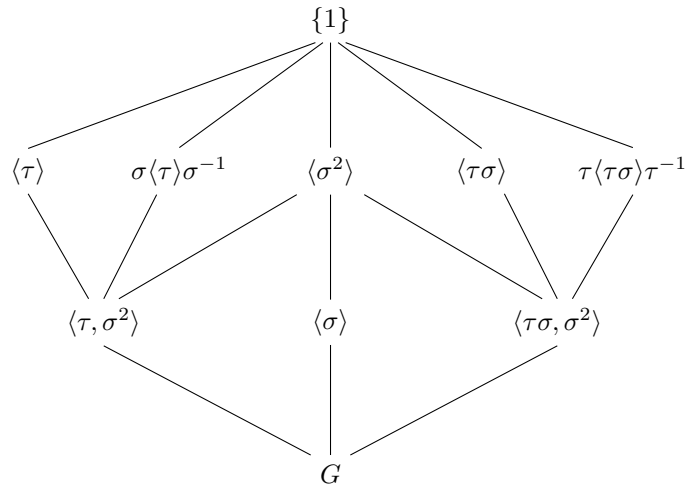
Solución. Primero hay que ver que $K/\mathbb{Q}$ es una extensión de Galois. Esto se sigue del hecho de que K es el campo de descomposición del polinomio

$$x^4 - 2 = (x - \sqrt[4]{2})\,(x + \sqrt[4]{2})\,(x - i\sqrt[4]{2})\,(x + i\sqrt[4]{2}).$$

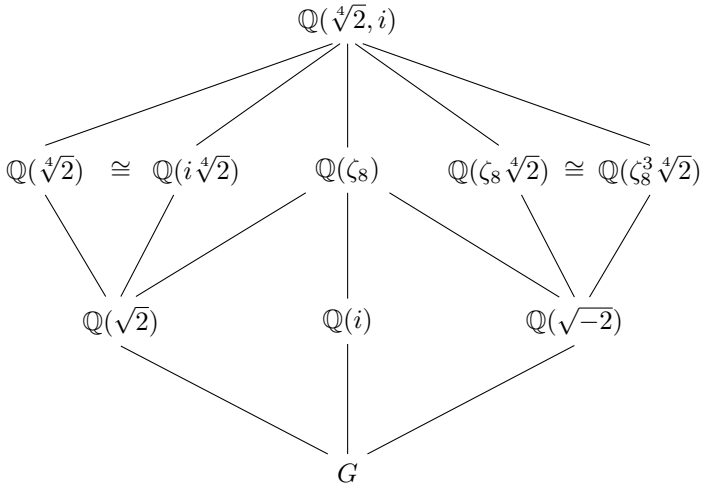
Se trata del compositum de campos $\mathbb{Q}(\sqrt[4]{2})$ y $\mathbb{Q}(i)$, y como una base de K sobre $\mathbb{Q}$ podemos tomar

$$1,\ 2^{1/4},\ 2^{1/2},\ 2^{3/4},\ i,\ i2^{1/4},\ i2^{1/2},\ i2^{3/4}.$$

Hay dos automorfismos evidentes: $\sigma\colon \sqrt[4]{2} \mapsto i\sqrt[4]{2}$ de orden 4 y $\tau\colon i \mapsto -i$ de orden 2 (la conjugación compleja). Calculamos que $\sigma\tau = \tau\sigma^3 \neq \tau\sigma$. De estas consideraciones se ve que σ y τ generan un grupo de 8 elementos que será isomorfo al grupo diédrico D_4 (también conocido como D_8). Aquí está el diagrama de subgrupos. Hay 5 subgrupos de índice 4 y 3 subgrupos de índice 2.



Es un poco trabajoso, pero no es muy difícil calcular uno por uno los subcampos fijos correspondientes.



(Para verificar los cálculos, note que $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$.) □

Ejercicio 6.3. Consideremos el campo bicuadrático $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$.

1) Describa cómo los primos racionales se factorizan en $\mathcal{O}_K$.

2) Calcule la densidad de primos que corresponden a cada tipo de descomposición.

Solución. En K tenemos tres subcampos cuadráticos:

$$F_1 = \mathbb{Q}(\sqrt{-3}), \quad F_2 = \mathbb{Q}(\sqrt{5}), \quad F_3 = \mathbb{Q}(\sqrt{-15}).$$

La descomposición en F_i se determina por los símbolos de Legendre correspondientes. Todo depende del resto de p módulo 15:

$$\left(\frac{-3}{p}\right) = \begin{cases} +1, & p \equiv 1 \pmod 3, \\ -1, & p \equiv 2 \pmod 3; \end{cases}$$

$$\left(\frac{5}{p}\right) = \begin{cases} +1, & p \equiv 1, 4 \pmod 5, \\ -1, & p \equiv 2, 3 \pmod 5; \end{cases}$$

$$\left(\frac{-15}{p}\right) = \begin{cases} +1, & p \equiv 1, 2, 4, 8 \pmod{15}, \\ -1, & p \equiv 7, 11, 13, 14 \pmod{15}. \end{cases}$$

La extensión $K/\mathbb{Q}$ es de Galois, así que $e_p\, f_p\, g_p = 4$. Primero podemos ver qué pasa con los primos ramificados. Tenemos $K = F_1F_2$ y los disciminantes son $\Delta_{F_1} = -3$, $\Delta_{F_2} = 5$, así que $\Delta_K = 3^2 \cdot 5^2$, y los primos ramificados en K son 3 y 5.

Si $p = 3$, entonces p se ramifica en F_1 y es inerte en F_2. Esto quiere decir que $2 \mid e_3$ y $2 \mid f_3$, así que el tipo de descomposición será $\mathfrak{p}^2$.

Si $p = 5$, entonces p se ramifica en F_2 y es inerte en F_1, así que el tipo de descomposición es $\mathfrak{p}^2$.

Para los primos no ramificados se cumple $f_p\, g_p = 4$.

Si p se escinde en uno de los subcampos cuadráticos, pero es inerte en otro, entonces $2 \mid f_p$ y $g_p \geq 2$, así que el tipo de descomposición será $\mathfrak{p}_1\, \mathfrak{p}_2$, donde $f = f' = 2$. Los primos correspondientes son los siguientes.

- Si $p \equiv 2, 8 \pmod{15}$, entonces p es inerte en F_1 y F_2, pero se escinde en F_3.
- Si $p \equiv 7, 13 \pmod{15}$, entonces p se escinde en F_1, pero es inerte en F_2 y F_3.
- Si $p \equiv 11, 14 \pmod{15}$, entonces p es inerte en F_1 y F_3, pero se escinde en F_2.

Nos queda el caso de $p \equiv 1, 4 \pmod{15}$ cuando p se escinde en los tres subcampos cuadráticos. Nos gustaría probar que en este caso la factorización tiene forma $p\mathcal{O}_K = \mathfrak{p}_1\, \mathfrak{p}_2\, \mathfrak{p}_3\, \mathfrak{p}_4$. Esto es equivalente a probar que para todo ideal primo $\mathfrak{p} \subset \mathcal{O}_K$ tal que $\mathfrak{p} \mid p$ se tiene $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = 1$. En otras palabras, hay que ver que para todo $\alpha \in \mathcal{O}_K$ existe un entero racional $a \in \mathbb{Z}$ tal que $\alpha \equiv a \pmod{\mathfrak{p}}$. Consideremos los ideales $\mathfrak{p}_1 = \mathfrak{p} \cap \mathcal{O}_{F_1}$ y $\mathfrak{p}_2 = \mathfrak{p} \cap \mathcal{O}_{F_2}$. Estos son ideales primos en $\mathcal{O}_{F_1}$ y $\mathcal{O}_{F_2}$ respectivamente. Por nuestra hipótesis, se tiene $[\mathcal{O}_{F_1}/\mathfrak{p}_1 : \mathbb{F}_p] = 1$ y $[\mathcal{O}_{F_2}/\mathfrak{p}_2 : \mathbb{F}_p] = 1$. En otras palabras, cualquier elemento $\alpha \in \mathcal{O}_{F_i}$ es congruente a algún entero racional módulo $\mathfrak{p}_i$. Ahora $K = F_1F_2$, y todo elemento $\alpha \in \mathcal{O}_K$ tiene forma $\sum_i \alpha_i\beta_i$, donde $\alpha_i \in \mathcal{O}_{F_1}$ y $\beta_i \in \mathcal{O}_{F_2}$. Dado que $\mathfrak{p} \mid \mathfrak{p}_1\mathcal{O}_K$ y $\mathfrak{p} \mid \mathfrak{p}_2\mathcal{O}_K$, sabemos que cada α_i y β_i se reduce a un entero racional módulo $\mathfrak{p}$, y por ende $\sum_i \alpha_i\beta_i$ cumple con la misma propiedad. Esto termina la prueba.

Notamos que el argumento que acabamos de ver se generaliza al siguiente resultado. Si un primo racional $p \in \mathbb{Z}$ se factoriza en $[K : \mathbb{Q}]$ ideales primos en

$\mathcal{O}_K$, entonces se dice que p **se escinde completamente** en K. Ahora si K es el compositum de F_1 y F_2, y p se escinde completamente en F_1 y F_2, entonces este también se escinde completamente en K.

Según el teorema de Dirichlet sobre primos en progresiones aritméticas, las densidades son entonces $\frac{3}{4}$ para $\mathfrak{p}_1\,\mathfrak{p}_2$ y $\frac{1}{4}$ para $\mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$. □

Ejercicio 6.4. Sea p un número primo y χ el carácter de Dirichlet de orden 2 mód p, definido por el símbolo de Legendre $\chi(n) = \left(\frac{n}{p}\right)$.

1) Demuestre que $\exp(g(\chi)\,L(1,\chi)) = \prod_n(1-\zeta_p^n)\prod_r(1-\zeta_p^r)^{-1}$, donde $g(\chi) = \sum_{1\le a\le p-1}\chi(a)\,\zeta_p^a$, y los productos son sobre los no-residuos y residuos cuadráticos mód p respectivamente.

2) Use la parte anterior para calcular $L(1,\chi)$, donde χ es el carácter de orden 2 mód 5. (Para el valor numérico en PARI/GP, basta digitar `lfun(5,1)`)

Solución. Denotemos

$$P = \prod_n(1-\zeta_p^n)\prod_r(1-\zeta_p^r)^{-1}.$$

Tenemos

$$\log P = \sum_n \log(1-\zeta_p^n) - \sum_r \log(1-\zeta_p^r) = \sum_a -\chi(a)\,\log(1-\zeta_p^a).$$

La serie $-\log(1-z) = \sum_{n\ge1}\frac{z^n}{n}$ converge para $|z|<1$ y también converge para $z=\zeta_p^r$ (el teorema de Abel). Podemos escribir

$$\log P = \sum_{m\ge1}\frac{1}{m}\sum_a \chi(a)\,\zeta_p^{am}.$$

Ahora ocupamos la identidad para las sumas cuadráticas de Gauss

$$\sum_a \chi(a)\,\zeta_p^{am} = g(\chi)\,\chi(m).$$

Entonces,

$$\log P = \sum_a \chi(a)\sum_{m\ge1}\frac{\chi(m)}{m} = g(\chi)\,L(1,\chi).$$

Esto establece la identidad deseada $\exp(g(\chi)\,L(1,\chi)) = P$.

En particular, si $p=5$, calculamos

$$g(\chi) = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$$

y

$$P = \frac{(1-\zeta_5^2)\,(1-\zeta_5^3)}{(1-\zeta_5)\,(1-\zeta_5^4)} = 1-\zeta_5^2-\zeta_5^3 = \frac{3+\sqrt{5}}{2}.$$

Ahora

$$L(1,\chi) = \frac{1}{\sqrt{5}} \log \frac{3+\sqrt{5}}{2}.$$

Lo podemos confirmar con PARI/GP:

```
? 1/sqrt(5) * log ((3 + sqrt(5))/2)
% = 0.43040894096400403888943323295060542543
? lfun (5,1)
% = 0.43040894096400403888943323295060542542
```

De manera similar, si $p = 3$, entonces $g(\chi) = \zeta_3 - \zeta_3^2 = \sqrt{-3}$ y $P = \frac{1-\zeta_3^2}{1-\zeta_3} = 1 + \zeta_3 = \zeta_6$. Así nos quedamos con la fórmula

$$\exp(2\pi i/6) = \exp(\sqrt{-3}\, L(1,\chi)).$$

Entonces (módulo $2\pi i\mathbb{Z}$) se cumple $\frac{2\pi i}{6} = i\sqrt{3}\, L(1,\chi)$. De aquí $L(1,\chi) = \frac{\pi}{3\sqrt{3}}$.

```
? lfun (-3,1)
% = 0.60459978807807261686469275254738524409
? Pi/(3*sqrt(3))
% = 0.60459978807807261686469275254738524409
```

□

Ejercicio 6.5. Consideremos funciones $f, g\colon \mathbb{Z}_{>1} \to \mathbb{C}$ y las series de Dirichlet correspondientes $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$ y $G(s) = \sum_{n\geq 1} \frac{g(n)}{n^s}$.

1) Demuestre que cuando las series convergen absolutamente en s, se tiene $F(s)\cdot G(s) = \sum_{n\geq 1} \frac{(f*g)(n)}{n^s}$, donde $(f*g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$.

2) Sean $\mu(n)$ la función de Möbius, $\tau(n)$ el número de divisores, $\sigma(n) = \sum_{d|n} d$ la suma de divisores, y $\phi(n)$ la función de Euler. Demuestre que

$$\sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)},\ \sum_{n\geq 1} \frac{\tau(n)}{n^s} = \zeta(s)^2,\ \sum_{n\geq 1} \frac{\sigma(n)}{n^s} = \zeta(s)\,\zeta(s-1),\ \sum_{n\geq 1} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

Solución. Usando la convergencia absoluta, podemos cambiar el orden de términos y escribir

$$F(s)\cdot G(s) = \Big(\sum_{m\geq 1} \frac{f(m)}{m^s}\Big)\cdot\Big(\sum_{n\geq 1} \frac{g(n)}{n^s}\Big) = \sum_{m,n\geq 1} \frac{f(m)\, g(n)}{(mn)^s} = \sum_{n\geq 1}\sum_{d|n} \frac{f(d)\, g(n/d)}{n^s}.$$

Además, la serie que acabamos de obtener también converge absolutamente en s, dado que

$$\sum_{n\geq 1}\frac{|(f*g)(n)|}{|n^s|}\leq \sum_{n\geq 1}\sum_{d|n}\frac{|f(d)|\cdot|g(n/d)|}{|n^s|}=\Big(\sum_{m\geq 1}\frac{|f(s)|}{|n^s|}\Big)\cdot\Big(\sum_{n\geq 1}\frac{|g(s)|}{|n^s|}\Big)<\infty.$$

La serie $\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}$ converge absolutamente para $\operatorname{Re} s>1$, así que la serie $\sum_{n\geq 1}\frac{\mu(n)}{n^s}$ converge absolutamente para $\operatorname{Re} s>1$.

Denotemos por 1 la función constante $n\mapsto 1$. Tenemos

$$(\mu*1)(n)=\sum_{d|n}\mu(d)=\begin{cases}1, & \text{si } n=1,\\ 0, & \text{si } n>1.\end{cases}.$$

De hecho, escribiendo $n=p_1^{e_1}\cdots p_s^{e_s}$, para $n>1$, tenemos

$$\sum_{d|n}\mu(d)=\sum_{(e_1,\ldots,e_n)}\mu(p_1^{e_1}\cdots p_s^{e_s}),$$

donde $e_i=0$ o 1. Luego,

$$\sum_{d|n}\mu(d)=1-s+\binom{s}{2}-\binom{s}{3}+\cdots+(-1)^s=(1-1)^s=0.$$

Para la segunda identidad, calculamos

$$(1*1)(n)=\sum_{d|n}1=\tau(n).$$

Entonces, $\zeta(s)^2=\sum_{n\geq 1}\frac{\tau(n)}{n^s}$, y esta serie converge absolutamente para $\operatorname{Re} s>1$.

Para la tercera identidad, notamos que

$$\zeta(s-1)=\sum_{n\geq 1}\frac{1}{n^{s-1}}=\sum_{n\geq 1}\frac{n}{n^s},$$

y esta serie converge absolutamente para $\operatorname{Re} s>2$. Calculamos entonces

$$(1*id)(n)=\sum_{d|n}d=\sigma(n).$$

Entonces, $\zeta(s)\,\zeta(s-1)=\sum_{n\geq 1}\frac{\sigma(n)}{n^s}$, y esta serie converge absolutamente para $\operatorname{Re} s>2$.

En fin, para la última identidad, calculamos

$$\frac{\zeta(s-1)}{\zeta(s)}=\Big(\sum_{m\geq 1}\frac{m}{m^s}\Big)\cdot\Big(\sum_{n\geq 1}\frac{\mu(n)}{n^s}\Big).$$

Ahora

$$(id * \mu)(n) = \sum_{d|n} \mu(d)\, \frac{n}{d} = \phi(n).$$

Esto se sigue de la fórmula $\sum_{d|n} \phi(d) = n$ y la inversión de Möbius. Entonces, podemos concluir que $\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n\geq 1} \frac{\phi(n)}{n^s}$, y esta serie converge absolutamente para $\operatorname{Re} s > 2$. □