Chapter 18 Divisibility in Integral Domains

A class of examples

Motivation Prime and composite numbers in $\mathbb{Z}$ have different meanings in an Integral Domain!

Definition Let D be an integral domain, and $a, b, c \in D$.
(a) If $a = ub$ for some unit u, then a and b are associates.
(b) If $a = bc$ will imply b or c is a unit, then a is irreducible.
(c) If $a|(bc)$ implies $a|b$ or $a|c$, then a is a prime.

Example Consider $D = \mathbb{Z}[d] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$, where $d \neq 1$ and not divisible by p^2 for a prime.

Define $N(a + b\sqrt{d}) = |a^2 - db^2|$. Then

- $N(x) = 0$ if and only if $x = 0$; $N(xy) = N(x)N(y)$;
- $N(x) = 1$ if and only if x is a unit;
- if $N(x)$ is prime then x is irreducible in $\mathbb{Z}[\sqrt{d}]$.

Specific examples

Example 1 In $D = \mathbb{Z}[-3] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$, the element 2 is irreducible, but it is not a prime.

Proof. If $2 = bc$ and $x, y \in D$ are not units, then $4 = N(2) = N(x)N(y)$. So, $2 = N(x) = N(a + b\sqrt{-3}) = a^2 + 3b^2$, a contradiction.

Note that $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ is divisible by 2, but none of $(1 \pm \sqrt{-3})$ is divisible by 2....

Example 2 The element 7 is irreducible in $\mathbb{Z}[\sqrt{5}]$.

More results

Theorem 18.1 In an integral domain, every prime is an irreducible.

Proof. Suppose $p \in D$ is prime. Assume $p = ab$. Then $p|a$ or $p|b$. WOLOG, $a = pt$ so that $p = ptb$ and $tb = 1$, i.e., b is a unit. □

Theorem 18.2 In a PID, every irreducible is a prime.

Proof. Suppose a is irreducible. and $a|(bc)$. Then $A = \{ax + by : x, y \in D\}$ is an ideal so that $A = \langle p \rangle$. So, $a = pt$, and p or t is a unit.
If p is a unit, then $A = D$ and we may assume that $ax + by = 1$ so that $c = (ax + by)c = acx + bcy$ is divisible by a.
If t is a unit, then $b = pr = (at^{-1})r = a(t^{-1}r)$ is divisible by a. □

More definitions

Definition An integral domain (ID) D is a Unique Factorization Domain (UFD) if every element is a product of irreducibles of D, and the factors are uniquely determined up to associates and the rearrangement.

It is a Euclidean domain (ED) if there is a function $d : D^* \to \mathbb{N}$ (called a measure) such that

- $d(a) \leq d(ab)$ for all $a, b \in D^*$,
- for any $a, b \in D$ with $b \neq 0$ there are $q, r \in D$ such that $a = bq + r$ with $r = 0$ or $d(r) < f(b)$.

Main result

Theorem 18.3/18.4 ED ⊂ PID ⊂ UFD ⊂ ID.

Proof. If D is ED, then for any ideal A, let $a \in A$ with minimum positive d value. Then $A = \langle a \rangle$. Else, there is $b \neq aq$ so that $b = aq + r$ with $r \neq 0$ and $d(r) < d(a)$, a contradiction. □

To prove PID ⊂ UFD, we need the following.

Lemma In a PID, any strictly increasing chain of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ must be finite in length.

Proof. Let $I = \cup U_i$. It is an ideal, and $I = \langle a \rangle$ for some $a \in I_r$. Then $I = I_r$.

Proof of Theorem 18.3

Let D be an PID. Suppose $a \in D$ is nonzero and non-unit.
Claim 1. a has an irreducible factor.
If a is irreducible, we are done.
If not, $a = b_1 a_1$ such that b_1 is not unit, and $a_1 \neq 0$.
If a_1 is irreducible, then we are done.
If not, write $a_1 = b_2 a_2$ such that b_2 is not unit, and $a_2 \neq 0$.
Repeating, we get a chain of elements $a, a_2, a_2, \dots$ and

$$\langle a \rangle \subset \langle a_2 \rangle \subset \langle a_2 \rangle \subset \cdots .$$

By the lemma, this chain is finite, and thus we get a irreducible factor a_r.

Claim 2. a can be factored as the product of irreducibles.
Apply the above process to get $a = p_1 c_1 = p_1 p_2 c_2 = p_1 p_2 p_3 c_3 \cdots$ so that $p_1, p_2, \dots$ are irreducible and $\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots$.
Again, the chain must stop after finitely many steps. Thus, $a = p_1 \cdots p_r$.

Claim 3. The irreducible factors are unique (up to associates and permutation).
Let $a = p_1 \cdots p_r = q_1 \cdots q_s$. Now, in a PID, $p_1 | q_1 \cdots q_s$ implies that $p_1 | q_i$ for some i. So, $q_i = u_1 p_1$. Repeating this, we see that there are associates of $p_1, \dots, p_r$ on the right sides. Canceling $p_1, \dots, p_r$ on both sides, we see that the right side will be left with a unit equal to 1. The result follows. □

Example $\mathbb{F}[x]$ is ED.

Example $\mathbb{Z}[\sqrt{-3}]$ is ID, but not UFD, say, $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$.

Example $\mathbb{Z}[x]$ is UFD but not PID; $A = \langle 2, x \rangle \neq \langle h(x) \rangle$ for any $h(x) \in \mathbb{Z}[x]$.

Example $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ is a PID and not ED.

See http://www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf

Theorem 18.5 If D is UFD, then $D[x]$ is a UFD.

Proof. Similar to that of $\mathbb{Z}[x]$.