Introducción a los Números Algebraicos

Clase 4: Factorización única

Gonzalo Tornaría

22 de marzo, 2007

3 Factorización única

A lo largo de esta sección R será un dominio de Dedekind con cuerpo de fracciones K. El ejemplo fundamental en este curso es el caso en que K es un cuerpo de números y $R = \mathcal{O}_K$.

3.1 El grupo de ideales fraccionales

Definición 3.1.1. Un *ideal fraccional* de R es un R-submódulo de K *distinto de cero* que sea finitamente generado como R-módulo.

Eliminando denominadores resulta que cualquier ideal fraccional de R se puede escribir como $\frac{1}{a}I$ con $a \in R$ e I un ideal entero.

Seguiremos la convención de que todos los ideales son distintos de cero.

Teorema 3.1.2. *Los ideales fraccionales de R forman un grupo abeliano con la multiplicación, con elemento identidad R.*

Lema 3.1.3. *Todo ideal de R contiene un producto de ideales primos.*

Demostración. Sea S el conjunto de los ideales de R que no satisfacen la afirmación, y supongamos que S no es vacío. Como R es noetheriano, existe un ideal I maximal en S. Observemos que I no puede ser primo. Entonces existen $a_1, a_2 \in R$ tales que $a_1 a_2 \in I$ pero $a_i \notin I$. Entonces $J_i = I + (a_i)$ contienen propiamente a I, por lo tanto no están en S (pues I es maximal) y entonces contienen cada uno un producto de ideales primos. Pero $J_1 J_2 = I^2 + a_1 I + a_2 I + (a_1 a_2) \subseteq I$, así que I contiene un producto de primos. □

Lema 3.1.4. *Todo ideal maximal es invertible.*

Demostración. Sea $\mathfrak{p}$ un ideal maximal de R. Mostraremos que

$$\mathfrak{p}^{-1} := \{a \in K \ : \ a\mathfrak{p} \subseteq R\}$$

es un ideal fraccional de R tal que $\mathfrak{p}^{-1}\mathfrak{p} = R$.

Fijemos $a \in \mathfrak{p}$, con $a \neq 0$. En primer lugar $\mathfrak{p}^{-1}$ es un ideal fraccional pues $a\mathfrak{p}^{-1} \subseteq R$ es un ideal entero. Además claramente $R \subseteq \mathfrak{p}^{-1}$, de modo que $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Como $\mathfrak{p}$ es maximal resta probar que $\mathfrak{p} \neq \mathfrak{p}^{-1}\mathfrak{p}$. En caso contrario, como $\mathfrak{p}$ es finitamente generado, tendríamos que todos los elementos de $\mathfrak{p}^{-1}$ son enteros, y como R es integralmente cerrado $\mathfrak{p}^{-1} = R$. Veamos que esto es imposible.

Por el lema anterior podemos elegir m minimal tal que

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subseteq (a) \subseteq \mathfrak{p}.$$

Algúno de los $\mathfrak{p}_i$, digamos $\mathfrak{p}_1$, estará contenido en $\mathfrak{p}$ (pues $\mathfrak{p}$ es primo). Como m es minimal, sabemos que

$$\mathfrak{p}_2 \cdots \mathfrak{p}_m \nsubseteq (a).$$

Sea $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$ con $b \notin (a)$. Entonces $b\mathfrak{p} \subseteq (a)$, i.e. $b/a \in \mathfrak{p}^{-1}$, pero $b/a \notin R$. □

Lema 3.1.5. *Todo ideal es invertible.*

Demostración. Si no fuera cierto, existirá un ideal I maximal entre los no invertibles. Por el lema anterior I no es maximal, así que $I \subsetneq \mathfrak{p}$ para algún ideal maximal $\mathfrak{p}$. Entonces $I \subseteq \mathfrak{p}^{-1}I \subseteq \mathfrak{p}^{-1}\mathfrak{p} = R$ y, como antes, $I \neq \mathfrak{p}^{-1}I$ ó $\mathfrak{p}^{-1}$ sería integral. Entonces $\mathfrak{p}^{-1}I$ es un ideal de R, que tiene que ser invertible (pues I es maximal entre los no invertibles), y se sigue que I también será invertible. □

Demostración del teorema. Lo único que hay que probar es que todo ideal fraccional de R es invertible. Pero los ideales enteros son invertibles por el último Lemma, y todo ideal fraccional se escribe como $\frac{1}{a}I$ con I entero, y por lo tanto tiene como inverso aI^{-1}. □

3.2 Factorización única

Dados dos ideales fraccionales I y J, decimos que $I \mid J$ si JI^{-1} es un ideal entero; equivalentemente, si $J \subseteq I$.

Proposición 3.2.1. *Sea $\mathfrak{p}$ un ideal primo. Si I, J son dos ideales tales que $\mathfrak{p} \mid IJ$, entonces $\mathfrak{p} \mid I$ o $\mathfrak{p} \mid J$.*

Demostración. De otro modo existirían $a \in I$ y $b \in J$ tales que $a \notin \mathfrak{p}$ y $b \notin \mathfrak{p}$. Pero entonces $ab \notin \mathfrak{p}$ y sin embargo $ab \in IJ$. □

Teorema 3.2.2. *Todo ideal entero de R puede escribirse como producto de ideales primos, de manera única salvo el orden.*

Demostración. Supongamos que I es un ideal maximal entre los ideales de R que no pueden escribirse como producto de primos. Entonces $I \subseteq \mathfrak{p}$ con algún ideal maximal $\mathfrak{p} \neq I$. Entonces $I\mathfrak{p}^{-1} \subseteq R$ y además $I \subsetneq I\mathfrak{p}^{-1}$. Por la maximalidad de I, se sigue que $I\mathfrak{p}^{-1}$ es producto de primos, pero entonces I lo será.

Consideremos ahora dos factorizaciones

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

Entonces $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_s$, y por la proposición sabemos que $\mathfrak{p}_1$ tiene que dividir alguno de los $\mathfrak{q}_i$. Entonces $\mathfrak{p}_1 = \mathfrak{q}_i$ y podemos cancelar $\mathfrak{p}_1$ y $\mathfrak{q}_i$ en la ecuación multiplicando por el inverso. La unicidad se sigue por inducción completa en $r + s$. □

Corolario 3.2.3. *Los ideales fraccionales de R forman un grupo abeliano libre con base el conjunto de ideales primos de R.*

Demostración. Lo que es lo mismo, todo ideal fraccional de R puede escribirse como producto de ideales primos o sus inversos, de manera única salvo el orden. En efecto, un ideal fraccional es de la forma $\frac{1}{a}I$ con I entero. Podemos aplicar el teorema a I y a (a), cancelando los primos que aparezcan en ambas descomposiciónes, etc. □

Corolario 3.2.4. *Si R es un dominio de Dedekind de factorización única, entonces es principal.*

Demostración. Alcanza probar que todo ideal primo $\mathfrak{p}$ es principal. Sea $a \in \mathfrak{p}$, $a \neq 0$. Como R es de factorización única, $a = p_1^{m_1} \cdots p_r^{m_r}$ donde $p_1, \ldots, p_r$ son irreducibles de R. Como $a \in \mathfrak{p}$ y $\mathfrak{p}$ es primo, se sigue que $p_j \in \mathfrak{p}$ para algún j. Luego $(p_j) \subseteq \mathfrak{p}$. Pero en un dominio de factorización única, un elemento irreducible genera un ideal maximal, luego $(p_j) = \mathfrak{p}$. □

Los dos teoremas que hemos demostrado son propiedades muy importantes de los dominios de Dedekind. Más aún, cualquiera de ellos caracteriza a los dominios de Dedekind:

Teorema 3.2.5. *Sea R un dominio integral y K su cuerpo de fracciones. Son equivalentes*

1. *R es un dominio de Dedekind;*
2. *Todo ideal de R es producto único de ideales primos;*
3. *Todo ideal de R es producto de ideales primos;*
4. *Todo ideal de R es invertible.*

Demostración. Ver Teorema 1, §I.3 en [Jones]. □

Ejemplo 3.2.6. Recordemos el ejemplo de $K = \mathbb{Q}[\sqrt{-5}]$. Como $-5 \equiv 3 \pmod 4$, sabemos que $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. En el ejercicio 18 se muestra que $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ es un ejemplo de factorización no única en irreducibles de $\mathcal{O}_K$. Se puede ver que

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

(ejercicio 26). Igualmente, se verifica que

$$(1 + \sqrt{-5}) = (2, 1 + \sqrt{-5})\,(3, 1 + \sqrt{-5}),$$
$$(1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})\,(3, 1 - \sqrt{-5}),$$

de modo que las dos factorizaciones de 6 son iguales.

Ejemplo 3.2.7. El ejemplo anterior puede calcularse con PARI/GP de la siguiente manera:

```
? K=nfinit(x^2+5);
? idealfactor(K,6)
[ 2, [1, 1]~, 2, 1, [1, 1]~] 2]
[ 3, [-1, 1]~, 1, 1, [1, 1]~] 1]
[ 3, [1, 1]~, 1, 1, [-1, 1]~] 1]
```