Introduction to Algebraic Number Theory
Lecture 8

Andrei Jorza

2014-01-31

Today: Unique factorization domains, primes under extensions. Textbook here is `http://wstein.org/books/ant/ant.pd`

4 Dedekind domains (continued)

(4.9) The classical theory of unique factorization.

Definition 1. In an integral domain R an element x is said to be irreducible if it cannot be written as $x = yz$ with $y, z \in R$ non-units. The integral domain R is said to be a unique factorization domain (UFD) if every $x \in R$ can be written uniquely (up to units and permutations) as a product of irreducible elements.

Example 2. 1. $\mathbb{Z}$, $F[X]$ for F a field and $\mathbb{Z}[X]$ are UFD but (cf. homework 2) $\mathbb{Z}[\sqrt{-13}]$ is not.

2. In fact if R is a UFD then $R[X]$ is a UFD.

Remark 1. If (x) is a prime ideal in R then x is irreducible (else $x = yz$ and so $(x) \mid (y)$ or $(x) \mid (z)$; in the first case deduce that z is a unit). However, the converse is not true. Indeed, $a = 2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ has norm $N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(a) = 9$ and if $a = xy$ then $N_{K/\mathbb{Q}}(x)N_{K/\mathbb{Q}}(y) = 9$. Since $N_{K/\mathbb{Q}}(x) = x\overline{x}$ it follows that x is a unit if and only if $N_{K/\mathbb{Q}}(x) = 1$ and so if x and y are not units it must be that $N_{K/\mathbb{Q}}(x) = 3$. But $N_{K/\mathbb{Q}}(u + v\sqrt{-5}) = u^2 + 5v^2$ can never be 3. At the same time $a = 2 + \sqrt{-5}$ is not a prime because $2 + \sqrt{-5} \mid (2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ but $2 + \sqrt{-5} \nmid 3$ as

$$\frac{3}{2 + \sqrt{-5}} = \frac{2 - \sqrt{-5}}{3} \notin \mathbb{Z}[\sqrt{-5}]$$

What is really going on in this example is that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proposition 3. *If R is a UFD then all irreducible are primes.*

Proof. Suppose x is irreducible and $x \mid ab$. Then $cx = ab$ for some c. Since R is a UFD we may decompose into irreducibles $a = \prod a_i$, $b = \prod b_i$ and $c = \prod c_i$ in which case the uniqueness of the decomposition implies that x is among the irreducibles a_i, b_j. Thus $x \mid a$ or $x \mid b$. ☐

Theorem 4. *If R is a PID then R is a UFD.*

Proof. First, if $I_1 \subset I_2 \subset \ldots$ is a chain of ideals of R then $I = \cup I_n$ is an ideal of R which is necessarily principal and so $I = (a)$. But then $a \in \cup I_n$ implies that $a \in I_n \subset I_{n+1} \subset \ldots$ for some n which implies that $I_n = I_{n+1} = \ldots = (a)$. Thus every PID is noetherian.

Existence. Since R is noetherian the set of (principal) ideals of R which don't decompose into irreducibles has a maximal element (x). Then x cannot be irreducible and so $x = yz$ for y, z not units. Then $(x) \subsetneq (y), (z)$ and by maximality $y = \prod y_i$ and $z = \prod z_i$ are products of irreducibles. But then $x = \prod y_i \prod z_j$ is a product of irreducibles yielding a contradiction.

Uniqueness. If R is a PID and x is irreducible then (x) is a maximal ideal. Indeed, if not then $(x) \subsetneq \mathfrak{m} \subset R$ where $\mathfrak{m} = (a)$ is some maximal ideal and so $a \mid x$ but $x \nmid a$. Thus $x = ab$ where $b \in R$ is not a unit contradicting the fact that x is irreducible. Now if $\prod x_i = \prod y_j$ are two products of irreducibles then, because the ideals (x_i) and (y_j) are maximal, analogously to the case of unique factorization into prime ideals in Dedekind domains, we deduce that $(x_1) = (y_i)$ for some i. Canceling terms we can inductively show that the two sets of factors are the same, up to units. ☐

From the homework: a Euclidean domain is an integral domain R with a Euclidean function $d : R - \{0\} \to \mathbb{Z}_{>0}$ such that division with remainder holds, i.e., if $m, n \in R$ ($n \neq 0$) then there exist $q, r \in R$ such that $m = nq + r$ and $r = 0$ or $d(r) < d(n)$.

Proposition 5. *Every Euclidean domain is a PID and thus a UFD.*

Proof. Homework 2. ☐

Examples are $\mathbb{Z}, \mathbb{Z}[\sqrt{d}]$ for $d = -1, -2, 2$ and $\mathbb{Z}[\zeta_3]$. For more examples and applications see the homework.

5 Ideals under extensions or Ramification theory

A basic question is the following. Suppose L/K are number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and will decompose into a product of prime ideals of $\mathcal{O}_L$. What are these prime factors? And what arithmetic significance do they have? Can they be predicted?

Example 6. (From homework 2) If $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. The ideal $(2)\mathbb{Z}[i]$ factors as $(1+i)^2$. If p is a prime $\equiv 3 \pmod 4$ then $(p)\mathbb{Z}[i]$ stays a prime ideal in $\mathbb{Z}[i]$. If $p \equiv 1 \pmod 4$ then $(p)\mathbb{Z}[i]$ splits as a product $(p)\mathbb{Z}[i] = \mathfrak{q}\bar{\mathfrak{q}}$. For example $(5)\mathbb{Z}[i] = (2+i)(2-i)$.

Proposition 7. *Suppose L/K are number fields (also works for a finite extension of fraction fields of integral rings). If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ then the following are equivalent:*

1. $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$
2. $\mathfrak{q} \supset \mathfrak{p}$
3. $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$
4. $\mathfrak{q} \cap K = \mathfrak{p}$.

If any of these condition are satisfied we say $\mathfrak{q} \mid \mathfrak{p}$ or $\mathfrak{q}$ lies above $\mathfrak{p}$ or $\mathfrak{p}$ lies below $\mathfrak{q}$.

Proof. 1 implies 2 becauase $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_L$. 2 implies 3 because $\mathfrak{q} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$, it is proper (otherwise 1 would be in $\mathfrak{q}$) and contains $\mathfrak{p}$ and so must equal $\mathfrak{p}$ by maximality of $\mathfrak{p}$. 3 implies 4 because $\mathcal{O}_L \cap K = \mathcal{O}_K$. Finally 4 implies 1 because then $\mathfrak{p} \subset \mathfrak{q}$ and so $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$. ☐

Proposition 8. *Suppose L/K are number fields.*

1. *Every prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lies above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*
2. *Every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies below a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$.*

Proof. For the first part note that $\mathfrak{q} \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. It cannot be everything because then $1 \in \mathfrak{q}$ and if $\alpha \in \mathfrak{q}$ then $\alpha \mid N_{L/K}(\alpha) \in \mathcal{O}_K$ and so $\mathfrak{q} \cap \mathcal{O}_K \neq 0$. Moreover,

$$\mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{q}) \cong (\mathcal{O}_K + \mathfrak{q})/\mathfrak{q} \subset \mathcal{O}_L/\mathfrak{q}$$

The RHS being a field implies that the LHS is an integral domain and so $\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

For the second part, we seek $\mathfrak{q}$ of the form $\mathfrak{p}\mathcal{O}_L$. Since $\mathfrak{p}$ is proper it follows that $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$ and so $\mathfrak{p}^{-1} = \sum \mathbb{Z}\alpha_i$ where at least one of the α_i is not in $\mathcal{O}_K$. With $\alpha = \alpha_i \notin \mathcal{O}_K$ we have $\alpha\mathfrak{p}\mathcal{O}_L \subset \mathfrak{p}^{-1}\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$. If $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$ it would follows that $\alpha\mathcal{O}_L \subset \mathcal{O}_L$ but then we'd deduce that $\alpha \cdot 1 \in \mathcal{O}_L$ contradicting our choice. Thus $\mathfrak{p}\mathcal{O}_L \subsetneq \mathcal{O}_L$. Finally, any prime factor $\mathfrak{q}$ of $\mathfrak{p}\mathcal{O}_L$ will lie above $\mathfrak{p}$. ☐