Introduction to Algebraic Number Theory
Lecture 7

Andrei Jorza

2014-01-29

Today: traces and norms, discriminants and integral bases. Textbook here is `http://wstein.org/books/ant/ant.pdf`

4 Dedekind domains

(4.6) We are ready for unique factorization in Dedekind domains. For clarity, start with a lemma.

Lemma 1. *Suppose R is a Dedekind domain and I, J are fractional ideals. If $I = IJ$ then $J \subset R$.*

Proof. We already did this implicitly in the prood of the fact that every ideal is invertible. Here is a sketch:

The fractional ideal I is finitely generated over $\mathbb{Z}$ and so $I = \oplus \mathbb{Z}\alpha_i$ for some α_i. If $x \in J$ then x acting by multiplication on I (since $I = IJ$) has $x\alpha_i = \sum m_{ij}\alpha_j$ and so multiplication by x on I is the same as multiplication on $\oplus\mathbb{Z}\alpha_i$ by the matrix $(m_{ij}) \in M_{n\times n}(\mathbb{Z})$. Multiplication by x thus satisfies, by Cayley-Hamilton, the characteristic polynomial of (m_{ij}) which is monic in $\mathbb{Z}[X]$ and so x will be integral over $\mathbb{Z}$. But R is integrally closed and so $x \in R$. Thus $J \subset R$. $\square$

Theorem 2. *Suppose R is a Dedekind domain. Then every fractional ideal I can be written uniquely (up to permutations) as a product $\prod_i \mathfrak{p}_i^{n_i}$ where $n_i \in \mathbb{Z}$ and $\mathfrak{p}_i$ are prime ideals.*

Proof. This is textbook Theorem 3.1.11

First, note that the case of fractional ideals can be reduced to that of ideals by multiplication. Next, if $\prod \mathfrak{p}_i = \prod \mathfrak{q}_j$ then $\prod \mathfrak{p}_i \subset \mathfrak{q}_j$ for each j. Thus by the observation at the end of the previous lecture it follows that $\mathfrak{p}_i = \mathfrak{q}_j$ for some i. Multiplying $\prod \mathfrak{p}_i = \prod \mathfrak{q}_j$ by the inverse of $\mathfrak{p}_i = \mathfrak{q}_j$ yields an equality of products of prime ideals containing fewer factors in each product. Repeating the argument proves the fact that the prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are permutations of each other.

For existence, if not every ideal is a product of primes ideals then there exists a maximal I which is not a product of prime ideals by the noetherian property. The trivial ideal R is a trivial product of primes and so $I \subset \mathfrak{p} \subset R$ where $\mathfrak{p}$ is some prime ideal (every ideal is contained in a maximal ideal!) Therefore $\mathfrak{p} \mid I$ and so $I\mathfrak{p}^{-1} \subset R$ is an ideal. If $I = I\mathfrak{p}^{-1}$ then the above lemma implies that $\mathfrak{p}^{-1} \subset R$ and of course this would imply that $R \subset \mathfrak{p}$ which is false. Thus $I \subsetneq I\mathfrak{p}^{-1}$ and by maximality of I it follows that $I\mathfrak{p}^{-1}$ is invertible and $I^{-1} = \mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1}$. $\square$

(4.7) The Chinese Remainder Theorem.

Proposition 3.

1. *Suppose n_i are pairwise coprime integers and $a_i \in \mathbb{Z}$. Then there exists $a \in \mathbb{Z}$ such that $a \equiv q_i \pmod{n_i}$. Equivalently,*

$$\mathbb{Z}/\prod n_i\mathbb{Z} \cong \prod \mathbb{Z}/n_i\mathbb{Z}$$

2. *If R is any commutative ring with unit and I_i are pairwise coprime ideals of R (i.e., if $i \neq j$ then $I_i + I_j = R$), then*

$$R/\prod I_i \cong \prod R/I_i$$

Proof. Done in class, see textbook §5.1.1 $\square$

(4.8) Generators for fractional ideals in Dedekind domains.

Lemma 4. *Suppose R is a Dedekind domain and I, J are two ideals. Then there exists $a \in I$ such that $(a)I^{-1}$ and J are coprime.*

Proof. Done in class, see textbook Lemma 5.2.2. $\square$

Theorem 5. *If R is a Dedekind domain then every fractional ideal is generated by 2 elements.*

Proof. It suffices to show this for ideals since fractional ideals are scalar multiples of ideals. Suppose $a \in I$ is nonzero. Then the lemma above implies the existence of $b \in I$ such that $(b)I^{-1}$ and (a) are coprime. Now $a, b \in I$ and so $(a, b) \subset I$ where $(a, b) = (a) + (b)$ is the ideal generated by (a) and (b). Thus $I \mid (a, b)$. If $\mathfrak{p}^n \mid (a, b) \mid (a), (b)$ it follows that $\mathfrak{p}^n \mid (a)$ and $\mathfrak{p}^n \mid (b)$. The ideals (a) and $(b)I^{-1}$ are coprime and so $\mathfrak{p} \nmid (b)I^{-1}$. Thus the power of $\mathfrak{p}$ in (b) equals the power of $\mathfrak{p}$ in I and so $\mathfrak{p}^n \mid I$. Thus $(a, b) \mid I$ and we conclude that $I = (a, b)$ is generated by two elements. $\square$