UNIVERSIDAD YACHAY TECH

School of Mathematical and Computational Sciences
Abstract Algebra

Prof. Pablo Rosero
& Christian Chávez
Lesson 12

1. Some special rings

In this lecture, we introduce some special rings:

(i) *Euclidean Domains*, i.e., rings with a division algorithm;

(ii) *Principal Ideal Domains (PID)*, i.e., rings where every ideal is principal; and

(iii) *Unique Factorization Domains (UFD)*, i.e., rings whose elements can be factored into primes.

The ring $\mathbb{Z}$ is the main example of such rings.

Important. All the rings in this lecture are assumed to be commutative.

2. Euclidean Domains

Let A be an integral domain. A *norm* is a function $N : A \to \mathbb{N}_*$ such that $N(0) = 0$. If $N(a) > 0$ for every $a \in A \setminus \{0\}$, we say that N is a *positive norm*.

Example 1 (10.1)**.** The function $|\cdot| : \mathbb{Z} \to \mathbb{N}_*$, which is a restriction of the absolute value function, is a norm on the integral domain $\mathbb{Z}$.

An *Euclidean domain* A is an integral domain for which a division algorithm holds, i.e., there exists a norm N such that:

$$\forall (a,b) \in A \times A \setminus \{0\}, \exists (r,q) \in A \times A \setminus \{0\} : \quad a = qb + r,$$

with

$$r = 0 \quad \text{or} \quad N(r) < N(b).$$

Example 2. $\mathbb{Z}$ becomes a Euclidean Domain whenever it is equipped with the norm mentioned in Example 10.1.

Example 3. For any field F, the polynomial ring $F[x]$ together with the norm N given by the degree of a polynomial is an Euclidean domain.

The existence of a division algorithm carries a very powerful implication for the integral domain A.

Proposition 2.1 (10.1)**.** *Every ideal I in an Euclidean Domain is principal. That is, if I is any nonzero ideal of the Euclidean domain A, then $I = \langle d \rangle$, where d is any nonzero element of I of minimum norm.*

Proof. Let I be an ideal of A. If I is the zero ideal, we are done.

(i) Suppose now that $d \in I$ is a nonzero element of minimum norm. This element d does exist by the well-ordering principle. We have that $\langle d \rangle \subseteq I$ because $d \in I$.

(ii) Let $a \in I$, generic. By the division algorithm in A, we can write

$$a = qd + r$$

with $r = 0$ or $N(r) < N(d)$. Since $r = a - qd$ and $a, q, d \in I$, we have that $r \in I$. Moreover, since d is of minimum norm in I, we have that $r = 0$. Therefore, $qd \in \langle d \rangle$.

From i) and ii), it follows that $I = \langle d \rangle$. □

An immediate result from Proposition 10.1 is that every ideal of $\mathbb{Z}$ is principal. It can also help us prove that some integral domains A are not Euclidean with respect to *any* norm by showing the existence of ideals that are not principal.

We have used the notion of greatest common divisor in the past. Now, we can generalize this concept to general Euclidean Domains. Let A be a commutative ring and let $a, b \in A$ with $b \neq 0$. The element b is said to be a divisor of a, denoted $b \mid a$, if

$$\exists x \in A : \quad a = bx.$$

The *greatest common divisor* of a and b, denoted $\gcd(a, b)$ — or, by an abuse of notation, simply (a, b) — is a nonzero element d such that:

(i) d is a *common divisor* of a and b, i.e., $d \mid a$ and $d \mid b$, and

(ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Remark 2.1.1 (10.1)**.** These defining properties of $\gcd(a, b)$ can be translated into the language of ideals. In fact, let's denote by $I \subseteq A$ the ideal generated by a and b, i.e., $I = \langle a, b \rangle$. Then $d = \gcd(a, b)$ if

(i) I is contained in the principal ideal $\langle d \rangle$, and

(ii) if $\langle d' \rangle$ is any principal ideal containing I, then $\langle d \rangle \subseteq \langle d' \rangle$.

This is the content of "Caesar's Lemma" below.

Lemma 2.2 (10.1 (Caesar's Lemma — To divide is to contain))**.** *It holds*

$$a \mid b \iff \langle b \rangle \subseteq \langle a \rangle.$$

3. Principal Ideal Domains (PIDs)

A *Principal Ideal Domain (PID)* is an integral domain where every ideal is principal. Proposition 10.1 proved that every Euclidean domain is a PID. Thus, every result for PIDs immediately holds for Euclidean domains.

Example 4 (10.4)**.** $\mathbb{Z}$ is a PID.

Example 5 (10.5)**.** The quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID. In fact, the ideal $\langle 3, 1+\sqrt{-5}\rangle$ is nonprincipal.

Remark 3.0.1 (10.2)**.** It is possible that the product IJ of two nonprincipal ideals I and J is principal. For example, $\langle 3, 1+\sqrt{-5}\rangle$ and $\langle 3, 1-\sqrt{-5}\rangle$ are nonprincipal, but their product, $\langle 3\rangle$, is a principal domain.

Recall that maximal ideals are always prime ideals, but the converse is not true in general. However, every nonzero prime ideal of $\mathbb{Z}$ is a maximal ideal.

Proposition 3.1 (10.2)**.** *Every nonzero prime ideal in a PID is a maximal ideal.*

Proof. Let $\langle p\rangle$ be a nonzero prime ideal in a principal ideal domain R, and let $I = \langle m\rangle$ be any ideal containing $\langle p\rangle$. Remember that, in order to show maximality of I, we have to show that

$$\text{either } I = \langle p\rangle \text{ or } I = R.$$

Since $\langle p\rangle \subseteq I$, we have that $p \in \langle m\rangle$, which implies that $p = rm$ for some $r \in R$. Since $\langle p\rangle$ is prime and $rm \in \langle p\rangle$, either r or m must be in $\langle p\rangle$. Therefore:

(i) If $m \in \langle p\rangle$, then $\langle p\rangle = \langle m\rangle = I$.

(ii) If $r \in \langle p\rangle$, we can write $r = ps$ for some $s \in R$. In this case, $p = rm = psm$, so $sm = 1$ and because m is an invertible element, we have that $I = R$.

□

4. Unique Factorization Domains (UFDs)

Throughout this lecture, we have used notions from the integers $\mathbb{Z}$ to generalize them. In the case of the integers, there is another method for determining the greatest common divisor of a and b. Namely, the notion of *factorization into primes*. This notion can be extended to a larger class of rings called *Unique Factorization Domains*. Moreover, we will see that every PID is a UFD.

Let A be an integral domain.

(i) Suppose that $r \in A \setminus \{0\}$ is *not invertible*. Then r is called *irreducible* in A if whenever $r = ab$ with $a, b \in A$, at least one of a or b must be invertible in A, i.e.,

$$r = ab \implies \left(a \in A^\times \vee b \in A^\times\right).$$

(ii) An element $p \in A \setminus \{0\}$ is called *prime* in A if the ideal $\langle p\rangle$ is prime. In other words, p is prime if it is not invertible and

$$p \mid ab \implies (p \mid a \vee p \mid b).$$

(iii) Two elements a and b are *associates*, denoted by $a \sim b$, if they differ by an invertible element, i.e.,

$$\exists u \in A^\times : \quad a = ub.$$

Proposition 4.1 (10.3). *In an integral domain, a prime element is always irreducible.*

Proof. Let R be an integral domain and $\langle p \rangle$ a nonzero prime ideal. Suppose that $p = ab$ for some $a, b \in R$. Then $ab \in \langle p \rangle$ and, by definition of a prime ideal, $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Without loss of generality, let us assume that $a \in \langle p \rangle$. Then $a = ps$ for some $s \in R$. Therefore,

$$p = ab = psb,$$

which implies that $sb = 1$. We conclude that p is irreducible. □

Proposition 4.2 (10.4). *In a PID, a non-zero element is prime if and only if it is irreducible.*

Proof. In Proposition 10.3, we have shown that prime implies irreducible. To show the converse, take a non-zero element p which is irreducible. If M is any ideal containing $\langle p \rangle$, then, by hypothesis, we have that $M = \langle m \rangle$ is a principal ideal. Since $p \in \langle m \rangle$, $p = rm$ for some r. But p is irreducible, so either r or m are invertible. That is, either $\langle p \rangle = \langle m \rangle$ or $\langle m \rangle = \langle 1 \rangle$, respectively. Therefore, the only ideals containing $\langle p \rangle$ are $\langle p \rangle$ or $\langle 1 \rangle$, i.e., $\langle p \rangle$ is a maximal ideal. The result follows from the fact that all maximal ideals are prime. □

Example 6 (10.6). The irreducible elements in $\mathbb{Z}$ are the prime numbers and their negatives.

A *Unique Factorization Domain (UFD)* is an integral domain A where every nonzero element $r \in A \setminus A^\times$ has the following properties:

(i) r can be written as a finite product of irreducibles p_i of A, i.e.,

$$r = p_1 p_2 \cdots p_n,$$

where the p_i's are not necessarily distinct.

(ii) The decomposition above is unique up to associates, i.e., if

$$r = q_1 q_2 \cdots q_m,$$

then $n = m$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \ldots, n$.

Proposition 4.3 (10.5). *In a UFD, a nonzero element is prime if and only if it is irreducible.*

Proof. The proof is left as an exercise for the reader. □

Theorem 4.4 (10.1). *Every PID is a UFD. In particular, every Euclidean Domain is a UFD.*

Proof. Note that the second assertion is a direct result of the first since Euclidean Domains are PIDs.

Let A be a PID and let $r \in A \setminus A^\times$ be nonzero. To prove the first assertion we need to check two things:

(i) that any r has a finite decomposition of irreducibles in A,

(ii) this decomposition is unique up to invertible elements.

If r is irreducible, we are done. If not, we can rewrite r as a product

$$r = r_1 r_2,$$

with neither r_1 nor r_2 being invertible. If both of them are irreducible, we are done as we produced a decomposition of r into irreducibles. If not, suppose r_1 is reducible and proceed to find its decomposition and so forth. But we must verify that this process actually finishes, that is, that after a finite amount of steps we have found a proper decomposition of r into irreducibles.

Suppose for a contradiction that this is not the case. From the factorization $r = r_1 r_2$ we obtain a proper infinite ascending chain of ideals

$$\langle r \rangle \subset \langle r_1 \rangle \subset \langle r_{11} \rangle \subset \cdots \subset R.$$

The Axiom of Choice ensures that such a chain exists. But now we will show that any ascending chain $I_1 \subset I_2 \subset \cdots \subset R$ of ideals in a principal ideal domain eventually stabilizes, i.e., there is some positive integer n such that

$$I_k = I_n, \quad k \geq n.$$

There is no possible way of having a chain like this where all containments are proper. Let

$$I = \bigcup_{i=1}^{\infty} I_i.$$

Then I is an ideal. Since R is a PID, $I = \langle a \rangle$ for some $a \in R$. This implies $I_n \subseteq I = \langle a \rangle \subseteq I_n$. So the chain becomes stationary.

To prove uniqueness of the above decomposition, we proceed by induction on the number n of irreducible factors. If $n = 0$, then r is invertible. If we had some other factorization $r = qc$ for some irreducible factor q, then q would divide an invertible element and would itself be an invertible element. A contradiction. Now, suppose that $n \geq 1$ and we have two factorizations for r,

$$r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \quad m \geq n,$$

where the p_i and q_j are not necessarily distinct irreducibles. Since then p_1 divides the product on the right, then it must divide one of the factors. Renumbering if necessary, $p_1 \sim q_1$. So, $p_1 \sim q_1$. Cancelling p_1, we obtain the following equality

$$p_2 \cdots p_n = u q_2 \cdots q_m = u q_2' \cdots q_m, \quad m \geq n,$$

where $q_2' = u q_2$ is again irreducible. By induction on n, we have that each of the factors on the left matches with the factors on the right up to associates. Since we already showed $p_1 \sim q_1$ after the initial renumbering, this concludes the induction step and the proof. □

Corollary 4.5 (10.1 (Fundamental Theorem of Arithmetic))**.** *The set $\mathbb{Z}$ is a UFD.*

Proof. The integers $\mathbb{Z}$ are an Euclidean Domain and thus, by Theorem 10.1, a Unique Factorization Domain. $\square$

To finish this section, we provide the following diagram summarizing the inclusion among domains we have developed:

$$\text{Fields} \subset \text{Euclidean Domains} \subset \text{PIDs} \subset \text{UFDs} \subset \text{Integral Domains.}$$