Groups, Rings and Modules

Chapter 1: Groups
- Simple Groups
- Sylow Theorems

Chapter 2: Rings
- Ideals
- Factorization

Chapter 3: Modules
- Like Vector Spaces, over a ring
- Structure Theorem

Books
- Harthley and Hawkes, "Rings, Modules and Linear Algebra", Chapman and Hall 1970
- Fadleigh, "A First Course in Abstract Algebra", Addison - Wesley
- Cameron, "Introduction to Algebra", O.U.P 1995

Chapter 0: Review from Groups IA

Groups, subgroups, order of an element, order of a subgroup

1. \((\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{C}, +)\)

2. \(\mathbb{Z}/n\), the integers modulo \(n\) (under addition), cyclic

3. \(\operatorname{D}_n\), the dihedral group, symmetries of a regular \(n\)-gon
   (\(n\) rotations, \(n\) reflections)

4. \(S_n\), the symmetric group, permutations of an \(n\)-point set
5. Matrix Groups, e.g. $GL_n(\mathbb{R})$, the group of invertible $n \times n$ real matrices.

**Lagrange's Theorem**

If $H$ is a subgroup of a finite group $G$, then $|H| \mid |G|$. This is true because the left cosets of $gH$ partition $G$, $|G| : |H| = [G : H]$.

**Group Actions**

An action of a group $G$ on a set $X$ is a function $*: G \times X \to X$ such that (writing $g \cdot x = *(g, x)$):

1. $g(h \cdot x) = (gh) \cdot x \quad \forall g, h \in G, \forall x \in X$

2. $e \cdot x = x \quad \forall x$

So each group element is permuting the set $X$. For example, $D_{2n}$ acts on the regular $n$-gon in the obvious way: $g \cdot x = g(x)$.

For $x \in X$, we have the orbit, $\text{orb}(x) = \{ g \cdot x : g \in G \}$, and the stabilizer $\text{stab}(x) = \{ g \in G : g \cdot x = x \}$.

In the above example, $D_{2n}$, $\text{orb}(x) = X$, $\text{stab}(x) = \{ e, \text{reflection in } x \}$.

**Orbit-Stabilizer Theorem**

$|\text{orb}(x)| \cdot |\text{stab}(x)| = |G|$

Writing $H = \text{stab}(x)$, we wish to show that $|\text{orb}(x)| = |H|$ if left cosets of $H$.

We have a bijection left cosets of $H \to \text{orb}(x)$, $gH \leftrightarrow g \cdot x$.

This is well-defined because $h \in H \Rightarrow g \cdot x = (gh) \cdot x$. 
Homomorphisms

A homomorphism $\Theta : G \to H$ is a map that preserves the structure of a group, i.e. $\Theta(gh) = \Theta(g)\Theta(h)$ $\forall g, h \in G$.

The image $\text{Im}(\Theta) = \Theta(G) = \{\Theta(g) | g \in G\} \leq H$.

The kernel $k = \ker(\Theta) = \{g \in G : \Theta(g) = e\} \triangleleft G$.

The kernel $k$ is always a normal subgroup of $G$.

$gk = g'k = e \Rightarrow \Theta(ghg^{-1}) = \Theta(g)\Theta(h)\Theta(g^{-1}) = \Theta(g)\Theta(g^{-1}) = e \Rightarrow ghg^{-1} \in k$.

This is the reason why normal subgroups are important.

Normal Subgroups

Equivalently:

1. $gHg^{-1} = H$ $\forall g \in G$ (our definition)

2. $gH = Hg$ $\forall g \in G$ (left cosets = right cosets)

3. The operation on left cosets given by $(gH)(g'H) = gg'H$ is well defined; it doesn't depend on how we wrote $gH$ and $g'H$. 

For $H$ a normal subgroup of $G$, we can make the left cosets of $H$ into a group by $(gH)(g'H) = gg'H$, called the quotient group, $G/H$. We can view $G/H$ as $G$, but with $g, g'$ regarded as the same if they differ by an element of $H$, i.e. $g = gh$ for some $h \in H$. For example, in $\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ is normal (as $\mathbb{Z}$ is abelian).

Elements of $\mathbb{Z}/7\mathbb{Z}$ are things like $7\mathbb{Z} + 3$. View it as $\mathbb{Z}$, with $x, y$ regarded as the same if $x - y \in 7\mathbb{Z}$ i.e. $x \equiv y \pmod{7}$. This is precisely $\mathbb{Z}_7$. Formally, we have an isomorphism $\mathbb{Z}_7 \to \mathbb{Z}/7\mathbb{Z}$, $x \mapsto x + 7\mathbb{Z}$.

We have $\pi : G \to G/H$, $g \mapsto gh$, the projection (or quotient) map. Clearly $\pi$ is injective, and $\ker \pi = H$. So $H$ normal means that $\exists \Theta$, a homomorphism, $\ker \Theta = H$. Thus, normal subgroups are the same as kernels of homomorphisms from $G$. So we can view $G/H$ just as the image of a homomorphism on $G$ with kernel $H$.

Indeed, we have the Isomorphism Theorem:

Given $\Theta : G \to H$, $\ker \Theta \cong \Theta(G)$ (because with $H = \ker \Theta$, we have an isomorphism $G/H \cong \Theta(G)$).

Permutations

Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

e.g. $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$ has $\sigma = (1\ 3\ 8\ 7\ 6\ 5)$

The cycle type means the set of its cycle lengths. Here, $\sigma$ has cycle type $6, 2$. 
Since every cycle is a product of transpositions, we can write every $\sigma \in S_n$ as a product of transpositions.

E.g. $\sigma = (1\,2\,3\,4\,5) = (1\,2)(2\,3)(3\,4)(4\,5) = (1\,5)(1\,4)(1\,3)$

We say $\sigma$ is even if $\sigma = T_1 T_2 \cdots T_{2k}$ (the $T_i$ are transpositions) and odd if $\sigma = T_1 T_2 \cdots T_{2k+1}$.

This is well defined. No $\sigma \in S_n$ is both odd and even, because composing with a transposition changes the number of cycles by $\pm 1$.

For example: $(1\,2\,3\,4\,9)(4\,7) = (1\,2\,3\,4\,8\,9)(5\,6\,7)$

and so also $(1\,2\,3\,4\,8\,9)(5\,6\,7)(4\,7) = (1\,2\,3\,4\,9)$

So $\sigma = T_1 T_2 \cdots T_{2k} \Rightarrow \#\text{cycles of } \sigma \equiv n \pmod{2}$
and $\sigma = T_1 \cdots T_{2k+1} \Rightarrow \#\text{cycles of } \sigma \equiv n+1 \pmod{2}$

We have the alternating group $A_n = \{ \sigma \in S_n \mid \sigma \text{ even} \}$
with $|A_n| = \frac{n!}{2}$ (since $\sigma \mapsto (1\,2) \sigma$ maps odd $\to$ even)

How many $\sigma \in S_6$ have cycle type $3^2$? We have $6!$ ways to name such a $\sigma$. But each $\sigma$ has been named $3 \times 3 \times 2$ times, so there are $6! \div (3 \times 3 \times 2)$

A subgroup of $S_n$ is a permutation group (of degree $n$). Given a group action on a set $X$, we have a homomorphism $\rho : G \rightarrow S_X$ given by $\rho(g) : X \mapsto x, x \mapsto gx$. Any such $\rho$ is called a permutation representation of $G$.

E.g. Let $D_{12}$ act on the diameters (through vertices of our hexagon) in the obvious way. So we have $\rho : D_{12} \rightarrow S_X$. If $r = \text{rotation by } 120^\circ$ then $r$ keeps each element of $X$ fixed, i.e. $\rho(r) = e$. 
We say that \( \rho \) is faithful if each \( g \neq e \) does something i.e. \( \rho \) is injective.

For example, the above action of \( D_{12} \) is not faithful, but the usual action of \( D_{12} \) (on the hexagon) is faithful.

Cauchy's Theorem (A sort of converse to Lagrange's Theorem)

If \( p \) is prime and \( p \mid |G| \), then \( G \) has an element of order \( p \).

N.B. We do need some restriction on \( p \), as \( 8 \nmid 10 \) in, but \( D_8 \) has no element of order 8, and similarly, \( 12 \nmid 15 \).

The proof of this theorem considers \( p \)-tuples \( (x_1, \ldots, x_p) \) with \( x_1x_2 \cdots x_p = e \).
Groups, Rings and Modules

Chapter 1: Groups

Conjugacy

We say that \( g, g' \) in \( G \) are conjugate if \( g = h g' h^{-1} \) (or equivalently, \( g' = h^{-1} g h \)) for some \( h \in G \).

E.g. in \( S_4 \), we have \( \sigma(1 2 3 4) \sigma^{-1} = (\sigma(1) \sigma(2) \sigma(3) \sigma(4)) \)

So we can view \( h g h^{-1} \) as "\( g \), but with our world view changed." (i.e. we have renamed \( x \) as \( h(x) \))

E.g. In \( D_{2n} \), write \( a \) for rotation by \( \frac{2\pi}{n} \) and \( b \) for a reflection (say in \( L \)). Then, \( a b a^{-1} \) is a reflection in \( aL \).

Note that here, \( b a b^{-1} = a^{-1} \).

Also note that \( (h g h^{-1})^n = h (g^n) h^{-1} \), so \( g \) and \( h g h^{-1} \) have the same order.

The conjugacy class of \( g \in G \) is \( ccl(g) = ccl(a, g) = \{ h g h^{-1} | h \in G \} \).

Examples

1. If \( G \) is abelian, then \( ccl(g) = \{ g \} \)

2. In \( D_{2n} \), \( ccl(a) = \{ a, a^{-1} \} \) and similarly \( ccl(a^r) = \{ a^r, a^{-r} \} \)

So if \( n \) is even, \( ccl(a^r) = \{ a^r, a^{-r} \} \) as \( a^2 = a^{-2} \).

3. In \( D_{2n} \), \( ccl(b) = \) all reflections in lines \( g(L), g \in D_{2n} \)

\[ ccl(b) = \{ b(L), \text{ all reflections, } n \text{ odd} \}
\]

\[ \text{ NOT } b(L), \text{ half of the reflections, } n \text{ even} \]
Conjugation in $S_n$

**Proposition 1** \( \sigma, \tau \in S_n \) are conjugate \( \iff \) \( \sigma, \tau \) have the same cycle type.

**Proof**

\( (\Rightarrow) \) Say \( \tau = \rho \sigma \rho^{-1} \). Write \( \sigma = \sigma_1 \cdots \sigma_k \) disjoint cycles, where \( \sigma_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \). Then, \( \rho \sigma \rho^{-1} = \sigma_1' \cdots \sigma_k' \), where \( \sigma_i' = (\rho(a_{i1}), \ldots, \rho(a_{in})) \), so \( \sigma, \tau \) have the same cycle type.

\( (\Leftarrow) \) Given \( \sigma, \tau \) of the same cycle type, say \( \sigma = \sigma_1 \cdots \sigma_k \) and \( \tau = \tau_1 \cdots \tau_k \), where \( \sigma_i = (a_{i1}, \ldots, a_{in}) \) and \( \tau_i = (b_{i1}, \ldots, b_{in}) \), define \( \rho \in S_n \) by \( \rho(a_{ij}) = b_{ij} \). Then \( \rho \sigma \rho^{-1} = \tau \). \( \Box \)

What happens in \( A_n \)?

Certainly, if \( \sigma, \tau \in A_n \), conjugate in \( A_n \), then they are conjugate in \( S_n \), so they have the same cycle type. However, the converse cannot always be true in \( A_n \). For example, \( A_3 \) is abelian (as it is cyclic), so \( (1 2 3) \) and \( (1 3 2) = (1 2 3)^2 \) are not conjugate.

**Proposition 2**

Let \( \sigma \in A_n \). Then \( \text{ccL}_{A_n}(\sigma) = \text{ccL}_{S_n}(\sigma) \), unless the cycle type of \( \sigma \) consists of only odd cycles of distinct lengths, in which case \( \text{ccL}_{S_n}(\sigma) \) breaks into two conjugacy classes in \( A_n \).

**Proof**

Certainly, \( \text{ccL}_{A_n}(\sigma) \subseteq \text{ccL}_{S_n}(\sigma) \). Conversely, if \( \sigma, \tau \) have the same cycle type, must they be conjugate in \( A_n \)?

If so then \( \text{ccL}_{A_n}(\sigma) = \text{ccL}_{S_n}(\sigma) \).
If not, then \( \sigma \) breaks into two conjugacy classes in \( A_n \), namely \( (p \sigma p^{-1} : p \text{ even}) \) (any of these are trivially conjugate in \( A_n \)) and \( (p \sigma p^{-1} : p \text{ odd}) \).

Given \( T \) of the same cycle type as \( \sigma \), say \( \sigma = c_1 \cdots c_k \) and \( T = c'_1 \cdots c'_k \), where \( c_i = (a_{i1} \ldots a_{ir_i}) \) and \( c'_i = (b_{i1} \ldots b_{ir_i}) \), then we define \( p(a_{ij}) = b_{ij} \) as before.

If \( p \) is even, then \( \sigma, T \) are conjugate in \( A_n \). If not:

If some cycle lengths are even; say \( c_i = (a_{i1} \ldots a_{an_i}) \) and \( c'_i = (b_{i1} \ldots b_{im_i}) \), then rewrite \( c'_i \) as \( b_2 b_3 \ldots b_{im_i} \). Then \( p \) is replaced by \( b_2 b_3 \ldots b_{im_i} \circ p = p' \).

Thus, \( p' \circ p'^{-1} = T \), and \( p' \) is even, as \( b_{im_i} \) is odd. So we may assume that all the \( r_i \) are odd.

If the \( r_i \) are not distinct; and \( r_1 = r_2 \) say, then \( c'_1 = (b_{11} \ldots b_{1m_1}) \), \( c'_2 = (d_{11} \ldots d_{1m_2}) \). Rewrite \( c'_1 c'_2 \cdots c'_k \) as \( c'_2 c'_1 \cdots c'_k \).

Then, \( p \) is replaced by \( (b_1 d_1)(b_2 d_2) \ldots (b_{im_i} d_{im_i}) \circ p = p' \).

Then, \( p' \circ p'^{-1} = T \), and \( p' \) is even (as \( r_i \) is odd).

If all the \( r_i \) are odd and distinct, then the only ways to write \( T \) are to cycle symbols in each \( c_i \) separately, hence we cannot replace \( p \) by an even permutation, as a product of odd length cycle is even.

Thus, \( \sigma \) is not conjugate to \( p \sigma p^{-1} \) for any odd \( p \in S_n \).
e.g. in $A_7$, the cycle types are $7, 5 \cdot 1^2, 4 \cdot 2 \cdot 1, 3^2 \cdot 1, 2^2$, $3^2 \cdot 1^4, 2^2 \cdot 1^3$.

Only elements of cycle type 7 have a conjugacy class in $S_7$ that breaks into two in $A_7$. 
Let $G$ be a group. $G$ acts on itself by conjugation: $g*x = gxg^{-1}$

(This is an action: $g*(h*x) = g*(hch^{-1}) = ghxh^{-1} = (gh)x(gh)^{-1} = (gh)x(gh)^{-1}$)

The orbit of $x$ is $cc(x)$, so the conjugacy classes partition $G$, and (for $G$ finite) have sizes dividing $|G|$ (by the Orbit-Stabilizer Theorem).

Both useful.

The stabilizer of $x$ is $\{g : gxg^{-1} = x\} = \{g : gx = xg\}$ called the centralizer of $x$, written $C(x)$.

So by the Orbit-Stabilizer Theorem, $|C(x)| \cdot |cc(x)| = |G|$ (for finite $G$).

For $G$ finite, say with conjugacy classes $cc(x), \ldots, cc(y)$, we have $\sum_{i=1}^n |cc(x_i)| = |G|$, the "class equation" of $G$. Using that $|cc(x_i)| = \frac{|G|}{|C(x_i)|}$ this is the same as $\sum_{i=1}^n \frac{|G|}{|C(x_i)|} = |G| \Leftrightarrow \sum_{i=1}^n \frac{1}{|C(x_i)|} = 1$.

e.g. in $D_6$: $C(a) = \langle a \rangle = \text{all rotations}$

$cc(x) = \{a, a^{-1}\} \Leftrightarrow n=2 \Rightarrow \sum_{i=1}^n \frac{1}{|C(x_i)|} = 1$.

For $n$ odd:

$C(b) = \{e, b\} = \langle b \rangle$, $cc(b) = \text{all reflections} = \langle b, 1 \rangle$, $|cc(b)| = \frac{|G|}{2}$

For $n$ even:

$C(b) = \{e, a^{\frac{n}{2}}, b, a^{\frac{n}{2}}b\}$

$cc(b) = \text{half of all reflections} = \{a^{\frac{n}{2}}, 0 \leq \theta \leq \frac{\pi}{2}\}$
Then, the class equation for $D_{2n}$ is:

\[
\begin{align*}
\text{(For } n \text{ odd)} & \quad 1 + 2 + \ldots + 2 + n = 2n \\
\text{ } & \quad \underbrace{e} \quad \frac{n}{2} \text{ times} \\
\text{(For } n \text{ even)} & \quad 1 + 1 + 2 + \ldots + 2 + \frac{n}{2} + \frac{n}{2} = 2n \\
\text{ } & \quad \underbrace{e} \quad \frac{n}{2} - 1 \text{ times}
\end{align*}
\]

The center of $G$ is $Z(G) = \{ g \in G \mid \forall h \in G, gh = hg \}$.

$Z = \{ g \in G : g \text{ commutes with all of } G \} = \{ e \} \iff G$ is abelian.

- **Example 1:** $Z(G) = G \iff G$ is abelian.
- **Example 2:** $Z(D_{2n}) = \begin{cases} \{ e \} & \text{if } n \text{ is odd} \\ \{ e, \alpha, \alpha^2 \} & \text{if } n \text{ is even} \end{cases}$
- **Example 3:** $Z(S_n) = \{ e \}$ ($n > 3$)

Note that $Z$ is a subgroup of $G$, either directly or because $Z = \bigcap_{g \in G} C(g)$. Also, $Z$ is normal, because if $g \in Z$, then $ghg^{-1} = g \in Z$. Alternatively, $Z = \ker p$, where $p : G \to S_n$ is the permutation representation of our action. Hence, $Z$ is normal.

**A useful lemma:**

**Lemma 3**

Let $G$ be a group with center $Z$. Then $G/Z$ cyclic $\Rightarrow G$ abelian.

**Proof:**

Let $gZ$ be a generator of $G/Z$, so that every left coset of $Z$ is of the form $g^iZ$ for some $i \in \mathbb{Z}$. 

2
Then every element of $g$ is of the form $g^ix$ for some $i \in \mathbb{Z}$, $x \in \mathbb{Z}$. But $\forall i, j \in \mathbb{Z}$, $x, y \in \mathbb{Z}$, $g^ix$ and $g^jy$ commute:

$g^ixg^jy = g^jg^ixy = g^jg^iyx = g^jyg^ix$

whence $G$ is abelian.

\[\square\]

Warning

It is tempting to think that $\mathbb{Z}/2\mathbb{Z}$ abelian $\Rightarrow G$ abelian, but this is false.

E.g. $|\mathbb{Z}/(08)| = 2$, so $|\mathbb{Z}/(08)| = 4$, so $\mathbb{Z}/(08)$ is abelian, whereas $D_4$ is not abelian.

Corollary

Every group $G$ of order $p^2$ ($p$ prime) is abelian (a strong statement).

Proof.

Each conjugacy class has size 1 or $p$ or $p^2$. We have $121 = 1$, $p$ or $p^2$, and $121 \equiv 0 \pmod{p}$ (as the sum of all conjugacy classes' sizes $\equiv 0 \pmod{p}$), and all other sizes are $\equiv 0 \pmod{p}$.

Hence, $121 \neq 1$, so $121 = p$ or $p^2$.

But $121 = p \Rightarrow |G/1| = p \Rightarrow G$ cyclic $\Rightarrow G$ abelian

$\Rightarrow 121 \neq p \Rightarrow p$

Thus $121 = p^2$. 
1. In fact, $G = \mathbb{Z}_p^2$ or $\mathbb{Z}_p \times \mathbb{Z}_p$ (This can be done directly, see Chapter 3)

2. This does not extend to $|C| = p^3$; i.e., $D_8$ is not abelian.
Simple Groups

A non-trivial group \( G \) is simple if it has no normal subgroups apart from \( \{ e \} \) and \( G \).

For example, \( \mathbb{Z}_p \) is simple (\( p \) prime), \( D_{2n} \) is not simple, and we can either see this directly, or because using normal subgroup \( \langle a \rangle \) or notice that \( \langle a \rangle \) has index 2.

If \( H \leq G \) has index 2, then \( H \) is normal, as left cosets = right cosets = \( \{ H, G/H \} \).

\( S_n \) is not simple, as \( A_n \triangleleft S_n \).

Proposition 5

\( G \) simple, abelian \( \Rightarrow G \cong \mathbb{Z}_p \) for some prime \( p \).

Proof

Choose \( x \in G \), \( x \neq e \). Then \( \langle x \rangle \) is normal (as \( G \) is abelian), so we must have \( \langle x \rangle = G \).

If \( \langle x \rangle \) is infinite, then \( \langle x^2 \rangle \) is a proper normal subgroup. \( \times \)

If \( \langle x \rangle \) is finite, then suppose \( x \) has order \( d \). Then if \( d \) is prime, \( G \cong \mathbb{Z}_p \).

If \( d \) is composite, choose \( d' | d \) with \( d' \neq 1, d \). Then \( \langle x^{d'} \rangle \) is a normal subgroup. \( \times \)

We can now view simple groups as the building blocks for finite groups. If a finite group \( G \) is not simple, then we can...
decompose $G$ into $H$ and $G/H$ with $H \leq G$, then repeat if either $H$ or $G/H$ are not simple.

Remark

Simple groups are quite elusive, e.g. there are none of order $p^2$ (for $p$ a prime). Later, we will prove that $A_n$ is simple for $n \geq 5$.

\textbf{P Groups}

Let $p$ be prime. $G$ is a $p$ group, if every element has order a power of $p$ (e.g. any group of order $p^n$ by Lagrange). Do any others exist? (e.g. a $5$-group of order $75$).

This cannot happen as a finite group is a $p$-group $\iff |G| = p^n$ for some $n$ (due to Cauchy).

\textbf{Proposition 5.}

Let $p$ be prime. Then $|G| = p^n$ (some $n \geq 1$) $\implies$ $G$ is not simple.

\textbf{Proof.}

By the class equation, if we have $|Z(G)| = 0 \pmod{p}$, (as every other conjugacy class not in $Z(G)$ has size $\equiv 0 \pmod{p}$) and so $Z(G) \neq 1$.

So we are done, unless $Z(G) = G$, i.e. $G$ is abelian, and then $G$ is not simple by proposition 5.

\textbf{Corollary 2}

Let $p$ be prime, $|G| = p^n$. Then $G$ has subgroups of all orders $p^m$ for $0 \leq m \leq n$. 

Groups, Rings and Modules

Note: This is a converse to Lagrange.

Proof

By induction on $n$. $n=1$ (and $n=0$) are true.

Given $G$ with $|G| = p^n$ for some $n>1$, we know that $Z \neq \{e\}$, so we choose $x \in Z$, $x \neq e$. WLOG, $x$ has order $p$ (because we can replace $x$ by a power of $x$ if necessary).

So $H = \langle x \rangle$ is normal (as $H \subseteq Z$). We have a projection map

$$\pi: G \to \mathbb{Z} / H, \quad g \mapsto gH$$

Now, $|\pi^{-1}(H)| = p^n$, so $\pi^{-1}(H)$ has subgroups of order $p^m$, for $0 \leq m \leq n-1$. But for a subgroup $K$ of $\pi^{-1}(H)$, we have $|\pi^{-1}(K)| = p^m$, with $|\pi^{-1}(K)| = 1 \leq m \leq n$.

Note: This is a good example of when knowledge of $H$ and $\pi^{-1}(H)$ tells us about the whole group.

The Sylow Theorems

Let $p$ be prime, and let $|G| = p^m m$, where $(p, m) = 1$.

A subgroup of $G$ is a Sylow-$p$-subgroup if it has order $p^m$ (the largest power of $p$ dividing the order of $G$).

e.g. in $D_6$, a Sylow-$5$-subgroup has order $25$, e.g. the rotations.

A Sylow-$2$-subgroup has order $2$ e.g. a reflection plane.
Theorem 8 (Sylow's Theorems)

Let $G$ be a group of order $p^aq$ where $p$ is prime and $(p, m) = 1$

i) There exists a Sylow-$p$-subgroup

ii) All the Sylow-$p$-subgroups are conjugate.

iii) The number $n_p$ of Sylow-$p$-subgroups is $\equiv 1 \pmod{p}$ and $n_p | m$.

Example

1. $|G| = 1000 \Rightarrow G$ is not simple.

   This is because $n_5 \equiv 1 \pmod{5}$ and $n_5 | 8$, so $n_5 = 1$. Hence $G$ has a
   unique subgroup of order 125. So $H$ is normal, as any conjugate
   $gHg^{-1} = H$ by uniqueness.

2. $|G| = 56 \Rightarrow G$ is not simple.

   This is because $n_7 \equiv 1 \pmod{7}$ and $n_7 | 8$, so $n_7 = 1$ or 2.
   If $n_7 = 1$, then $G$ is not simple, as above, so WLOG let $n_7 = 2$.

   The Sylow-$7$-subgroups meet pairwise at $\geq 3$ giving us
   at least $2 \times 6 = 12$ elements of order 7.

   Also, by Sylow, $G$ has a subgroup of order 2. Now, $H$ cannot
   have an element of order 7, so as $56 - 12 - 12 = 8$, it follows that
   $H = \text{All elements not of order 7}$.

   Hence $H$ is unique, and $G$ is not simple.
Corollary 9

Let \( p, q \) be primes, WLOG \( p < q \). Then \( 1G = p \Leftrightarrow G \text{ not simple} \).

Proof:

\[ n_q \equiv 1 \pmod{p}, \ n_q \nmid p \Rightarrow n_q = 1 \ (n_q \neq p \Rightarrow p \neq 1 \pmod{q}, p < q) \].

The Sylow-\( p \)-subgroup is therefore unique, and hence normal. \( \square \)

Corollary 10

Let \( p, q \) be primes, \( p < q \). \( q \neq 1 \pmod{p} \Rightarrow \) the only group of order \( pq \) is \( \mathbb{Z}_{pq} \) (e.g. every group of order 15 is cyclic).

Proof:

Let \( G \) be a group of order \( pq \). Then

\[ n_q \equiv 1 \pmod{q}, \ n_q \nmid p \Rightarrow n_q = 1 \ (as \ p \neq 1 \pmod{q}). \]

Similarly, \( n_p = 1 \).

Every element of \( G \) has order 1, \( p, q \), or \( pq \). We have exactly

\( p-1 \) elements of order \( p \), and exactly \( q-1 \) of order \( q \).

But \( 1 + (p-1) + (q-1) < pq \) (nice \( p, q \); \( \geq 2 \).

\( \Rightarrow \exists \) an element of order \( pq \). \( \square \)

For a group \( G \), \( G \) acts on all subgroups of \( G \) by conjugation:

\[ g \ast H = g H g^{-1} \].

\( \text{Ord}(H) = \{ g H g^{-1} \} \text{ set of all conjugates of } H \)

\[ \text{Stab}(H) = \{ g \in G \mid g H g^{-1} = H \} \text{ the Normalizer of } H, N(H) \).

1. \( H \leq N(H) \), as \( H H^{-1} = H \forall H \in H \)

2. \( H \leq N(H) \), normal in \( N(H) \), by definition

3. \( N(H) \) is the largest subgroup in which \( N \) is normal, by definition.
Example.

\[ S_3 \leq S_5 \quad (\text{Here, } S_3 = \{ \sigma \in S_5 \mid \sigma(4) = 4, \sigma(5) = 5 \}) \]

Then \((34) \in N(S_3)\). But \((45) \in N(S_3)\) since \((45)S_3(45)^{-1} = S_3\).

Proof of Theorem 2

We have \(|G| = p^aq \cdot (p, q) = 1\).

Let \(P\) be a maximal \(p\)-subgroup. We would like \(|P| = p^a\), i.e., \(\frac{G}{P}\) is congruence to \(p\). We write \(\frac{G}{P} = \frac{G}{P} \cdot \frac{P}{P}\), \(\frac{G}{P} \approx \frac{P}{P}\), where \(N = N(P)\). This is helpful as \(\frac{G}{P} \approx \frac{P}{P} \cdot \frac{N}{P}\), where \(\frac{G}{P} = \text{ congruence of } P\), by the orbit-stabilizer theorem.

We must show that \(\frac{G}{P}\) are conjugate to \(P\).

For \(\text{If } \frac{G}{P} \approx \frac{P}{P} \cdot \frac{N}{P}\), \(\frac{N}{P} \geq 0 \pmod{p}\) then \(\frac{N}{P}\) has a subgroup \(K\) of size \(\frac{P}{P}\) (Cauchy). Then \(\frac{G}{P}\) has size \(p\cdot \frac{P}{P}\) contradicting the maximality of \(P\).

For \(\text{If } \frac{G}{P} \approx \frac{P}{P} \cdot \frac{N}{P}\), \(\frac{N}{P} \geq 0 \pmod{p}\). We have \(P\) acting on \(X\), so that the orbit of the action have nizes \(1, p, p^2, \ldots\). There is an orbit of size \(1\), namely \(x_p\) since \(pP^{-1} = P\) \(\forall x \in P\).

Claim: There are no other orbits of size \(1\) (completing the proof as then \(|X| = 1 \pmod{p}\)).

Proof of Claim:

Suppose \(pP^{-1}\) is an orbit of size \(1\). Then \(P\) fixes \(pP^{-1}\) i.e., \(pP^{-1} = xP^{-1} \forall x \in P\) and \(x \in pP^{-1}\)

fixes \(P\) as \((xP^{-1})P(xP^{-1})^{-1} = pP^{-1}\) \(\forall x \in P\).
Therefore \( g'^{-1} P g \subset N \).

Now, \( \pi \) (\( g'^{-1} P g \)) has order dividing \( [g'^{-1} P g] \) (as \( \pi \) is a homomorphism) so must have \( |\pi (g'^{-1} P g)| = 1 \) as \( P \not\subseteq \pi (g'^{-1} P g) \) i.e. \( g'^{-1} P g \subset P \).

Hence \( g'^{-1} P g = P \).

ii) Let \( Q \) be a Sylow-\( p \)-subgroup of \( G \). We would like \( Q, P \) conjugate. We have \( Q \) acting on \( X \) (with orbit sizes \( 1, p, p^2, \ldots \)).

But \( |X| \not\equiv 0 \pmod{p} \), so \( 3 \) an orbit of size \( 1 \): say \( Q \) fixes \( g' P g'^{-1} \). Thus \( g'^{-1} Q g \) fixes \( P \) (as before) so \( g'^{-1} Q g \subset P \).

Hence, \( \pi (g'^{-1} Q g) = \{ e \} \) (as before) and so \( g'^{-1} Q g \subset P \), and \( g'^{-1} Q g = P \).

iii) We know that \( n_P = \{ x \} \) (by (ii)) and \( |X| \equiv 1 \pmod{p} \), so \( n_P \equiv 1 \pmod{p} \). Also, \( n_P | k_1 \) as \( n_P \) is an orbit of \( G \) and \( (n_P, p) = 1 \), so we must have \( n_P | k_1 \).
1. It is not true that \( d \mid |G| \Rightarrow G \) has a subgroup of size \( d \).

\[ \text{e.g. } \mathbb{Z}_4 \text{ has no subgroup of order } 6 \text{ (direct check)} \]

OR We are about to show that \( A_5 \) is simple, so \( A_5 \) has no subgroup of order 30 (as a subgroup of index 2 would be normal).

OR There is no subgroup of order 15 in \( S_5 \) (since there is no element of order 15).

2. Corollary 10 is the best possible. If \( p < q \) are primes with \( q \equiv 1 \pmod{p} \), then \( \exists \) a non-cyclic (even non-Abelian) group of order \( pq \).

**Warnings** about identifying a group:

1. If \( G \) has a normal subgroup \( H \), we need not have \( G \cong H \times J \).

\[ \text{e.g. } \mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \]

2. We can know \( H \) and \( J \) but not know \( G \).

\[ \text{e.g. } G = \mathbb{Z}_4, H = \mathbb{Z}_2, J = \mathbb{Z}_2, \text{ but } \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ also has } H \cong \mathbb{Z}_2, J \cong \mathbb{Z}_2 \]

3. If \( G \) has subgroups \( H, K \), with \( H \cup K = \{e, j\} \) and \( |H| | |K| = |G| \), we need not have \( G \cong H \times K \).

\[ \text{e.g. } G = S_3, H = \langle (1 2) \rangle, K = \langle (1 2 3) \rangle, \text{ but } S_3 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \Rightarrow S_3 \text{ is non-Abelian while } \mathbb{Z}_2 \times \mathbb{Z}_3 \text{ is Abelian.} \]

However, if \( H, K \) commute, then \( G \cong H \times K \).

Define \( \theta : H \times K \rightarrow G \), \( (h, k) \mapsto hk \).
Then $\Theta$ is a homomorphism, due to commutativity.

$\Theta$ is injective because $hk = e \Rightarrow h = k^{-1} \in H \Rightarrow k \Rightarrow k = e$.

$\Theta$ is injective as $|G| = |H||k|$.

We say that $G$ is the internal direct product of $H$ and $K$.

We know that if $H \triangleleft G$, index 2, then $H$ is normal. This is not true for a higher index, e.g. $\langle (1,2) \rangle$ in $S_3$. It is not even true if $G$ is large, e.g. $\langle (1,2) \rangle \times \mathbb{Z}_{1000}$ in $S_3 \times \mathbb{Z}_{1000}$. However:

**Theorem II**

Let $G$ be a group with a subgroup $H$ of index $k$. Then, $|G| > k$.

$\Rightarrow H$ is not simple.

**Proof.** (Very Important!)

Let $H$ have left cosets $g_1H, g_2H, \ldots, g_kH$. $G$ acts on $H$ by left multiplication i.e. we have a homomorphism $\Theta : G \rightarrow S_k$.

Then $\ker \Theta$ is normal, so we are done, unless $\ker \Theta = \{1\}$ or $G$.

We cannot have $\ker \Theta = \{1\}$ as $|G| > |S_k| = k!$, and we cannot have $\ker \Theta = G$ (e.g. $\Theta(g_1^{-1}(g_2)) = g_1^{-1}g_2 \not\in S_k$).

E.g., $|G| = 48 \Rightarrow G$ not simple (as a Sylow-2-subgroup has order 16, index 3, and $48 > 3!$).

The techniques we have so far, such as Sylow, element-counting, and subgroup sizes, all small indices, are enough to show that there is no simple group (apart from $Z_p$, p prime) of order less than 60, which brings us to $A_5$. 
Simplicity of $A_n$

$A_n$ is not simple, as it has a normal subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\}$ which is normal, as it is a union of conjugacy classes.

We aim to show that $A_n$ is simple for $n \geq 5$.

**Proposition 12**

$A_n$ is generated by its 3-cycles.

**Proof**

For $i, j, k$ distinct, $(i j)(j k) = (i j k)$

For $i, j, k, l$ distinct, $(i j)(k l) = (i j)(j k)(j k)(k l) = (i j k)(j k l)$

Hence, any product of an even number of transpositions is a product of 3-cycles.

Now, all 3 cycles are conjugate in $A_n$ for $n \geq 5$. Hence, it is normal in $A_n$, $(n \geq 5)$ and it contains any 3 cycle, then $H = A_n$ (or $H$ must be the union of conjugacy classes).

**Theorem 12**

$A_n$ simple for $n \geq 5$.

**Proof**

By induction on $n$:

$n = 5$: Conjugacy classes in $A_5$ have sizes 1, 15, 20, 12, 12 (sum = 60) and no sum of these, including 1, divides 60.
Alternatively, suppose $H$ is a proper normal subgroup of $A_5$. If $|H| = 3$, then by Cauchy, $3 | H$, order 3, so $H$ has a 3 cycle and $H = A_5$.

If $|H| = 2$, then $H$ has order 2 by Cauchy. WLOG, $h = (12)(34) \in H$, then also $(15)(34) \in H$, as they are conjugate and $H$ is normal. Then the product $(12)(15) = (215) \in H$.

The only case left is $|H| = 5$. WLOG, $H = \langle (12345) \rangle$, not normal.
Groups, Rings, and Modules

Proof that $A_n$ is simple \((n \geq 5)\) \(\Rightarrow f \in \mathfrak{g}_{A_n} : \sigma(n) = n^2\)

Given $H$ normal in $A_n$, we have $A_{n-1} \triangleleft A_n$

Claim \(\exists \sigma \in H, \sigma \neq 1, \sigma(n) = n\)

Proof of Claim Choose $\sigma \in H, \sigma \neq 1$. Say $\sigma(n) = i$ \(\text{(WLOG } i \neq n\)}

We seek $\sigma \in H, \sigma \neq 1, \sigma(n) = i$. Then $\sigma^{-1} \sigma(n) = n$.

Pick $j \neq i, n, \sigma(j) \neq j$ \(\text{(as } \sigma \neq \text{conjugation)}\) \(\text{(we may have } \sigma(j) = n, \text{ no effect)}\)

Now choose distinct $x, y \neq i, n, j, \sigma(j)$ \(\text{(} \rightarrow 6\) \)

and let $\sigma' = (i \ x \ y) \sigma (i \ x \ y)^{-1}$

Then $\sigma' \in H, \sigma'(n) = i$, and $\sigma' \neq 1 \Rightarrow \sigma'(3) = i \Rightarrow \sigma'(3) = \sigma(3)$

So $H \cap A_{n-1} \neq \{1\}$. But $H \cap A_{n-1}$ is normal in $A_{n-1}$, so $H$ is normal in $A_n$.

$H \cap A_{n-1} = A_{n-1}$ \(\text{ (induction hypothesis)}\)

Thus $(1, 2, 3) \in H$

Finite Simple Groups as Building Blocks

Write $H \triangleleft G$, $H$ normal in $G$.

For a finite group $G$, a composition series for $G$ is a sequence

\[ G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_r = \{e\} \text{ with each } G_i \text{ simple.} \]

(Equivalently, $G_i$ is a maximal proper normal subgroup of $G_i$)

The $G_i$ are the composition factors of $G$.

\[ \text{e.g. } S_4 : 1 \triangleright D_8 \triangleright A_4 \triangleright D_6 \triangleright \{e, (12)(34)\} \triangleright \{e\} \]

\[ \text{Factors: } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \]

\[ Z_6 : Z_6 \triangleright [0, 2, 4] \triangleright \{1\} \text{ or } Z_6 \triangleright [0, 3] \triangleright \{e\} \]

\[ \text{Factors: } \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \]

\[ D_8 : D_8 \triangleright \langle a \rangle \triangleright \{e, a^3, a^5\} \triangleright \{e\} \]

\[ \text{Factors: } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \]

\[ \text{or } D_8 : D_8 \triangleright \langle a, b \rangle \triangleright \{e, a, b, ab\} \triangleright \{e\} \]

\[ \text{Factors: } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \]
Clearly, every finite group has a composition series.

Jordan-Hölder Theorem: The factors are unique (up to re-ordering?).

We say $G$ is soluble if all factors $\frac{G_i}{G_{i-1}}$ are cyclic.

$\Rightarrow$ "$G$ is built out of cyclic groups"

$\Rightarrow$ "$G$ is $G_0 \odot G_1 \odot \ldots \odot G_k \cong \mathbb{Z}^j$ with all $G_i$, abelian"

$\Rightarrow$ "$G$ is built out of abelian groups." $\Rightarrow$ "$G$ is nice." (1)

2.3.1 Any abelian group

3. $D_4$

4. $S_n \text{ (n \geq 5)}$

If $H \triangleleft G$, $G$ soluble $\Rightarrow$ $H, \frac{G}{H}$ soluble.

So for example, any $p$-group is soluble (as $\mathbb{Z} \cong \mathbb{Z}_p^j$).

Burnside's $p^aq^b$ Theorem: If $p, q$ primes, $|G| = p^aq^b \Rightarrow G$ soluble.

The Non-Abelian Finite Simple Groups

We have $\mathbb{Z}_p$ (p prime) and $A_n \text{ (n \geq 5)}$. The next simple group has order $168$:

$\text{GL}_3(\mathbb{Z}_2) = 3 \times 3 \text{ invertible matrices, entries in the field } \mathbb{Z}_2$

and similarly, $\text{GL}_n(\mathbb{Z}_2), \forall n \geq 3$.

What about $\text{GL}_n(\mathbb{Z}_p)$, (p prime)?

No, as $\text{det}$ is a homomorphism with non-trivial kernel.

So try $S\text{Ln}(\mathbb{Z}_p) = \{ A \in \text{GL}_n(\mathbb{Z}_p) : \text{det} A = 1 \}$

but this might have a centre $\mathbb{Z} = \{ \lambda I, \lambda^n = 1 \}$

So we try $P\text{SL}_n(\mathbb{Z}_p) = S\text{Ln}(\mathbb{Z}_p) / \mathbb{Z}$. These are simple except for $n=2, p=2$, and $n=2, p=3$.\]
In total, we get 16 such infinite classes, 'Simple groups of Lie type', analogues of some continuous matrix groups.

**Classification Theorem for finite simple groups**

All the finite simple groups are:

1. \( Z_p \) (p prime)
2. \( A_n \) (n \& 5)
3. The 16 infinite families of groups of Lie type
4. The 26 sporadic simple groups, ranging in size from 7920 (\( M_{11} \), one of the Mathieu groups) to \( 2^{64} \cdot 3^{12} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 23 \cdot 29 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \) (IM, the monster)
Chapter 2: Rings

A ring is a set $R$, with binary operations $+$ and $\cdot$, and elements $0$, $1$ such that

1) Under $+$, $R$ is an abelian group with identity $0$

2) $\cdot$ is commutative, associative, and distributive over $+$
   
   $\forall x, y, z \in R, \quad xy = yx, \quad x(yz) = (xy)z, \quad x(y+z) = (xy) + (xz)$

3) $1x = x \quad \forall x \in R$

Examples

1) $\mathbb{Z}$ (usual $+$ and $\cdot$)  
2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
3) $\mathbb{Z}_n$ (any $n$)  
4) $R[x]$ - the set of polynomials with coefficients

5) $\mathbb{Z}[\mathbb{Z}] = \{a+b\mathbb{Z} | a, b \in \mathbb{Z}\}$ (this is a dense subset of $\mathbb{R}$)

6) $\mathbb{Z}/(i) = \{a+bi | a, b \in \mathbb{Z}\}$

7) All functions from $\mathbb{R}$ to $\mathbb{R}$ with pointwise operations
   
   e.g. $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$

   $0$ is the constant function $0$, $1$ is the constant function $1$.

8) $C[0, 1] = \{\text{continuous functions} | [0, 1] \rightarrow \mathbb{R}\}$

9) For any set $X$, we can make $P(X)$ into a ring by
   
   $A + B = A \cup B = A \cup (B \cup (A \cup B))$, $A \cdot B = A \cap B$

   The $0$ is $\emptyset$, and the $1$ is $X$.

10) The trivial ring $R = \{0\}$ (with $1 = 0$), unimportant

Our rings are "commutative with $1$", so for example

$M_n(\mathbb{R}) = \mathbb{R}^{n \times n}$, real matrices are not a ring.
Remarks

1) We can write 0, 1 as 0x and 1x.

2) We have 0x = 0 \forall x \in R \text{ because } 0x = (0+0)x = 0x + 0x

3) We have \((-x)y = -(xy) \forall x, y \in R \text{ because } (-x)y + xy = (-x+x)y = 0y = 0 \Rightarrow (-x)y = -(xy)

We say \(x \in R \) is invertible, or a unit, if there exists \(y \) with \(xy = 1\).

E.g. \(x \in \mathbb{Z} ; \) \(x \) is a unit iff \(x \mid 1\) or \(x \mid -1\).

In \(\mathbb{Z}(i) \), units are \(\pm 1, \pm i\).

Note: If \(y \) does exist, it is unique.

Suppose \(xy' = 1\). Then \(xy = xy' \Rightarrow y = y'\).

Write \(y = x^{-1}\).

A field is a ring \(R\) in which every \(x \neq 0\) is invertible (and \(0 \neq 1\)).

E.g. \(\mathbb{Z}\) is not a field, \(\mathbb{Q}, \mathbb{R}, \mathbb{C}\) are fields.

\(\mathbb{Z}_p\) (p prime) is a field, but not \(\mathbb{Z}_n\) for composite \(n\).

New Rings from Old

Sub-Rings

A subset \(S\) of a ring \(R\) is a sub-ring if it too is a ring under the same operations and constants.

So \(S \subseteq R\) is a sub-ring if:

i) \(S\) is a subgroup of \(R\) under +

ii) \(xy \in S \Rightarrow xy \in S\)

iii) \(1 \in S\)
e.g. in \( \mathbb{Q} \), \( \mathbb{Z} \) is a sub-ring.

In \( \mathbb{Q} \): The dyadic rationals form a sub-ring \( \frac{\mathbb{Q}}{\mathbb{Z}} \), \( a, b \in \mathbb{Q}, b \neq 0 \).

It is the sub-ring "generated by \( \frac{1}{2} \)."

In \( \mathbb{R}[x] \), the constants form a sub-ring. (1 \& 103)

In \( \mathbb{Z} \), \( \mathbb{Z} \) is NOT a sub-ring (1 \& 22), and 0 is not a sub-ring.

In fact, the only sub-ring of \( \mathbb{Z} \) is \( \mathbb{Z} \) itself because \( \mathbb{Z} \) is a sub-group.

\( \Rightarrow S = \mathbb{Z} \).

Direct Sums

For rings \( R \) and \( S \), we have a direct sum \( R \oplus S \) defined on \( R \times S \) with pointwise operations, \((x, y) + (x', y') = (x + x', y + y')\)

and \((x, y)(x', y') = (xx', yy')\).

The 0 is \((0_R, 0_S)\), and the 1 is \((1_R, 1_S)\).

E.g. \( \mathbb{Z} \oplus \mathbb{Z} \) is just the usual \( \mathbb{Z} \times \mathbb{Z} \).

Warning: \( R, S \) fields \( \Rightarrow R \oplus S \) not a field

E.g. \((1, 0)\) NOT a unit
Given a ring, we can form \( R[X] \), the polynomials with coefficients in \( R \) as follows:

\[
R[X] = \{ (a_0, a_1, a_2, \ldots) : a_i \in R \land a_i = 0 \text{ for some } i \}
\]

We can write \( (a_0, a_1, \ldots, a_m) \) as \( a_0 x^m + a_1 x^{m-1} + \ldots + a_m x + a_0 \).

The greatest \( d \) with \( a_d \neq 0 \) is the degree of the polynomial, except for \( 0 = (0, 0, \ldots) \) which does not have a degree.

\( R[X] \) is a ring, with

\[
\sum_{i=0}^{2} a_i x^i + \sum_{i=0}^{2} b_i x^i = \sum_{i=0}^{2} (a_i + b_i) x^i
\]

\[
(\sum_{i=0}^{2} a_i x^i)(\sum_{i=0}^{2} b_i x^i) = \sum_{i=0}^{2} (\sum_{j=0}^{i} a_j b_{i-j}) x^i
\]

\( 0 = (0, 0, \ldots) \), \( 1 = (1, 0, 1) \).

We can view \( R \) as a subring of \( R[X] \) by identifying it with the constants; \( r \leftrightarrow (r, 0, 0, \ldots) \).

Given \( f \in R[X] \), we have an induced function \( f : R \rightarrow R, x \mapsto \sum_{i=0}^{n} a_i x^i \)

(\( f = \sum_{i=0}^{n} a_i x^i \))

E.g. In \( R[X] \), \( x^3 \) induces a function \( x \mapsto x^3 \) from \( R \) to \( R \).

**Warning!** In \( \mathbb{Z}_2[X] \), let \( f = x^2 + x \). Then \( f \neq 0 \) (\( \deg f = 2 \)).

But \( \overline{f} = 0 \) (\( a_0 x^2 + x = 0 \forall x \in \mathbb{Z}_2 \)).

Let \( f \in R[X] \), say \( f = \sum_{i=0}^{n} a_i x^i \) with \( a_n \neq 0 \). We say \( f \) is monic if \( a_n = 1 \).

**Proposition 1** (Division Algorithm for polynomials)

Let \( f, g \in R[X] \), with \( g \) monic. Then we can write \( f = qg + r \) for some \( q, r \in R[X] \) with \( \deg r < \deg g \) (or \( r = 0 \)).
Example
In \( \mathbb{Z}[x] \), write \( x^3 + x^2 + 1 \) as \( q(x^2 - 3) + r \):

We have:
\[
\begin{align*}
x^3 + x^2 + 1 &= x(x^2 - 3) + x^2 + 3x + 1 \\
&= x(x^2 - 3) + 1(x^2 - 3) + 3x + 4 \\
&= (x+1)(x^2 - 3) + 3x + 4
\end{align*}
\]

Note (on video): CANNOT write \( x^3 + x^2 + 1 \) as \( q(2x^2 - 3) + r \)
(deg \( r < 2 \)) failing because 2 is not invertible in \( \mathbb{Z} \)

Proof (by induction on deg \( f \))
\[\text{deg } f < n = \text{deg } g \implies f = 0 \cdot g + f\]

Given \( \text{deg } f = m > n \), say \( f = \sum_{i=0}^{m} a_i x^i \).

Then \( f - a_n x^{m-n} \) has degree \( < m \), so \( f - a_n x^{m-n} g = q g + r \)
i.e. \( f = (q + a_n x^{m-n}) g + r \)
\[\square\]

Homomorphisms, Ideals and Quotients

Let \( R \) and \( S \) be rings. A function \( \theta : R \to S \) is a homomorphism
if it preserves the ring structure.
i.e. \( \theta \) is a group homomorphism from \((R, +)\) to \((S, +)\), and
\[\theta(xy) = \theta(x)\theta(y) \quad \forall x, y \in R, \quad \text{and} \quad \theta(1) = 1\]

Equivalently, \( \theta \) is a homomorphism
\[\iff \theta(x+y) = \theta(x) + \theta(y), \quad \theta(xy) = \theta(x) \theta(y), \quad \theta(1) = 1 \quad \forall x, y \in R\]

If \( \theta \) is also bijective, we say \( \theta \) is an isomorphism and that
\( R, S \) are isomorphic, written \( R \cong S \).
Example

1. \( \Theta : \mathbb{Z} \to \mathbb{Z}_3, x \mapsto x \pmod{3} \)

2. \( \Theta : \mathbb{Z}[x] \to \mathbb{C} \) "put \( x = i \)", \( \sum_{j = 0}^{\infty} a_n x^n \mapsto \sum_{j = 0}^{\infty} a_n i^n \) called "evaluation at \( \alpha \"

Similarly, for any \( \alpha \in \mathbb{C} \) we have a homomorphism \( \mathbb{Z}[x] \to \mathbb{C} \)

3. \( \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \). Define \( \Theta : \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3, x \mapsto (x \pmod{2}, x \pmod{3}) \).

This is well defined, a homomorphism, injective, and surjective (both sides have 6 elements).

The image of \( \Theta \) is \( \text{Im}(\Theta) = \Theta(\mathbb{R}) = \{ \Theta(x) : x \in \mathbb{R} \} \)

e.g., in example 2, \( \text{Im}(\Theta) = \mathbb{Z}[i] \). The image is always a sub-ring of \( S \). It is certainly a subgroup and \( \Theta(x) \Theta(y) = \Theta(xy) \) (So \( \text{Im}(\Theta) \) is closed under \( \cdot \)) \( \Theta(1) = 1_S \) (So \( 1_S \in \text{Im}(\Theta) \))

The kernel of \( \Theta \) is \( \ker(\Theta) = \{ x \in \mathbb{R} : \Theta(x) = 0 \} \)

e.g., in example 1, \( \ker(\Theta) = \{ x \in \mathbb{Z} : x \equiv 0 \pmod{3} \} = 3\mathbb{Z} \)

This is not a sub-ring of \( \mathbb{Z} \).

In fact, if \( \ker(\Theta) \) is a sub-ring, then \( 1 \in \ker(\Theta) \) so \( \forall x \in \ker(\Theta), \Theta(x) = \Theta(x) \Theta(1) = 0 \), so \( \Theta \) is the zero-map, which is not a homomorphism unless \( S = \{ 0 \} \) is trivial, \( 0 = 1 \) \]

That motivates the following definition:

A subset \( I \subset R \) is called an ideal if it is a subgroup of \( (R, +) \) and \( x, y \in I \implies x + y \in I \).

Thus, \( I \) an ideal \( \iff O \in I, x, y \in I \implies x + y \in I \)

So no need
Example

1. $3\mathbb{Z} \subseteq \mathbb{Z}$. Similarly, for any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal.
2. In \( \mathbb{Z}[x] \), the set \( \{ (1+x^2)f : f \in \mathbb{Z}[x] \} \) is an ideal.

**Digression** Is the \( \text{ker } \Theta \) for \( \Theta \) in example 2? (Put \( x = x^2 \))

Certainly if \( g \) is of the form \( (1+x^2)f \) then \( \Theta(g) = 0 \).

\[
\Theta(g) = \Theta(1+x^2) \Theta(f) = (1+x^2) \Theta(f) = 0
\]

Conversely, given \( g \in \text{ker } \Theta \), write \( g = q(1+x^2) + r \) for some \( q, r \in \mathbb{Z}[x] \) with \( r \) of the form \( aX + b \) (by the division algorithm).

So we must have \( \Theta(ax + b) = 0 \), i.e., \( a + b = 0 \) \( \Rightarrow \) \( a = -b = 0 \).

3. In any ring, we have ideals \([0]\) and \(R\). We say ideal \(I\) is proper if \(I \neq R\). An ideal \(I\) is proper \(\iff\) \(1 \notin I\). (If \(1 \in I\), then \(1r, r \in I \Rightarrow I = R\).)

4. In \( \mathbb{Q} \), the only ideals are \([0]\) and \(\mathbb{Q}\).

(If \(q \in I\), and some \(q \neq 0\), then also \(q^{-1} \cdot q = 1 \in I \Rightarrow I = \mathbb{Q}\).

[This is the same for any field.]

Let \(r \in R\). The set \((r) = rR = \{rx : x \in R\}\) is called the ideal generated by \(r\); it is the smallest ideal containing \(r\).

An ideal is principal if \(I = (r)\) for some \(r\).

**Proposition 2**

Every ideal of \( \mathbb{Z} \) is principal \((= (n)\) for some \(n \in \mathbb{Z}\))

**Proof**

WLOG \(I \neq [0]\) \(([0] = (0))\).

Let \(n\) be the least positive element of \(I\).

We claim that \(I = (n)\).
Proof of claim:

If \( m \in \mathbb{Z}_n \) then \( m \in I \) (as \( I \) is an ideal).

Conversely, given \( m \in I \), \( m = qn + r \) for some \( 0 \leq r < n \).

Then \( r \in I \) (as \( r = m - qn \) \( \implies r = 0 \) (choice of \( m \))

i.e. \( m \in \langle n \rangle \).

\[ \Box \]

Similarly, given \( r, s \in I \), write \( (r, s) = rR + sR = \{rx + sy \mid x, y \in \mathbb{Z} \} \).

This is the smallest ideal containing \( r \) and \( s \), and we say that it is generated by \( r \) and \( s \).

Examples/Warning:

1. In \( \mathbb{Z}[x] \), we have ideal \( (x) = \) all polynomials with no constant term.

   and ideal \( (2) = \) all polynomials with even coefficients.

2. In \( \mathbb{Z}[x] \), we also have an ideal \( (2, x) = \) all polynomials with constant even coefficients.

   It is not a principal ideal.

   Indeed, suppose \( (2, x) = (f) \) for some \( f \in \mathbb{Z}[x] \).

   Then \( 2 \) is a multiple of \( f \), so \( f = \pm 2 \), and \( x \) is a multiple of \( f \), so \( f = \pm 1, \pm x \).

   So \( f = \pm 1 \), which is not in \( (2, x) \).

3. Similarly, in \( \mathbb{Q}[x, y] = (\mathbb{Q}[x])[y] \),

   we have ideal \( (x, y) = \) all polynomials with no constant term.

   This is not principal, so if \( (x, y) = (f) \), then \( x \) is a multiple of \( f \), so \( f = \) constant or \( \text{constant} \times x \).

   and similarly for \( y \), so \( f = \) constant \& \( (x, y) \).
Groups, Rings and Modules

A + B = A ⊕ B, A ⋅ B = AnB

4. Even worse, in \( P(\mathbb{N}) \), we have ideal

\[ I = \{ A \in P(\mathbb{N}) : A \text{ is finite} \} \]

Then \( I \) is not even finitely generated.

Indeed, suppose \( I = (A_1, \ldots, A_n) \)

Then \( (A_1, \ldots, A_n) \subseteq A_1 \cup A_2 \cup \ldots \cup A_n \)

but \( \exists A \), finite with \( A \nsubseteq A_1 \cup A_2 \cup \ldots \cup A_n \)

Given these examples, it is reasonable to have:

**Theorem 3**

Let \( F \) be a field. Then all ideals of \( F[x] \) are principal.

**Note** Proofs is the same as for \( \mathbb{Z} \)

**Proof**

Given ideal \( I \) in \( F[x] \), WLOG \( I = \langle 03 \rangle \) (\( 03 = (0) \))

Choose \( f \in I \) with degree minimal. WLOG, \( f \) is monic, because if

\[ f = \sum_{i=0}^{k} a_i x^i \]

we look at \( a_k^{-1} f \) instead.

**Claim** \( I = (f) \)

**Proof of Claim** Certainly if \( g \in (f) \), then \( g \in I \).

Conversely, given \( g \in I \), write \( g = q f + r \) where \( \deg r < \deg f \), or \( r = 0 \).

Then \( r = g - q f \in I \) \( \Rightarrow 0 \), otherwise we contradict minimality

\( \Rightarrow g \in (f) \)
We know that for any homomorphism \( \Theta : R \to S \), \( \ker \Theta \) is an ideal of \( R \) (ker \( \Theta \) is a subgroup, and \( r \in \ker \Theta \Rightarrow \Theta(rx) = \Theta(r)0 = 0 \Rightarrow rx \in \ker \Theta \)).

Conversely, given an ideal \( I \) in a ring \( R \), we have the quotient group \( R/I \).

Elements are of the form \( x+I \), with \( (x+I) + (y+I) = (x+y)+I \).

Define \( \cdot \) on \( R/I \) by \((x+I) \cdot (y+I) = xy+I \).

Note: This is well defined. We need that if \( x+I = x'+I \) and \( y+I = y'+I \), then \( xy+I = x'y'+I \).

Equivalently, \( x-x' \in I \), \( y-y' \in I \) and we want \( xy - x'y' \in I \).

But \( xy - x'y' = (x-x')(y+y') + x'y' - xy' \in I \).

Then \( R/I \) is a ring (inherited from \( R \)).

Ex. \((x+I)(y+I) = (y+I)(x+I)\) because \( xy = yx \).

The 1 is \( 1+I : (x+I)(1+I) = x+I \).

We have \( \pi : R \to R/I \) being a homomorphism with kernel \( I \).

Thus

**Proposition 1** Let \( R \) be a ring, \( I \subseteq R \). Then \( I \) is an ideal.

\( (\Rightarrow) \) If \( \Theta \) a homomorphism, \( \Theta : R \to S \) with \( \ker \Theta = I \).

**Proof**

\( (\Rightarrow) \) \( \ker \Theta \) is always an ideal.

\( (\Leftarrow) \) Given an ideal \( I \), look at the projection map \( \pi : R \to R/I \).
View \( R/I \) as "\( R \), with \( x \) and \( y \) the same if \( x - y \in I \)", i.e. "\( R \), but with \( I \) set to zero"

e.g. \( \mathbb{Z}[x]/\langle 1+x^2 \rangle \) : Elements of the form \( ax + b + \langle 1+x^2 \rangle \) (\( a, b \in \mathbb{Z} \))

So view \( \mathbb{Z}[x]/\langle 1+x^2 \rangle \) as polynoms of the form \( ax + b \), which we add in the usual way, and multiply in the usual way except that \( 1 + x^2 = 0 \)

Thus \( 2 + 3x + (1+x^2) + 3 + 4x + (1+x^2) = 5 + 7x + (1+x^2) \)
and \( (2+3x+(1+x^2))(3+4x+(1+x^2)) = (2+3x)(3+4x) + (1+x^2) \)

\[ \begin{align*}
&= 6 + 17x + 12x^2 + (1+x^2) = -6 + 17x + (1+x^2)
\end{align*} \]

It looks as though \( \mathbb{Z}[x]/\langle 1+x^2 \rangle \cong \mathbb{Z}[i] \)

**Theorem 5 (Isomorphism Theorem)**

Let \( \theta : R \to S \) be a ring homomorphism. Then \( R/\ker \theta \cong \text{Im} \theta \)

**Proof**

The map \( T: R/\ker \theta \to \text{Im} \theta \), \( r + \ker \theta \to \theta(r) \) is a well defined group isomorphism (Isomorphism Theorem for groups).

Also, \( T(rs) = \theta(rs) = \theta(r) \theta(s) = T(r)T(s) \)

i.e. \( T(r + \ker \theta)(s + \ker \theta) = T(r + \ker \theta)T(s + \ker \theta) \)
and \( T(1 + \ker \theta) = \theta(1) = 1 \)

Thus, \( T \) is a ring isomorphism.

**Example** We have \( \theta : \mathbb{Z}[x] \to \mathbb{C} \), \( f \to f(i) \)

with \( \text{Im} \theta = \mathbb{Z}[i] \) and \( \ker \theta = \langle 1 + x^2 \rangle \), so \( \mathbb{Z}[x]/\langle 1+x^2 \rangle \cong \mathbb{Z}[i] \)

A proper ideal \( I \) in a ring \( R \) is maximal if there is no ideal \( J \) with \( I \not\subseteq J \neq R \) (i.e. \( I \subseteq J \subseteq R \Rightarrow J = I \) or \( J = R \))
Examples
1. In \( \mathbb{Z} \), n composite \( \implies \) (n) not maximal (e.g. (6) \( \not\approx \) (2))
2. In \( \mathbb{Z} \), p prime \( \implies \) (p) is maximal
   Indeed, suppose (p) \( \not\approx \) (n) \( \not\approx \) \( \mathbb{Z} \) (valid because all ideals of \( \mathbb{Z} \) are of the form \( n\mathbb{Z} \))
   So n \mid p, but n \( \not\approx \) \pm 1 \( \not\approx \) as p is prime
3. In \( \mathbb{Z}[x] \), the ideal (x) is NOT maximal (surprisingly?)
   \( (x) \not\approx (2, x) \)
   No constant term \( \not\approx \) Even constant term
4. In \( \mathbb{Z}[x] \), (2, x) IS maximal.
   Indeed, suppose \( (2, x) \not\approx J \not\approx \mathbb{Z} \) (J has an element f with odd constant term. But then f-1 \( \in \) (2, x) (as the constant term is even)
   whence 1 \( \in \) J \( \implies \) J = \( \mathbb{Z}[x] \)
5. In \( \mathbb{Q} \), \( 0 \not\approx \) is maximal - the same for any field.
6. In fact, every proper ideal I in \( R \) is contained in a maximal ideal
   (Prove: Logic and Set Theory)
Maximal ideals are important because:

Theorem 6
Let \( I \) be a proper ideal in a ring \( R \).
Then \( I \) maximal \( \iff \) \( R/I \) is a field.

Proof
If \( R/I \) is not a field
We have a \( \in \) \( R/I \), a \( \not\approx \) 0 but a is not invertible.
So \( (a) \) is a proper ideal in \( R/I \)
But then \( J = \pi^{-1}(a) \) is an ideal in \( R \) with \( I \not\subseteq J \not\subseteq R \)

If \( I \) is not maximal

We have an ideal \( J \) with \( I \not\subseteq J \not\subseteq R \)

Choose \( a \in J \setminus I \). Then in \( R/I \), \( a+I \neq 0 \), but \( a+I \) is not invertible. \([\text{If } (a+I)(b+I) = 1+I, \text{ then } ab-1 \not\in I \Rightarrow 1 \not\in J \] \)

\[ \square \]

Example

Consider \( \mathbb{Z}_3[x]/(x^3-x+1) \). Elements are \( a+bx+cx^2+(x^3-x+1) \), so there are \( 27 \) elements. Also, \( (x^3-x+1) \) is maximal, because:

Suppose \( (x^3-x+1) \not\subseteq (f) \not\subseteq \mathbb{Z}_3[x] \) for some \( f \)

(All ideals in \( \mathbb{Z}_3[x] \) are of this form as \( \mathbb{Z}_3 \) is a field.)

\( f \) is not cubic or constant otherwise \( (f) = (x^3-x+1) \) or \( \mathbb{Z}_3[x] \)

So \( x^3-x+1 = \) Linear \cdot Quadratic, which is impossible as \( x^3-x+1 \) has no root.

Conclusion: A finite field of size \( 27 \) \( \not\subseteq \) Highly non-obvious.
Integral Domains

A ring $R$ is an integral domain if $ab = 0 \implies a = 0$ or $b = 0$ (and $0 \neq 1$)
i.e. "$R$ has no zero-divisors"

e.g. $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{R}$ (any field: if $a \neq 0$, $ab = 0$ then $a \cdot ab = 0 \implies b = 0$)
$\mathbb{Z}_p$ ($p$ prime) but NOT $\mathbb{Z}_n$ (a composite) ($\mathbb{Z}_6 : 2 \cdot 3 = 0$)

Note

1. In an integral domain we can cancel a non-zero multiplier
   i.e. $ab = ac$, $a \neq 0$, $a \cdot (b - c) = 0 \implies b = c$

2. If $R$ is an integral domain, and $f, g \in R[x]$ with $\deg f = r$
   $\deg g = s$, then $\deg (f^s g) = r + s$. (Leading terms don't cancel)
   [In $\mathbb{Z}_6[x]$, $(3x^2 + 2x + 1)(2x + 1)$ is not cubic]

3. A homomorphic image of an integral domain may NOT be an integral domain, e.g. $\mathbb{Z} \not\to \mathbb{Z}_n \cong \mathbb{Z}_6$

4. In any ring $R$, the characteristic of $R$ written $\text{char} (R)$, is the least
   positive integer $m$ with $1 + 1 + \ldots + 1 = 0$. (If no such $m$ exists we say
   that $\text{char} (R) = 0$)

   e.g. $\text{Char} (\mathbb{Z}) = \text{Char} (\mathbb{Z}[x]) = \text{Char} (\mathbb{R}) = 0$

   $\text{Char} (\mathbb{Z}_n) = \text{Char} (\mathbb{Z}_n[x]) = n$

   If $R$ is an integral domain, then $\text{char} (R)$ cannot be composite, as
   if $n = ab$, then $(1 + \ldots + 1) = 0 = (1 + \ldots + 1) \cdot (1 + \ldots + 1)$
   So, in an integral domain, the subring generated by $1$ is isomorphic to
   $\mathbb{Z}_p$ ($p$ prime) or $\mathbb{Z}$. 
Proposition 7 Every finite integral domain is a field.

Proof Given a \( a \in R, a \neq 0 \), we seek \( b \in R \) with \( ab = 1 \).

The map \( f : R \rightarrow R, x \mapsto ax \) is injective (\( a(x) = ay \Rightarrow x = y, x \neq y \)). Hence, \( f \) is injective (as \( R \) is finite) so \( \exists x \) with \( ax = 1 \). \( \square \)

Fields of fractions

Given a ring \( R \), how do we "make it a field"?

We could quotient by the maximal ideal to get \( R/I \) (e.g. \( \mathbb{Z}/2\mathbb{Z} \)).

Or, we could try to extend e.g. \( \mathbb{Z} \rightarrow \mathbb{Q} \).

Theorem 8

Let \( R \) be an integral domain. Then, \( R \) a field if it contains \( R \), (i.e. \( R \) has a sub-ring isomorphic to \( R \)).

Remark

1. If \( R \) is not an integral domain, trivially, we cannot extend \( R \) to a

field \( (a, b, 0) \) with \( ab = 0 \).

2. For \( \mathbb{Z} \), take \( \mathbb{Q} = \text{Things of the form } \frac{a}{b} \), which contains a

copy of \( \mathbb{Z} \) via \( n \mapsto \frac{n}{1} \).

Proof

Define an equivalence relation \( \sim \) on \( \{(a, b) \mid a, b \in \mathbb{R}, b \neq 0\} \) by

\[(a, b) \sim (c, d) \text{ if } ad = bc.\]

This is an equivalence relation: Given \( (a, b) \sim (c, d) \) and \( (c, d) \sim (e, f) \), we would like \((a, b) \sim (e, f)\). Given \( ad = bc, cf = de \), we want

\[a \cdot f = be.\]
Multiplying: \( a \cdot c \cdot F = b \cdot c \cdot d \) also cancel \( cd \) if \( c \neq 0 \), as \( R \) is an integral domain, whereas if \( c = 0 \), then \( a = 0 \) and \( e = 0 \).

Write \( F \) for the set of equivalence classes; write \( [a:b] \) for \( [\{a, b\}] \).

Define + on \( F \) by \( \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \).

Well-defined, as \( \frac{a}{b} = \frac{a'}{b'} \Rightarrow \frac{a}{b} \frac{c}{d} = \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d} \).

Indeed, given \( ab = ba \), we want \( \frac{ad + bc}{bd} = \frac{ad + bc}{bd} \) i.e. \( bd(a + bc) = bd(a + bc) \).

Define \( \cdot \) on \( F \) by \( \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \).

Well-defined, as \( \frac{a}{b} = \frac{a'}{b'} \Rightarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'}{b'} \cdot \frac{c}{d} \).

Indeed, given \( a'b = ab' \) we want \( \frac{ac}{bd} = \frac{ac}{bd} \) i.e. \( acbd = a'c'd \).

Ring structure inherited from \( R \), e.g. \( \frac{a}{b} \cdot \frac{c}{d} = \frac{ad}{bd} \Rightarrow \frac{a}{b} = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \).

The 0 is \( \frac{0}{1} \) and the 1 is \( \frac{1}{1} \).

\( F \) is a field as if \( \frac{a}{b} \neq 0 \), then \( a \neq 0 \), so \( \frac{a}{b} = \frac{1}{1} \).

Finally, \( \Theta : R \rightarrow F, r \mapsto r' \) is a homomorphism, and is injective:

\( \frac{r}{r'} \Rightarrow r = r' \), so \( \Theta(R) \cong R \).

**Prime Ideals**

A proper ideal \( I \) in a ring \( R \) is prime if \( ab \in I \Rightarrow a \in I \) or \( b \in I \).

E.g., 1. In \( \mathbb{Z} \), \( (p) \) is a prime ideal for prime number \( p \).

\( ab \in (p) \Rightarrow p | ab \Rightarrow p | b \) or \( p | a \).

2. In \( \mathbb{Z} \), \( (n) \) is not prime if \( n \) is composite (e.g. \( 2 \cdot 3 \in (6) \) but \( 2 \cdot 3 \notin (6) \)).

3. In \( \mathbb{Z}[X] \), \( (a) \) is prime (e.g. \( \Phi \) have constant terms \( \neq 0 \) due \( \Phi \)).

4. In a ring \( R \), \( (0) \) prime \( \iff R \) is an integral domain.
Proposition 9. Let $I$ be an ideal in a ring $R$. Then $R/I$ is an integral domain $\iff I$ is prime.

Proof:

$R/I$ is not an integral domain $\iff \exists a, b \in R$ with $ab + I = 0$ $\implies$ $R/I$ is not prime.

Corollary 10:

Let $I$ be an ideal in a ring $R$. Then $I$ maximal $\implies I$ prime.

Proof:

If $R$ is a field, then $R/I$ is an integral domain.

OR directly:

If $I$ is not prime, then $\exists a, b + I$ with $ab \in I$ so the ideal generated by $I$ and $a$

(namely $(I, a) = I + aR$) must be the whole of $R$.

Hence $1 = x + aR$ for some $x \in I, r \in R$.

Similarly, $1 = y + bR$ for some $y \in I, s \in R$.

Multiply: $1 = x + ab + jar + abrs \in I$

So $I = R$. 

\[ R \]
Factorisation
Euclidean Domain $\iff$ Has division algorithm
$\downarrow$ Trivial
Principal Ideal Domain $\iff$ All ideals are maximal
$\downarrow$ Heart of the section
Unique Factorisation Domain $\iff$ Factorisation works
$\downarrow$
Integral Domain

An integral domain is a principal ideal domain or PID if every ideal is principal (r for some r), e.g., $\mathbb{Z}$, $F[x]$ (F any field)
Not $\mathbb{Z}[x]$ as $(2, x)$ is not principal.

An integral domain $R$ is a Euclidean Domain if $\exists \phi \in R \setminus \{0\}$ such that
1. $\phi(a) \leq \phi(b)$ whenever $a/b$ (a divisor, i.e. $b = ac$ for some c)
2. For $b \neq 0$, we can write $a = qb + r$ for some $q, r \in R$ with $\phi(r) < \phi(b)$ (or $r = 0$)
We say $\phi$ is a Euclidean Function for $R$.

Examples 1. $\mathbb{Z}$, with $\phi(n) = |n|
2. $F[x]$ (F any field) with $\phi(f) = \deg f$
3. Silly example: any field with $\phi(r) = 0 \forall r \neq 0$

Proposition 11. Every Euclidean Domain is a PID

Remarks
1. This is why we care about Euclidean Domains.
2. We've seen the proof twice already ($\mathbb{Z}$, $F[x]$)

Proofs
Given an ideal $I$ in $R$, $I \neq \{0\}$, choose $r \in I$ with $\phi(r)$ minimal.
Claim $I = (r)$
Proof of Claim: Certainly $(r) \subseteq I$ (as $I$ an ideal)
Conversely, given $s \in I$, write $s = x r + y$, for some $x, y \in R$ with $\varphi(y) \leq \varphi(r)$ if $y \neq 0$

Then $y = s - x r \in I$, whence $y = 0$ (choice of $r$)

Irrelevant Remark: PIDs that are not EDs (Examples are quite hard)

A more interesting example of a Euclidean Domain:

**Proposition 12** $\mathbb{Z}[i]$ is a Euclidean Domain.

**Proof:** For all $z \in \mathbb{Z}[i]$, put $\varphi(z) = N(z) = |z|^2$ (the Norm of $z$)

Then $\varphi$ multiplicative:

$\varphi(z) \varphi(w) = \varphi(z w) \forall z, w \in \mathbb{Z}[i]$

Given $z, w \in \mathbb{Z}[i], w \neq 0$: we seek $q, r \in \mathbb{Z}[i]$ with $z = q w + r$

i.e. $q \in \mathbb{Z}[i]$ with $\varphi(z - q w) < \varphi(w)$

But for any $u \in \mathbb{Z}, \exists q \in \mathbb{Z}[i]$ with $|u - q| < 1$ (just choose the closest $q$ to $u$, i.e. choose $x \in \mathbb{Z}$ with $|x - \text{Re}(u)| < \frac{1}{2}$ and $y \in \mathbb{Z}$ with $|y - \text{Im}(u)| < \frac{1}{2}$, and then $|x + iy| < \sqrt{1 + 1} = 1$)

Let $R$ be an integral domain, and $r \in R$, with $r \neq 0$, $r$ not a unit. We say that $r$ is irreducible if $r = ab \Rightarrow a, b$ a unit.

e.g. in $\mathbb{Z}$, any prime $p$ (or $-p$)

In $\mathbb{Z}[x]$, $x$ irreducible, $x^2 + 1$ irreducible (no linear factor)

In $\mathbb{Z}[x]$, $x^3 - x + 1$ irreducible (or else = linear x quadratic, but it has no roots)

We say $a, b$ (in an integral domain $R$) are associates, if $a = bc$ for some unit $c$.

e.g. $3, -3$ in $\mathbb{Z}$

$3 + 4i, i(3 + 4i)$ in $\mathbb{Z}[i]$
Equlivalently, \(a|b\) and \(b|a\).
(Indeed, if \(a, b\) are associates, then \(a|b, b|a\). Conversely, if \(a = cb, b = da\), then \(a = cd\alpha\) whence \(cd = 1\), i.e. \(c\) a unit, unless \(a = 0\) but then \(b = 0\).)

Equllivalently, \((a) = (b) \iff a|b, b|a\)

An integral domain \(R\) is a Unique Factorisation Domain (UFD) if it satisfies:

(UFD1): For \(r \in R, r \neq 0\), not a unit \(\Rightarrow\) we can write \(r\) as a product of irreducibles (i.e. \(r = a_1 \cdots a_k\) for some \(a_1, \ldots, a_k\) irreducible).

(UFD2): This is unique, up to reordering and multiplying by units. (i.e. if \(a_1 \cdots a_k = b_1 \cdots b_l\), some \(a_i, b_j\) irreducible, then \(k = l\) and after reordering, \(a_i\) and \(b_j\) are associates.)

Example 2 (UFD): was an easy induction. UFD 2 was considerably harder; it rested on "\(p|ab \Rightarrow p|a\) or \(p|b\)"
(\textbf{Example 5}) Let's consider two functions, \( f(x) \) and \( g(x) \), where \( f(x) = x^2 \) and \( g(x) = x^3 - 2x + 1 \). We are interested in finding the points where these two functions intersect.

To find the intersection points, we set \( f(x) = g(x) \):

\[ x^2 = x^3 - 2x + 1 \]

Rearranging the equation,

\[ x^3 - x^2 - 2x + 1 = 0 \]

This is a cubic equation, and finding its roots analytically is not straightforward. However, we can use numerical methods to approximate the roots.

Let's denote the roots of this equation as \( a, b, c \) (assuming they are real and distinct for simplicity).

We can then write the intersection points as:

\[ (a, a^2), (b, b^3 - 2b + 1), (c, c^3 - 2c + 1) \]

By plotting these points on a graph, we can visualize the behavior of the two functions and the points of intersection.
Example

\[ \mathbb{Z}[1-3] = \{a + b(1-3) \mid a, b \in \mathbb{Z}\} \text{ not a UFD} \]

We have \(2 \cdot 2 = (1+1)(1-1)\) but \(2 \in \mathbb{Z}[1-3]\) is a unit.

In \(R = \mathbb{Z}[1-3]\), the units are only \(\pm 1\) (since \(1 \neq 0, 1 \neq -1\)).

So \(1 + 1\) is certainly not associate of \(2\).

We just need to check that \(2, 1 + 1\) are irreducible.

2: Suppose \(ab = 2\) for some \(a, b \in R\), non-units.

So \(N(a)N(b) = N(2) = 4\) (since \(N\) is multiplicative), often a useful step.

But \(N(a), N(b) \in \{\pm 1, \pm 2, \pm 4\}\). We cannot have \(N(a) = 1\) (as then \(a\) is a unit).

So \(N(a) = N(b) = 2\). But this is impossible as \(x^2 + y^2 = 2\) has no solutions with \(x, y \in \mathbb{Z}\).

\[ N(1 + 1) = N(1 - 1) = 4, \text{ so the same argument applies.} \]

Remarks 1. Or in \(\mathbb{Z}[1-5]: 2-3 = (1+1)(1-1)\).

2. Historically, many mathematicians were led astray by the fact that sub-rings of \(\mathbb{Z}\) may not be UFDs.

Let \(R\) be an integral domain, \(r \neq 0, r\) non-zero, non-unit. We say that \(r\) is prime if \((r) = \{0, r\} \) or \(r = 1\).

e.g., in \(\mathbb{Z}\), any prime \((\text{in the usual sense})\) \(p\). or \(-p\).

Note that \(r\) prime \(\Rightarrow r\) irreducible. Indeed, if \(r = ab\), then \(r, a, b\) are in \(R\) or \(-R\). But \(r = \pm r\) a associates (as \(r, -r\) are unit.

The converse is false: If \(\mathbb{Z}[1-3]\), \(2\) is irreducible, but not prime.

because \(2 \neq 1(1-1)\) while \(2 + 1 = 3\) (\(1-3\) irreducible).

Lemma 13. Let \(R\) be an integral domain. Then \(R\) is a UFD if it satisfies UFD1 AND UFD2:

1. All irreducibles are prime.

Proof. (\(\Rightarrow\)) Suppose \(r_1, \ldots, r_n = s_1, \ldots, s_m\), where all \(r_i, s_j\) are irreducible. Then \(r_i\) prime, \(r_i = s_i\).
So \( r_1 \mid S_i \) for some \( i \), WLOG, \( r_1 \mid S_1 \). But \( S_i \) is irreducible.

\( r_2 \) is an associate of \( S_i \) \( (r_1 \not \mid a \) unit \( ) \). So WLOG, \( r_1 = S_1 \)

(multiply out other \( r_i \) or \( S_i \) by a unit if necessary)

Hence \( r_2 \triangleq r_1 = S_2 = \ldots = S_k \), and we are done by induction on \( k+1 \).

\((3)\) Suppose \( r \) irreducible, but not prime. We may \( r = r_1 r_2 r_3 \ldots r_k \).

Write \( rS = ab \). We have \( a = r_1 \ldots r_k \), \( b = S_1 \ldots S_k \), for some

\( r_i, S_i \) irreducible. Also have \( S = t_1 \ldots t_m \), all \( t_i \) irreducible.

But now \( r = t_1 \ldots t_m \). \( r \) and \( S \) are different factorisations

\( (a) \) \( r_i \) or \( S_i \) are associates of \( r \), since \( r, r_k \), \( r_k \).

\[ \text{Note that, for } r \neq 0 : (r) \text{ prime } \iff r \text{ prime.} \]

\[ \text{Indeed, if prime says } r | ab \iff r | a \text{ or } r | b \]

\[ \text{Also, } r \text{ a non-unit } \iff (r) \text{ a proper I} \]

\[ \text{Let } R \leq R_0 \leq \ldots \leq R_n, n \neq 0. \text{ Then the following are equivalent:} \]

(i) \( r \) irreducible

(ii) \( r \) prime \iff \( r \) is prime

(iii) \( r \) maximal

\[ \text{Proof:} \]

(ii) \( \Rightarrow \) (i): Prime, are always irreducible in a \( \text{PI} \)

(iii) \( \Rightarrow \) (ii): Maximal ideals are always prime.

(i) \( \Rightarrow \) (ii): (r) proper as \( r \not \mid a \) non-unit. Suppose (r) \( \not \subseteq J \), for some ideal \( J \). We want \( J = R \). We have \( J = (x) \) for some \( x \).

 Thus \( x \) is a unit (r irreducible), so \( J = R \).

Remark: So in a \( \text{PI} \), \( \text{Maximal } \not \subseteq \text{I } \text{prime} \)

(unless \( I = (0) \), always prime, locally even maximal).
Lemma 15

Let \( R \) be a PID, \( r \in R \), non-zero, non-unit. Then \( r \) is a product of irreducible. Suppose not.

Proofs

Suppose not, and \( r \) is not a product of irreducible. (bad)

Then \( r \) is not irreducible, so \( r = a \cdot b \), with \( a, b \) non-unit. So we must have \( a \) or \( b \) also bad. (otherwise \( r \) is not bad).

So \( a_1 = a_2 \cdot b_2 \), for some \( a_2, b_2 \) non-units, with \( a_2, b_2 \) bad.

Continue on, to obtain \( (r) \cong (a_1) \cong (a_2) \cong \cdots \).

Then, let \( I = \langle \text{gcd}(a_i) \rangle \). This is an ideal, and \( xI = (a) \) for some \( x \), (as \( x \) is a PID).

Hence, \( x \in (a) \) for some \( x \).

But then, \( (ac) = 1 \Rightarrow (ac) = (ac+1) = \cdots \). □
Theorem 16
Every PID is a UFD.

Proofs
UFD1 (can factorise into irreducibles): Lemma 15
UFD2 (irreducibles are prime): Lemma 14 □

So we know \( \mathbb{Q}[x] \) (or \( F[x] \) for any field \( F \)) and \( \mathbb{Z}[i] \) are UFDs.

Application: Sums of Two Squares
Which natural numbers are of the form \( x^2 + y^2 \), \( x, y \in \mathbb{Z} \)?
\[
2 = 1^2 + 1^2, \quad 5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2
\]
\( 19 = x \) along \( \mathbb{Z} \) cannot get any \( n \equiv 3 \pmod{4} \) since squares \( \equiv 0 \) or \( 1 \pmod{4} \).

Aim: Prime \( p \equiv 3 \pmod{4} \) \( \Rightarrow \) \( p \) is a sum of two squares.

Reminder. For \( p \) an odd prime, \( -1 \) is a square in \( \mathbb{Z}_p \) \( \Leftrightarrow \) \( p \equiv 1 \pmod{4} \) because if \( p = 4k + 3 \), in \( \mathbb{Z}_p \), if \( x^2 = -1 \), then \( x(x^2) = (x^2)^2 \equiv x^2 \).

Counteracting Fermat.
If \( p = 4k + 1 \), \( (4k)! = -1 \) in \( \mathbb{Z}_p \) (Wilson). But \( (2k)! = (2k)^2 \) (we multiply by \(-1\) even), so take \( x = (2k)! \).

So, for \( p \equiv 1 \pmod{4} \), \( p \mid x^2 + 1 \) for some \( x \).

We want \( p = x^2 + y^2 \) for some \( x \).

Theorem 17
Let \( p \equiv 1 \pmod{4} \) by prime. Then \( p \) is a sum of two squares.

Proofs
We have \( x \in \mathbb{Z} \) with \( p \mid x^2 + 1 \), so in \( \mathbb{Z}[i] \), \( p \mid (x+i)(x-i) \)
but \( p \not\mid (x+i) \), \( (x-i) \) (As \( p(x+i) = p(x+i) \)).

So \( p \) is not prime (in \( \mathbb{Z}[i] \)). So \( p \) is not irreducible (as \( \mathbb{Z}[i] \) is a UFD). We write \( p = a \cdot b \) with \( a, b \) non-units.

So \( p^2 = N(p) = N(a)N(b) \).

But \( N(a), N(b) \neq 1 \) (as \( a, b \) are not units), so \( N(a) = p \), as required.

\[ \square \]

Corollary 18
\( n \) is a sum of two squares \( \Leftrightarrow \) in the prime factorisation of \( n \), each prime \( \equiv 3 \pmod{4} \) occurs to an even power.

Proofs
\(
(\Rightarrow) \text{ For } p \text{ prime, } p \equiv 1 \pmod{4}, \text{ then } p \text{ is a sum of two squares.}
\]
\[
p = 2^1 + 1^2. \text{ If } p = 3 \pmod{4}, \text{ then } p^2 = p^2 + 0^2.
\]
But if \( r, s \) are of two squares \( \Rightarrow \) \( r s \) is a square (as \( N(ab) = N(a)N(b) \))

\[ (\Rightarrow) \quad \text{Let } n = x^2 + y^2, \quad p \equiv 3 \pmod{4}, \text{ a prime with } p \mid n. \]

We will show that \( x, y \) are multiples of \( p \) (indeed \( p^2 = (\frac{x}{p})^2 + (\frac{y}{p})^2 \)

In \( \mathbb{Z}_p \), \( x^2 + y^2 \equiv 0 \), and \( x = y = 0 \), (otherwise \( (xy)^2 + 1 = 0 \) contradicting \(-1 \) not a square in \( \mathbb{Z}_p \)).

\[ \Box \]

\( \text{e.g. } 5, 13, 19^2 \) is a sum of two squares, but \( 7, 13, 19 - 23 \) is not.

We have seen that if \( p \equiv 1 \pmod{4} \) is prime in \( \mathbb{Z} \), then \( p \) is not irreducible (= prime) in \( \mathbb{Z}[i] \). What are the irreducibles in \( \mathbb{Z}[i] \)?

(These are sometimes called the complex primes or Gaussian primes.)

**Theorem 19. The irreducibles in \( \mathbb{Z}[i] \) are precisely**

i) All \( r \in \mathbb{Z}[i] \) with \( N(r) \) prime (in \( \mathbb{Z} \))

ii) All primes \( p \) in \( \mathbb{Z} \) with \( p \equiv 3 \pmod{4} \) (and their associates, \(-p, \pm ip, \pm \bar{p})

**Proof**

If \( N(r) \) is prime: Suppose \( r = ab \), then \( N(r) = N(a)N(b) \).

So \( N(a) \) or \( N(b) = 1 \), i.e. \( a, b \) is a unit.

If \( p \) is prime in \( \mathbb{Z} \) with \( p \equiv 3 \pmod{4} \), suppose \( p = ab \). Then \( p^2 = N(a)N(b) \). But we cannot have \( N(a) = p \) (otherwise \( p \) would be a sum of two squares).

Conversely, let \( r \) be irreducible. If \( N(r) \) is prime (in \( \mathbb{Z} \)) \( \Rightarrow \) \( \text{conclude ...} \)

**Note:** \( r, r^{-1} \) are both, or neither, irreducible in \( \mathbb{Z}[i] \).

If \( N(r) = p^2 \) for some prime \( p \), then \( r = \sqrt{p} \). But \( r, r^{-1} \) are irreducible, so \( r = p \) (up to a unit) or \( \mathbb{Z}[i] \) is an UFD. Also \( \text{we must have } p \equiv 3 \pmod{4} \) otherwise \( p \) is not irreducible.

If \( N(r) = a, p^2 \) for any prime \( p : N(r) = ab \) where \( 1 < a < b < p \).

Thus \( r^2 = ab \), whereas \( r = a, r = b \) or \( r = \bar{a} (\text{up to units}) = \mathbb{Z}[i] \) is a UFD. But a, b are not conjugates.
Gauss' Lemma

\[ \text{Let } f \in \mathbb{Z}[x] \text{ irreducible in } \mathbb{Z}[x] \Rightarrow \text{ irreducible in } \mathbb{Q}[x] \text{ (except for the constant factor)} \]

\[ \text{e.g., } x^2 + x + 1 \text{ irreducible in } \mathbb{Z}[x] \text{ and } \mathbb{Q}[x] \text{ (no linear factor)} \]

but \( 7(x^2 + x + 1) \) is irreducible in \( \mathbb{Q}[x] \) but not in \( \mathbb{Z}[x] \)

**Helpful because**

- **Helpful for showing** \( \mathbb{Z}[x] \) is a UFD
- **To show that polynomials are irreducible in** \( \mathbb{Q}[x] 

**HCFs**

**In an integral domain,** \( a, b \in R 

We say \( \gcd(a, b) \) is an HCF of \( a \) and \( b \) if:

1. \( a \) and \( b \) are both divisible by the HCF
2. \( d \) divides \( a \) and \( b \) for any \( d \) dividing both \( a \) and \( b \)

Hence, \( \gcd(a, b) \) is unique (up to associates).

**If** \( a, c \) are HCFs for \( a \) and \( c \)

\( a \) and \( c \) are associates.

- **Proof:**
  
  \[ a = a_1, b = b_1 \text{ and } a_1 \text{ and } b_1 \text{ are HCFs} \]
  
  \[ a_1b_1 = c, \text{ hence } a_1 = c, \text{ and } b_1 = \text{ an associate of } c \]

- **For a UFD, HCFs do always exist.**

Indeed, given \( a = r \), \( a = r_1 \cdots r_n \) (all irreducible), the factors \( f \) of \( a \) are all products \( \prod r_i \) (and their associates). We cannot have any other factor, \( s \) as otherwise, \( a = st \) would contradict the uniqueness of prime factorization. Hence if \( a = \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m \) and \( a = \beta_1, \beta_2, \ldots, \beta_n \) are both irreducible, no \( \alpha_i \) is an associate of \( \beta_j \) for the HCF of \( a \) and \( b \)

For a UFD, we say \( f \in \mathbb{Z}[x] \) is primitive if no non-unit divides all coefficients of \( f \) (i.e., HCF of coefficients is 1)

Again in \( \mathbb{Z}[x], x^2 + x + 1 \), \( 2x^2 + 3x + 1 \) is not.

**Theorem 2c**

Let \( f \in \mathbb{Z}[x] \) be primitive. Then \( f \) is irreducible in \( \mathbb{Z}[x] \) if and only if \( f \) is irreducible in \( \mathbb{Q}[x] \)

**Proofs**

(1) If \( f \) is not irreducible in \( \mathbb{Z}[x] \), then \( f = gh \) for some \( g, h \in \mathbb{Z}[x] \), both non-constant (\textit{i.e.} \( f \) is primitive), but \( g, h \) are not units in \( \mathbb{Z}[x] \)

(2) Every non-constant \( f \) is irreducible in \( \mathbb{Z}[x] \).
5) Given \( f \in \mathbb{Z}[x] \), suppose \( f = gh \) in \( \mathbb{Q}[x] \), \( g, h \) non-units.
We'll show that some rational multiples \( g' \) and \( h' \) of \( g \) and \( h \) have
\( g'h' = f \) and \( g, h' \in \mathbb{Z}[x] \). Multiplying up, we have
\( nf = g'h' \) for some \( n \in \mathbb{Z} \)
and \( g', h' \in \mathbb{Z}[x] \) (non-constant). If \( n \) is a unit in \( \mathbb{Z} \) (i.e., \( \pm 1 \))
we are done. If not, choose a prime \( p \) with \( p | n \).
Claim: \( p \) divides all coefficients of \( g' \) or all coefficients of \( h' \).
Proof of Claim. Suppose not. Write \( g' = \sum a_i x^i \), \( h' = \sum b_i x^i \), and
choose the least \( i \) with \( p | a_i \) and let \( k \) be the least \( k \) with \( p | b_k \).
Then the \( x^{i+k} \) coefficient of \( g' h' \) is not a multiple of \( p \).
Say \( p | a_g \). Then \( \frac{f}{p} = \left( \frac{p}{a_g} \right) h' \) — done by induction on \( n \)
or the number of prime factors of \( n \).

Remarks
1. The key fact in the proof, namely "\( p | f \) if \( p | f' \) or \( p \not| f' \)" is sometimes
also called Gauss' Lemma.

2. We can rephrase this key fact as \( c(f_g) = c(f) c(g) \) where \( c(f) \) is called
the content of \( f \): the HCF of its coefficients.

Theorem 20 (Gauss' Lemma): \( \mathbb{R} \) a UFD, with field of fractions \( F \).
Then a primitive \( f \in \mathbb{R}[x] \) is irreducible in \( \mathbb{R}[x] \) if and only if irreducible in \( F[x] \).

Theorem 21: \( \mathbb{Z}[x] \) is a UFD
Proof: Given \( f \in \mathbb{Z}[x] \), write \( f = n g \), where \( n \in \mathbb{Z} \), \( g \) primitive.
Write \( n = r_1 \cdots r_k \), each \( r_i \) irreducible in \( \mathbb{Z} \) (\( \mathbb{Z} \) a UFD), so in \( \mathbb{Z}[x] \).
If \( g \) irreducible in \( \mathbb{Z}[x] \), we are done.
If not, write \( g = h h' \), for some \( h, h' \in \mathbb{Z}[x] \) with \(\deg h, \deg h' < \deg g \) (as \( g \) is primitive).
But we can factorise \( h, h' \)
(by induction on degree).

Uniqueness
Suppose \( f = r_1 \cdots r_k g_1 \cdots g_s \) and \( f = r'_1 \cdots r'_k g'_1 \cdots g'_s \)
where the \( r_i, r'_i \) are irreducible in \( \mathbb{Z} \) and the \( g_i, g'_i \) are primitive,
and irreducible
Then \( \overline{r_1 \cdots r_n} = \overline{r_1} \cdots \overline{r_n} = \text{HCF of coefficients of } F \), as a product of primitives is primitive.

So \( \overline{r_1 \cdots r_n} = \overline{r_1} \cdots \overline{r_n} \) in some order (multiplying by a unit if necessary) as \( R \) is a UFD.

So \( \overline{a_1 \cdots a_n} = \overline{a_1} \cdots \overline{a_n} \)

But all the \( \overline{a_i} \), \( \overline{a_i} \) are irreducible in \( \overline{R[x]} \) by Theorem 20, so

\( \overline{a_1 \cdots a_n} = \overline{a_1} \cdots \overline{a_n} \) in some order, because \( \overline{R[x]} \) is a UFD.

Theorem 21

\( R \times UFD \Rightarrow R[x] \times UFD \)

Proof is the same.

Hence, \( \overline{Z[X,Y]} \) or \( \overline{Q[x,y]} = \overline{Q[x,y]} \) are UFD.
...
Proposition 22 (Eisenstein's Criterion) 

Let \( f = \sum a_i x^i \) be primitive. Say \( f = 2a_0 x^i \). Suppose \( f \) is irreducible with primes \( p_1, p_2, \ldots, p_n \) and \( p^2 \mid a_0 \). Then \( f \) is irreducible.

\[ x^3 - 2 \quad (p = 3) \]

Remarks

1. Hence, \( f \) irreducible in \( \mathbb{Q}[x] \) (Gauss' Lemma).

2. We do need \( p^2 \mid a_0 \), e.g. \( (x+2)^2 \) is not irreducible.

Proof:

Suppose not. We have \( f = g_1 \), with \( g_1 = \frac{x}{x+2} \). We have \( x^3 - 2 = 3 \) and \( x^2 + 4 \), so exactly one of \( 3 \) or \( 0 \) is a multiple of \( p \), say \( 3 \).

Hence \( p \mid 3 \) or \( p \mid x+2 \), so \( p \mid g_1 \) or \( p \mid x+2 \).

Proof of Lemma: For any \( f \), \( g \), we have \( f \mid g \) if and only if \( f \mid g \). So \( p \mid 3 \) or \( p \mid x+2 \).

Example:

An irreducible polynomial satisfied by \( p \), \( p \) prime?

For \( (x^p - 1)/(x-1) = x^{p-1} + x^{p-2} + \ldots + x + 1 \)

(a cyclotomic polynomial)

Put \( X = Y + 1 \): The above polynomial is irreducible.

So \( Y^{p-1} + (1) Y^{p-2} + \ldots + (p-2) Y + (p-1) \)

This is irreducible by Eisenstein's criterion.

Two views of \( \mathbb{Z}[\alpha] \)

Let \( \alpha \in \mathbb{C} \). Write \( \mathbb{Z}[\alpha] \) for the subring of \( \mathbb{C} \) generated by \( \mathbb{Z} \) and \( \alpha \). \( \mathbb{Z}[\alpha] = \{ \sum a_i \alpha^i : a_i \in \mathbb{Z} \} \)

Recall that \( \alpha \) is algebraic if it is a root of a non-zero polynomial \( f \in \mathbb{Z}[x] \). We say \( \alpha \) is an algebraic integer if it is the root of a monic polynomial in \( \mathbb{Z}[x] \). e.g. \( 7, x - 7, x^3 - 2 = 3 \).
Let \( \alpha \in \mathbb{C} \) be an algebraic integer, say \( \alpha \) is the root of a monic 
\[ f \in \mathbb{Z}[x], \quad \deg f = n \]
Then \( \mathbb{Z}[\alpha] = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i : a_i \in \mathbb{Z} \right\} \) (division algorithm)

E.g., \( \mathbb{Z}[\alpha] \), \( \alpha \) a root of \( x^2 + 2x + 2 \), is \( \{a + b\alpha, a, b \in \mathbb{Z}\} \)

WLOG, \( f \) is irreducible: if \( f = gh \) look at \( g \) for \( h \) instead.

Other Viewpoint: We have a homomorphism \( \theta : \mathbb{Z}[x] \to \mathbb{Z}[\alpha], \quad g \mapsto g(\alpha) \)
This is injective.

What's \( \ker \theta \)? Certainly, all multiples of \( f \) are in \( \ker \theta \). We cannot have any
other \( g \in \ker \theta \). Indeed, given such a \( g \), \( \deg g < n \)
In \( \mathbb{Q}[x] : \left\{ g : g(\alpha) = 0 \right\} \neq \{0\} \). But \( \{g : g(\alpha) = 0\} = \mathbb{Q}[x] \)
Thus, \( \mathbb{Z}[\alpha] \subseteq \mathbb{Q}[x] \)

In conclusion: Quotienting by \( \langle f \rangle \) can be viewed as "adding in a root of \( f \)"

Noetherian Rigs
A ring \( R \) is Noetherian if every ideal is finitely generated, e.g., any PID.
Not \( \mathbb{P}(\mathbb{N}) \) -- the ideal of \( \mathbb{N} \) is not finitely generated (\( f.g. \))
Not \( \mathbb{Z}[x, y, z, \ldots] \) -- ideal \( \langle x, y, z, \ldots \rangle \) is not finitely generated.

AIM
\( \mathbb{Z}[x] \) Noetherian \( \langle \text{Ideals in } \mathbb{Z}[x] \text{ aren't too bad} \rangle \)
We say that \( R \) has the ascending chain condition (ACC) if whenever
we have ideals \( I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \), then \( I_n = I_{n+1} = \ldots \) for some \( n \).

Proposition 23
\( R \) is Noetherian
\( \implies R \) has an ACC

Proof (\( \Rightarrow \))
Given \( I \subseteq I_2 \subseteq \ldots \), let \( I = I_r I_2 \cup \ldots \)
Then \( I = (r_1, \ldots, r_n) \) for some \( r_1, \ldots, r_n \in I \)
We have \( r_k = I_{r_k} \) for some \( r_k \).
Let $\mathfrak{I}$ be an ideal of $R$, not finitely generated.

Choose $r_1 \in \mathfrak{I}$

Then $(r_1) \neq \mathfrak{I}$ (as $\mathfrak{I}$ is not finitely generated)

So $\exists (r_2) \in \mathfrak{I} \setminus (r_1)$

Then $(r_1, r_2) \neq \mathfrak{I}$ (as $\mathfrak{I}$ is not finitely generated)

Proceed by induction, to obtain,

$(r_1, r_2, r_3, \ldots) \neq \mathfrak{I}$
Theorem 24 (Hilbert's Basis Theorem)

R Noetherian \Rightarrow R[x] Noetherian

Proof:
Let I be an ideal in R[x]. For \( n = 0, 1, 2, \ldots \), let \( I_n \) be

\[ I_n = \left\{ r \in R \mid \text{the leading coefficient of some } f \in I, \text{ of degree } \leq n \right\} \]

\[ = \left\{ r \in R : r x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in I, \text{ for some } a_{n-1}, \ldots, a_0 \in R \right\} \]

Each \( I_n \) is an ideal in \( R \).

We have \( I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots \). (If \( f \in I \), \( \deg f = n \), then \( x^n \notin I, \deg(x^n) = n \).)

So by ACC we have \( I_n = I_m \) for some \( n \).

For each \( n \in \mathbb{N} \), we have \( I_n = (f_n, r_{n1}, \ldots, r_{nk_n}) \) for some \( f_n \), \( r_{nj} \in R \).

For each \( f_n \), choose \( f_{n}^{(j)} \in I \) with \( \deg f_{n}^{(j)} = n \), leading term \( r_{nj} \).

CLAIM: \( I = (f_{n}^{(j)} : n \in \mathbb{N}, j \leq k_n) \subseteq J \)

Proof of Claim: Certainly \( J \subseteq I \).

Conversely, if \( I \subseteq J \), then choose \( g \in I \) of minimal degree.

Say \( \deg g = n \), with leading coefficient \( r_n \).

If \( n \in \mathbb{N} \)

We have \( r_n = \sum c_i f_{n}^{(i)} \), for some \( c_i \in R \).

But then \( g - \sum c_i f_{n}^{(i)} \in I \) and has degree \( < n \), and does not belong to \( J \) (otherwise \( g \) does)

If \( n > \mathbb{N} \)

We have \( r_n I_n = I_n \), so we have \( r_n = \sum c_i f_{n}^{(i)} \), for some \( c_i \).

But then \( g - (\sum c_i f_{n}^{(i)}) x^n \in I \) and has degree \( < n \), and does not belong to \( J \) (otherwise \( g \) does).

\[ \Box \]

Examples:

1. \( \mathbb{Z}[x] \) Noetherian

2. \( \mathbb{C}[x, y] \) (or \( \mathbb{C}[x_1, \ldots, x_n] \)) Noetherian, as \( \mathbb{C}[x] \) is - even though \( \mathbb{C}[x, y] \) is not a P.I.D.

E.g. Let \( f_i \in \mathbb{C}[x_1, \ldots, x_n] \), \( i \in I \), and let \( A = \{ (z_1, \ldots, z_n) \in \mathbb{C}^n : f_i(z_1, \ldots, z_n) = 0 \} \).

Then in fact \( A \) is equal to where a finite set of polynomials vanish.
Chapter 3: Modules

A module is like a vector space, but over a ring \( \mathcal{R} \) instead of a field.

Let \( \mathcal{R} \) be a ring. An \( \mathcal{R} \)-module \( M \) is a set \( M \) with operations

\[ +: M \times M \rightarrow M \text{ and } \cdot: \mathcal{R} \times M \rightarrow M \]

such that

1. \((M, +)\) is an abelian group.
2. \((x+y) \cdot r = x \cdot r + y \cdot r \) \( \forall x, y \in M, r \in \mathcal{R} \)
3. \((r+s)x = rx + sx \) \( \forall x \in M, r, s \in \mathcal{R} \)
4. \(1x = x \) \( \forall x \in M \)

Note that these are exactly the usual vector space axioms.

Examples

1. Any field, \( \mathcal{R} \), any vector space over \( \mathcal{R} \).
2. Any ring \( \mathcal{R} \), \( M = \mathcal{R}^n = \{ (x_1, \ldots, x_n) : x_i \in \mathcal{R} \} \) (with \( (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1+y_1, \ldots, x_n+y_n) \))
3. \( \mathcal{R} = \mathbb{Z} \): ANY abelian group \( G \) becomes a \( \mathbb{Z} \)-module, via \( nx = x + \ldots + x \) \( n \) times. (Or note that if \( n \) is negative, \( -nx = (-1)n x = x + \ldots + x \) \( n \) times.) This is the only way to make \( G \) a \( \mathbb{Z} \)-module; e.g. \( 2x = (1+1)x = x + x \).
   \( \mathbb{Z} \) modules are equal to \( \mathbb{Z} \)-modules.
4. \( \mathcal{R} = \mathbb{Z}_6, M = \mathbb{Z}_6 \) is a \( \mathbb{Z}_6 \)-module, via \( nx = (n \mod 2) x \) (mod 2)
   (This is well defined as 6 is even)
   More generally, for any ring \( \mathcal{R} \), any ideal \( I \) is an \( \mathcal{R} \)-module.
5. \( \mathcal{R} = \mathcal{R}, M = \mathcal{R}[x] \)
6. Let \( V \) be a complex vector space, and \( \alpha: V \rightarrow V \) a linear map.
   Then \( V \) is a \( \mathbb{C}[x] \)-module, via \( f \cdot x = f(x)x \)
   e.g. \( (x^2 + 3x + 2) = ax^2 + 3ax + 2x \)

Note

In an \( \mathcal{R} \)-module, \( 0 \cdot x = 0 \cdot 0 \cdot x = 0 + 0 \cdot x = 0x + 0 = 0 \).
\( 0 \cdot (-1) = -0 = 0 \)
\( 0 \cdot (-1)x = -0x = (1+0)x = x + x = x \cdot (-1) = -1 \)
Groups, Rings and Modules

For \( x_1, \ldots, x_n \in M \) (a module over a ring \( R \)), a linear combination is an element of the form \( r_1 x_1 + \ldots + r_n x_n \) for some \( r_1, \ldots, r_n \in R \). This is sometimes called an \( R \)-linear combination.

We say that the set \( x_i : i \in I \) spans \( M \) if every \( x \in M \) is a finite linear combination of the \( x_i \). The set \( \{ x \} \) is linearly independent if no linear combination is \( 0 \) (unless \( r_i = 0 \)).

A basis is a linearly independent spanning set, i.e.,
1. \( R^n \) has a basis \( \{ e_1, \ldots, e_n \} \) where \( e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \).
2. \( R[x] \) has a basis \( \{ 1, x, x^2, \ldots \} \).

Warnings:
1. \( R = \mathbb{Z}, M = \mathbb{Z}; \{ 2, 3 \} \) is spanning, but does not contain a basis.
2. \( \{ 2 \} \) is linearly independent, but does not extend to a basis.
3. \( \mathbb{Z} \) has a basis of the same size (namely \( \{(1)\} \) ), but the proper subset \( \mathbb{Z}/2\mathbb{Z} \) has a basis of the same size (namely \( \{1\} \)).
4. \( \mathbb{Z} \text{ module } \mathbb{Z} \) has no basis, as any single element \( x \) is linearly dependent (as \( 5x = 0 \)).

For intuition understanding, think of \( R = \text{ Field and } R = \mathbb{Z} \).

New Modules from Old

Submodules:
A submodule of an \( R \)-module \( M \) is a subset \( N \subseteq M \) that is a module under the induced operation.

i.e., i) \( N \) a subgroup of \( (M,+) \)
ii) \( rN \subseteq N \) for \( r \in R, x \in N \)

Examples:
1. \( R = \text{ Field, } M \text{ a vector space over } R \). Then submodules are just subspaces.
2. \( R = \mathbb{Z}; \text{ Submodules are subgroups.} \)
3. \( R \text{ any ring, } M = R; \text{ Submodules are ideals.} \)
4. \( \mathbb{C} \text{ complex vector space, } M: V + V \text{ linear, so } V \text{ is } \{0\} \text{ module.} \)

In this case, submodules are subspaces $W$ that are $\alpha$-invariant ($\alpha(x) \in W$ for all $x \in W$, also called '$\alpha$ acts on $W$').

For $x_1, \ldots, x_n \in M$, the submodule generated by $x_1, \ldots, x_n$ is $\langle x_1, \ldots, x_n \rangle = \{ r_1 x_1 + \ldots + r_n x_n : r_1, \ldots, r_n \in R \}$.

We say $M$ is finitely generated if $M = \langle x_1, \ldots, x_n \rangle$ for some $x_1, \ldots, x_n \in M$, the same as saying that $M$ has a finite spanning set.

E.g., $M = R$, an ideal is finitely generated as an $R$-module.

$\implies$ It is finitely generated as an ideal.

Warning: A submodule of a finitely generated module need not be finitely generated.

E.g., $R = \text{IP}(R)$. Then $R$ is finitely generated ($R = (1)$), but the submodule (ideal) $\{ a < N \mid A \text{ finite} \}$ is not finitely generated.

Direct Sums

For $R$-modules $M$ and $N$, their direct sum $M \oplus N$ consists of the abelian group $M \times N$, made into an $R$-module via $r(x, y) = (r_1 x_1, r_2 y_2)$.

E.g., $R \oplus R = R^2$.

Homomorphisms and Quotients

Let $M$ and $N$ be $R$-modules. A function $\Theta : M \rightarrow N$ is a homomorphism or $R$-homomorphism if it preserves the module structure, i.e., $\Theta(x + y) = \Theta(x) + \Theta(y)$.

If $\Theta$ is bijective, we say that $\Theta$ is an isomorphism between $M$ and $N$, written $M \cong N$.

Examples:

1. $R = \text{Field}$: $R$-homomorphisms are linear maps.
2. $R = \mathbb{Z}$: $R$-homomorphisms are group homomorphisms.
3. If an $R$-module $M$ has a basis, we say that $M$ is free (e.g., $R$, $R^2$, $R^3$, $R[x]$ are all free, $\mathbb{Z}$ is not a free $\mathbb{Z}$-module).
If \(\mathbf{a}\) is a basis \(x_1, \ldots, x_n\) of \(M\), we say that \(M\) is free of rank \(n\) (e.g. \(\mathbb{R}^n\)). Note that if \(M\) is free of rank \(n\), then \(M \cong \mathbb{R}^n\), via \(\theta: \mathbb{R}^n \rightarrow M, (r_1, \ldots, r_n) \mapsto r_1x_1 + \cdots + r_nx_n\).

(\(n \neq m\) is not obvious that \(\mathbb{R}^n \cong \mathbb{R}^m\) when \(n \neq m\)).

4. Similarly, \(M\) finitely generated (i.e. \(M = (x_1, \ldots, x_n)\)) \(\Rightarrow M\) is an image of \(\mathbb{R}^n\) (using the same \(\theta\)).

The image of \(\theta\) is \(\theta(M) = \{\theta(x) \mid x \in M\}\). This is a submodule of \(N\), as it is certainly a subgroup, and \(\theta(\mathbf{a}) = \theta(\mathbf{a}) \in \theta(M)\) for \(\mathbf{a} \in \mathbb{R}, x \in M\).

The kernel of \(\theta\) is \(\ker \theta = \{x \in M \mid \theta(x) = 0\}\). This is a submodule of \(N\), as it is certainly a subgroup, \(x \in \ker \theta \Rightarrow \theta(x) + \theta(x) = \theta(x) = 0\). \(\Rightarrow x \in \ker \theta\). So kernels are submodules. Conversely:

Given an \(R\)-module \(M\), and submodule \(N\), the quotient module \(M/N\) consists of the group \(M/N\), made into an \(R\)-module via \(R(\mathbf{x} + N) = \mathbf{r} \mathbf{x} + N\) (well-defined, as \(\mathbf{x} + N = \mathbf{x}' + N\).

\[\Rightarrow \mathbf{x} - \mathbf{x}' \in N, \mathbf{r}(\mathbf{x} - \mathbf{x}') \in N, \mathbf{r} \mathbf{x} + N = \mathbf{r} \mathbf{x}' + N\]

**Note:** This is an \(R\)-module. The projection map \(\pi: M \rightarrow M/N, \mathbf{x} \mapsto \mathbf{x} + N\) is an \(R\)-homomorphism.

This is a group homomorphism, and \(\pi(\mathbf{r} \mathbf{x}) = \mathbf{r} \mathbf{x} + N = \mathbf{r}(\mathbf{x} + N) = \mathbf{r} \pi(\mathbf{x})\).

**Proposition:** \(M\) an \(R\)-module, \(N \leq M\).

Then \(N\) is a submodule \(\Leftrightarrow N = \ker \theta\) for some \(R\)-homomorphism \(\theta: M \rightarrow P\) (some \(R\)-module \(P\)).

**Proof:**

(\(\Rightarrow\)) kernels are always submodules.

(\(\Leftarrow\)) We have \(N = \ker \pi\), where \(\pi: M \rightarrow M/N\) is the projection map.
Proposition 2 (Isomorphism Theorem). Let $\theta : M \rightarrow N$ be an $R$-homomorphism. Then $\frac{M}{\ker \theta} \cong \theta(M)$.

Proof. We have $f : \frac{M}{\ker \theta} \rightarrow \theta(M)$, a well-defined group isomorphism $x + \ker \theta \rightarrow \theta(x)$.

Also, $f^{-1}(\theta(x) + \ker \theta) = f(x) = x + \ker \theta$.

We know that $M$ finitely generated (say by $x_1, \ldots, x_n$).

$\Rightarrow M$ is an image of $R^n$ by $\theta : R^n \rightarrow M, (x_1, \ldots, x_n) \mapsto x_1 + \ldots + x_n$.

So finitely generated $R$-modules are quotient of $R^n (n = 1, 2, 3, \ldots)$.

A module is cyclic if it is generated by 1 element.

e.g. If $R$ is a field, then the cyclic $R$-modules are $R^1$ and $R$.

$R = \mathbb{Z}$, the cyclic $\mathbb{Z}$-modules are the cyclic groups $\mathbb{Z}$ and $\mathbb{Z}_n$, any $n$.

Note: $M$ cyclic $\Rightarrow M$ an image of $R^n \Rightarrow M \cong R^k$, for some $k$.

The Structure Theorem.

We know a structure theorem for finitely generated modules over a field $F$.

They are $F^n = F \oplus \cdots \oplus F$ ($n = 0, 1, 2, \ldots$). What about over a general ring?

For $R$ a Euclidean Domain, every finitely generated $R$-module is a direct sum of (finitely many) cyclic modules. (The exact result depends on $R$.)

e.g. $R = \mathbb{Z}$

Every finitely generated Abelian group is of the form $\mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \cdots \oplus \mathbb{Z}_n$ (so every finite Abelian group is of the form $\mathbb{Z}_n \oplus \mathbb{Z}_m$).

Remark. Let $R$ be $\mathbb{Z}[x]$ and consider the $R$-module $M = \mathbb{R} \times \mathbb{R}$.

Then $M$ is not a direct sum of cyclic modules.

Indeed, $M$ itself is not cyclic (as $\mathbb{R} \times \mathbb{R}$ is not principal.

And if $M$ is a direct sum of more than one $R$-module, choose non-zero $a_i$ in distinct summands. e.g. $M = M_1 \oplus M_2 \oplus \cdots$. 

Then \( a \cdot b = b \cdot a \), so the two summands meet.

Task: Understand finitely generated \( R \)-modules, i.e., \( R^n \), where \( N \) is a submodule of \( R \).

**Key Ideas**

\( R^n \) is easy to describe if \( N \) "lines up nicely" with respect to the axes of \( R \).

**Example** \((R = \mathbb{Z})\)

1. What is \( \mathbb{Z}^2 / \langle (3, 1) \rangle \)?
   - \( \mathbb{Z}^2 \) is now the submodule generated by \( (3, 1) \).
   - \( (3, 1) \) means " submodule generated by "
   - \( \mathbb{Z}^2 + \mathbb{Z} \)

2. What is \( \mathbb{Z}^2 / \langle (3, 0) \rangle \)?
   - \( \mathbb{Z}^2 + \mathbb{Z} \)

3. What is \( \mathbb{Z}^2 / \langle (3, 6) \rangle \)?
   - Not obvious, because the generators of the subgroups do not "line up" with respect to our basis \( e_1, e_2 \) of \( \mathbb{Z}^2 \).
   - We have a basis \( e_1 = (1, 2), e_2 = (0, 1) \).
   - These are certainly linearly independent, and span because \( e_1 = \frac{1}{2} - 2e_2 \) and \( e_2 = \frac{1}{2} - e_1 \).
   - Thus our quotient i

Let \( A \) be an \( m \times n \) matrix over a ring \( R \).

The elementary row operations on \( A \) are:

1. Swap two rows
2. Multiply a row by a unit
3. Subtract a multiple of a row from another row.

This works similarly for column operations.

**Theorem**

Let \( A \) be a matrix over a Euclidean Domain. Then \( A \) can be obtained from a finite sequence of elementary row and column operations that puts \( A \) into the form

\[
\begin{pmatrix}
    d_1 & \cdots & 0 \\
    \vdots & \ddots & \vdots \\
    0 & \cdots & d_n
\end{pmatrix}
\]

where \( d_1, d_2, \ldots, d_n \) are units.
Proof
If $A = 0$ we are done. If $A \neq 0$ WLOG $a_{i1} \neq 0$
(otherwise, we row and column swap)
Using elementary operations, we produce
either $\left( \begin{array}{c|c} 
0 & \vdots \\
\vdots & B \\
\end{array} \right)$ with $a_{i1}$ dividing each entry of $B$ (so we are done
by induction)
or $\left( \begin{array}{c|c} 
a_{i1} & \vdots \\
\vdots & \end{array} \right)$
with $\|a_{i1}\| < \|a_{i1}\|$, (then repeat, and we are
done as we cannot decrease $\| \cdot \|$ infinitely often)

Write $b = a_{i1}$

Suppose some entry of the top row is not a
multiple of $b$, say $a_i$ in column $j$.
Write $a_i = q_i b + r_i, \|r_i\| < \|b\|$

Now replace column $j$ with column $j + q_i$ column $j$ and then swap columns $1$ and $j$.

Hence, we may assume that all entries of row 1, column 1 are
multiples of $b$. So, by subtracting multiples of row 1 or column 1, we can
make all entries in row 1 and column 1 (except $a_{i1}$) be zero.

Suppose some entry $b_{ii}$ of this matrix is not a
multiple of $b$. Add row $i$ to row 1: We now have
an entry of row 1, not a multiple of $b$, so we are
done as before.

Remarks
1. Sometimes, we say $n \times n$ matrices $A, B$ are equivalent if one can be obtained
   form the other by elementary operations. So Theorem 3 says that any
   matrix $A$ is equivalent to one of the form

2. The $d_i$ are invariant factors for $A$, and the matrix
   is called a Smith Normal Form.

3. In the language of linear maps: Let $\theta : R^n \to R^m$ be an $R$
   homomorphism and $e_1, \ldots, e_n$ basis vectors for $R^n$, $e_1', \ldots, e_m'$ basis
   vectors for $R^m$. The matrix of $\theta$ with respect to $e_1, \ldots, e_n$ and
   $e_1', \ldots, e_m'$ is the $m \times n$ matrix $A' = (a_{ij})$ given by the following:
Then row operations correspond to changes in the basis $e_1, \ldots, e_n$ and column operations to changes in $e_1, \ldots, e_n$.

(e.g. "Swap rows 1 and 2" replaces $f_1, f_2, \ldots, f_m$ with $f_2, f_1, \ldots, f_m$.)

So Theorem 3 is saying that 3 bases with respect to which $\Theta$ has a diagonal matrix.

4. **Hilbert's Remark** Row ops correspond to pre-multiplying $A$ by an invertible matrix, e.g. "Swap rows 1 and 2" is pre-multiplying $A$ by

\[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]

Similarly, column ops correspond to post-multiplication.

So Theorem 3 tells us that if an invertible matrix $P$, $n \times n$ with

$PAQ = \Theta$, diagonal.

**Corollary 4** Let $R$ be a Euclidean domain. Then $R^m \not\cong R^n$ for $m \neq n$.

Note: this is not obvious as we do not have an exchange lemma.

**Proof.** Say $n > m$. Suppose $\Theta : R^n \to R^m$ an isomorphism. Then, by our linear map from of Theorem 3, 3 bases $e_1, \ldots, e_m$ of $R^n$, and $\Theta(e_i)$ of $R^m$, with respect to which $\Theta$ has matrix

\[ \begin{pmatrix} \Theta(e_1) & \cdots & \Theta(e_m) \\ 0 & \cdots & 0 \end{pmatrix} \]

But then, $\Theta(e_i) = 0$

\[ \square \]

**Remarks**

1. Hence, all bases of $R^n$ have size $n$.

2. In fact $R^n \not\cong R^n$ for any ring $R$, but this is harder to prove.
Uniqueness in Smith Normal Form

For an $m \times n$ matrix $A$, over a Euclidean Domain $R$, a $t \times t$ minor of $A$ is the determinant of any $t \times t$ sub-matrix of $A$.

E.g., over $\mathbb{Z}$, \[
\begin{pmatrix}
3 & 4 \\
8 & 7
\end{pmatrix}
\] has a $2 \times 2$ minor $\det \begin{pmatrix} 3 & 4 \\ 8 & 7 \end{pmatrix} = -27$

Note: For $\det$, we have a choice.

Either define $\det X = \sum_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)}$
where entries are in the field of fractions of $R$, so we already have $\det$

Note that row and column operations do not change the HCF of the $t \times t$ minors (for any fixed $t$).

Indeed:

1. Multiplying a row by a unit does not change any $t \times t$ minor (up to multiplying some by that unit).

2. Swapping two rows permutes the $t \times t$ minor (up to a factor $-1$).

3. Adding a row $j$ to row $i$: a minor involving both rows $i$ and $j$ or neither is unchanged.

Finally, consider two matrices $A, B$, identical except that $A$ has row $i$ (and not row $j$) while $B$ has row $j$ (and not row $i$).

Let $a = \det A$, $b = \det B$.

Then the new $b$ has $\det B = b$, and the new $A$ has $\det = a + \lambda b$.

But HCF $(a + \lambda b, b) = \text{HCF}(a, b)$.
Theorem 5 Let $A$ be an $m \times n$ matrix over $R$, a Euclidean Domain with Smith Normal Form $B = \begin{pmatrix} d_1 & \cdots & 0 \\ 0 & \ddots & \vdots \\ 0 & \cdots & d_n \end{pmatrix}$ where $\gcd(a_i, b_i, \ldots, d_n) = 1$ and set $d_0 = d_n = 0$.

Then $\det A = d_1 \cdots d_n$ = HCF of the $t \times t$ minors of $A$ (up to associates).

In particular, the Smith Normal Form is unique (up to multiplying $a_i$ by a unit).

Proof: Elementary operations do not change the HCF of the $t \times t$ minors, so the HCF of the $t \times t$ minors of $A = \text{HCF of } t \times t$ minors of $B = d_1 \cdots d_n$ (where we used $a_i, b_i, \ldots, d_n$).

Example:

Smith Normal Form of $\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$ over $\mathbb{Z}$

Slow way: $\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 4 & -3 \\ -1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 4 & 0 \\ 0 & 3 \end{pmatrix}$

Fast way: HCF of $1 \times 1$ minors = HCF of entire $= 1$

For the $2 \times 2$ minors, $\det \begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix} = 7$, so $d_1 = 1, d_2 = 4$.

One final ingredient:

Lemma 6 Let $R$ be a Euclidean Domain. Then every sub-module of $R^n$ is finitely generated.

Proof (by induction on $n$):

Base case: for $n = 1$, $R$ is a module of $R$, and all ideals of $R$ are principal.

Given $N$, a submodule of $R^n$, for some $n > 1$.

Let $I = \{ r \in R : (r_1, \ldots, r_n) \in N \text{ for some } r_1, \ldots, r_n \}$

Then $I$ is an ideal of $R$, or $I = (a)$ for some $a \in R$.

Choose $x = (x_1, \ldots, x_n) \in N$ with $a_i = x_i$.

Let $N' = \{ (r_2, \ldots, r_n) \in R^{n-1} : (0, r_2, \ldots, r_n) \in N \}$

Then $N'$ is a submodule of $R^{n-1}$, so by induction, we have that $N' = \langle y_1, \ldots, y_k \rangle$ for some $y_1, \ldots, y_k \in R^{n-1}$.

Then $x_i = (0, y_i)$ generates $N$. Indeed, if $y \in N$, then $3 \text{ nd}$ with $y - \text{nd}$ of the form $(0, y_2, \ldots, y_n)$ which is a linear combination of the vectors $(0, y_i)$.
Theorem 7. Let $N$ be a submodule of $R^n$ (with $R$ a Euclidean domain). Then if a basis $e_1, \ldots, e_n$ of $R^n$ and non-zero $d_1, \ldots, d_k \in R$ (for some $k$ such that $N = \langle d_1 e_1, \ldots, d_k e_k \rangle$) is i.e. "$N$ lives up nicely".

Proof. Assume they are a basis for $N$.

Let $e_1, \ldots, e_n$ be a basis of $R^n$ and let $g_1, \ldots, g_m$ generate $N$.

Let $A = [a_{ij}]$ be matrix of the $g_j$ with respect to the $e_i$. Let $g_j = \sum_{i=1}^{n} a_{ij} e_i$.

We can transform $A$ to \[
\begin{pmatrix}
a_{11} & \cdots & a_{1m} \\
0 & \ddots & 0 \\
0 & \cdots & 0
\end{pmatrix}
\]
by elementary row and column operations.

Now, row operations correspond to changing the basis of $R^n$, and column operations to changing the generator of $N$.

Hence $\exists$ a basis $e'_1, \ldots, e'_n$ for $R^n$ such that $N$ has generators $d_1 e'_1, \ldots, d_k e'_k$.

Corollary 8. Every submodule of $R^n$ (with $R$ a Euclidean domain) is free.

Proof. Consider $d_1 e'_1, \ldots, d_k e'_k$ are linearly independent (any dependence would be a dependence among $e'_1, \ldots, e'_n$).

Remarks.
1. In fact, a submodule of any free $R$-module ($R$ a Euclidean domain) is free (harder to prove).

2. Let $R = \mathbb{Z}[x]$. Then the $R$-module $\mathbb{Z}[x]$ is free (it's $R^1$) but the submodule $R(x)$ is not free, and not even a direct sum of any non-zero submodules.
Corollary 7 (Structure Theorem for (finite) generated modules over a Euclidean Domain $R$. Theorem $13$ (finite) direct sum of cyclic modules)

We know that $M \cong R^n$ for some $n$, and $M$ is a finitely generated module over a Euclidean Domain $R$. (Theorem $13$ (finite) direct sum of cyclic modules)

Proof:

We know that $M \cong R^n$ for some $n$, and $M$ is a finitely generated module over a Euclidean Domain $R$. (Theorem $13$ (finite) direct sum of cyclic modules)

Conclude:

For a finite abelian group, we know that $G \cong Z_n \oplus Z_m$. For $G$, we can further break up $G$, obtaining $G \cong Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$. (Theorem $13$ (finite) direct sum of cyclic modules)

In general, a cyclic $R$-module $R/I$ is called primary if $I = (p^a)$, where $p$ is a prime in $R$, or $I = (p_1) \cdots (p_k)$.

In fact, the $p_i^a_i$ are unique (up to ordering). Indeed, for $p$ prime, let $I = (p^a) \cap R = (p_1^a_1^a_1 \cdots p_k^a_k^a_k)$.

and $1/q_i = p^{a_1}\oplus p^{a_2}\oplus \cdots \oplus p^{a_k}$

Generating "$Z_{n_1} \oplus Z_{n_2} \oplus Z_{n_k}$":

Proposition 1 (Chinese Remainder Theorem)

Let $R$ be a PID, and let $x, y, z \in R$ be coprime (i.e., $\gcd(x, y) = 1$).

Then $R/(x) \cong R/(y) \oplus R/(z)$ (isomorphic as $R$-modules).

Proof:

Define $\varphi : R \rightarrow R/(x) \oplus R/(y)$ by $a \mapsto (ax + y, ay + z)$.

Then $\varphi$ is an $R$-homomorphism with ker $\varphi = \langle x, y \rangle$.

Also, we have $1 = ax + y$, so $x, y$ are coprime and $(x, y) = 1$.

Thus $R/(x) \cong R/x$. (Theorem $13$ (finite) direct sum of cyclic modules)

Note: This proof shows that $R/(x) \cong R/x$, so primary.

Corollary 12 (Primary Decomposition Theorem)

Let $M$ be a finitely generated module over a Euclidean Domain $R$. Then $M$ is a finite direct sum of primary modules $R/P_i$, or $0$.

Proof:

By the Structure Theorem, followed by the Chinese Remainder Theorem.
Jordan Normal Form

A linear map on a finite-dimensional complex vector space $V$ has matrix (with respect to some basis) that is a diagonal matrix with blocks (for various $i$).

Remarks

1. Given the Jordan Normal Form, we can record off many properties of $A$. For example, for an eigenvalue $\lambda$, the algebraic multiplicity (as a root of the characteristic polynomial) $= \text{sum of sizes of } \lambda \text{ blocks}$

geometric multiplicity (dimension of the eigenspace) $= \# \lambda \text{ blocks}$

the minimum polynomial multiplicity (as a root of the minimum polynomial) $= \text{size of the biggest } \lambda \text{ block}$

2. The Jordan Normal Form is unique (up to reordering of blocks). Indeed, $\dim \ker (A - \lambda I) = \# \lambda \text{ blocks}$

$\dim \ker (A - \lambda I)^2 = \# 2 \text{ blocks} + \# 2 \text{ blocks of size } 2$, etc.

This is really the same idea as for our finite abelian groups.