Graduate Algebra, Fall 2014
Lecture 30

Andrei Jorza

2014-11-10

2 Rings

2.6 Special types of rings

2.6.1 Euclidean domains

Definition 1. A **Euclidean function** on a ring R is a function $d : R - 0 \to Z_{\geq 0}$ such that for every $x, y \in R$ with $y \neq 0$ there exists $q, r \in R$ such that $x = qy + r$ and either $r = 0$ or $d(r) < d(y)$.

A ring R is said to be **Euclidean** if it admits some (not necessarily unique) Euclidean function.

Example 2.

1. On $\mathbb{Z}$ take $d(n) = |n|$. Then division with remainder shows that this is a Euclidean function.
2. On $F[X]$ take $d(P) = \deg(P)$. Again, division with remainder gives that d is a Euclidean function.
3. Let F be a field. On $F[\![X]\!]$ take $d(a_n X^n + O(X^{n+1})) = n$ if $a_n \neq 0$. Indeed, if $f, g \in F[X]$ then either $d(f) < d(g)$ in which case take $q = 0, r = f$ or $d(f) \geq d(g) = n$ in which case $q = f/g = (fX^{-n})/(gX^{-n}) \in F[\![X]\!]$ as gX^{-n} is invertible, and $r = 0$.

Proposition 3. *The ring $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ is Euclidean.*

Proof. Define $d(a + bi) = |a + bi|^2 = a^2 + b^2$. If $x, y \in \mathbb{Z}[i]$, the complex number x/y lands inside (or on the boundary) of a unit square in the lattice $\mathbb{Z}[i] \subset \mathbb{C}$. Let q be the corner of this/one of these squares that closest to the complex number x/y. Then $|q - x/y| \leq 1/\sqrt{2}$ by inspection. Thus $r = x - qy \in \mathbb{Z}[i]$ has the property that $d(r) = |x - qy|^2 \leq |y|^2/2$ as desired. □

2.6.2 PID

Definition 4. A **principal ideal domain (PID)** is a ring R such that every ideal is generated by a single element.

Theorem 5. *Every Euclidean domain is a PID.*

Proof. Choose $x \in I$ nonzero with $d(x)$ minimal. If $y \in I$ then $y = qx + r$ with $d(r) < d(x)$. If $r \neq 0$ it contradicts the choice of x. Thus $y = qx$ and so $I = (x)$. □

Example 6.

1. $\mathbb{Z}$ is a PID.
2. $F[X]$ is a PID.
3. $\mathbb{Z}[i]$ is a PID.
4. $F[\![X]\!]$ is a PID.
5. but $\mathbb{Z}[X]$ is not a PID since $(2, X)$ cannot be generated by a single element as 2 and X are coprime.

2.6.3 UFD

Definition 7. An element $x \in R$ is **prime** if $(x) \subset R$ is a prime ideal. It is **irreducible** if $x = ab$ implies a or b is a unit in R.

Definition 8. A **unique factorization domain (UFD)** is a ring R such that every nonzero $x \in R$ can be written as

$$x = y_1 \dots y_n$$

where $y_1, \dots, y_n$ are irreducibles and if this expression is unique up to permutation and multiplication by units.

Proposition 9. *Let R be a commutative integral domain.*

1. *Every prime is irreducible.*
2. *If, furthermore, every irreducible is prime then every factorization into irreducibles is unique up to units and permutations.*
3. *If R is a UFD then every irreducible is prime.*

Proof. (1): Suppose x is prime but reducible. Then $x = ab$ with a, b not units. But then $ab \in (x)$ so by primality get $a \in (x)$ or $b \in (x)$. Suppose $a \in (x)$. then $a = xc$ and $x = ab = xbc$. Thus $bc = 1$ so b is a unit.

(2): Suppose every irreducible is a prime and

$$x = \prod y_i = \prod z_j$$

with y_i, z_j irreducible and thus prime. Going to ideals get

$$\prod (y_i) = \prod (z_j) \subset (z_1)$$

Since (z_1) is a prime ideal, from homework 8 deduce that $(y_i) \subset (z_1)$ for some i and so $y_i = az_1$. By irreducibility get a is a unit and so $(z_1) = (y_i)$. Since we are in an integral domain we deduce that

$$\prod_{j \neq i} y_j = \prod_{k > 1} z_k$$

up to a unit (or equality as ideals).

By induction, it follows that every factorization into irreducibles is unique up to units and up to permutations.

(3): Suppose (x) is not a prime ideal. Then there exist $a, b \in R$, $a, b \notin (x)$ such that $ab \in (x)$. Thus $ab = xy$. Since x is irreducible, by the uniqueness of factorization of a and b into irreducibles it follows that x appears, up to a unit, among the irreducible factors of a of b. But the a or b is in (x). □

Theorem 10. *Every PID is a UFD.*

Proof. First, let $x \in R$ be irreducible (nonzero and not a unit) and let $\mathfrak{m}$ be a maximal ideal of R containing x. Since R is a PID it follows that $\mathfrak{m} = (a)$ and so $(x) \subset (a)$ so $a = xy$. But (a) is maximal and so prime and so either x is a unit or y is a unit. Since x is not a unit it follows that $(a) = (xy) = (x)$ is a prime ideal.

To be continued. □