Recall An integral domain R is a UFD (unique factorization domain) iff 1) every $r \in R$, $r \neq 0$, $r \neq$ unit is a product of irreducibles and

2) if $p_1 \cdots p_n = q_1 \cdots q_m$, with $p_1, \dots p_n, q_1, \dots q_m$ irreducible, then $n = m$ and $p_i = \text{unit} \times q_{\sigma(i)}$ for all i, where $\sigma \in S_n$.

[Note: $x \in R$ irreducible, $u \in R$ a unit $\Rightarrow ux$ is irreducible. Prove it!]

We want to show: any PID is a UFD.

Lemma 28.4 Let $\{I_k\}_{k=1}^{\infty}$ be an ascending chain of ideals in a ring R. (i.e. $I_k \subseteq I_{k+1}$ $\forall k$) Then $J := \bigcup_{k=1}^{\infty} I_k$ is an ideal.

Proof 1) $0 \in I_1 \subset J$.

2) If $a, b \in J$ then $a \in I_{k_1}$, $b \in I_{k_2}$ for some k_1, k_2. Let $\ell = \max(k_1, k_2)$. Then $a, b \in I_\ell$. Since I_ℓ is an ideal, then $a - b \in I_\ell \subseteq J$.

3) $\forall r \in R$ $\forall a \in J$ $\exists k$ s.t. $a \in I_k$. And then $ra, ar \in I_k \subseteq J$.

$\therefore$ J is an ideal.

Theorem 28.5 Let R be a PID and $\{I_k\}_{k=1}^{\infty}$ an ascending chain of ideals. Then $\exists m$ s.t. $\bigcup_{k=1}^{\infty} I_k = I_m$. (hence $I_j = I_m$ $\forall j \geq m$)

Proof By 28.4 $\bigcup_{k=1}^{\infty} I_k$ is an ideal. Since R is a PID $\exists a \in R$ s.t. $\bigcup_{k=1}^{\infty} I_k = \langle a \rangle$. Then $a \in \bigcup_{k=1}^{\infty} I_k$. $\Rightarrow \exists m$ s.t. $a \in I_m \Rightarrow \langle a \rangle \subseteq I_m$. Since $I_m \subseteq \langle a \rangle$, $\langle a \rangle = I_m$. □

Theorem 29.1 Any PID is a UFD.

Proof Let R be a PID. We need to show: any $r \in R$, $r \neq 0$, $r \neq$ unit, is a product of irreducibles (or is an irreducible) and the factorization into irreducibles is (essentially) unique.

(Existence of factorization) Let $r \in R$, $r \neq 0$, $r \neq$ unit. If r is irreducible, we're done. If not, $\exists r_1, r_2 \in R$, r_1, r_2 not units so that $r = r_1 r_2$. If both r_1, r_2 are irreducible, we're done. If not, one of the r_i's can be factored. Say $r_1 = r_{11} r_{12}$, r_{11}, r_{12} not units.

Keep going. We're done if the process stops.

Suppose the process doesn't stop. We get $r = r_1 r_2$

$r_1 = r_{11} r_{12}$

$r_{11} = r_{111} r_{112}$

$\vdots$

Since none of the r's are units, we get a strictly increasing chain of ideals:

$$\langle r \rangle \subsetneq \langle r_1 \rangle \subsetneq \langle r_{11} \rangle \subsetneq \langle r_{111} \rangle \subsetneq \cdots$$

which is impossible in a PID.

(Uniqueness)

Recall that if $x \in R$ is irreducible and $u \in R$ a unit, then ux is also irreducible.

So to prove uniqueness of factorization into irreducibles, enough to show: if $p_1 \cdots p_m = q_1 \cdots q_n$ where $p_1, \ldots p_m, q_1, \ldots q_n$ are irreducible, then $m = n$ and $\exists \sigma \in S_n$ s.t. p_i, $q_{\sigma(i)}$ are associates $\forall i$, i.e., $p_i = \text{unit} \cdot q_{\sigma(i)}$

Proof by induction on $\max(m,n)$.

If $1 = \max(m,n)$, nothing to prove

Inductive step suppose claim is true for all m, n s.t. $\max(m,n) < k$ and $p_1 \cdots p_m = q_1 \cdots q_n$, $\max(n,m) = k$.

Since R is a PID and p_1 is irreducible, p_1 is prime.

Since $p_1 \mid p_1 \cdots p_m$, $p_1 \mid (q_1 \cdots q_n)$. Since p_1 is prime $p_1 \mid q_j$ for some j. After reindexing $q_1, \ldots q_n$, may assume $p_1 \mid q_1$

$\Rightarrow \exists \alpha \in R$ s.t. $q_1 = \alpha p_1$

Since p_1 is irreducible, it's not a unit. Since q_1 is irreducible, it forces α to be a unit.

$\Rightarrow p_1 \cdots p_m = (p_1 (\alpha q_2)) \cdots q_n$.

Since R is an integral domain, we may cancel p_1.

$\Rightarrow p_2 \cdots p_m = (\alpha q_2) q_3 \cdots q_n$

By inductive assumption $m = n$. Also, after reordering,

p_2 & $q q_2$ are associates, p_3 & q_3 are associates...
This proves uniqueness. □

Products of ideals

Let R be a ring. We have seen that if $I, J \subseteq R$ are ideals, then so is $I \cap J$ and $I + J = \{i+j \mid i \in I, j \in J\}$.
However in general $\{ij \mid i \in I, j \in J\}$ is not an ideal:
given $i_1, i_2 \in I$, $j_1, j_2 \in J$; $i_1 j_1 + i_2 j_2$ need not be of the form $i' \cdot j'$ for any $i' \in I$, $j' \in J$.
Hence one defines $IJ = \langle \{ij \mid i \in I, j \in J\} \rangle$,
The ideal generated by the set $\{ij \mid i \in I, j \in J\}$.

Ex Let $R = \mathbb{Z}[x]$, $I = \langle 2, x \rangle$, $J = \langle 3, x \rangle$.
Then $x = \underset{\in I}{(-2)} \cdot \underset{\in J}{x} + \underset{\in I}{x} \cdot \underset{\in J}{3} \in IJ$ but there is no $p \in \langle 2, x \rangle$, $q \in \langle 3, x \rangle$ s.t. $x = p(x) q(x)$

In general, since $\{ij \mid i \in I, j \in J\} \subseteq I \cap J$, $IJ \subseteq I \cap J$ and the inclusion may be strict:
Let $R = \mathbb{Z}$, $I = 4\mathbb{Z}$, $J = 6\mathbb{Z}$. Then $I \cap J = \{n \in \mathbb{Z} \mid 4 \mid n, 6 \mid n\}$
$= 12\mathbb{Z}$.
While $IJ = \langle \{4n \cdot 6k \mid n, k \in \mathbb{Z}\} \rangle = 24\mathbb{Z}$, and
$24\mathbb{Z} \subsetneq 12\mathbb{Z}$

Ex If R is a PID, $I = \langle a \rangle$, $J = \langle b \rangle$ then
$IJ = \langle \{qa \cdot rb \mid q, r \in R\} \rangle = \langle ab \rangle$

Modules

Slogan: "A module is a vector space over a ring"

WARNING We will assume throughout that our rings are commutative.

Definition Let R be a (commutative) ring. An R-module (or a module over R) is

1) an abelian group $(M, +, 0)$
2) a function $R \times M \to M$ $(r, m) \mapsto rm$ so that
   (a) $(r_1 + r_2)m = (r_1 m) + (r_2 m)$ $\forall r_1, r_2 \in R,\ m \in M$
   (b) $r(m_1 + m_2) = (rm_1) + (rm_2)$ $\forall r \in R,\ m_1, m_2 \in M$
   (c) $r_1(r_2 m) = (r_1 r_2)m$ $\forall r_1, r_2 \in R,\ m \in M$
   (d) $1_R m = m$ $\forall m \in M$.

"Ex" For any field F, an F-module is a vector space over F

Lemma 29.2 Let M be an R-module. Then $\forall m \in M$

$$0_R \cdot m = 0_M \quad \text{and} \quad (-1_R)m = -m.$$

Proof (1) $0_R \cdot m = (0_R + 0_R)m = 0_R m + 0_R m$. Now add $-(0_R m)$ to both sides. We get $0_M = 0_R \cdot m$

(2) $m + (-1_R)m = 1_R m + (-1_R)m = (1_R + (-1_R))m = 0_R \cdot m = 0_M$.

$\Rightarrow (-1_R)m = -m$. □