1 Divisibility in Integral Domains

We now consider the notion of *factoring* in a more abstract setting.

1.1 Associates, Irreducibility, and Prime

Definition 1.1

Let D be an integral domain.

- We say that $a, b \in D$ are **associates** if $a = bu$ for some unit $u \in D$.
- Additionally, we say that a non-unit $a \in D$ is **irreducible** if, whenever $a = bc$ for $b, c \in D$, that b or c is a unit.
- An element $a \in D$ is **prime** if $a|bc \implies a|b$ or $a|c$.

Fact: $a \in D$ is *prime* if and only if $\langle a \rangle \subseteq D$ is a prime ideal.

1.1.1 Example 1: Ring Example

Consider $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$.

- This ring has irreducible elements which are not prime.
- To show this, we define the *norm* map

$$N(a + b\sqrt{-3}) = a^2 + 3b^2$$

This is analogous to $|a + bi| = |a^2 + b^2|$. This respects multiplication, but not addition.

Fact: $N(xy) = N(x)N(y)$ for all $x, y \in \mathbb{Z}[\sqrt{-3}]$.

Proof. Left as an exercise. □

Fact: $x \in \mathbb{Z}[-\sqrt{3}]$ is a unit if and only if $N(x) = 1$.

Proof. If x is a unit, then $xx^{-1} = 1$. This implies that

$$N(x)N(x^{-1}) = N(1) = 1$$

This tells us that $N(x)$ is a unit in $\mathbb{Z}$ and $N(x) \geq 0$. This thus implies that $N(x) = 1$.

Suppose that $N(x) = 1$. Then, $N(x) = xx'$, where x' is the conjugate of x, so $N(x) = 1 \implies \frac{1}{x} = x^{-1}$. □

1.1.2 Example 2: Showing Irreducibility by Contradiction

Show that $1 + \sqrt{-3}$ (from the previous example) is irreducible.

Proof. Suppose, by way of contradiction, that this element is reducible. Then, let $1 + \sqrt{-3} = xy$ for non-units x, y. Then,

$$\begin{aligned} N(1+\sqrt{-3}) &= N(x)N(y) \\ &\implies 4 = N(x)N(y) && \text{For } N(x), N(y) \neq 1 \\ &\implies N(x) = N(y) = 2 && \text{Only possible integer solutions} \end{aligned}$$

Write $x = a + b\sqrt{-3}$. Then
$$N(x) = 2 \implies a^2 + 3b^2 = 2$$
which has no integer solutions. To check this, note that the range of $a^2 + 3b^2$ is $\{0, 1, 3, 4, \dots\}$ because

- If $a = b = 0$, then we get 0.
- If $a = 1$ and $b = 0$, then we get 1.
- If $a = 0$ and $b = 1$, then we get 3.
- If $a = b = 1$, then we get 4.
- As we keep increasing a and b, we will only get larger numbers.

The key is that we can't get 2, a contradiction. □

1.1.3 Example 3: Showing Non-Primeness

Show that $1 + \sqrt{-3}$ (from the previous example) is not prime.

Proof. Note that $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$ (if we expand out the left-hand side, we get 4, which can be broken up into 2 and 2). Then
$$1 + \sqrt{-3} | 2 \cdot 2$$
but, we claim that $1 + \sqrt{-3} \nmid 2$. To do so, suppose towards a contradiction that $1 + \sqrt{-3} | 2$. Then,
$$\begin{aligned}
2 &= (1 + \sqrt{3})(a + b\sqrt{-3}) \\
&\implies 2 = (a - 3b) + (a + b)\sqrt{-3} \\
&\implies \begin{cases} 2 = a - 3b \\ 0 = a + b \end{cases} \\
&\implies a = \frac{1}{2} \text{ and } b = -\frac{1}{2}
\end{aligned}$$
A contradiction. □

1.2 Prime Implies Irreducibility

Theorem 1.1

In an integral domain, every prime is irreducible.

Proof. Let $p \in D$ be prime and suppose
$$p = ab$$
This implies that
$$p | ab$$
But since p is prime, it follows that
$$p | a \text{ or } p | b$$
WLOG, suppose $p | a$. Then, write $a = pk$. This implies that
$$p = (pk)b$$

Since we're in an integral domain, we have multiplicative cancellation so that

$$1 = kb$$

But this implies that b is a unit. $\square$

In particular, irreducible elements in $\mathbb{F}[x]$, where $\mathbb{F}$ is a field, are prime. Thus, they satisfy the property that

$$p(x)|a(x)b(x) \implies p(x)|a(x) \text{ or } p(x)|b(x)$$

1.3 PIDs and Irreducibility

Theorem 1.2

In a PID, an element is irreducible if and only if it is prime.

Remark: The ring $\mathbb{Z}[\sqrt{-3}]$ is not a PID because we were able to construct an element that was not prime.

Proof. If it is prime, then we already showed that it is irreducible. So, suppose that an $a \in D$ element is irreducible. Suppose $a|bc$. Let $I = \langle a, b\rangle = \{r_1 a + r_2 b \mid r_1, r_2 \in D\}$. D is a PID, so there exists some element $d \in D$ such that

$$I = \langle d \rangle$$

$a \in I$ tells us that $a = dr$. But, d is a unit or r is a unit.

- <u>Case 1:</u> Suppose d is a unit. Then, $I = \langle d \rangle = D$. This in particular means that $1 \in I$ and so $1 = xa + yb$ for some $x, y \in D$. Then, we have

  $$c = xac + ybc$$

  Both xac and ybc are divisible by a so

  $$c = a(xc + yq) \implies a|c$$

- <u>Case 2:</u> If r is a unit, then we claim that

  $$\langle a \rangle = \langle d \rangle$$

  This is because

  $$a = dr \implies a \in \langle d \rangle \implies \langle a \rangle \subseteq \langle d \rangle$$

  But as r is a unit, we know that

  $$r^{-1}a = d \implies d \in \langle a \rangle \implies \langle d \rangle \subseteq \langle a \rangle$$

  So, it follows that

  $$\langle a \rangle = \langle d \rangle = I = \langle a, b \rangle$$

  and so

  $$b \in \langle d \rangle = \langle a \rangle \implies a|b$$

So, we are done. $\square$

Fact: If $x, y \in D$ are associates, then $\langle x \rangle = \langle y \rangle$.