Review

Definition

Let R be a commutative ring.

- An ideal I is **principal**, if there is $a \in R$ such that

$$I = (a) \overset{\text{def}}{=} aR = \{ax \ : \ x \in R\}.$$

- A *domain* R is a **principal ideal domain (PID)** if every ideal of R is principal.

Example

The following are PIDs: $\mathbb{Z}$, F where F is a *field*, $F[x]$ where F is a *field*.

Note that $\mathbb{Z}[x]$ is *not* a PID, as $(2, x)$ is not principal.

Review (cont.)

Definition

Let R be a *domain*. Then:

- b is an **associate** of a if there is $u \in R^{\times}$ such that $b = au$. We shall write $b \sim a$. Note that $a = bu^{-1}$ [and $u^{-1} \in R^{\times}$], and hence also $a \sim b$. Therefore, we may say a and b are **associates**. [In fact, $\sim$ is an *equivalence relation*.]
- We say that a **divides** b, or b is a **multiple** of a, if $b = ac$ for some $c \in R$. We write $a \mid b$. [So, $b \in (a)$ iff $a \mid b$.] **Note:** $a \sim b$ iff $a \mid b$ and $b \mid a$ iff $(a) = (b)$.
- An element $a \notin R^{\times} \cup \{0\}$ is **irreducible** if the only divisors are units or associates of a.
- An element $p \notin R^{\times} \cup \{0\}$ is **prime** if whenever $p \mid ab$, then either $p \mid a$ or $p \mid b$. [This means (p) is a prime ideal iff p is prime.]

Note that associates of primes (resp. irreducibles) are also primes (resp. irreducibles). Also, primes are always irreducible.

Review (cont.)

Definition

Let R be a *domain*. Then:

- d is *a* **GCD** of $\{a_1, \ldots, a_n\} \subseteq R$ if $d \mid a_i$ for all i and if $e \mid a_i$ for all i, then $e \mid d$. [Note that two GCDs must be *associates*.]
- $a, b \in R$ are **relatively prime** if their GCD is a unit.
- m is *a* **LCM** of $\{a_1, \ldots, a_n\} \subseteq R$ if $a_i \mid m$ for all i and if $a_i \mid n$ for all i, then $m \mid n$. [Note that two LCMs must be *associates*.]

UFDs

Definition

A domain R is a **unique factorization domain (UFD)** if for all $a \in R$, with $a \notin R^\times \cup \{0\}$:

- **Finite Factorization:** there is $u \in R^\times$ and $p_1, \ldots, p_n$ irreducible such that $a = u \cdot p_1 \cdots p_n$; and
- **Uniqueness:** if also $a = v \cdot q_1 \cdots q_m$, where $v \in R^\times$ and the q_i's are irreducible, then $m = n$ and after possibly reordering, we have that p_i and q_i are associates.

Goal: show that PIDs are UFDs.

GCDs

Theorem

Let R be a PID and $a_1, \ldots, a_n \in R \setminus \{0\}$, with $n \geq 1$. Then there is a GCD, say d, of the a_i's, and $r_i \in R$ such that $d = \sum r_i a_i$. [Thus, any GCD of the a_i's is a **linear combination** *of them.]*

Proof.

Idea: $(a_1, \ldots, a_n) = (d)$. □

Corollary

Let R be a PID. Then every irreducible is prime. [I've shown an example of R not a PID where this is false! Remember the converse is always true!] Also note that this is true for UFDs! [Exercise.]

Corollary

A non-zero ideal (a) in a PID is maximal iff a is prime [or irreducible].

Noetherian Rings

Definition

Let R be a ring. R satisfies the **ascending chain condition (ACC)** or is **noetherian** if every ascending chain of ideals:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots ,$$

eventually becomes constant [i.e., $I_n = I_{n+1} = I_{n+1} = \cdots$ for some n large enough].

PIDs Are Noetherian

Theorem

PIDs are Noetherian.

Proof.

Let:

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots .$$

Let $I = \bigcup_{i=1}^{\infty} (a_i)$. Since R is a PID, there is $a \in R$ such that $I = (a)$. Then $(a_i) \subseteq I = (a)$, i.e., $a \mid a_i$ for all i.
Also, since $a \in I$, $a \in (a_n)$ for some n, i.e., $a_n \mid a$. Since $(a_n) \subseteq (a_k)$ for all $k \geq n$, we have that $a_k \mid a$ for all $k \geq n$.
Since also, $a \mid a_i$ for all i, we have that a and a_k are associates for all $k \geq n$. Thus, $(a) = (a_k)$ for all $k \geq n$ and hence the sequence is eventually constant. $\square$

Maximal Ideal

Corollary

In a noetherian ring [and in particular in a PID], every proper ideal [i.e., different from R] is contained in a maximal ideal.

Proof.

Suppose not and let I be an ideal not contained in a maximal ideal. Since I is not maximal, $I \subsetneq I_2 \neq R$, where I_2 is an ideal. I_2 is not maximal, since I is not contained in a maximal ideal. Repeating, we would get a chain

$$I \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots ,$$

which is a contradiction. Thus, I is contained in a maximal ideal. □

Note: This is in fact true for all rings with 1. The proof uses *Zorn's Lemma*.

Divisibility by Irreducible

Theorem

Let R be a noetherian domain [e.g., a PID]. Then, every $a \in R$, with $a \notin R^\times \cup \{0\}$, is divisible by an irreducible.

Proof.

Let a as above. If a is irreducible, then we are done. Suppose it is not. Then, $a = a_1 b_1$, where $a_1, b_1 \notin R^\times \cup \{0\}$. If either a_1 or b_1 is irreducible, we are done. So suppose not. Repeating for a_1, we have $a_1 = a_2 b_2$, and again if either is irreducible, we are done [as $a = (a_2 b_2) b_1$].

Suppose this procedure does *not* end. Then, we have:

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

which is a contradiction. So, eventually, this has to stop, and a is divisible by some irreducible. $\square$

Finite Factorization

Theorem

Let R be a noetherian domain [e.g., a PID]. Then, we have finite factorization in R.

Proof.

Let $a \in R$, with $a \notin R^\times \cup \{0\}$. Since R is noetherian, a is divisible by an irreducible, say $a = p_1 \cdot a_1$, p_1 irreducible. If $a_1 \in R^\times$, we are done. So, suppose not. Then, as before, $a_1 = p_2 \cdot a_2$, p_2 irreducible. [So, $a = p_1 p_2 a_2$.] Repeat. It must stop, as otherwise:

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

So, $a = p_1 \cdots p_n a_n$, where p_i's are irreducible and $a_n \in R^\times$. $\square$

PID Implies UFD

Theorem (Fundamental Theorem of Arithmetic)

If R is a PID, then R is a UFD.

Proof.

Since R is a PID, it is notherian, and as seen above, we have finite factorization. Thus, it only remains to show uniqueness.
Suppose

$$a = p_1 \cdots p_n = vq_1 \cdots q_m, \qquad p_i,\ q_j \text{ irreducibles.}$$

Since p_1 is *prime* [as R is a PID], it must divide one of the q_j's. WLOG, assume $p_1 \mid q_1$. Since both are irreducible, we must have $p_1 \sim q_1$. Now repeat for $p_2, p_3, \ldots$. [**Exercise:** Write a proper proof.] □

Factorization

Corollary

Let R be a PID and $a \in R$, with $a \notin R^\times \cup \{0\}$. Then, there is $u \in R^\times$ and $p_1, \ldots, p_k$ non-associate primes such that

$$a = up_1^{n_1} \cdots p_k^{n_k}.$$

Moreover, if also

$$a = vq_1^{m_1} \cdots q_l^{m_l},$$

where $v \in R^\times$ and $q_1, \ldots, q_l$ are non-associate primes, then $k = l$ and after reordering for each i we have p_i and q_i are associates and $n_i = m_i$.