Introducción a los Números Algebraicos
Clase 7: Cuerpos cuadráticos

Gonzalo Tornaría

10 de abril, 2007

5 Cuerpos cuadráticos

Un *cuerpo cuadrático* es una extensión $K/\mathbb{Q}$ de grado 2. Cualquier cuerpo cuadrático puede escribirse como $K = \mathbb{Q}(\sqrt{m})$ (ejercicio 12a). En efecto, si $\alpha \in K$ es un elemento de grado 2, es raíz de un polinomio irreducible $aX^2 + bX + c \in \mathbb{Z}[X]0$. Es fácil ver que, entonces, $K = \mathbb{Q}(\sqrt{b^2 - 4ac})$.

Por otra parte, si $K = \mathbb{Q}(\sqrt{m})$, podemos suponer que $m \in \mathbb{Z}$ y es libre de cuadrados (si $m = m_1 m_2^2$ entonces $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{m_1})$.) Además m libre de cuadrados determina K (ejercicio 12b).

Ya hemos observado que K tiene un automorfismo no trivial dado por $\sqrt{m} \mapsto -\sqrt{m}$. Se sigue pues que K es una extensión normal (o de Galois). Su grupo de Galois es el grupo de 2 elementos.

Todos los elementos de K son de la forma $\alpha = a + b\sqrt{m}$, y el automorfismo no trivial lleva α en $\alpha' = a - b\sqrt{m}$. Luego, $T(\alpha) = \alpha + \alpha' = 2a$, y $N(\alpha) = \alpha\alpha' = a^2 - mb^2$.

5.1 Enteros cuadráticos

Si α es un entero algebraico entonces $T(\alpha), N(\alpha) \in \mathbb{Z}$. Esto es cierto en cualquier cuerpo de números, pero en el caso particular de cuerpos cuadráticos el recíproco es cierto: si $T(\alpha), N(\alpha) \in \mathbb{Z}$, entonces α, siendo raíz de

$$X^2 - T(\alpha)X + N(\alpha) \in \mathbb{Z}[X],$$

será un entero algebraico.

De esta manera es posible determinar $\mathcal{O}_K$ (ejercicio 14): si $m \equiv 2, 3 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Pero si $m \equiv 1 \pmod 4$, entonces $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{m}}{2}$. Para abreviar puede decirse que $\mathcal{O}_K = \mathbb{Z}[\frac{\Delta+\sqrt{\Delta}}{2}]$ en cualquier caso (verificar).

Utilizando esta base entera de $\mathcal{O}_K$ podemos calcular el discriminante de un cuerpo cuadrático:

Si $m \equiv 2, 3 \pmod 4$, entonces $\{1, \sqrt{m}\}$ es una base entera de $\mathcal{O}_K$. Podemos calcular $\Delta(1, \sqrt{m})$ de dos maneras diferentes:

$$\Delta(1, \sqrt{m}) = \det \begin{pmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{pmatrix}^2 = (-2\sqrt{m})^2 = 4m,$$

o usando la forma bilineal dada por la traza

$$\Delta(1, \sqrt{m}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} = 4m,$$

ya que $T(1) = 2$, $T(\sqrt{m}) = 0$, y $T(m) = 2m$.

Si $m \equiv 1 \pmod 4$ podemos observar que $\mathcal{O}_K$ contiene a $\mathbb{Z}[\sqrt{m}]$ con índice 2. Según el cálculo anterior $\Delta(\mathbb{Z}[\sqrt{m}]) = 4m$ y se sigue que $\Delta(\mathcal{O}_K) = m$. También es posible calcularlo directamente usando la base entera

$$\Delta\left(1, \frac{1+\sqrt{m}}{2}\right) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{pmatrix}^2 = (-\sqrt{m})^2 = m,$$

o utilizando la forma bilineal correspondiente a la traza

$$\Delta\left(1, \frac{1+\sqrt{m}}{2}\right) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+m}{2} \end{pmatrix} = m.$$

Observemos que el discriminante Δ determina unívocamente el cuerpo cuadrático. Y cualquier $\Delta \equiv 1 \pmod 4$ libre de cuadrados o $\Delta = 4m$ con $m \equiv 2, 3 \pmod 4$ libre de cuadrados es discriminante de algún cuerpo cuadrático.

Definición 5.1.1. Un *discriminante fundamental* es un número $\Delta \equiv 1 \pmod 4$ libre de cuadrados o $\Delta = 4m$ donde $m \equiv 2, 3 \pmod 4$ es libre de cuadrados.

Dicho de otro modo los discriminantes fundamentales son los números que son discriminantes de cuerpos cuadráticos.

5.2 Factorización de primos

Investiguemos ahora la factorización de primos racionales en K Sea $p \in \mathbb{Z}$ un primo. Por 3.5.3 y 3.5.7 sabemos que $efg = 2$, de modo que tenemos tres casos:

1. $e = 2$, $f = g = 1$, es decir que $(p) = \mathfrak{p}^2$ con $\mathfrak{p}$ un primo de grado 1. En este caso decimos que p *ramifica.*

2. $g = 2$, $e = f = 1$, es decir que $(p) = \mathfrak{p}\mathfrak{p}'$ con $\mathfrak{p} \neq \mathfrak{p}'$ primos de grado 1. Decimos que p *descompone.*

3. $f = 2$, $e = g = 1$, es decir que $(p) = \mathfrak{p}$ es un primo de grado 2 en $\mathcal{O}_K$. Decimos que (p) es *inerte.*

Podemos usar el Teorema 3.6.1, que siempre puede aplicarse en el caso de cuerpos cuadráticos, para determinar cuál de los tres casos ocurre para cada p. En efecto, p se factoriza según lo hace módulo p un polinomio cuadrático mónico que tiene discriminante $\Delta(\mathcal{O}_K)$. Pero en cualquier cuerpo (de característica $\neq 2$) se cumple que un polinomio cuadrático:

1. es un cuadrado perfecto sii tiene una raíz repetida sii su discriminante es 0;

2. es producto de dos polinomios lineales distintos sii su discriminante es un cuadrado distinto de cero;

3. es irreducible sii su discriminante no es un cuadrado.

Dicho de otro modo, la ramificación, descomposición, o inercia de un primo racional p impar depende exclusivamente del símbolo de Legendre $\left(\frac{\Delta(\mathcal{O}_K)}{p}\right)$:

$$\left(\frac{\Delta}{p}\right) := \begin{cases} 0 & \text{si } \Delta \equiv 0 \pmod p; \\ +1 & \text{si } \Delta \text{ es un cuadrado no nulo módulo } p; \\ -1 & \text{si } \Delta \text{ no es un cuadrado módulo } p. \end{cases}$$

Asímismo puede verse que la ramificación, descomposición, o inercia de 2 en $\mathcal{O}_K$ depende de la siguiente extensión del símbolo de Legendre (conocido como *símbolo de Kronecker*):

$$\left(\frac{\Delta}{2}\right) := \begin{cases} 0 & \text{si } \Delta \equiv 0 \pmod 4; \\ +1 & \text{si } \Delta \equiv 1 \pmod 8; \\ -1 & \text{si } \Delta \equiv 5 \pmod 8. \end{cases}$$

Es importante destacar una de las versiones de la *ley de reciprocidad cuadrática*, que afirma que (asumiendo $\Delta \equiv 0, 1 \pmod 4$), el símbolo de Legendre $\left(\frac{\Delta}{p}\right)$ depende tan solo de $p \bmod \Delta$. Más concretamente, suponiendo Δ impar, se tiene $\left(\frac{\Delta}{p}\right) = \left(\frac{p}{|\Delta|}\right)$, y algo similar ocurre para los casos en que Δ es par. En todo caso se puede observar que el valor del símbolo de Legendre divide a las clases módulo Δ (coprimas con Δ) en dos partes iguales.

Proposición 5.2.1. *Los primos racionales que ramifican en $\mathcal{O}_K$ son un número finito (son los divisores de $\Delta(\mathcal{O}_K)$. Con estos resultados puede probarse que tanto los primos racionales que descomponen en $\mathcal{O}_K$ como aquellos que son inertes en $\mathcal{O}_K$ son infinitos en número. Más aún, "la mitad" de los primos descomponen y "la otra mitad" son inertes (en el sentido del ejercicio 34).*

Demostración. Para ver ésto hay que utilizar el Teorema de Dirichlet que asegura que en toda progresión aritmética (sin factores triviales) hay infinitos números primos. Los resultados anteriores indican que los primos que descomponen o los primos que ramifican son los que pertenecen a ciertas progresiones aritméticas. El Teorema de Dirichlet es más fuerte aún: para un módulo fijo Δ, los primos se dividen "en partes iguales" entres las $\varphi(\Delta)$ progresiones aritméticas módulo Δ. Resta mostrar que las clases módulo Δ se dividen en dos partes iguales correspondientes al caso p descompone y p inerte: esto se sigue de la Ley de Reciprocidad Cuadrática. □

En la demostración hemos utilizado dos teoremas no triviales: la Ley de Reciprocidad Cuadrática (daremos una demostración más adelante utilizando cuerpos ciclotómicos), y el Teorema de Dirichlet de los primos en progresiones aritméticas, cuya demostración utiliza herramientas de Análisis Complejo.

Para una versión explícita de la factorización de primos racionales en cuerpos cuadráticos, ver el ejercicio 29.

Ejemplo 5.2.2. Sea $K = \mathbb{Q}[\sqrt{5}]$, de modo que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ tiene discriminante $\Delta = 5$. El único primo racional ramificado es $5 = (\sqrt{5})^2$. Para cualquier otro p se tiene, por la Ley de Reciprocidad Cuadrática,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod 5, \\ -1 & \text{si } p \equiv \pm 2 \pmod 5. \end{cases}$$

De modo que los primos $p \equiv \pm 1$ descomponen y aquellos $p \equiv \pm 2$ son inertes.

5.3 Unidades

Determinemos la estructura del grupo de unidades en $\mathcal{O}_K$, según m. Ya hemos observado que $\alpha \in \mathcal{O}_K$ es una unidad si y sólo si $N(\alpha) = \pm 1$ (como en ejercicios 1b, 7a). Llamemos U_Δ al grupo de unidades de $\mathcal{O}_K$ donde $\Delta = \Delta(\mathcal{O}_K)$. Consideramos primero los cuerpos cuadráticos imaginarios.

Proposición 5.3.1. *Si $\Delta < -4$, entonces $U_\Delta = \{\pm 1\}$ es un grupo cíclico de orden 2. Por otra parte, $U_{-4} = \{\pm 1, \pm i\}$ es un grupo cíclico de orden 4, y $U_{-3} = \left\{\pm 1, \pm e^{\frac{\pi i}{3}}, \pm e^{\frac{2\pi i}{3}}\right\}$ es un grupo cíclico de orden 6.*

Demostración. Ejercicios 16a, 1b, 7a. Esencialmente se trata de resolver la ecuación diofántica $x^2 + |\Delta| y^2 = 4$. Cuando $\Delta < -4$ es claro que $y = 0$, mientras que si $\Delta = -4, -3$ hay también soluciones con $y = \pm 1$. □

El caso de los cuerpos cuadráticos reales es considerablemente más difícil, y U_Δ es infinito para $\Delta > 0$ (ver ejercicio 17 para $\Delta = 8$).

Proposición 5.3.2. *Si $\Delta > 0$, entonces existe una (única) unidad $\varepsilon > 1$ tal que $U_\Delta = \{\pm\varepsilon^i \,:\, i \in \mathbb{Z}\}$. Como grupo, $U_\Delta \cong \{\pm 1\} \times \mathbb{Z}$.*

Demostración. Es un caso particular del Teorema de las unidades de Dirichlet. Notemos primero que $\mathcal{O}_K$, siendo real, no contiene raíces de la unidad otras que ± 1, de modo que su subgrupo de torsión es $\{\pm 1\}$. Consideremos el mapa $\varphi : K \to \mathbb{R}^2$ dado por

$$\varphi(\alpha) := (\log|\alpha|, \log|\alpha'|),$$

donde α' es el conjugado de α. Este mapa restringe a un homomorfismo de grupos $\varphi : U_\Delta \to \mathbb{R}^2$, cuya imagen está contenida en el subespacio $H = \{(x, y) \,:\, x + y = 0\}$, de dimensión 1, y cuyo núcleo es claramente $\{\pm 1\}$. Para demostrar la proposición alcanza probar

1. que $\varphi(U_\Delta) \neq \{(0, 0)\}$;
2. que $\varphi(U_\Delta)$ es discreto en H.

Pues en tal caso podemos elegir $\epsilon \in U_\Delta$ tal que $\varphi(\epsilon) = (x, y)$ con $x > 0$ el mínimo posible en $\varphi(U_\Delta)$. Cambiando eventualmente ϵ por $-\epsilon$ se sigue que $\epsilon > 1$ es una unidad, y un argumento estándar muestra que cualquier unidad tendrá que ser $\pm\epsilon^i$ con $i \in \mathbb{Z}$ (solamente estamos diciendo que $\varphi(U_\Delta)$ es un subgrupo cíclico infinito generado por $\varphi(\epsilon)$, lo que es cierto para cualquier subgrupo discreto de un espacio vectorial de dimensión 1). □

Lema 5.3.3. *Dado $M > 0$, hay un número finito de enteros $\alpha \in \mathcal{O}_K$ tales que* $\max(|\alpha|, |\alpha'|) \leq M$.

Demostración. Ejercicio 35. □

Lema 5.3.4. *Dado $n > 0$ entero racional existen soluciones no triviales en $\mathbb{Z}$ a la* ecuación de Pell

$$x^2 - ny^2 = 1.$$

Demostración. Ejercicio 36. □

La única unidad como en la Proposición (i.e. $\epsilon > 1$ generador de las unidades positivas) se llama *unidad fundamental.*

Ejemplo 5.3.5. Sea $K = \mathbb{Q}[\sqrt{2}]$, con $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ de discriminante $\Delta = 8$. Entonces $1 + \sqrt{2}$ es una unidad de $\mathcal{O}_K$ (ejercicio 17a). Por ser la unidad "más pequeña" (es fácil verificar que $x^2 - 2y^2 = \pm 1$ no tiene soluciones más chicas), se sigue que tiene que ser la unidad fundamental. Esto significa que las soluciones encontradas en 17b son *todas* las soluciones de la ecuación $x^2 - 2y^2 = \pm 1$.

Ejemplo 5.3.6. La unidad fundamental puede ser bastante grande: por ejemplo, para $\mathbb{Q}[\sqrt{31}]$ la unidad fundamental es $1520 + 273\sqrt{31}$; para $\mathbb{Q}[\sqrt{46}]$ la unidad fundamental es $24335 + 3588\sqrt{46}$; para $\mathbb{Q}[\sqrt{94}]$ la unidad fundamental es $2143295 + 221064\sqrt{94}$... Para $\mathbb{Q}[\sqrt{991}]$ la unidad fundamental es $379516400906811930638014896080 + 12055735790331359447442538767\sqrt{991}$.

Es posible calcular las unidades fundamentales de un cuerpo de números usando PARI/GP:

```
? K=bnfinit(x^2-94);
? K.fu
[Mod(221064*x - 2143295, x^2 - 94)]
```