<u>Theorem 18.1</u> In an integral domain, every prime is irreducible.

<u>Proof</u> Let a be a prime element of an integral domain D.

Let $b, c \in D$ such that $a = bc$, so that

$$a \neq bc. \qquad (1)$$

Since a is prime, $a | b$ or $a | c$; say $a | b$.
Then there exists $t \in D$ with

$$at = b. \qquad (2)$$

This implies that c is a unit, and so a is irreducible, as follows:

$$1b = b \overset{(2)}{=} at \overset{(1)}{=} bct$$

by Cancellation (Thm. 13.1),

$$1 = ct,$$

and so c is a unit. $\square$

Theorem 18.2 In a principal ideal domain, an element is irreducible iff it is prime.

Proof

($\Leftarrow$) is by Theorem 18.1.

($\Rightarrow$) Let a be an irreducible element of a principal ideal domain D.

Let $b, c \in D$ and assume $a \mid bc$.

(We must show $a \mid b$ or $a \mid c$.)

Define $I = \{ax + by \mid x, y \in D\}$, which is an ideal (Exercise).

D is a PID, so $I = \langle d \rangle$ for some $d \in D$.

$$a = a \cdot 1 + b \cdot 0 \in I = \langle d \rangle,$$

and so $a = d \cdot r$ for some $r \in D$.

a is irreducible $\Rightarrow$ d a unit or r is a unit.

Case 1 d is a unit.

Then $I = D$, and

$$1 = ax + by \quad \text{for some } x, y \in D$$

$$c = cax + bcy$$

and $a \mid cax$ and $a \mid bcy \Rightarrow a \mid c$.

Case 2 r is a unit.

Then $\langle a \rangle = \langle d \rangle$, and

$$b = a \cdot 0 + b \cdot 1 \in \langle a \rangle$$

implies that $b = at$ for some $t \in D$, so that $a \mid b$. $\square$

Lemma B $\mathbb{Z}[x]$ is not a PID.

Proof

Assume to the contrary that $\mathbb{Z}[x]$ is a PID.
Define the ideal

$$I = \{ f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even} \}$$

Then $I = \langle h(x) \rangle$ for some $h(x) \in \mathbb{Z}[x]$.

Note $2 \in I$ and $x \in I$.

Then

$$\begin{aligned} &(1) \quad 2 = h(x) f(x) \\ &(2) \quad x = h(x) g(x) \end{aligned} \qquad \text{for some } f(x), g(x) \in \mathbb{Z}[x].$$

By (1), $h(x)$ is a constant.

$h(x) \mid 2 \Rightarrow h(x) \in \{\pm 1, \pm 2\}$.

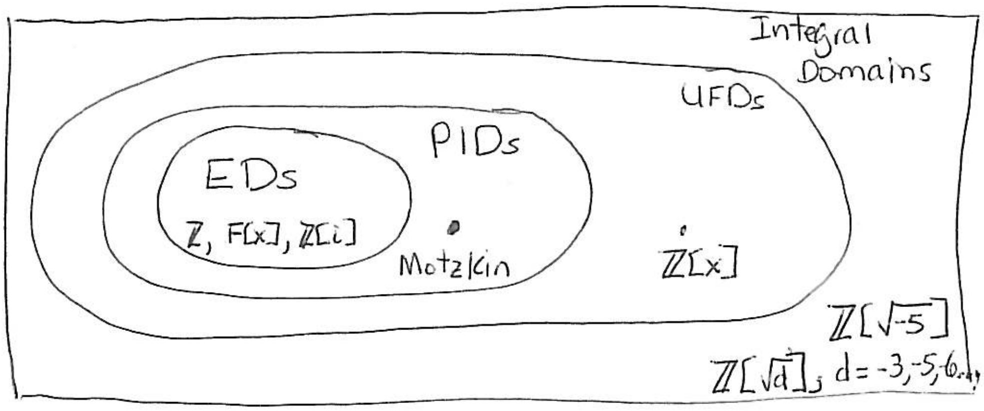
$1 \notin I \Rightarrow h(x) = \pm 2$.

WLOG, assume $h(x) = 2$, since $2, -2$ are associates in $\mathbb{Z}[x]$, and $\langle 2 \rangle = \langle -2 \rangle$.

By (2), $x = 2g(x)$. $\times\!\!\!\times$

Thus $\mathbb{Z}[x]$ is not a PID. $\square$

Integral Domains Diagram



<u>Euclidean Domains</u> Equipped with a division algorithm via a measure function $d : D \to \mathbb{N}$

1. $d(a) \leq d(ab) \quad \forall a, b \in D$
2. $a, b \in D,\ b \neq 0 \Rightarrow \exists q, r \in D$

$$a = bq + r$$

and $r = 0$ or $d(r) < d(b)$

<u>PIDs</u> Every ideal is of form $\langle d \rangle$.

<u>UFDs</u> Every $a \in D \setminus \{0\}$:

1. Can be written as product of irreducibles
2. the product is unique up to associates and order of factors.

Lemma Ascending Chain condition for a PID

In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length.

Proof

Set $I = I_1 \cup I_2 \cup \cdots$.

Then $I = \langle a \rangle$ by the PID assumption, since I is an ideal.

Since $a \in I$, $a \in I_n$ for some I_n in the chain. We must have

$$\langle a \rangle \subseteq I_n \subseteq I,$$

forcing equality throughout;

since $I_i \subseteq I_n$ for all ideals in the chain, I_n must be the last one. $\square$

Theorem 18.3 PID $\Rightarrow$ UFD

Proof Sketch

Let $a_0 \in D$ be a nonzero non-unit.
Iteratively reduce a_0:

$$\begin{aligned} a_0 &= b_1 a_1 \\ &= b_1 b_2 a_2 \\ &\vdots \\ &= b_1 \cdots b_r a_r \end{aligned} \qquad \langle a_0 \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_r \rangle$$

By lemma, this process terminates with an irreducible $a_r \mid a_0$;
Every nonzero nonunit a_0 has an irreducible factor p_1.
Iteratively forward factor:

$$\begin{aligned} a_0 &= p_1 c_1 \\ &= p_1 p_2 c_2 \\ &\vdots \\ &= p_1 \cdots p_s c_s \end{aligned} \qquad \langle a_0 \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots \subset \langle c_s \rangle$$

All p_i's are irred., and by lemma we terminate with an irreducible c_s.
This gives existence of factorization.
Uniqueness is by inductive application of Euclid's Lemma to

$$a_0 = p_1 \cdots p_r = q_1 \cdots q_s . \qquad \square$$

Euclidean domain examples

$\mathbb{Z}$ $\qquad d(a) = |a|$

$F[x]$ $\qquad d(f(x)) = \deg(f(x))$

$\mathbb{Z}[i]$ $\qquad d(a+bi) = a^2 + b^2$

Ex

Form: $a, b \in D$, $b \neq 0$

$\exists q, r \in D$ such that

$a = bq + r$, where $r = 0$ or

$d(r) < d(b)$.

$d : D \to \mathbb{N}$ guarantees termination of repeated division, e.g. Euclidean Algorithm.

in $\mathbb{Z}[i]$, set $a = 3-4i$, $b = 2+5i$.

Then

$$(3-4i) = (2+5i) \cdot \underbrace{(-i)}_{q} + \underbrace{(-2-2i)}_{r}$$

where $d(3-4i) = 25$

$d(-2-2i) = 8$.