Math 250A Lecture 9 Notes

Daniel Raban

September 26, 2017

1 Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

1.1 Euclidean Domains and Principal Ideal Domains

1.1.1 Euclidean Domains

Recall that every integer $\neq 0$ is a product of primes in an essentially unique way. $12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = (-2) \times (-3) \times 2$. So the product is unique up to order and multiplication by *units*.

This was essentially proved by Euclid. The key point he used was division with a remainder. That is, given a, b with $a \neq 0$, we can write $a = bq + r$, where r is smaller than b. Here, q is called the quotient, and r is the remainder.

What does smaller mean in this context? For integers, this means $|r| < |b|$. We can do the same thing for polynomials $a, b \in \mathbb{R}[x]$; a smaller than b means that $\deg(a) < \deg(b)$ (or $a = 0$).

Definition 1.1. A commutative ring R is a *Euclidean domain* if it has a function $|\cdot| : R \to \mathbb{N}$ such that given a, b with $b \neq 0$, we can find r, q such that $a = bq + r$ and $|r| < |b|$.[1]

Example 1.1. Let $Z[i] = \left\{a + bi : a, b \in \mathbb{Z}, i^2 = -1\right\}$ be the Gaussian integers. $Z[i]$ is a Euclidean domain. Define $|a + bi| = a^2 + b^2$. This is the usual Euclidean norm but squared to make sure we get an integer. Given a, b, we need to find r, q such that $a = bq + r$, which means $a/b = q + r/b$, where $|r/b| < 1$. Given any a/b, we can find $q \in Z[i]$ of distance < 1 from a/b. Draw an open disk of radius 1 around each elements of $Z[i]$. These cover $\mathbb{C}$, so we can find r, q.

1.1.2 Principal Ideal Domains

Definition 1.2. The *ideal generated by elements* $g_1, g_2, \ldots$ is the smallest ideal containing these elements.

[1] We don't actually need the codomain of the norm function to be $\mathbb{N}$; we just need it to be a well-ordered set. In practice, however, the useful examples are all with sets that are basically $\mathbb{N}$.

We denote $(a, b, c, \dots)$ as the ideal generated by $a, b, c \dots$.

Definition 1.3. A *principal ideal domain* is a commutative ring where all ideals are generated by one element.

Example 1.2. $\mathbb{Z}$ is a principal ideal domain. In $\mathbb{Z}$, we only have ideals of the form $n\mathbb{Z}$.

Example 1.3. Here is an example of a commutative ring that is not a PID. Let $R = \mathbb{C}[x, y]$, and let $I = (x, y)$ be the set of all polynomials with constant term 0. If $I = (f)$, then f divides x and f divides y. This means $f = 1$, but $1 \notin (x, y)$.

Theorem 1.1. *Euclidean domains are principal ideal domains.*

Proof. Let I be any ideal. Choose $a \in I$ with $a \neq 0$ and $|a|$ minimal. Then we claim that $I = (a)$. Suppose $b \in I$. Then $b = aq + r$ with $|r| < |a|$. So $r = b - aq$ means that $r \in I$, and the minimality of $|a|$ forces $r = 0$. So $b = aq$ for some q, and this holds for any $b \in I$, so $I = (a)$. □

Example 1.4. $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ is a PID that is not Euclidean. R is a PID; for proof, see an algebraic number theory course. Here is a sketch that R is not Euclidean. Let $a \in R$ be nonzero and not a unit, with $|a|$ minimal. Then look at $R/(a)$. If $b \in R$, $b = aq + r$ with $|r| < |a|$. Then r is 0 or a unit. So every element of $R/(a)$ is represented by 0 or a unit. The only units of R are ± 1, so $R/(a)$ has ≤ 3 elements. If $a \neq \pm 1, 0$, then $R/(a)$ has ≥ 4 elements (actually $|a|^2$).

1.2 Unique factorization domains

1.2.1 Definitions and relationship to principal ideal domains

Definition 1.4. Let $a, b \in R$. We say a *divides* b (denoted $a|b$) if there exists some $c \in R$ such that $ac = b$.

Definition 1.5. An element a is called *irreducible* if $a \neq 0$, a is not a unit, and $a = bc$ implies that either b or c is a unit.

Definition 1.6. An element a is called *prime* if $a|bc$ implies that $a|b$ or $a|c$.

For $\mathbb{Z}$, these two definitions are equivalent, but this is not the case in all rings.

Lemma 1.1. *In a principal ideal domain, irreducible elements are prime.*

Proof. Suppose p is irreducible and $p|ab$. We want to show that $p|a$ or $p|b$. Suppose that $p \nmid a$. Then $(p, a) = (c)$ since R is a principal ideal domain. Then $c|p$, so c is a unit or is a unit times p. The second case is not possible because $pu = c$ divides a, but a is not divisible by p. So (c) contains 1 (by multiplying c by c^{-1}) and is then equal to R. So $(p, a) = (1) = R$.

We now have $px + ay = 1$ for some $x, y \in R$, which makes $pbx + aby = b$. Both terms are divisible by p, so $p|b$. Hence, p is prime. □

Definition 1.7. A *unique factorization domain* is a commutative ring in which every element can be uniquely expressed as a product of irreducible elements, up to order and multiplication by units.

Theorem 1.2. *Every principal ideal domain is a unique factorization domain.*

Proof. We first show existence of factorization into irreducibles. Given $a \in R$, first find irreducible p dividing a if a is not a unit. Let $a = bc$; if b is irreducible, stop. Otherwise, let $b = de$, and repeat the process until we get an irreducible element. Can this go on forever? No. Suppose we have $a, b, c, d, e, \dots$ with $a = b'b$, $b = c'c$, etc., where $b', c', \dots$ are not units. Then the ideal $(a, b, c, d, \dots) = (x)$, since we are in a PID. But then $x \in (a, b, c, d, e)$ (some finite sequence of the variables), so the sequence must stop after finitely many steps.

Now put $a = bc$ with b irreducible, $c = de$ where d is irreducible, $e = fg$, where f is irreducible and so on. This stops after a finite number of steps by a similar argument. So every nonzero element is a product of irreducibles.[2]

To prove uniqueness, suppose $a = p_1 \cdots p_m = q_1 \cdots q_n$ with p_i, q_j irreducible. We want to show that these factorizations are unique up to order and units. p_1 is irreducible, so p_1 divides some q_i as p_1 is prime. The q_i are irreducible, so $q_i = p_1 u$ for some unit $u \in R$. By removing p_1 and this q_i from their respective sides (really we are bringing the two products to the same side, factoring out the p_1, and asserting that the rest equals 0), we can repeat this to eventually get our result. □

Example 1.5. R be the set of polynomials in x^q for rational $q > 0$; this is a set of terms of elements like $3 + 3x^{5/7} + 2x^{17/3}$. This argument goes wrong here because $x = x^{1/2}x^{1/2} = x^{1/4}x^{1/4}x^{1/4}x^{1/4} = \cdots$. The ideal $(x^{1/2}, x^{1/4}, x^{1/8}, \dots)$ is not principal.

1.2.2 Examples and Applications

Example 1.6. Suppose $a+bi \in \mathbb{Z}[i]$ is prime. Then $(a+bi)(a-bi) = a^2+b^2 \in Z$. So we can use this to factor elements in Z into elements in $\mathbb{Z}[i]$. For example, $5 = 2^2+1 = (2+i)(2-i)$.

$$65 = 5 \times 13 = (2+i)(2-i)(3+2i)(3-2i) = (4+7i)(4-7i) = (8-i)(8+i)$$

This gives us $65 = 4^2+7^2 = 8^2+1^2$. So the different factorizations of $x \in \mathbb{Z}$ in the Gaussian integers give us the ways to write x as a sum of two squares.

Example 1.7. Let $R = \mathbb{Z}[\sqrt{-2}]$. Imagine this as a rectangular lattice in $\mathbb{C}$. The circles of radius 1 around these points cover $\mathbb{C}$, so as we argued before with $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ is a euclidean domain and hence is a unique factorization domain.

Now let $R = \mathbb{Z}[\sqrt{-3}]$. The circles of radius 1 do not cover the point $1/2 + \sqrt{-3}/2$. In fact, R is not a unique factorization domain. We have $2 \times 2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$, and

[2] This is still true if R has the following property: there is no strictly increasing sequence of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. These are called *Noetherian rings.*

the only units are ± 1. These are all irreducible elements. If $2 = ab$, then $|a|\,|b| = |2| = 2$, which means $|a| = \pm 1$ or $|b| = \pm 1$.

Multiplying $z \in R$ by a multiplies $|z|$ by $|a|$ and rotates z by $\arg(a)$. So a principal ideal in $\mathbb{Z}[\sqrt{-3}]$ looks like a rotated and rescaled rectangular lattice. What does a non-principal ideal look like? Look at $(2, 1+\sqrt{-3})$; we get a "diamond" lattice instead of a rectangular one.

Unique factorization domains need not be principal ideal domains.

Example 1.8. $\mathbb{Z}[x]$ is a UFD and has the non-principal ideal $(2, x)$.

Example 1.9. Let K be a field. $K[x, y]$ is a UFD and has the non-principal ideal (x, y).

We will see later that if R is a UFD, then so is $R[x]$, the ring of polynomials over R.

Theorem 1.3 (Fermat)**.** *Any prime $p \in \mathbb{Z}$ with $p > 0$ and $p \equiv 1 \pmod 4$ can be uniquely expressed as $a^2 + b^2$ (up to sign differences in a, b).*

Proof. $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1 = 4n$. It has an element -1 of order 2. Let g be a generator, so $g^{4n} = 1$. So $-1 \equiv g^{2n} \pmod p$, which means that -1 is a square mod p. This gives us that $-1 = a^2 - np$ for some n, a. So $np = a^2 + 1 = (a+i)(a-i)$ in $\mathbb{Z}[i]$. $p|(a+i)(a-i)$, but does not divide either of these two factors, so p is not prime and hence is not irreducible in $\mathbb{Z}[i]$. So $p = (a+bi)(a-bi)$ for some $a, b \in \mathbb{Z}$ (we must have this decomposition because $a+bi$ times any other number would not be purely real). This makes $p = a^2 + b^2$.

For uniqueness, suppose that $p = x^2 + y^2$. Then $p = (x+iy)(x-iy)$, which means $x + iy = u(a+bi)$ for some unit u because $Z[i]$ is a unique factorization domain. Then $x = \pm 1$ and $b = \pm b$. $\square$