PMATH 347 Groups and Rings Notes

Benjamin Chen

September 2019

1 September 9th

Defined group, rings and field

1.8 Theorem: (Cancellation)

Proof of 2

Let $a, b \in G$, suppose $ab = b$, (the case $ba = b$ is similar)

Then

$$ba = b$$
$$ba = be$$
$$a = e \text{ by } (1)$$

Proof of 3

Let $a, b \in G$

Suppose $ab = e$.

Then

$$(ab)b^{-1} = eb^{-1}$$
$$a(bb^{-1}) = eb^{-1}$$
$$ae = eb^{-1}$$
$$a = b^{-1}$$
$$ba = b \cdot b^{-1}$$
$$ba = e$$

Remark the above rules does not hold in rings in general

eg, in $\mathbb{Z}_{12}$, $3 \cdot 2 = 3 \cdot 6$ but $2 \neq 6$.

and $3 \cdot 9 = 3$ but $9 \neq 1$.

eg. Let $R^\omega = \{(a_1, a_2, ...)|$ each $a_k \in \mathbb{R}\}$ and let

$$\begin{aligned} R &= End(\mathbb{R}^\omega) = Hom(\mathbb{R}^\omega, \mathbb{R}^\omega) \\ &= \{\text{linear maps } L : \mathbb{R}^\omega \to \mathbb{R}^\omega\} \end{aligned}$$

under addition and composition
Let L be given by
$L(a_1, a_2, a_3, ...) = (a_2, a_3, a_4, ...)$
and let R be given by

$$R(a_1, a_2, a_3, ...) = (0, a_1, a_2, a_3, ...)$$

Then $LR = I$.
but $RL \neq I$.
Subgroups
eg. In $\mathbb{C}^*$ we have the subgroups
The section below is in notes actually.

$$\begin{aligned} C_n &= \{z \in \mathbb{C}^* | z^n = 1\}, \text{where } n \in \mathbb{Z}^+\} \\ &= \{e^{i2\pi k/n} | k \in \mathbb{Z}_n\} \end{aligned}$$

$$\begin{aligned} C_\infty &= \bigcup_{n \in \mathbb{Z}^+} C_n \\ &= \{z \in \mathbb{C}^* | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\} \end{aligned}$$

$$\mathbb{S}' = \{z \in \mathbb{C}^* || z| = 1\}$$

When R is a commutative ring with 1, we have the following subgroups of the general linear group

$$\begin{aligned} GL_n(R) &= \{A \in M_n(R) | A \text{ is invertible } \} \\ &= \{A \in M_n(R) | \det A \text{ is a unit in R}\} \end{aligned}$$

The special linear group

$$SL_n(R) = \{A \in GL_n(R) | \det A = 1\}$$

eg.

$$\begin{aligned} O_2(R) &= \{(u, v) | u \in \mathbb{R}^2, v \in \mathbb{R}^2, |u| = 1, |v| = 1, u \cdot v = 0\} \\ &= \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} | \theta \in \mathbb{R}(\text{or } \theta \in [0, 2r]) \right\} \\ &= \{R_\theta, F_\theta | \theta \in \mathbb{R}\} \end{aligned}$$

where $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, F_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$

2 September 11th raw notes

$- - - - - - - - - - - -$
$O_2(\mathbb{R}) = \{R_\theta, F_\theta | \theta \in \mathbb{R}\}$
R_θ: rotation F_θ: reflection
Let us find a matrix formula for the rotation in $\mathbb{R}^2$ about $O = (0,0)$ by θ. (counterclockwise)
See Pictures
Let's find a matrix formula for the reflection F_θ in the line in $\mathbb{R}^2$, through $0 = (0,0)$, which makes the angle $\frac{\theta}{2}$ with the positive x-axis.
Solution:
When L has normal unit vector n,'
When L is the line through o which makes the angle $\frac{\theta}{2}$ with
See Pictures.
$- -$
$O_n(\mathbb{R}) = \{A \in M_n(R), A^T A = I\} \leq GL_n(R)$
1.32 Theorem: (The Subgroup Test I)
Theorem: Subgroup Test I
Proof:
In order for H to be subgroup, we need (2) to hold so that $*$ restricts to give a well-defined operation or H. If H has an identity elements e_H, then $e_H * e_H = E_H$ is inclusive.
Then $G_H * G_H in P$ So $e_H + e_H = e_H$ in G $G_H = e_G$ by cancellation
If $a \in H$ has an inverse in H, say $a * b = b * a = e$ in H.
THen we also have $a * b = b * a$ in G.
So must have $b = a^{-1}$ in G
Thus, for H to be a subgroup of G, properties (1), (2), and (3) hold.
When (1), (2), and (3) hold, note that $*$ is automatically associative in H because it is associative in G.
So H is a subgroup of G.
$- -$
Remark, when R is a ring with identity 1_R and S is subring of R with identity 1_S, it is not always the case that $1_S = 1_R$.
and when $a \in S$ has an inverse in S, that inverse is not always an inverse for a in R.
Examples:
When $R = \mathbb{Z}_{12}$ and $S = 3\mathbb{Z}_{12} = \{0, 3, 6, 9\}$. The multiplication operation in S is given by
A table.
See picture.
We see that $1_S = 9$, but $1_R = 1$.
and that the inverse of 3 in S is 3. But 3 has no inverse in $\mathbb{Z}_{12}$
eg.
When R is a commutative ring,
$O_n(R) \leq GL_n(R)$
because

if $A \in O_n(R)$, then $A^T A = I$.
So $|A|^2 = 1$ so $|A|$ is a unit in R.
so $A \in GL_n(R)$
This shows that $O_n(R) \subseteq GL_n(R)$.
and
See pictures.
$- - - - - - - - - - - - -$
$|G|$
For $a \in G$ ...

3 September 11th

Let us find a matrix formula for the rotation in $\mathbb{R}^2$ about $O = (0,0)$ by θ (counterclockwise).
If $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r\cos\psi \\ r\sin\psi \end{bmatrix}$
then the rotation R_θ about 0 by θ is given by

$$\begin{aligned} R_\theta \begin{bmatrix} x \\ y \end{bmatrix} &= R_\theta \begin{bmatrix} r\cos\psi \\ r\sin\psi \end{bmatrix} \\ &= \begin{bmatrix} r\cos(\theta+\psi) \\ r\sin(\theta+\psi) \end{bmatrix} \\ &= \begin{bmatrix} r\cos\theta\cos\psi - r\sin\theta\sin\psi \\ r\sin\theta\cos\psi + r\cos\theta\sin\psi \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

Thus, we have $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.
Let us find a matrix formula for the reflection F_θ in the line in $\mathbb{R}^2$ through $O = (0,0)$ which makes the angle $\frac{\theta}{2}$ with the positive x-axis.
Solution:
When L has unit normal vector n. Recall that

$$\text{Proj}_n x = (x \cdot n) \cdot n$$

So the reflection in the line L.

$$
\begin{aligned}
F_L(x) &= x - 2\text{Proj}_n x \\
&= x - 2(x \cdot n)n \\
&= x - 2(n^T x)n \\
&= x - 2nn^T x \quad \text{Using matrix multiplication}
\end{aligned}
$$

Thus, $F_L(x) = (I - 2nn^T)x$
That, $F_L = I - 2nn^T$
(eg. If L has equation $ax + by + c = 0$. We can take $n = \frac{(a,b)^T}{\sqrt{(a^2+b^2)}}$)
So

$$
\begin{aligned}
F_L \begin{pmatrix} x \\ y \end{pmatrix} &= (I - 2nn^T) \begin{pmatrix} x \\ y \end{pmatrix} \\
&= \left(I - \frac{2}{a^2 + b^2} \begin{pmatrix} a^2 & ab \\ ab & a^2 \end{pmatrix} \right) \begin{pmatrix} x \\ y \end{pmatrix}
\end{aligned}
$$

Side note: $\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} a^2 & ab \\ ab & a^2 \end{pmatrix}$
When L is the line through O which makes the angle $\frac{\theta}{2}$ with the positive x-axis.
A unit direction vector for L is $u = \begin{pmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} \end{pmatrix}$
and a unit normal vector is

$$
n = \begin{pmatrix} -\sin \frac{\theta}{2} \\ \cos \frac{\theta}{2} \end{pmatrix}
$$

So

$$
\begin{aligned}
F_\theta = F_L &= I - 2nn^T \\
&= I - 2 \begin{pmatrix} -\sin \frac{\theta}{2} \\ \cos \frac{\theta}{2} \end{pmatrix} \begin{pmatrix} -\sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \\
&= \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}
\end{aligned}
$$

$$
\begin{aligned}
O_n(R) =& \{A \in M_n(R) | A^T A = I\} \\
&\leq GL_n(R)
\end{aligned}
$$

Theorem: (Subgroup Test I)
Let G be a group with identity $e = e_G$ and operation $*$, and let $H \subseteq G$ be a subset.
Then, $H \leq G$ (that is H is a subgroup of G) if and only if

1. $e \in H$
2. H is closed under $*$ for all $a, b \in H$, we have $a * b \in H$
3. H is closed under inversion for all $a \in H$, we have $a^{-1} \in H$.

Proof:
In order for H to be a subgroup, we need (2) to hold so that $*$ restricts to give a well-defined operation on H.
If H has an identity element e_H, then $e_H * e_H = e_H$ in H.
So $e_H * e_H = e_H$ in G
So $e_H = e_G$. by cancellation in G.
If $a \in H$ has an inverse in H,
say $a * b = b * a = e$ in H.
Then, we also have $a * b = b * a$ in G, so must have $b = a^{-1}$ in G
Thus, for H to be a subgroup of G properties (1), (2) and (3) hold.
When (1), (2), and (3) hold, note that $*$ is automatically associative in H because it is associative in G.
So H is a subgroup of G.
Remark:
When R is a ring with identity 1_R and S is a subring of R with identity 1_S, it is not always the case that $1_S = 1_R$ and when $a \in S$ has an inverse in S, that inverse is not always an inverse for a in R.
For example, when $R = \mathbb{Z}_{12}$, and $S = 3\mathbb{Z}_{12} = \{0, 3, 6, 9\}$. The multiplication operation in S is given by:

	0	**3**	**6**	**9**
0	0	0	0	0
3	0	9	6	3
6	0	6	0	6
9	0	3	6	9

We see that $1_S = 9$ but $1_R = 1$, and that the inverse of 3 in S is 3 but 3 has no inverse in $\mathbb{Z}_{12}$.
When R is a commutative ring,
Eg.

$$O_n(R) \leq GL_n(R)$$

because
if $A \in O_n(R)$, then $A^T A = I$
So $|A|^2 = 1$, so $|A|$ is a unit in R. So $A \in GL_n(R)$.
(This shows that $O_n(R) \subseteq GL_n(R)$)
and

1. $I \in O_n(R)$, Since $\big(I^T I = T\big)$.

2. if $A, B \in O_n(R)$, then

$$\begin{aligned}(AB)^T(AB) &= B^T A^T AB \\ &= B^T I B \\ &= B^T B \\ &= I\end{aligned}$$

3. If $A \in O_n(R)$, $\left(A^T A = I\right)$

   then

$$\begin{aligned}(A^{-1})^T A^{-1} &= (A^T)^{-1} A^{-1} \\ &= (AA^T)^{-1} = I^{-1} = I\end{aligned}$$

   because when $A^T A = I$, A is invertible with $A^{-1} = A^T$.

   So $AA^T = I$.

   $|G|$ = number of elements in G when G is finite

   For $a \in G = \begin{cases} \text{smallest } \ell \in \mathbb{Z}^+ \ \ a^\ell = e \\ \infty \quad \text{if no such } \ell \text{ exists} \end{cases}$

4 September 13th

Definition:
Let G be a group. The order of G, denoted by $\operatorname{ord}(G)$ or by $|G|$, is the cardinality of G:
So we have

$$|G| = \begin{cases} \text{the number of elements in } G\text{, if } G \text{ is finite} \\ \infty \ \text{, if } G \text{ is infinite} \end{cases}$$

For $a \in G$, the order of a in G, denoted by $\operatorname{ord} a$ or $\operatorname{ord}_G(a)$ or by $|a|$, is

$$|a| = \begin{cases} \text{the smallest positive integer } n \in \mathbb{Z}^+ \\ \ \text{such that } a^n = e & \text{if such a positive integer exists,} \\ \infty & \text{if no such positive integer exists.} \end{cases}$$

Eg.

$$|\mathbb{Z}_n| = n$$

$$|U_n| = \phi(n)$$

where
$\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is the Euler phi function (also called the Euler totient function)
By definition, $\phi(n) = |U_n| =$ number of $\{1 \leq k \leq n | \gcd(k, n) = 1\}$
eg. When p is a prime

$$\phi(p) = p - 1$$

because $U_p = \mathbb{Z}_p \setminus \{0\}$, so $|U_p| = p - 1$.
and when $k \in \mathbb{Z}^+$,
$\phi(p^k) = p^k - p^{k-1}$
Because $U_{p^k} = \{1, 2, 3, ..., p^k = 0\} \setminus \{p, 2p, 3p, ..., p^k\}$
We shall prove later that when $n = \prod_{i=1}^{l} p_i^{k_i}$ where the p_i are distinct primes,

$$\phi(n) = \prod_{i=1}^{l} \phi(p_i^{k_i}) = \prod_{i=1}^{l} \left(p_i^{k_i} - p_i^{k_i - 1}\right)$$

Eg. When p and q are distinct primes

$$\phi(pq) = |U_{pq}| = (p-1)(q-1)$$

Eg. Find the order of the group $GL_n(\mathbb{Z}_p)$ where p is prime.
Solution:
We need to count the number of matrices $A \in GL_n(\mathbb{Z}_p)$, say $A = (u_1, u_2, ..., u_n)$ with each $u_k \in \mathbb{Z}_p^n$.
For A to be invertible, the columns need to be linearly independent.
We need the first column u_1 to be non-zero. So the number of possible ways to choose $u_1 \in \mathbb{Z}_p^n \setminus \{0\}$ is $p^n - 1$.
Having chosen u_1, the second column u_2 can be any vector in $\mathbb{Z}_p^n$ which is not in $\text{Span}\{u_1\} = \{tu_1 | t \in \mathbb{Z}_p\}$
Since $|\text{Span}\{u_1\}| = p$, there are $p^n - p$ choices for u_2.
Having chosen u_1, u_2, we can choose u_3 to be any element in $\mathbb{Z}_p^n \setminus \text{Span}\{u_1, u_2\}$ and $\text{Span}\{u_1, u_2\} = \{t_1 u_1 + t_2 u_2 | t_1, t_2 \in \mathbb{Z}_p\}$. So that $|\text{Span}\{u_1, u_2\}| = p^2$.
So the number of possible choices for u_3 is $p^n - p^2$.
This continues similarly for each column.
Thus, $|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-1}$
If we had $s_1 u_1 + s_2 u_2 = t_1 u_1 + t_2 u_2$, then $s_1 = t_1$ and $s_2 = t_2$.
Exercise: Show that $|GL_2(\mathbb{Z})| = \infty$
Exercise: Show that if $a \in G$ and $b \in H$, and $ord_G(a) = n$ and $ord_H(b) = m$ then $ord_{G \times H}(a, b) = lcm(n, m) = \frac{mn}{\gcd(n,m)}$
Note: If G is an additive abelian group, and $a \in G$, then

$$|a| = \text{ the smallest } n \in \mathbb{Z}^+ \text{ such that } na = 0 \text{ (if such a } n \in \mathbb{Z}^+ \text{ exists)}$$

Eg. In $\mathbb{Z}_{20}$, find $|6| = ord(6)$
Additive notation.
Brute force
Solution:

k	0	1	2	3	4	5	6	7	8	9	10
k · 6	0	6	12	18	4	10	16	2	8	14	0

So $|6| = 10$ in $\mathbb{Z}_{20}$.
Eg. Find $|7|$ in U_{100}
Solution:
Make a multiplication table and figure out that $|7| = 4$.

4.1 Chapter 2 Cyclic Groups and Generators

Note that if G is a group and $H_k \leq G$ for each $k \in K$. Then $\bigcap_{k\in K} H_k \leq G$ by the Subgroup Test.

1. $e \in H_k$ for all $k \in K$ So $e \in \bigcap_{k\in K} H_k$
2. If $a, b \in \bigcap_{k\in K} H_k$, then for every $k \in K$, $a, b \in H_k$, so $ab \in H_k$ Since $ab \in H_k$ for every $k \in K$, we have $ab \in \bigcap_{k\in K} H_k$.
3. Similarly, if $a \in \bigcap_{k\in K} H_k$, then $a^{-1} \in \bigcap_{k\in K} H_k$

Definition:
Let G be a group and let $S \subseteq G$ be a subset. The subgroup of G generated by S, denoted by $\langle S \rangle$, is the smallest subgroup of G which contains S.
Equivalently, $\langle S \rangle$ is the intersection of the set of all subgroups of G which contains S.
When S is the finite set, we often omit the set brackets and write

$$\langle \{a_1, a_2, \ldots, a_n\} \rangle = \langle a_1, a_2, \ldots, a_n \rangle$$

A **cyclic group** is a group G such that $G = \langle a \rangle$ for some $a \in G$.
If G is any group and $a \in G$, then $\langle a \rangle$ is a cyclic subgroup of G.
Theorem: (Elements in a Cyclic Group)
Let G be a group and let $a \in G$

1. $\langle a \rangle = \{a^k | k \in \mathbb{Z}\}$
2. If $|a| = \infty$, then for $k, l \in \mathbb{Z}$, we have $a^k = a^l \iff k = l$.

   (So the elments, $a^k, k \in \mathbb{Z}$ are distinct)
3. If $|a| = n$, then for $k, l \in \mathbb{Z}$, we have $a^k = a^l \iff k = l \mod n$

   (So we have $\langle a \rangle = \{a^k | 0 \leq k \leq n\} = \{a^k | k \in \mathbb{Z}_n\}$ with the listed elements distinct)

Proof:

1. $\langle a \rangle$ is the smallest subgroup of G which contains a. Since $a \in \langle a \rangle$, by closure under the operation and inversion and induction, $a^k \in \langle a \rangle$ for all $k \in \mathbb{Z}$.

   So $\{a^k | k \in \mathbb{Z}\} \subseteq \langle a \rangle$.

5 September 16th

Elements in Cyclic Group (Continue)

1. Also, note that $H = \{a^k | k \in \mathbb{Z}\}$ is a subgroup of G because
   (a) $e = a^0 \in H$
   (b) For $k, l \in \mathbb{Z}$
   $a^k \cdot a^l = a^{k+l} \in H$, and
   (c) For $k \in \mathbb{Z}$,
   $(a^k)^{-1} = a^{-k} \in H$

   Since $a \in H$ and $H \leq G$, it follows that $\langle a \rangle \subseteq H$.

2. Suppose $|a| = \infty$, (this means there is no positive integer r such that $a^r = e$).
   Let $k, l \in \mathbb{Z}$,
   If $k = l$, then of course $a^k = a^l$.
   Suppose that $a^k = a^l$
   Suppose $k \neq l$, say $k < l$. Then

$$\begin{aligned} a^k \cdot a^{-k} &= a^l \cdot a^{-k} \\ e &= a^{l-k} \end{aligned}$$

   This contradicts the fact that there is no $r \in \mathbb{Z}^+$ such that $a^r = e$.

3. Suppose $|a| = n$. (So n is the smallest positive integer such that $a^n = e$)
   If $k = l \mod n$,
   say $l = k + nq$ with $q \in \mathbb{Z}$
   Then

$$\begin{aligned} a^l &= a^{k+nq} = a^k \cdot a^{nq} \\ &= a^k \cdot (a^n)^q = a^k e^q \\ &= a^k e = a^k \end{aligned}$$

   Suppose, conversely, that $k, l \in \mathbb{Z}$ and $a^k = a^l$.
   Then

$$\begin{aligned} a^k \cdot a^{-k} &= a^l \cdot a^{-k} \\ e &= a^{l-k} \end{aligned}$$

   Use the Division Algorithm, to write

$$l - k = q \cdot n + r$$

with $q, r \in \mathbb{Z}$ and $0 \leq r < n$.

Then

$$\begin{aligned} e = a^{l-k} &= a^{q \cdot n + r} \\ &= (a^n)^q \cdot a^r = e \cdot a^r = a^r \end{aligned}$$

Thus, we must have $r = 0$

(Otherwise, r would be a positive integer less than n with $a^r = e$, contradicting the fact that $|a| = n$).

Since $r = 0$, we have

$$l - k = qn + r = qn$$

So $l = k + qn$, hence $l = k \mod n$.

Corollary:

When G is a group and $a \in G$, we have

$$|a| = |\langle a \rangle|$$

Theorem: (Subgroups of Cyclic Groups)
Let G be a group and let $a \in G$.

1. Every subgroup of $\langle a \rangle$ is cyclic.
2. If $|a| = \infty$, then for $k, l \in \mathbb{Z}$, we have

   $$\langle a^k \rangle = \langle a^l \rangle \iff l = \pm k$$

   So the distinct subgroups of $\langle a \rangle$ are
   The trivial group $\langle a^0 \rangle = \{e\}$
   and the groups $\langle a^k \rangle$ with $k \in \mathbb{Z}^+$.
3. If $|a| = n$, then
   for $k, l \in \mathbb{Z}$, we have

   $$\begin{aligned} &\langle a^k \rangle = \langle a^l \rangle \\ &\qquad \iff \gcd(k, n) = \gcd(l, n) \end{aligned}$$

   and if $d = \gcd(k, n)$.

Then

$$\begin{aligned}\langle a^k \rangle &= \langle a^d \rangle \\ &= \{a^0, a^d, a^{2d}, \ldots, a^{n-d}\} \\ &= \{a^{kd} | k \in \mathbb{Z}_{n/d}\}\end{aligned}$$

So the distinct subgroups of $\langle a \rangle$ are the groups

$$\langle a^d \rangle = \{a^{kd} | k \in \mathbb{Z}_{n/d}\}$$

where d is a positive divisor of n.

Note that: $n - d = (\frac{n}{d} - 1)d$

(Otherwise, r would be a positive integer less than n with $a^r = e$, contradicting the fact that $|a| = n$).

Since $r = 0$, we have

$$l - k = qn + r = qn$$

.

So $l = k + qn$, hence $l = k \mod n$

Proof:

(a) Let $H \leq \langle a \rangle = \{a^k | k \in \mathbb{Z}\}$.
If $H = \{e\}$, then $H = \langle a^0 \rangle$ (which is cyclic).
Suppose $H \neq \{e\}$
Choose $t \in \mathbb{Z}$ so $e = a^t \in H$.
Note that $a^{-t} = (a^t)^{-1} \in H$ too
So we have $a^{|t|} \in H$ with $|t| > 0$.
Let n be the smallest positive integer such that $a^n \in H$
We claim that $H = \langle a^n \rangle$.
Since $a^n \in H$, we have

$$a^{kn} \in H$$

for all $k \in \mathbb{Z}$.
So $\langle a^n \rangle = \{a^{kn} | k \in \mathbb{Z}\} \subseteq H$
We need to show that

$$H \subseteq \langle a^n \rangle = \{a^{kn} | t \in \mathbb{Z}\}$$

Let $l \in \mathbb{Z}$ with $a^l \in H$.
write $l = qn + r$ with $0 \leq r < n$.

Then

$$\begin{aligned} a^r &= a^{l-qn} \\ &= a^l \cdot (a^n)^{-q} \\ &\in H \end{aligned}$$

Since $a^l \in H$ and $a^n \in H$.
Since n is the smallest positive integer for which $a^n \in H$, we must have $r = 0$
Thus,

$$\begin{aligned} l &= qn \\ a^l &= (a^n)^q \in \langle a^n \rangle \end{aligned}$$

Thus, $H \subseteq \langle a^n \rangle$
September 18th:

(b) Part 2 as an exercise

(c) Suppose $|a| = n$,
So $\langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$
Note that if d is a positive divisor of n, then ,

$$\begin{aligned} \langle a \rangle &= \{a^0, a^d, a^2d, \ldots, a^{n-d}\} \\ &= \{a^{kd} | k \in \mathbb{Z}_{n/d}\} \end{aligned}$$

By the definition of order:
with $|a^d| = |\langle a^d \rangle| = \frac{n}{d}$
It follows from the previous theorem:
We claim that for any integer $k \in \mathbb{Z}$, we have

$$\langle a^k \rangle = \langle a^d \rangle$$

where $d = \gcd(k, n)$
Let $k \in \mathbb{Z}$ and let $d = \gcd(k, n)$
Since $d|k$, it follows that

$$a^k \in \langle a^d \rangle = \{a^{qd} | q \in \mathbb{Z}\}$$

Hence,

$$\langle a^k \rangle \leq \langle a^d \rangle$$

Also, because $d = \gcd(k, n)$, we can choose $s, t \in \mathbb{Z}$ so that $d = ks + nt$.

It follows that

$$\begin{aligned} a^d &= a^{ks+nt} = (a^k)^s \cdot (a^n)^t \\ &= (a^k)^s \text{ since } a^n = e \end{aligned}$$

Hence, $a^d \in \langle a^k \rangle = \{a^{ks} | s \in \mathbb{Z}\}$
Hence, $\langle a^d \rangle \leq \langle a^k \rangle$.
Thus, $\langle a^k \rangle = \langle a^d \rangle$, where $d = \gcd(k, n)$, as claimed.
Now, let $k, l \in \mathbb{Z}$.
If $\gcd(k, n) = \gcd(l, n) = d$,
then $\langle a^k \rangle = \langle a^d \rangle = \langle a^l \rangle$
Suppose that $\langle a^k \rangle = \langle a^l \rangle$ and let $d = \gcd(k, n)$ and $c = \gcd(l, n)$.
Then

$$\langle a^d \rangle = \langle a^k \rangle = \langle a^l \rangle = \langle a^c \rangle$$

$$|\langle a^d \rangle| = |\langle a^c \rangle|$$

$$\frac{n}{d} = \frac{n}{c}$$

$$d = c$$

Eg. In the $C_{12} = \{z \in \mathbb{C}^* | z^{12} = 1\} = \{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{11}\} = \langle a \rangle$
The divisors of 12 are 1, 2, 3, 4, 6, 12.
The distinct subgroups of C_{12} are:

$$\begin{aligned} \langle a^1 \rangle &= \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^10, \alpha^11\} = C_{12} \\ \langle \alpha^2 \rangle &= \{1, \alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}\} = C_6 \\ \langle \alpha^3 \rangle &= \{1, \alpha^3, \alpha^6, \alpha^9\} = C_4 \\ \langle \alpha^4 \rangle &= \{1, \alpha^4, \alpha^8\} = C_3 \\ \langle \alpha^6 \rangle &= \{1, \alpha^6\} = \{\pm 1\} = C_2 \\ \langle \alpha^{12} \rangle &= \{1\} = C_1 \end{aligned}$$

Corollary (Orders of Elements in Cyclic Groups):
For $a \in G$,
If $|a| = \infty$, then $|a^0| = 1$

and $|a^k| = \infty$ for $0 \neq k \in \mathbb{Z}$.

If $|a| = n$, then for $k \in \mathbb{Z}$, $|a^k| = \frac{n}{\gcd(k,n)}$.

Corollary (Generators of Cyclic Groups):

For $a \in G$,

If $|a| = \infty$, then for $k \in \mathbb{Z}$

$$\langle a^k \rangle = \langle a \rangle \iff k = \pm 1$$

and if $|a| = n$, then for $k \in \mathbb{Z}$ (or for $k \in \mathbb{Z}_n$).

$$\langle a^k \rangle = \langle a \rangle \iff \gcd(k,n) = 1 \iff k \in U_n$$

$C_{12} = \langle \alpha \rangle = \langle \alpha^5 \rangle = \langle \alpha^7 \rangle = \langle \alpha^{11} \rangle$.
$\alpha = e^{i2\pi/12}$

Corollary (The Number of Generators in a Cyclic Group):

For $a \in G$,

If $|a| = \infty$, then the number of elements in $\langle a \rangle$ which generate $\langle a \rangle$ is equal to 2.

And if $|a| = n$, then the number of generators of $\langle a \rangle$ (the number of elements $b \in \langle a \rangle$ such that $\langle b \rangle = \langle a \rangle$) is equal to $\phi(n) = |U_n|$.

Corollary (The Number of Elements of Each Order in a Cyclic Group):

Let $a \in G$,

If $|a| = \infty$, then in $\langle a \rangle$, there is 1 element of order 1. (namely $a^0 = e$).

and if $|a| = n$, then in $\langle a \rangle$, the order of every element in $\langle a \rangle$ is a positive divisor of n and given a positive divisor, d of n, the number of elements in $\langle a \rangle$ of order d is $\phi(d)$.

Corollary (Number of Elements of Each Order in a Finite Group):

If G is a finite group, then for each $d \in \mathbb{Z}^+$.

The number of elements in G of order d is a multiple of $\phi(d)$; indeed

it is equal to $\phi(l)$ multiplied by the number of distinct cyclic subgroups of order d in G.

Corollary:

For $n \in \mathbb{Z}^+$, we have

$$n = \sum_{d|n} \phi(d)$$

\sum d—n : Sum of all positive divisors

(where the sum is taken over all the positive divisors of n)

Example:

In $\mathbb{Z}_{12} = \langle 1 \rangle$

We have the subgroups with generators bolded.

$$\begin{aligned}
\langle 1 \rangle &= \{0, \mathbf{1}, 2, 3, 4, \mathbf{5}, 6, \mathbf{7}, 8, 9, 10, \mathbf{11}\} \\
\langle 2 \rangle &= \{0, \mathbf{2}, 4, 6, 8, \mathbf{10}\} \\
\langle 3 \rangle &= \{0, \mathbf{3}, 6, \mathbf{9}\} \\
\langle 4 \rangle &= \{0, \mathbf{4}, \mathbf{8}\} \\
\langle 6 \rangle &= \{0, \mathbf{6}\} \\
\langle 12 \rangle &= \{\mathbf{0}\}
\end{aligned}$$

6 September 20th

Theorem:
Let G be a group and let $S \subseteq G$ be a subset. Then

$$\begin{aligned}
\langle S \rangle &= \{a_1^{k_1} a_2^{k_2} \dots a_l^{k_l} | l \in \mathbb{N}, a_i \in S, k_i \in \mathbb{Z}\} \\
&= \{a_1^{k_1} a_2^{k_2} \dots a_l^{k_l} | l \in \mathbb{N}, a_i \in S \text{ with } a_i \neq a_{i+1}, k_i \in \mathbb{Z} \text{ with } k_i \neq 0\}
\end{aligned}$$

where $\mathbb{N} = \{0, 1, 2, \dots\}$
and we use the convention that the empty product, $(a_1^{k_1}, \dots, a_l^{k_l}$ with $l = 0)$. is the identity $e \in G$
If G is abelian, then

$$\langle S \rangle = \{a_1^{k_1} a_2^{k_2} ... a_l^{k_l} | l \in \mathbb{N}, a_i \in S \text{ with } a_i \neq a_j \text{ when } i \neq j, 0 \neq k_i \in \mathbb{Z}\}$$

If G is an additive abelian group, then

$$\begin{aligned}
\langle S \rangle &= \{k_1 a_1 + k_2 a_2 + \dots + k_l a_l | l \in \mathbb{N}, a_i \in S \text{ with } a_i \neq a_j \text{ when } i \neq j, 0 \neq k_i \in \mathbb{Z}\} \\
&= \mathrm{Span}_{\mathbb{Z}}(S)
\end{aligned}$$

Sketch Proof:
Let $H = \{a_1^{k_1} a_2^{k_2} \dots a_l^{k_l} | l \in \mathbb{N}, a_i \in S, k \in \mathbb{Z}\}$
By the definition of $\langle S \rangle$, we have $a_i \in \langle S \rangle$ for all i (Since $a_i \in S$) Hence, every element $a^{k_1} a^{k_1} \dots a^{k_l} \in H$ lies in $\langle S \rangle$.
By closure of $\langle S \rangle$ under the operation and inversion. So we have $H \subseteq \langle S \rangle$.
Also, note that $H \leq G$ because $e \in H$ (by taking $l = 0$) and since the product of two elements of H lies in H.

$$(a_1^{j_1} a_2^{j_2} \dots a_l^{j_l})(b_1^{k_1} b_2^{k_2} \dots b_m^{k_m}) = a_1^{j_1} a_2^{j_2} \dots a_l^{j_l} b_1^{k_1} b_2^{k_2} \dots b_m^{k_m}$$

and the inverse of each element of H lies in H.

$$(a_1^{k_1}a_2^{k_2}\dots a_l^{k_l})^{-1} = a_l^{-k_l}\dots a_2^{-k_2}a_1^{-k_1}$$

Since $S \subseteq H$ (if $a \in S$ then $a = a^1 \in H$) and $H \leq G$ it follows that $\langle S\rangle \subseteq H$.
If $a_i = a_{i+1}$
Then

$$a_1^{k_1}\dots a_i^{k_i}a_{i+1}^{k_{i+1}}\dots a_l^{k_l} = a_1^{k_1}\dots a_i^{k_i+k_{i+1}}a_{i+2}^{k_{i+2}}\dots a_l^{k_l}$$

If $k_i = 0$, then

$$a_1^{k_1}\dots a_i^{k_i}a_{i+1}^{k_{i+1}}\dots a_l^{k_l} = a_1^{k_1}\dots a_{i-1}^{k_{i-1}}a_{i+1}^{k_{i+1}}\dots a_l^{k_l}$$

Examples:
In $\mathbb{Z}^2$ (or in $\mathbb{Q}^2$ or $\mathbb{R}^2$),

$$\begin{aligned}\langle(3,1),(1,2)\rangle &= \{s(3,1)+t(1,2)|s,t\in\mathbb{Z}\}\\ &= \mathrm{Span}_{\mathbb{Z}}\{(3,1),(1,2)\}\\ &= \mathrm{Span}_{\mathbb{Z}}\{(5,0),(2,-1)\}\\ &= \langle(5,0),(2,-1)\rangle\end{aligned}$$

Because

$$(5,0) = 2(3,1) - 1(1,2) \in \langle(3,1),(1,2)\rangle$$
$$(2,-1) = (3,1) - (1,2) \in \langle(3,1),(1,2)\rangle$$

So

$$\langle(5,0),(2,1)\rangle \leq \langle(3,1),(1,2)\rangle$$

And similarly

$$(3,1) = (5,0) - (2,-1)$$
$$(1,2) = (5,0) - 2(2,-1)$$

So $\langle(3,1),(1,2)\rangle \leq \langle(5,0),(2,-1)\rangle$
Eg.
Recall that

$$O_2(\mathbb{R}) = \{R_\theta, F_\theta|\theta\in\mathbb{R}\}.$$

with $R_\beta R_\alpha = R_\beta F_\alpha = F_{\beta+\alpha}, F_\beta R_\alpha = F_{\beta-\alpha}, F_\beta F_\alpha = R_{\beta-\alpha}$
and for $n \in \mathbb{Z}^+$

$$D_n = \{R_k, F_k|k\in\mathbb{Z}_n\}$$

where $R_k = R_{\theta_k}, F_k = F_{\theta_k}$ with $\theta_k = \frac{2\pi k}{n}$
and we have

$$R_l R_k = R_{k+l}, R_l F_k = F_{l+k}$$
$$F_l R_k = F_{l-k}, F_l F_k = R_{l-k}$$

with $k, l \in \mathbb{Z}_n$.
Note that $D_n = \langle R_1, F_0 \rangle$.
because $R_k = R_1^k$
and $F_k = R_k F_0 = R_1^k F_0$
Often books write R_1 as σ and F_0 as τ and $I = R_0 = e$
So $D_n = \langle \sigma, \tau \rangle$ with $\sigma^n = e, \tau^2 = e$

$$\begin{aligned} \sigma\tau &= R_1 F_0 = F_1 \\ &= F_0 R_{n-1} \\ &= \tau\sigma^{n-1} \end{aligned}$$

(Since $0 - (n-1) = 1$) in $\mathbb{Z}_n$
Remark
If S is a set (with no operation), then the free group on S is the set of expressions

$$F(S) = \{a_1^{k_1} a_2^{k_2} \dots a_l^{k_l} | l \in \mathbb{N}, a_i \in S \text{ with } a_i \neq a_{i+1}, 0 \neq k_i \in \mathbb{Z}\}$$

where the operation is given by concatenation followed by grouping and cancellation.
So the product

$$\left(a_1^{j_1} \dots a_l^{j_l}\right) * \left(b_1^{k_1} \dots b_m^{k_m}\right)$$

is given by $\left(a_1^{j_1} \dots a_{l-1}^{j_{l-1}} a_l^{j_l} b_1^{k_1} b_2^{k_2} \dots b_m^{k_m}\right)$ and the if $a_l = b$, we group by replacing $a_l^{j_l} b_1^{k_1}$ by $a_l^{j_i + k_1}$ and then if $j_l + k_1 = 0$ then we cancel the form $a_l^{j_l + k_1} = a_l^0$ and check to see if $a_{l-1} = b_2$.
Example:
In $F(a, b)$,

$$\begin{aligned} (a^2 b^3 a b^2)(b^{-2} a^{-1} b) &= a^2 b^3 a b^2 b^{-2} a^{-1} b \\ &= a^2 b^3 a b^0 a^{-1} b \\ &= a^2 b^3 a a^{-1} b \\ &= a b^3 b \\ &= a b^4 \end{aligned}$$

Eg.
$F(\sigma, \tau) = \langle \sigma, \tau \rangle$ and $D_n = \langle \sigma, \tau \rangle$
but in $F(\sigma, \tau), \sigma^n \neq e, \tau^2 \neq e$, and $\sigma\tau \neq \tau\sigma^{n-1}$.
Remark

When S is a set, the free abelian group on S is

$$A(S) = \{k_1a_1 + k_2a_2 + \cdots + k_la_l | k \in \mathbb{N}, \\ \text{the } a_i \text{ are distinct elements in } S, 0 \neq k_i \in \mathbb{Z}\}$$

If we identify

$$k_1a_1 + k_2a_2 + \cdots + k_la_l$$

with the function $f : S \to \mathbb{Z}$ given by $f(a_i) = k_i$ and $f(x) = 0$ when $x \notin \{a_1, \ldots, a_l\}$. Then $A(S) = \mathbb{Z}^S = \{f : S \to \mathbb{Z}\}$ under addition of functions

$$(f + g)(x) = f(x) + g(x) \text{ for all } x \in S$$

7 September 23th

Definition:
For a group G, the centre of G is the subgroup

$$Z(G) = \{a \in G | ab = ba \text{ for all } b \in G\}$$

For $a \in G$, the centralizer of a in G is the subgroup

$$C(a) = C_G(a) = \{b \in G | ab = ba\}$$

Exercise:
Show that $Z(G)$ and $C(a)$ are subgroups of G.
Chapter 3 The Symmetric Group
Recall that when S is a set, the group of permutations of S, denoted by $\text{Perm}(S)$, is the set of bijective maps $f : S \to S$ under composition.
For $n \in \mathbb{Z}^+$, the n^{th} symmetric group is the group

$$S_n = \text{Perm}(\{1, 2, \ldots, n\})$$

under composition.
Definition:
For $\alpha \in S_n$, we can specify α by giving its table of values as follows.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \ldots & \alpha(n) \end{pmatrix}$$

When we can express α in this form, we are using array notation.
Eg.
In array notation,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

If $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
Then,
$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
and
$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \alpha\beta.$$

Eg. We can think of D_n as being a subgroup of S_n, because D_n permutes the elements in $C_n = \{\alpha^0, \alpha^1, \alpha^2, \dots, \alpha^{n-1}\}$ with $\alpha = e^{i2\pi/n}$, and we can consider that an element of D_n permutes the exponents of the elements α^k where $k \in \{1, 2, \dots, n\}$.
If we consider D_4 as a subgroup of S_4 in this way.
$$D_4 = \{I, R_1, R_2, R_3, F_0, F_1, F_2, F_3\}$$
with
$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$
$$F_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Definition:
When $a_1, a_2, \dots, a_l$ are distinct elements in {1, 2, 3, …, n }, we write
$$\alpha = (a_1, a_2, a_3, \dots, a_l)$$
to denote the permutation $\alpha \in S_n$ such that
$\alpha(a_1) = a_2, \alpha(a_2) = a_3, \dots, \alpha(a_{l-1}) = a_l, \alpha(a_l) = a.$
(So $\alpha(a_j) = a_{j+1}$ with $j \in \mathbb{Z}_l$).
and $\alpha(k) = k$ for $k \notin \{a_1, a_2, \dots, a_l\}$
A permutation $\alpha \in S_n$ of the above form is called an $l-$cycle.
Notes:

1. $e = (1) = (2) = \cdots = (n)$
2. $(a_1, a_2, \dots, a_n) = (a_2, a_3, \dots, a_n, a_1) = (a_3, a_4, \dots, a_n, a_1, a_2) = \dots$
3. We can write an $l-$cycle uniquely in the form $\alpha = (a_1, a_2, \dots, a_l)$ with $a_1 = \min(a_1, a_2, \dots, a_l)$.

4. If α is an $l-$cycle, then $|\alpha| = l$.

Definition:
Two cycles $\alpha = (a_1, a_2, \ldots, a_l)$ and $\beta = (b_1, b_2, \ldots, b_m)$ in S_n are called <u>disjoint</u> when $\{a_1, a_2, \ldots, a_l\} \cap \{b_1, b_2, \ldots, b_n\} = \emptyset$.
(So no a_i is equal to any b_j).
More generally, the cycles

$$\alpha_1 = (a_{1,1}, a_{1,2}, \ldots, a_{1,l_1})$$
$$\alpha_2 = (a_{2,1}, a_{2,2}, \ldots, a_{2,l_2})$$
$$\ldots$$
$$\alpha_m = (a_{m,1}, a_{m,2}, \ldots, a_{m,l_m})$$

are disjoint when no $a_{i,j}$ is equal to and $a_{k,l}$ unless $i = k$ and $j = l$.
Eg.
In S_8, we have

$$(25134)(72651)(31826) = (18624)(375)$$

Theorem (Cycle Notation)
Every $\alpha \in S_n$ can be written as a product of disjoint cycles. Indeed, every $e \neq \alpha \in S_n$ can be written uniquely as a product of disjoint cycles in the form

$$\alpha = \alpha_1 \alpha_2 \ldots \alpha_m$$

with

$$\alpha_k = (a_{k,1}, a_{k,2}, \ldots, a_{k,l_k})$$

where $m \geq 1$, each $l_k \geq 2$, for each $k, a_{k,1} = \min\{a_{ki} | 1 \leq i \leq l_k\}$ and $a_{11} < a_{21} < \ldots a_{m1}$.
Let $e \neq \alpha \in S_n$
Proof:
For α to be in the given unique form, we need to choose a_{11} to be the smallest $k \in \{1, 2, \ldots, n\}$ such that $\alpha(k) \neq k$. Having chosen a_{11}, we must choose

$$a_{12} = \alpha(a_{11}), a_{13} = \alpha(a_{12}) = \alpha^2(a_{11}), \alpha_{14} = \alpha(a_{13}) = \alpha^3(a_{11})$$

and so on.
Eventually, we must reach a positive integer l such that $\alpha^l(a_{11}) = a_{11}$ and we must choose l to be the smallest such l.
This uniquely determines the first cycle $\alpha_1 = (a_{1,1}, a_{1,2}, \ldots, a_{1,l_1})$.
If $\alpha = \alpha_1$, we are done.
Otherwise, we must choose $a_{2,1}$ to be the smallest $k \in \{1, 2, \ldots, n\} \backslash \{a_{1,1}, a_{1,2}, \ldots, a_{1,l_1}\}$ with $\alpha(k) \neq k$.

8 September 25th

Disjoint cycles commute.
We must have

$$a_{2,2} = \alpha(a_{2,1}), a_{2,3} = \alpha(a_{2,2}) = \alpha^2(a_{2,1}) \dots$$

and l_2 must be the smallest positive integer such that $\alpha^{l_2}(a_{2,1}) = a_{2,1}$
Then $\alpha_2 = (a_{2,1}, a_{2,2}, \dots, a_{2,l_2})$
Note that α_1 and α_2 are disjoint because if we have

$$\alpha^l(a_{1,1}) = \alpha^j(a_{2,1}) \text{ for some} i, j$$

Hence,

$$\begin{aligned} a_{2,1} &= \alpha^{-j}\left(\alpha^j(a_{2,1})\right) \\ &= \alpha^{-j}\left(\alpha^i(a_{1,1})\right) \\ &= \alpha^{i-j}(a_{1,1}) \in \{a_{1,1}, a_{1,2}, \dots a_{1,l_1}\} \end{aligned}$$

But we chose $a_{2,1} \notin \{a_{1,1}, a_{1,2}, \dots, a_{1,l_1}\}$
If $\alpha = \alpha_1\alpha_2$, we are done and otherwise we repeat the above procedure.
<u>Note</u>:
Disjoint cycles commute indeed if $\alpha = (a_1, a_2, \dots, a_l)$ and $\beta = (b_1, b_2, \dots, b_m)$ are disjoint cycles, then
for $k \in \{1, 2, \dots, n\}$
If $k = a_i$, then

$$\alpha(\beta(k)) = \beta(\alpha(k)) = a_{i+1}$$

If $k = b_j$, then

$$\alpha(\beta(k)) = \beta(\alpha(k)) = b_{j+1}$$

and if $k \in \{a_1, \dots, a_l\} \cup \{b_1, \dots, b_m\}$
Then, $\alpha\left(\beta(k)\right) = \beta\left(\alpha\left(k\right)\right) = k$
<u>Note</u>:
If $\alpha = \alpha_1\alpha_2 \dots \alpha_m$ where the α_k are disjoint cycles with $|\alpha_k| = l_k$, then

$$\begin{aligned} |\alpha| &= \operatorname{lcm}\left(|\alpha_1|, \dots, |\alpha_m|\right) \\ &= \operatorname{lcm}\left(l_1, \dots, l_m\right) \end{aligned}$$

Proof:
Let $p \in \mathbb{Z}^+$. If p is a common multiple of $l_1, \dots, l_m$, then $\alpha_k^p = e$ for all k.
(when $|a| = l$, we have $a^k = e \iff l|k$)
So

$$
\begin{aligned}
\alpha^p &= (\alpha_1\alpha_2\ldots\alpha_m)^p \\
&= \alpha_1^p\alpha_2^p\ldots\alpha_m^p \quad \text{Since disjoint cycles commute} \\
&= e
\end{aligned}
$$

If p is not a common multiple of $l_1,\ldots,l_m$, then we can choose k so that p is not a multiple of l_k.
Write $p = q \cdot l_k + r$ with $0 \leq r \leq l_k$.
Then for $\alpha_k = (a_{k,1}a_{k,2}\ldots a_{k,l_2})$
We have $\alpha_k^p\,(a_{k,1}) = \alpha_k^r(a_{k,1}) = a_{k,1+r} \neq a_{k,1}$.
So,

$$
\begin{aligned}
&\alpha^p\,(a_{k,1}) \\
=&(\alpha_1\ldots\alpha_m)^p\,(a_{k,1}) \\
=&\alpha_k^p\left(\prod_{i\neq k}\alpha_i^p\right)(a_{k,1}) \\
=&\alpha_k^p\,(a_{k,1}) \\
\neq& a_{k,1}
\end{aligned}
$$

Hence, $\alpha \neq e$.
Eg. Find the number of elements of each order in S_6.
Solution:

Form of α	# of such α	$\lvert\alpha\rvert$
$(a\ b\ c\ d\ e\ f)$	$\binom{6}{6}5! = 120$	6
$(a\ b\ c\ d\ e)$	$\binom{6}{5}4! = 144$	5
$(a\ b\ c\ d)$	$\binom{6}{4}3! = 90$	4
$(a\ b\ c\ d)\,(e\ f)$	$\binom{6}{4}\binom{2}{3}3!1! = 90$	4
$(a\ b\ c)$	$\binom{6}{3}2! = 40$	3
$(a\ b\ c)\,(d\ e\ f)$	$\binom{6}{6}\cdot 5\cdot 4\cdot 1\cdot 2\cdot 1 = 40$	3
$(a\ b\ c)\,(d\ e)$	$\binom{6}{3}\binom{3}{2}2! = 120$	6
$(a\ b)$	$\binom{6}{2} = 15$	2
$(a\ b)\,(c\ d)$	$\binom{6}{4}1\cdot 3\cdot 1\cdot 1 = 45$	2
$(a\ b)\,(c\ d)\,(e\ f)$	$\binom{6}{6}1\cdot 5\cdot 1\cdot 3 = 15$	2
(a)	1	1
Total	720	

$\lvert\alpha\rvert$	# of such α
6	240
5	144
4	180
3	80
2	75
1	1

9 September 27th

Theorem: (Parity of Permutations)
Let $n \geq 2$ and consider S_n,

1. Every permutation in S_n can be written as a product of 2-cycles.
2. If $e \in S_n$ is equal to a product of l 2-cycles, $e = (a_1\ b_1)\,(a_2\ b_2)\ldots(a_l\ b_l)$ with $a_i \neq b_i$, then l is even.
3. If $\alpha \in S_n$ is a product of l 2-cycles and a product of m 2-cycles, then $m = l \mod 2$.

Proof:

1. We already know every $\alpha \in S_n$ can be written as a product of (disjoint) cycles, and for $\alpha = (a_1\ a_2\ \ldots\ a_l)$, note that
$$\alpha = (a_1\ a_l)\,(a_1\ a_{l-1})\ldots(a_1\ a_3)\,(a_1\ a_2)$$
2. Note that we cannot write e as a 2-cycle. ($e \neq (a, b)$ where $a \neq b$) and we can write e as a product of 2 2-cycles $e = (1\ 2)\,(1\ 2)$

   Let $l \geq 3$. Suppose, inductively, for all $m < l$, if e can be written as a product of m 2-cycles, then m must be even.

   Suppose e can be written as a product of l 2-cycles,

   say $e = (a_1\ b_1)\,(a_2\ b_2)\ldots(a_l\ b_l)$ where $a_i \neq b_i$ and let $a = a_1$.

   Of all the ways in which we can write e as a product of l 2-cycles, $e = (x_1\ y_1)\,(x_2\ y_2)\ldots(x_l\ y_l)\,, x_i \neq y_i$ in which $a = x_i$ for some.

   Choose one such way
$$e = (r_1\ s_1)\,(r_2\ s_2)\ldots(r_l\ s_l)$$
   with $r_i \neq s_i$,
$$a = r_k \text{ for some } k$$
   $r_i \neq a$ and $s_i \neq a$ for $i < k$ with k chosen to be as large as possible.

   Note that we cannot have $k \neq l$ because a product of 2-cycles $(x_1\ y_1)\,(x_2\ y_2)\ldots(x_k\ y_k)$ with $x_k = a$ and $x_i, y_i \neq a$ for $i < k$ is not equal to e since it sends y_k to $x_k = a \neq y_k$.

   Note that $(r_k\ s_k)\,(r_{k+1}\ s_{k+1})$ must be of one of the following forms (after possibly interchanging r_{k+1} and s_{k+1})
$$\begin{matrix} (a\ b)\,(a\ b) & (a\ b)\,(a\ c) \\ (a\ b)\,(b\ c) & (a\ b)\,(c\ d) \end{matrix}$$

where a, b, c, d are distinct elements in $\{1, 2, \ldots, n\}$.

But notice that

$$(a\ b)\,(a\ c) = (a\ c\ b) = (b\ c)\,(a\ b)$$
$$(a\ b)\,(b\ c) = (a\ b\ c) = (b\ c)\,(a\ c)$$
$$(a\ b)\,(c\ d) = (c\ d)\,(a\ b)$$

which would contradict our choice of k.

Thus, $(r_k\ s_k)\,(r_{k+1}\ s_{k+1})$ is of the form $(a\ b)\,(a\ b)$

After cancelling these two 2-cycles, we can rewrite e as a product of $(l-2)$ 2-cycles.

By the induction hypothesis, $l-2$ is even, so l is even.

3. Let $\alpha \in S_n$,

   Suppose $\alpha = (a_1\ b_1)\,(a_2\ b_2)\ldots(a_l\ b_l)\,, a_i \neq b_i$.

   and $\alpha = (c_1\ d_1)\,(c_2\ d_2)\ldots(c_m\ d_m)\,, c_i \neq d_i$.

   Then $e = \alpha\alpha^{-1} = (a_1\ b_1)\ldots(a_l\ b_l)\,(c_m\ d_m)\ldots(c_2\ d_2)\,(c_1\ d_1)$

   By part 2, $l + m$ is even, so $m = l \mod 2$.

Definition:
For $\alpha \in S_n$ with $n \geq 2$, we say that α is even, and we write $(-1)^\alpha = 1$, when α can be written as a product of an even number of 2-cycles, and we say that α is odd, and we write $(-1)^\alpha = -1$, when α can be written as a product of an odd number of 2-cycles.
$(-1)^\alpha$ is called the **parity** of α.
Note:
In S_n with $n \geq 2$, we have

1. $(-1)^e = 1$
2. If α is an l-cycle, then $(-1)^\alpha = (-1)^{l-1}$.
3. For all $\alpha, \beta \in S_n$, $(-1)^{\alpha\beta} = (-1)^\alpha\,(-1)\,\beta$.
4. For $\alpha \in S_n$, $(-1)^{\alpha^{-1}} = (-1)^\alpha$

Definition:
The n^{th} alternating group is the subgroup

$$A_n = \{\alpha \in S_n | (-1)^\alpha = 1\} \leq S_n$$

Eg.
Also, recall that when $n \geq 3$, we can consider D_n as a subgroup of S_n.
Using cycle notation,

$$\begin{aligned}
S_3 &= \{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}\\
A_3 &= \{(1),(1\ 2\ 3),(1\ 3\ 2)\}\\
D_3 &= \{R_0,R_1,R_2,F_0,F_1,F_2\}\\
&= \{(1)\,,(1\ 2\ 3)\,,(1\ 3\ 2)\,(1\ 2)\,,(1\ 3)\,,(2\ 3)\}\\
&= S_3
\end{aligned}$$

$$\begin{aligned}
S_4 = \{&(1)\,,(1\ 2)\,,(1\ 3)\,,(1\ 4)\,,(2\ 3)\,,(2\ 4)\,,(1\ 2\ 3)\,,(1\ 3\ 2)\,,(1\ 2\ 4)\,,\\
&(1\ 4\ 2)\,,(1\ 3\ 4)\,,(1\ 4\ 3)\,,(2\ 3\ 4)\,,(2\ 4\ 3)\,,(1\ 2\ 3\ 4)\,,(1\ 2\ 4\ 3)\,,\\
&(1\ 3\ 2\ 4)\,,(1\ 3\ 4\ 2)\,,(1\ 4\ 2\ 3)\,,(1\ 4\ 3\ 2)\,,(1\ 2)\,(3\ 4)\,,\\
&(1\ 3)\,(2\ 4)\,,(1\ 4)\,(2\ 3)\}\\
A_4 = \{&(1)\,,(1\ 2\ 3)\,,(1\ 3\ 2)\,,(1\ 2\ 4)\,,(1\ 4\ 2)\,,(1\ 3\ 4)\,,(1\ 4\ 3)\,,(2\ 3\ 4)\,,\\
&(2\ 4\ 3)\,,(1\ 2)\,(3\ 4)\,,(1\ 3)\,(2\ 4)\,,(1\ 4)\,(2\ 3)\}\\
D_4 = \{&I,R_1,R_2,R_3,F_0,F_1,F_2,F_3\}
\end{aligned}$$

with for example, $R_1 = (1\ 2\ 3\ 4)\,, R_2 = R_1^2 = (1\ 3)\,(2\ 4)\,, F_0 = (1\ 3)\,, F_1 = (1\ 4)\,(2\ 3)$ etc.

Example:

$$\begin{aligned}
S_n &= \langle (1\ 2)\,,(1\ 3)\,,(1\ 4)\,,\dots(1\ n)\\
&= \langle (1\ 2)\,,(2\ 3)\,,(3\ 4)\,,\dots,(n-1,n)\rangle\\
&= \langle (1\ 2)\,,(1\ 2\ 3\dots\ n)\rangle.
\end{aligned}$$

Example:

Show that A_n is generated by 3-cycles. $(a\ b\ c)$.

$$A_n = \langle (1\ 2\ 3)\,,(1\ 2\ 4)\,,(1\ 2\ 5)\,,\dots,(1\ 2\ n)\rangle$$

10 September 30th

Exercise:

If $a \in G$ and $b \in H$ and $|a|$ and $|b|$ are finite, then in $G \times H$, we have $|(a,b)| = \operatorname{lcm}(|a|,|b|)$

$$\mathbb{Z}_9 \times \mathbb{Z}_{15}$$

Generators for S_n and A_n:

Since every $\alpha \in S_n$ is a product of 2-cycles,

$$S_n = \langle (a\ b)\,|a,b \in \{1,\dots,n\}, a < b\rangle$$

Since when a, b are distinct

$$(a\ b) = (1\ a)\,(1\ b)\,(1\ a)$$

It follows that $S_n = \langle (1\ 2)\,, (1\ 3)\,, (1\ 4)\,, \ldots, (1\ n) \rangle$.
Also, note that for $k \neq 1$,

$$\begin{aligned}(1\ k) = (1\ 2)\,(2\ 3)\,(3\ 4) \ldots (k-2\ k-1)\,(k-1\ k)\\ (k-2\ k-1) \ldots (3\ 4)\,(2\ 3)\,(1\ 2)\end{aligned}$$

and so we also have

$$S_n = \langle (1\ 2)\,, (2\ 3)\,, (3\ 4)\,, \ldots, (n-1, n) \rangle$$

Also note that

$$S_n = \langle (1\ 2)\,, (1\ 2\ 3 \ldots n) \rangle$$

because

$$(k\ k+1) = (1\ 2 \ldots n)^{k-1}\,(1\ 2)\,(1\ 2 \ldots n)^{-(k-1)}$$

If we think of D_n as a subgroup of S_n,

$$\begin{aligned}D_n &= \langle R_1, F_0 \rangle\\ &= \langle (1\ 2\ 3 \ldots n)\,, (1\ n-1)\,(2\ n-2) \ldots (k\ n-k)\end{aligned}$$

where $k = \left\lfloor \frac{n-1}{2} \right\rfloor$
Since every $\alpha \in A_n$ is a product of an even number of 2-cycles, A_n is generated by all products of pairs of 2-cycles.

$$A_n = \langle (a\ b)\,(c\ d)\,|a, b, c, d \in \{1, \ldots, n\}, a \neq b, c \neq d \rangle$$

Also, we claim that A_n is generated by 3-cycles,

$$A_n = \langle (a\ b\ c)\,|a, b, c \text{ are distinct elements of } \{1, 2, \ldots, n\} \rangle$$

Proof:
Every product of a pair of 2-cycles is of one of the forms,

$$(a\ b)\,(a\ b)\,, (a\ b)\,(a\ c)\,, (a\ b)\,(b\ c)\,, (a\ b)\,(c\ d)$$

with a, b, c and d distinct, and we have

$$
\begin{aligned}
&(a\ b)\,(a\ b) = e = (a\ b\ c)^3 = (a\ b\ c)^0 \\
&(a\ b)\,(a\ c) = (a\ c\ b) \\
&(a\ b)\,(b\ c) = (a\ b\ c) \\
&(a\ b)\,(c\ d) = (a\ d\ c)\,(a\ b\ c)
\end{aligned}
$$

Exercise:
Show that $A_n = \langle (1\ 2\ 3)\,, (1\ 2\ 4)\,, (1\ 2\ 5)\,, \ldots, (1\ 2\ n)\rangle$
Equivalence Classes
Definition:
An equivalence relation on a set S is a binary relation $\sim$ on S such that

1. For all $a \in S$, $a \sim a$.

2. For all $a, b \in S$, if $a \sim b$, then $b \sim a$.

3. For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

When $\sim$ is an equivalence relation on S and $a \in S$, the equivalence class of a is the set $[a] = \{x \in S | x \sim a\}$
Note that for $a, b \in S$,

$$a \sim b \iff b \in [a] \iff [a] = [b]$$

and when $a \not\sim b$, (so $[a] \neq [b]$), we have $[a] \cap [b] = \emptyset$.
Sketch Proof:
Suppose $a \sim b$, then $b \sim a$ by (2), so $b \in [a]$.
If $x \in [a]$, then $x \sim a$.
Then since $x \sim a$ and $a \sim b$, we have $x \sim b$ by (3), hence $x \in [b]$.
Thus, $[a] \subseteq [b]$.
If $x \in [b]$, then $x \sim b$.
Since $a \sim b$, we have $b \sim a$ by (2).
Since $x \sim b$ and $b \sim a$, we have $x \sim a$ by (3).
Hence, $x \in [a]$.
Thus, $[b] \subseteq [a]$.
Thus proves part of the 1st statement.
Suppose $a \not\sim b$, (so $[a] \neq [b]$).
Suppose, for a contradiction, that $[a] \cap [b] \neq \emptyset$,
Choose $c \in [a] \cap [b]$.
Since $c \in [a]$, we have $[c] = [a]$.
Since $c \in [b]$, we have $[c] = [b]$.
Thus, $[a] = [c] = [b]$, (giving a contradiction).
Example:
When $n \in \mathbb{Z}^+$, we can define a relation $\sim$ on $\mathbb{Z}$ by $a \sim b \iff a = b \mod n$.
Then, $\sim$ is an equivalence relation,

$$\mathbb{Z}_n = \{[a] | a \in \mathbb{Z}\}$$

Definition:
When $\sim$ is an equivalence relation on a set S, the quotient of S by $\sim$ denoted by $S/\sim$, is the set of equivalence classes.

$$S/\sim = \{[a] | a \in S\}$$

Definition:
For a group G and an element $a \in G$, the left multiplication by a is the map $L_a : G \to G$ given by $L_a(x) = ax$.
and the right multiplication by a is the map $R_a : G \to G$ given by $R_a(x) = xa$.
The conjugation by a is the map $C_a : G \to G$ given by $C_a(x) = axa^{-1}$.
Also, for $a, b \in G$, we say that a and b are conjugate in G, and we write $a \sim b$, when $b = C_g(a) = gag^{-1}$ for some $g \in G$.
Note that every conjugacy is an equivalence relation on G.

1. $a \sim a$ since $C_e(a) = eae^{-1} = a$
2. If $a \sim b$, say $b = C_g(a) = gag^{-1}$, then $a = g^{-1}bg = C_{g^{-1}}(b)$ and
3. If $a \sim b$, say $b = gag^{-1}$, and if $b \sim c$, say $c = hbh^{-1}$, then

$$\begin{aligned} c &= hbh^{-1} = hgag^{-1}h^{-1} \\ &= (hg)a(hg)^{-1} \\ &= C_{hg}(a) \end{aligned}$$

So $c \sim a$.
The equivalence class of $a \in G$ under conjugacy is called the conjugacy class of a in G, and it is denoted by $Cl(a)$, so

$$Cl(a) = [a] = \{x \in G | x = gag^{-1} \text{ for some } g \in G\}$$

11 October 2nd

Conjugacy Classes
For $a, b \in G$, we say a is conjugate to b, and write $a \sim b$, when $b = C_g(a) = gag^{-1}$ for some $g \in G$.
This is an equivalence relation, the equivalence class of $a \in G$ is called the conjugacy class and is denoted by $Cl(a)$, so

$$Cl(a) = [a] = \{x \in G | x = gag^{-1} \text{ for some } g \in G\}$$

G is the disjoint union of the conjugacy classes.
Theorem: Conjugacy Classes in S_n

For $\alpha, \beta \in S_n$, we have $\alpha \sim \beta$ and if and only if when α and β are written in cycle notation, they have the same number of cycles of each length.
Proof:
When α is written in cycle notation as

$$\alpha = (a_{11}\ a_{12} \dots a_{1l_1})\,(a_{21}\ a_{22} \dots a_{2l_2}) \dots (a_{m1}\ a_{m2} \dots a_{ml_m})$$

For all $\sigma \in S_n$, we have

$$\sigma\alpha\sigma^{-1} = (\sigma(a_{11}), \sigma\,(a_{12})\,, \dots, \sigma\,(a_{1,l_1})) \dots (\sigma(a_{m1}), \dots, \sigma\,(a_{m,l_m}))$$

(On the right, $\sigma\,(a_{ij})$ is sent to $\sigma\,(a_{i,j+1})$, and on the left, $\sigma(a_{ij})$ is sent by σ^{-1} to a_{ij}, which is sent by α to $\alpha(a_{ij}) = a_{i,j+1}$, which is sent by σ to $\sigma(a_{i,j+1})$)
Eg.
When we listed the possible "types" or "forms" for elements in S_6 as
$(a\ b\ c\ d\ e\ f)\,, (a\ b\ c\ d\ e)\,, (a\ b\ c\ d)\,(e\ f)\,, (a\ b\ c\ d)\,,$
$(a\ b\ c)\,(d\ e\ f)\,, (a\ b\ c)\,(d\ e)\,, (a\ b)\,(c\ d)\,(e\ f)\,, (a\ b)\,(c\ d)\,, (a\ b)\,, (a)$.
We were actually listing the conjugacy classes in S_6.

Chapter 4: Group Homomorphisms

Definition:
Let G and H be groups.
A (group) homomorphism from G to H is a function $\phi = G \to H$ such that

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

for all $a, b \in G$
A bijective (group) homomorphism $\phi : G \to H$ is called a (group) isomorphism.
We say that G and H are isomorphic, and we write $G \cong H$, when there exists an isomorphism $\phi : G \to H$.
An endomorphism of G is a homomorphism from G to G and an automorphism of G is an isomorphism from G to G.
We write

$$\begin{aligned}
\mathrm{Iso}(G, H) &= \{\phi : G \to H | \phi \text{ is an isomorphism}\} \\
\mathrm{Hom}(G, H) &= \{\phi : G \to H | \phi \text{ is an homomorphism}\} \\
\mathrm{End}(G) &= \{\phi : G \to G | \phi \text{ is an endomorphism}\} \\
\mathrm{Aut}(G) &= \{\phi : G \to G | \phi \text{ is an automorphism}\}
\end{aligned}$$

Note:
Let $\phi : G \to H$ be a homomorphism of groups.

1. $\phi(e) = e$
2. $\phi(a^{-1}) = \phi(a)^{-1}$
3. $\phi(a^k) = \phi(a)^k$ for $k \in \mathbb{Z}$

Proof:

1. $\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$
   $\therefore \phi(e) = e$ by cancellation.

2. $\phi(a) \cdot \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(e) = e$
   $\therefore \phi(a)^{-1} = \phi(a^{-1})$ by cancellation.

3. Follows from (b) and from induction.

Question: How is $|a|$ related to $|\phi(a)|$?
Note:

1. $I : G \to G$ given by $I(x) = x$ is a group homomorphism.

2. If $\phi : G \to H$ and $\psi : H \to K$ are group homomorphisms, then so is $\psi \circ \phi : G \to K$

3. If $\phi : G \to H$ is an isomorphism (an invertible homomorphism), then $\phi^{-1} : H \to G$.

Proof (3)
Suppose $\phi : G \to H$ is an isomorphism and let $\psi = \phi^{-1} : H \to G$. Let $c, d \in H$
Let $a = \psi(c)$ and $b = \psi(d)$ so that $c = \phi(a), d = \phi(b)$.
Then

$$\begin{aligned}
\psi(cd) &= \psi\left(\phi(a)\phi(b)\right) \\
&= \psi(\phi(a \cdot b)) \text{ Since } \psi \text{ is a homomorphism} \\
&= a \cdot b \text{ (since } \psi = \phi^{-1} \text{)} \\
&= \psi(c) \cdot \psi(d)
\end{aligned}$$

Corollary:
Isomorphism of groups is an equivalence relation (on the class of all groups).
$\{x | F(x) \text{ is true}\}$ is a "class".
If A is a set, then

$$\{x \in A | F(x) \text{ is true}\}$$

is a set.
For all groups G, H, K

1. $G \cong G$.

2. If $G \cong H$, then $H \cong G$.

3. If $G \cong H$ and $H \cong K$, then $G \cong K$.

Note:
Let $\phi : G \to H$ be a homomorphism of groups. Then

1. If $K \leq G$, then $\phi(K) = \{\phi(a)|a \in K\} \leq H$, in particular, $\text{Im}(\phi) = \text{Range}(\phi) = \phi(G) \leq H$.

2. If $L \leq H$, then $\phi^{-1}(L) = \{a \in G|\phi(a) \in L\} \leq G$, in particular, $\text{Ker}(\phi) = \phi^{-1}(e) \leq G$.

Proof:
Suppose $K \leq G$

12 October 4th

Definition:
Let G and H be groups.
A group homomorphism from G to H is a function $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.
A group isomorphism from G to H is a bijective group homomorphism from G to H.
Note:
For a homomorphism $\phi : G \to H$

1. $\phi(e) = e$

2. $\phi(a^{-1}) = \phi(a)^{-1}$

3. $\phi(a^k) = \phi(a)^k$ for all $k \in \mathbb{Z}$

If $|\phi(a)| = n$ in H, then $\phi(a^n) = \phi(a)^n = e$
So $|a|$ is a multiple of $n = |\phi(a)|$
Note:
$I : G \to G$ is an isomorphism if $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then so is $\psi \circ \phi : G \to K$.
If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is too.
Corollary:
Isomorphism is an equivalence relation (on the class of groups)
Definition:
When $\phi : G \to H$ is a group homomorphism, the image of ϕ is denoted by $\text{Im}(\phi)$, so

$$\text{Im}(\phi) = \text{Range}(\phi) = \phi(G) = \{\phi(a)|a \in G\}$$

and the kernel of ϕ is the set

$$\text{Ker}(\phi) = \phi^{-1}(e) = \{a \in G|\phi(a) = e\}$$

Side Note: Relation to Matrix

$A \in M_{n\times m}(\mathbb{R}), A : \mathbb{R}^m \to \mathbb{R}^n$.

$$\begin{aligned}\mathrm{Ker}(A) &= \mathrm{Null}(A)\\ &= A^{-1}(0) = \{x \in \mathbb{R}^m | Ax = 0\}\end{aligned}$$

In $GL_n(\mathbb{C})$,

$$A \sim B \iff B : PAP^{-1}$$

for some $P \in GL_n(\mathbb{C})$.
Note:
Let $\phi : G \to H$ be a homomorphism.

1. If $K \leq G$, then $\phi(K) \leq H$.
   In particular, $\mathrm{Im}(\phi) = \phi(G) \leq H$.
2. If $L \leq H$, then $\phi^{-1}(L) \leq G$.
   In particular, $\mathrm{Ker}(\phi) \leq G$.

Proof:

1. Suppose $K \leq G$
   Then $\phi(K) \leq H$ because

   $$e_H = \phi(e_G) \in \phi(K)$$

   since $e_G \in K$
   and if $a, b \in K$. So $\phi(a), \phi(b) \in \phi(K)$,
   then $\phi(a) \cdot \phi(b) = \phi(ab) \in \phi(K)$ since $ab \in K$
   and if $a \in K$, so $\phi(a) \in \phi(K)$, then

   $$\phi(a)^{-1} = \phi(a^{-1}) \in \phi(K)$$

   since $a^{-1} \in K$.
2. Exercise.

Examples of Homomorphisms
The map $\phi : \mathbb{R} \to \mathbb{R}^+$ given by $\phi(t) = e^t$ is a homomorphism, because for $s, t \in \mathbb{R}$

$$\begin{aligned}\phi(s+t) &= e^{s+t} = e^s \cdot e^t\\ &= \phi(s) \cdot \phi(t)\end{aligned}$$

We have $\text{Ker}\phi = \phi^{-1}(1) = \{0\}$
The map

$$\phi : \mathbb{R} \to \mathbb{S}^1 = \{z \in \mathbb{C}^* || z| = 1\}$$

given by $\phi(t) = e^{i2\pi t}$
is a homomorphism because for $s, t \in \mathbb{R}$,

$$\begin{aligned}\phi(s+t) &= e^{i2\pi(s+t)} \\ &= e^{i2\pi s} \cdot e^{i2\pi t} \\ &= \phi(s) \cdot \phi(t)\end{aligned}$$

We have $\text{Ker}(\phi) = \phi^{-1}(1) = \mathbb{Z}$
The map $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ given by $\phi(A) = \det(A)$
Missing parts ...
Examples:
Let G be any group, describe $\text{Hom}(\mathbb{Z}, G)$
Solution:
Let $a \in G$, define $\phi_a : \mathbb{Z} \to G$ given by $\phi_a(K) = a^k$.
Then ϕ_a is a homomrophism, because

$$\begin{aligned}\phi_a(k+l) &= a^{k+l} = a^k \cdot a^l \\ &= \phi_a(k) \cdot \phi_a(l)\end{aligned}$$

Note:
Every homomorphism $\phi : \mathbb{Z} \to G$ is equal to one of the homomorphisms $\phi_a, a \in G$.
Indeed, given a homomorphism $\phi : \mathbb{Z} \to G$, let $a = \phi(1)$ and then for all $k \in \mathbb{Z}$

$$\phi(k) = \phi(k \cdot 1) = \phi(1)^k = a^k = \phi_a(k)$$

So we have $\phi = \phi_a$
Thus, $\text{Hom}(\mathbb{Z}, G) = \{\phi_a | a \in G\}$
Exercise:
Let G be any group, describe $\text{Hom}(\mathbb{Z}_n, G)$

13 October 7th

Note:
For a group homomorphism, $\phi : G \to H$, note that

$$\phi \text{ is injective } \iff \text{Ker}(\phi) = \{e\}$$

Proof:
If ϕ is injective, then since $\phi(e) = e$. It follows that

$$\phi(a) = e_H \iff a = e_G$$

So

$$\begin{aligned}\text{Ker}(\phi) &= \phi^{-1}(e_H) \\ &= \{a \in G | \phi(a) = e_H\} \\ &= \{e_G\}\end{aligned}$$

Suppose $\text{Ker}(\phi) = \{e\}$.
Let $a, b \in G$ and suppose $\phi(a) = \phi(b)$.
Then

$$\begin{aligned}\phi(ab^{-1}) &= \phi(a)\phi(b)^{-1} = \phi(a)\phi(a)^{-1} \\ &= e_H\end{aligned}$$

So $ab^{-1} \in \text{Ker}(\phi) = \{e_G\}$
Hence $ab^{-1} = e$
$\therefore a = b$
Examples of Isomorphisms
Examples:

1. The map $\phi : \mathbb{R} \to \mathbb{R}^+$ given by $\phi(x) = e^x$ is a group isomorphism with inverse $\psi : \mathbb{R}^+ \to \mathbb{R}$ given by $\psi(y) = \log(y) = \ln(y)$.
2. The map $\phi : SO_2(\mathbb{R}) \to \mathbb{S}^1$ given by $\phi(R_\theta) = e^{i\theta}$ is a group isomorphism.
3. Show that $U_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Solution:
In U_{12} we have the operation table.

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

and in $\mathbb{Z}_2 \times \mathbb{Z}_2$, we have the operation table

	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

From the table, we see that the map $\phi : U_{12} \to \mathbb{Z}_2 \times \mathbb{Z}_2$ given by $\phi(1) = (0,0), \phi(5) = (1,0), \phi(7) = (0,1)$ and $\phi(11) = (1,1)$ is an isomorphism.
Examples:
If $a \in G$ with $|a| = \infty$, then $\langle a \rangle \cong \mathbb{Z}$.
Indeed, the map $\phi : \langle a \rangle = \{a^k | k \in \mathbb{Z}\} \to \mathbb{Z}$ given by $\phi(a^k) = k$ is an isomorphism with inverse $\psi : \mathbb{Z} \to \langle a \rangle$ given by $\psi(k) = a^k$. (ψ is a homomorphism because $\psi(k+l) = a^{k+l} = a^k \cdot a^l = \psi(k) \cdot \psi(l)$ and ψ is bijective by the Elements in Cyclic Groups Theorem.)
Examples:
If $a \in G$ with $|a| = n \in \mathbb{Z}^+$, then $\langle a \rangle \cong \mathbb{Z}_n$
Indeed, the map $\psi : \mathbb{Z}_n \to \langle a \rangle$ given by $\psi(k) = a^k$ is a group isomorphism. (by the Elements in Cyclic Groups Theorem)
Theorem:
When $k, l \in \mathbb{Z}^+$ with $\gcd(k,l) = 1$, we have $\mathbb{Z}_{kl} \cong \mathbb{Z}_k \times \mathbb{Z}_l$ and $U_{kl} \cong U_k \times U_l$.
Indeed, the map $\phi : \mathbb{Z}_{kl} \to \mathbb{Z}_k \times \mathbb{Z}_l$ and the map $\phi : U_{kl} \to U_k \times U_l$ given by $\phi(a) = (a,a)$, that is

$$\phi(a \bmod kl) = (a \bmod k, a \bmod l)$$

are group isomorphisms.
Proof:
Let us show that $\phi : U_{kl} \to U_k \times U_l$ is an isomorphism.
Note that ϕ is well-defined because, for $a \in \mathbb{Z}$, if $a \in U_{kl}$, so $\gcd(a, kl) = 1$ then $\gcd(a,k) = 1$ and $\gcd(a,l) = 1$.
So $a \in U_k$ and $a \in U_l$
Hence $\phi(a) = (a,a) \in U_k \times U_l$
Also note that ϕ is group homomorphism because, for $a, b \in \mathbb{Z}$

$$\begin{aligned} \phi(a \cdot b) &= (a \cdot b, a \cdot b) \in U_k \times U_l \\ &= (a,a) \cdot (b,b) \in U_k \times U_l \end{aligned}$$

Finally note that ϕ is bijective by the Chinese Remainder Theorem:
Given a with $\gcd(a,k) = 1$, so $a \in U_k$ and b with $\gcd(b,l) = 1$, so $b \in U_l$
We can solve the pair of congruences

$$x = a \bmod k$$
$$x = b \bmod l$$

by the CRT.
and then
Since $x = a \bmod k$, we have $\gcd(x,k) = \gcd(a,k) = 1$.
And since $x = b \bmod l$, we have $\gcd(x,l) = \gcd(b,l) = 1$.
And since $\gcd(x,k) = 1$ and $\gcd(x,l) = 1$, we have $\gcd(x,kl) = 1$, so $x \in U_{kl}$.
and since $x = a \bmod k$ and $x = b \bmod l$
We have

$$\phi(x) = (a, b) \in U_k \times U_l$$

This shows that ϕ is surjective.
The CRT also implies that ϕ is injective because the solution to the pair of congruences

$$x = a \bmod k$$

$$x = b \bmod l$$

is unique modulo, $\text{lcm}(k, l) = kl$, (since $\gcd(k, l) = 1$)
Corollary:

1. When $k, l \in \mathbb{Z}^+$ with $\gcd(k, l) = 1$, we have $\phi(kl) = \phi(k)\phi(l)$. Since $\phi(kl) = |U_{kl}| = |U_k \times U_l| = |U_k| \cdot |U_l| = \phi(k) \cdot \phi(l)$

2. When $n = \prod_{i=1}^{l} p_i^{k_i}$, where the p_i are distinct primes,

$$\phi(n) = \prod_{i=1}^{l} \phi(p_i^{k_i}) = \prod_{i=1}^{l} (p_i^{k_i} - p_i^{k_i - 1})$$

Example:

$$\begin{aligned} |U_{3000}| &= \phi(3000) \\ &= \phi(2^3 \cdot 3^1 \cdot 5^3) \\ &= \left(2^3 - 2^2\right)\left(3^1 - 3^0\right)\left(5^3 - 5^2\right) \\ &= 4 \cdot 2 \cdot 100 = 800 \end{aligned}$$

Theorem: (Properties Shared by Isomorphic Groups)
Let $\phi : G \to H$ be a group isomorphism. Then

1. $|G| = |H|$

2. G is abelian $\iff$ H is abelian.

3. For $a \in G$, we have $|a| = |\phi(a)|$

4. G is cyclic $\iff$ H is cyclic.

5. G and H have the same number of elements of each order

   For $n \in \mathbb{Z}^+ \cup \{\infty\}$, we have

$$|\{a \in G||a| = n\}| = |\{b \in H||b| = n\}|$$

6. For $a, b \in G$, we have

$$a \sim b \iff \phi(a) \sim \phi(b)$$

7. G and H have the same number of conjugacy classes (and the same number of classes of each size)

8. For $K \leq G$, the restriction $\phi : K \to \phi(K)$ is an isomorphism.

9. G and H have the same number of subgroups (and the same number of n-element subgroups, and the same number of subgroups isomorphic to a particular group L).

14 October 9th

Sample Proof:
Let $\phi : G \to H$ be a group homomorphism, and let $a \in G$.
Let us show that $|a| = |\phi(a)|$
For $n \in \mathbb{Z}^+$,

$$\begin{aligned} a^n = e &\iff \phi(a^n) = \phi(e) \text{ Since } \phi \text{ is injective.} \\ &\iff \phi(a)^n = e \text{ Since } \phi(a^n) = \phi(a)^n \text{, and } \phi(e) = e \end{aligned}$$

Example:

1. $U_{35} \ncong U_{42}$
   Since $|U_{35}| = \phi(35) = 24$, $|U_{42}| = \phi(42) = 12$.

2. $S_5 \ncong GL_3(\mathbb{Z}_2)$
   Since $|S_5| = 5! = 5 \cdot 4 \cdot 3 \cdot 2$
   and $|GL_3(\mathbb{Z}_2)| = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 7 \cdot 6 \cdot 4$

3. $\mathbb{R}^* \ncong \mathbb{C}^*$
   Since $\mathbb{R}^*$ has no elements of order 3, but in $\mathbb{C}^*$, $\alpha = e^{i2\pi/3}$ and also $\alpha^2 = e^{i4\pi/3}$ have order 3.

Inner Automorphisms
Recall that for a group G, $\text{Aut}(G)$ is the set of isomorphisms $\phi : G \to G$. Note that $\text{Aut}(G)$ is a group under composition.
Note that for $a \in G$, the conjugation map $C_a : G \to G$ given by $C_a(x) = axa^{-1}$ is a group automorphism indeed.

$$\begin{aligned} C_a(xy) &= axya^{-1} \\ &= axa^{-1}aya^{-1} \\ &= C_a(x)C_a(y) \end{aligned}$$

and for $a, b \in G$,

$$\begin{aligned} C_a(C_b(x)) &= C_a(bxb^{-1}) = abxb^{-1}a^{-1} \\ &= (ab)x(ab)^{-1} = C_{ab}(x) \end{aligned}$$

So that in particular,

$$(C_a)^{-1} = C_{a^{-1}}$$

An automorphism of G of the $C_a : G \to G$ for some $a \in G$ is called an inner automorphism and we denote the set of inner automorphisms by $\mathrm{Inn}(G)$

$$\mathrm{Inn}(G) = \{C_a : G \to G | a \in G\}$$

Note that the above calculations show that

$$\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$$

Exercise:

1. Show that $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$
2. Find $|\mathrm{Aut}\, D_6|$ and $|\mathrm{Inn}\, D_6|$

Theorem: (Cayley's Theorem)

1. If G is any set with n elements, then $\mathrm{Perm}(G) \cong S_n$.

   Indeed, if $f : G \to \{1, 2, \ldots, n\}$ is any bijection, then the map $\phi : \mathrm{Perm}(G) \to S_n$ given by $\phi(\sigma)(k) = f(\sigma(f^{-1}(k)))$ for $k \in \{1, 2, \ldots, n\}$.

   That is, $\phi(\sigma) = f\sigma f^{-1}$.
2. If G is any group, then G is isomorphic to a subgroup of $\mathrm{Perm}(G)$. Indeed, the map $\psi : G \to \mathrm{Perm}(G)$ given by $\psi(a) = L_a$ (where $L_a : G \to G$ is given by $L_a(x) = ax$) is an injective group homomorphism. (So $\psi : G \to \psi(G)$ is an isomorphism)
3. If G is a finite group with $|G| = n$, then G is isomorphic to a subgroup of S_n.

Sketch Proof:

1. Verify that if $\sigma \in \mathrm{Perm}(G)$, then $\phi(\sigma) = f\sigma f^{-1} \in S_n$.

   (So $\phi(\sigma) = f\sigma f^{-1} \in \mathrm{Perm}\{1, 2, \ldots, n\}$)

   Also, verify that ϕ is a homomorphism.

   (**Proof:** $\phi(\sigma\tau) = f\sigma\tau f^{-1} = f\sigma f^{-1} f\tau f^{-1} = \phi(\sigma)\phi(\tau)$)

   Also, verify that ϕ is bijective.

2. Let $\psi : G \to \text{Perm}(G)$ be given by $\psi(a) = L_a$.

   Verify that ψ is well-defined. $((L_a)^{-1} = L_{a^{-1}})$

   Verify that ψ is a group homomorphism. $(\psi(ab) = L_{ab} = L_a L_b = \phi(a)\phi(b))$

   Verify that ϕ is injective.

   (For $a, b \in G$, if $\phi(a) = \phi(b)$, so $L_a = L_b$ (as functions), then $L_a(x) = L_b(x)$ for all $x \in G$. So $a = L_a(e) = L_b(e) = b$)

3. Compose ψ and ϕ from parts (1) and (2).

Example:
U_{12}

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

If we use the bijection $f : U_{12} \to \{1, 2, 3, 4\}$ given by $f(1) = 1, f(5) = 2, f(7) = 3, f(11) = 4$.
Then U_{12} is isomorphic to the subgroup $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = A_4 \leq S_4$

15 October 11th

Chapter 5: Cosets, Quotient Groups
Definition:
Let G be a group and let $H \leq G$.
For $a \in G$, the left coset of H in G containing a is the set

$$\begin{aligned} aH &= \{ah | h \in H\} \\ &= L_a(H) \end{aligned}$$

and the right coset of H in G containing a is the set

$$\begin{aligned} Ha &= \{ha | h \in H\} \\ &= R_a(H) \end{aligned}$$

When G is abelian, there is no difference between left and right cosets, so we just call them cosets.
When G is an additive abelian group, we write aH (and Ha) as $a + H$ and then

$$a + H = \{a + h | h \in H\}$$

Exercise:
Think about cosets of $\langle n \rangle = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}$ in $\mathbb{Z}$.
Theorem:
Let G be a group and let $H \leq G$,

1. For $a, b \in G$, $aH = bH \iff a \in bH \iff b^{-1}a \in H$
2. For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$
3. For all $a \in G$, $|aH| = |H|$

Proof:

1. Let $a, b \in G$.
   - If $aH = bH$, then $a \in bH$ because $a = ae \in aH$.
   - If $a \in bH$, say $a = bh$ where $h \in H$, then $b^{-1}a = h \in H$.

   Suppose that $b^{-1}a \in H$, say $b^{-1}a = h \in H$.

   If $x \in aH$, say $x = ak$ with $k \in H$, then $x = ak = (bh)k = b(hk) \in bH$ (since $hk \in H$).

   If $y \in bH$, say $y = bl$ with $l \in H$, then $y = bl = \left(ah^{-1}\right) l = a\left(h^{-1}l\right) \in aH$

2. Part(2) holds because we can (obviously) define an equivalence relation $\sim$ on G by define

$$\begin{aligned} a \sim b &\iff aH = bH \\ &(\iff a \in bH \iff b^{-1}a \in H) \end{aligned}$$

   and then, for $a \in G$, the equivalence class of a is

$$\begin{aligned} [a] &= \{b \in G | b \sim a\} \\ &= \{b \in G | b \in aH\} \\ &= aH \end{aligned}$$

3. Note that for $a \in H$, we have $|aH| = |H|$ because the map $L_a : H \to aH$ is bijective with inverse $L_{a^{-1}} : aH \to H$.

Notation:
When $H \leq G$ and, for $a, b \in G$, we define

$$a \sim b \iff aH = bH$$

the quotient $G/\sim$ is also written as G/H so

$$G/H = \{aH | a \in G\}$$

Theorem: (Lagrange's Theroem)
Let G be a group and let $H \leq G$.
Then $|G/H| \cdot |H| = |G|$
Proof:
This holds because G is the disjoint cosets and the cosets all have size $|H|$.
Corollary:
Let G be a finite group.

1. If $H \leq G$, then $|H| \Big| |G|$.

2. If $a \in G$, then $|a| \Big| |G|$.

Corollary: (Euler-Fermat Theorem)
Corollary:
If $a \in U_n$, then $a^{\phi(n)} = 1$.
Corollary: (The Classification of Groups of Order p)
Let p be a prime number and let G be a group with $|G| = p$. Then $G \cong \mathbb{Z}_p$.
Proof:
For any $a \in G$, we have $|a| \Big| |G|$. So $|a| \Big| p$, so $|a| = 1$ or p.
The only element of order 1 is e. So all the other elements have order p (and generate G).
Side Note:
For $a, b \in \mathbb{Z}$,

$$\begin{aligned} a \sim b &\iff a - b \in n\mathbb{Z} \\ &\iff a = b \bmod n \end{aligned}$$

So $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
Theorem:
Let $H \leq G$. Then the following are equivalent.

1. We can define a binary operation on G/H by $(aH)(bH) = (ab)H$

2. For all $a \in G$ and $h \in H$, we have $aha^{-1} \in H$.

3. For all $a \in G$, we have $aH = Ha$.

4. For all $a \in G$, $aHa^{-1} = H$, where $aHa^{-1} = \{aha^{-1} | h \in H = C_a(H)\}$

Proof:
Note that (1) means that for all $a, b, c, d \in G$, if $aH = cH$ and $bH = dH$, then $(ab)\,H = (cd)\,H$. Equivalently, it means that for all $a, b, c, d \in G$, if $c^{-1}a \in H$ and $d^{-1}b \in H$, then $d^{-1}c^{-1}ab = uhu^{-1} \in H$.
Suppose (1) holds (in the above form)
Let $u \in G$ and $h \in H$. Choose $b = d = u^{-1}$, and $a = h$ and $c = e$.
Then, $c^{-1}a = h \in H$ and $d^{-1}b = u \cdot u^{-1} = e \in H$.
So $d^{-1}b^{-1}ab \in H$, that is $uhu^{-1} \in H$.
Suppose, conversely, that (2) holds, (so we have $uhu^{-1} \in H$ for all $u \in G$ and $h \in H$)
Let $a, b, c, d \in G$ with $c^{-1}a \in H$ and $d^{-1}b \in H$, say $c^{-1}a = k \in H$, and $d^{-1}b = l \in H$.
Then $d^{-1}c^{-1}ab = d^{-1}kb = d^{-1}kdl \in H$,
since $d^{-1}kd \in H$ (by (2) using $u = d^{-1}, h = k$)
and $l \in H$.
Let us show that (2) $\iff$ (3).
Suppose (2) holds, ($aha^{-1} \in H$ for all $a \in G, h \in H$).
If $x \in aH$, say $x = ah$ with $h \in H$. Then $x = ah = aha^{-1}a \in Ha$, since $aha^{-1} \in H$.
If $y \in Ha$, say $y = ha$ with $h \in H$, then $y = ha = aa^{-1}ha \in aH$, since $a^{-1}ha \in H$.
This proves that (2) $\Rightarrow$ (3).

16 October 21st

Normal Subgroups
For $H \leq G$, $a \in G$, $aH = \{ah | h \in H\}$.

$$\begin{aligned} a \sim b \iff & b \in aH \iff a^{-1}b \in H \\ \iff & a \in bH \\ \iff & aH = bH \end{aligned}$$

Side Notes:
$|aH| = |H|$.
For $H \leq G, a \in G$, $|H| \Big| |G|, |a| \Big| |G|$.

Theorem:
Let $H \leq G$. The following are equivalent.

1. We can define a well-defined binary operation on G/H by $(aH)(bH) = (ab)H$ for all $a, b \in G$.
2. For all $a \in G, h \in H : aha^{-1} \in H$.

3. For all $a \in G$, $aH = Ha$.

4. For all $a \in G, C_a(H) = aHa^{-1} = H$.

Proof:
Proof 1 $\iff$ 2; Done.
Proof 2 $\iff$ 3; Done.
Proof 3 $\iff$ 2;
Suppose that 3 holds. Let $a \in G$ and $h \in H$, by (3), we have $aH = Ha$.
So in particular, $ah \in Ha$, say $ah = ka$ where $k \in H$.
Then $aha^{-1} = k \in H$.
The equivalence of part 4 is left as an exercise.
Remark:
For $a \in G$, the map $C_a : G \to G$ given by $C_a(x) = axa^{-1}$ is an automorphism of G.
So $C_a : H \to C_a(H) = aHa^{-1}$.
Hence, $aHa^{-1} \leq G$ with $aHa^{-1} \cong H$.
The groups H and aHa^{-1} are called conjugate subgroups of G.
Definition:
When a subgroup $H \leq G$ satisfies the equivalent conditions of the above theorem, we say that H is a normal subgroup of G, and we write $H \trianglelefteq G$.
In this case, the (well-defined) operation on G/H given by $(aH)(bH) = (ab)H$ makes G/H into a group, which we call the quotient group of G by H.
The identity element in G/H is $eH = H$.
The inverse of aH is $a^{-1}H$.
Remark:
When G is an abelian group, every subgroup $H \leq G$ is a normal subgroup.
Exmaples:
In $\mathbb{Z}$, for $n \in \mathbb{Z}^+$,

$$\langle n \rangle = n\mathbb{Z} = \{\dots, -n, 0, n, 2n. \dots\}$$

and $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
Theorem (The First Isomorphism Theorem)

1. Let $\phi : G \to H$ be a group homomorphism and let $K = \text{Ker } \phi \leq G$. Then $K \trianglelefteq G$ and $G/K \cong \phi(G)$.

   Indeed, the map $\Phi : G/K \to \phi(G)$ given by $\Phi(aK) = \phi(a)$ is a well-defined group homomorphism.

2. Let $K \trianglelefteq G$. Then the map $\phi : G \to G/K$ given by $\phi(a) = aK$ is a group homomrophism with $\text{Ker } \phi = K$.

Proof:

1. Note that $K \trianglelefteq G$ where $K = \text{Ker } \phi$ because if $a \in G$ and $k \in K$, so $\phi(k) = e$, then $aka^{-1} \in K$ since

$$
\begin{aligned}
\phi(aka^{-1}) &= \phi(a)\phi(k)\phi(a)^{-1} \\
&= \phi(a) \cdot e \cdot \phi(a)^{-1} \\
&= \phi(a)\phi(a)^{-1} = e
\end{aligned}
$$

(We used part (2) of the definition of normal.)

Note that $\Phi : G/K \to \phi(G)$ given by $\Phi(aK) = \phi(a)$ for $a \in G$ is well-defined because for $a, b \in G$ with $aK = bK$, we have $a^{-1}b \in K$, say $a^{-1}b = k \in K = \text{Ker } \phi$.

So $\phi(a^{-1}b) = e$, hence $\phi(a)^{-1}\phi(b) = e$.

Hence $\phi(b) = \phi(a)$.

Note that Φ is a group homomorphism because, for $a, b \in G$

$$
\begin{aligned}
\Phi((aK)(bK)) &= \Phi((ab)K) \\
&= \phi(ab) = \phi(a)\phi(b) \\
&= \Phi(aK)\Phi(bK)
\end{aligned}
$$

Side note: $\phi : G \to H, K = \text{Ker } \phi, \Phi(aK) = \phi(a), \Phi : G/K \to \phi(G)$.

Note that Φ is surjective because given $b \in \phi(G)$, say $b = \phi(a)$ with $a \in G$, then $\Phi(aH) = \phi(a) = b$.

Note that Φ is injective because for $a \in G$,

$$
\Phi(aK) = e \implies \phi(a) = e \implies a \in K \implies aK = eK = K
$$

(So that aK is the identity element in G/K).

17 October 23rd

$H \trianglelefteq G$ when $aha^{-1} \in H$ for all $a \in G, h \in H$ or when $aH = Ha$ for all $a \in G$. Then G/H is a group under $(aH)(bH) = (ab)H$ for $a, b \in G$.
Theorem: (The First Isomorphism Theorem)

1. If $\phi : G \to H$ is a group homomorphism, and $K = \text{Ker } \phi$, then $K \trianglelefteq G$ and $G/K \cong \text{Image}(\phi) = \phi(G)$.

   Indeed, the map $\Phi : G/K \to \phi(G)$ given by $\Phi(aK) = \phi(a)$ is an isomorphism.

Examples:

The map $\phi : G \to H$ given by $\phi(a) = e$ is a homomorphism. We have Ker $\phi = G$ and Im $\phi = \{e\}$ and $G/G \cong \{e\}$.

The map $\phi : G \to G$ given by $\phi(a) = a$ for all $a \in G$, is a homomorphism.

We have Ker $\phi = \{e\}$ and Im $\phi = G$ and $G/\{e\} \cong G$.

For $n \in \mathbb{Z}^+$, the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(k) = k$ is a homomorphism, Ker $\phi = n\mathbb{Z} = \langle n \rangle = \{\dots, -n, 0, n, 2n, \dots\}$

Im $\phi = \mathbb{Z}_n$

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

(Indeed, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$).

The map $\phi : \mathbb{R} \to \mathbb{S}^1$ given by $\phi(t) = e^{i2\pi t}$ is a homomrophism with Ker $\phi = \mathbb{Z}$ and Im $\phi = \mathbb{S}^1$. So $\mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.

The map $\phi : \mathbb{C}^* \to \mathbb{R}$ given by $\phi(z) = |z|$ is a homomorphism (since $|zw| = |z||w|$) with Ker $\phi = \mathbb{S}^1$ and Im $\phi = \mathbb{R}^+$.

So $\mathbb{C}^*/\mathbb{S}^1 \cong \mathbb{R}^+$

The map $\phi : \mathbb{C}^* \to \mathbb{C}^*$ given by $\phi(z) = \frac{z}{|z|}$ is a homomorphism, (since $\frac{zw}{|zw|} = \frac{z}{|z|} \cdot \frac{w}{|w|}$) with Ker $\phi = \mathbb{R}^+$ and Im $\phi = \mathbb{S}^1$.

So $\mathbb{C}^*/\mathbb{R}^+ = \mathbb{S}^1$.

Note also that

$$\mathbb{C}^* \cong \mathbb{R}^+ \times \mathbb{S}^1$$

with an isomorphism

$$\phi : \mathbb{R}^+ \times \mathbb{S}^1 \to \mathbb{C}^*$$

given by $\phi(r, e^{i\theta}) = re^{i\theta}$

When R is a commutative ring with 1, the map

$$\phi : GL_n(R) \to R^*$$

given by $\phi(A) = \det(A)$ is a group homomorphism with Ker $\phi = SL_n(R)$ and Im $\phi = \mathbb{R}^*$. (Since $a \in \mathbb{R}^*, \det \begin{pmatrix} a & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = a$)

So $SL_n(R) \trianglelefteq GL_n(R)$ and $GL_n(R)/SL_n(R) \cong \mathbb{R}^*$.

Let G be any group. Then the map $\phi : G \to \mathrm{Aut(G)}$ given by $\phi(a) = C_a$ where $C_a : G \to G$ is given by $C_a(x) = axa^{-1}$ for $x \in G$, is a group homomorphism with

$$
\begin{aligned}
\text{Ker } \phi &= \{a \in G | C_a = I\} \\
&= \{a \in G | C_a(x) = x \text{ for all } x \in G\} \\
&= \{a \in G | axa^{-1} = x \text{ for all } x \in G\} \\
&= \{a \in G | ax = xa \text{ for all } x \in G\} \\
&= Z(G) \quad \text{(The centre of } G)
\end{aligned}
$$

and Im $\phi = \{C_a | a \in G\} = \text{Inn}(G)$
So $Z(G) \trianglelefteq G$ and $G/Z(G) \cong \text{Inn}(G)$.
Example:
Let $H = \text{Span}_{\mathbb{Z}}\{(2,6),(6,3)\} \leq \mathbb{Z}^2$.
Show that $\mathbb{Z}^2/H \cong \mathbb{Z}_{30}$ and find a homomorphism $\phi : \mathbb{Z}^2 \to \mathbb{Z}_{30}$ with Ker $\phi = H$.
Sketch Solution:
A graph here, see pictures.
$(0,0) + H = H$
$(1,0) + H$
$(10,0) + H = H$ since $(10,0) \in H$.
In G/H, the order of $(1,0) + H = 10$.
Verify that G/H is generated by $(1,1) + H$.

$$
\det \begin{pmatrix} 2 & 6 \\ 6 & 3 \end{pmatrix} = |-30| = 30
$$

So G/H is cyclic of order 30.
$\therefore G/H \cong \mathbb{Z}_{30}$.
Define $\phi : \mathbb{Z}^2 \to \mathbb{Z}_{30}$ by $\phi(k(1,1) + H) = k$, or equivalently by $\phi((k,l) + H) = 9k - 8l$.
Verify that for ϕ as above, we do have Ker $\phi = H$
Side Note:
To get $\phi(k(1,1)+H) = k$, we need $\phi((1,0)+H) = 9$ and $\phi((0,1)+H) = 22 = -8$.
If $(k,l) \in H$, say

$$
\begin{aligned}
(k,l) &= s(2,6) + t(6,3) \\
&= (2s + 6t, 6s + 3t)
\end{aligned}
$$

for some $s,t \in \mathbb{Z}$
and then

$$
\begin{aligned}
9k - 8l &= 9(2s + 6t) - 8(6s + 3t) \\
&= -30s + 30t \\
&= 30(t - 3)
\end{aligned}
$$

So $9k - 8l = 0 \mod 30$

Hence, $\phi((k,l)+H) = 0 \in \mathbb{Z}_{30}$
Verify that if $9k - 8l = 0 \mod 30$, then

$$(k,l) = s(2,6) + t(6,3)$$

for some $s, t \in \mathbb{Z}$.
We have

$$\begin{aligned}
&\begin{pmatrix} k \\ l \end{pmatrix} = s\begin{pmatrix} 2 \\ 6 \end{pmatrix} + t\begin{pmatrix} 6 \\ 3 \end{pmatrix} \\
\iff &\begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 6 & 3 \end{pmatrix}\begin{pmatrix} s \\ t \end{pmatrix} \\
\iff &\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 6 & 3 \end{pmatrix}^{-1}\begin{pmatrix} k \\ l \end{pmatrix} = \frac{1}{30}\begin{pmatrix} -3 & 6 \\ 6 & -2 \end{pmatrix}\begin{pmatrix} k \\ l \end{pmatrix}
\end{aligned}$$

Definition:
A group G is called simple when G has no non-trivial proper normal subgroups.
Exercise: (Fairly hard)
Show that for $n \geq 3$, A_n is simple.

18 October 25th

Theorem: (Characterization of Internal Direct Products)
Let G be a group and let $H, K \subseteq G$. Suppose $H \trianglelefteq G, K \trianglelefteq G$, $H \cap K = \{e\}$ and $HK = G$ (where $HK = \{ab | a \in H, b \in K\}$). Then $G \cong H \times K$. Indeed, the map $\phi : H \times K \to G$ given by $\phi(a,b) = ab$ is an isomorphism.
Proof:
We claim that ϕ is a homomorphism.
For $a, c \in H$ and $b, d \in K$. We have

$$\begin{aligned}
\phi((a,b)\cdot(c,d)) &= \phi(ac, bd) \\
&= acbd
\end{aligned}$$

and

$$\begin{aligned}
\phi(a,b)\cdot\phi(c,d) &= abcd \\
&= acc^{-1}bcb^{-1}bd \\
&= acebd \\
&= acbd
\end{aligned}$$

because

$$c^{-1}bcb^{-1} = c^{-1}(bcb^{-1}) \in H$$

Since $c^{-1} \in H, bcb^{-1} \in H$. Since $H \trianglelefteq G$.
and

$$c^{-1}bcb^{-1} = (c^{-1}bc)b^{-1} \in K$$

Since $b^{-1} \in K$ and $c^{-1}bc \in K$.
So we have

$$c^{-1}bcb^{-1} \in H \cap K = \{e\}$$

Note that ϕ is surjective since $HK = G$. (So every element in G is of the form ab for some $a \in H, b \in K$)
Also, ϕ is injective because for $a \in H, b \in K$, we have

$$\begin{aligned}\phi(a,b) = e &\Rightarrow ab = e\\ &\Rightarrow a = b^{-1}\\ &\Rightarrow a \text{ and } b^{-1} \text{ are both in } H \cap K = \{e\}\\ &\Rightarrow a = b^{-1} = e\\ &\Rightarrow (a,b) = (e,e)\end{aligned}$$

Theorem (Classification of Groups of Order $2p$)
Let p be a prime number and let G be a group with $|G| = 2p$. Then, either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.
Proof: Exercise.
Theorem (Classification of Groups of Order p^2)
Let p be a prime number and let G be a group with $|G| = p^2$. Then, either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
Proof:
For $a \in G$. Since $|a| \Big| |G|$, we have $|a| = 1, p,$ or p^2.
Suppose $G \ncong \mathbb{Z}_{p^2}$. So G is not cyclic. Then G has no elements $a \in G$ with $|a| = p^2$.
So every $e \neq a \in G$ has order p.
Let $e \neq a \in G$. We claim that $\langle a \rangle \trianglelefteq G$.
Suppose, for a contradiction, that $\langle a \rangle \ntrianglelefteq G$.
Side Note:
$H \trianglelefteq G$ when $xhx^{-1} \in H$ for all $x \in G$, $h \in H$.
Choose $x \in G$ and $a^k \in \langle a \rangle$. So that $xa^kx^{-1} \notin \langle a \rangle$.
It follows that $xax^{-1} \notin \langle a \rangle$, since if we had $xax^{-1} \in \langle a \rangle$, then we would have $\left(xax^{-1}\right)^k \in \langle a \rangle$, but $\left(xax^{-1}\right)^k = xax^{-1}xax^{-1} \ldots xax^{-1} = xa^kx^{-1}$.
Since $xax^{-1} \neq e$, $\therefore |xax^{-1}| = p$.
Since $\langle a \rangle$ and $\langle xax^{-1} \rangle$ are distinct p-element subgroups of G, $\langle a \rangle \cap \langle xax^{-1} \rangle$ is a proper subgroup of $\langle a \rangle$ whose only subgroups are $\{e\}$ and $\langle a \rangle$ (because $\langle a \rangle \cong \mathbb{Z}_p$)

Thus, $\langle a\rangle \cap \langle xax^{-1}\rangle = \{e\}$
Since $\langle a\rangle \cap \langle xax^{-1}\rangle = \{e\}$, it follows that the cosets,
$e\langle xax^{-1}\rangle, a\langle xax^{-1}\rangle, a^2\langle xax^{-1}\rangle, \ldots, a^{p-1}\langle xax^{-1}\rangle$ are all distinct. Indeed

$$\begin{aligned}
a^k\langle xax^{-1}\rangle = a^l\langle xax^{-1}\rangle &\Rightarrow a^{l-k} \in \langle xax^{-1}\rangle \\
&\Rightarrow a^{l-k} \in \langle a\rangle \cap \langle xax^{-1}\rangle = \{e\} \\
&\Rightarrow a^{l-k} = e \\
&\Rightarrow a^l = a^k
\end{aligned}$$

Since $|G| = p^2$ and these p-element cosets are distinct, G is the union of these cosets.
In particular, x^{-1} lies in one of the cosets, say $x^{-1} \in a^k\langle xax^{-1}\rangle$, say $x^{-1} \in a^k\left(xax^{-1}\right)^l = a^kxa^lx^{-1}$.
Then, $e = a^kxa^l$.
So $x = a^{-k-l} \in \langle a\rangle$.
Hence, $xax^{-1} \in \langle a\rangle$, which contradicts our choice of x.
This proves that $\langle a\rangle \trianglelefteq G$. Since $e \neq a \in G$ was arbitrary, $\langle a\rangle \trianglelefteq G$ for all $a \in G$.
Let $e \neq a \in G$. Choose $b \in G$ with $b \notin \langle a\rangle$. Then $\langle a\rangle$ and $\langle b\rangle$ are distinct, p-element cyclic subgroups of G.
So $\langle a\rangle \cap \langle b\rangle = \{e\}$
(Since it is a proper subgroup of $\langle a\rangle \cong \mathbb{Z}_p$).
As above, it follows that the cosets $e\langle b\rangle, a\langle b\rangle, a^2\langle b\rangle, \ldots, a^{p-1}\langle b\rangle$ are all distinct.
(if $a^k\langle b\rangle = a^l\langle b\rangle$, then $a^{l-k} \in \langle b\rangle$. So that $\langle a\rangle \leq \langle b\rangle$).
As above, G is the union of these distinct cosets.
Thus, every element in G is of the form a^kb^l for some $k, l \in \mathbb{Z}$.
So we have

$$G = \langle a\rangle\langle b\rangle$$

Since $\langle a\rangle \trianglelefteq G, \langle b\rangle \trianglelefteq G, \langle a\rangle \cap \langle b\rangle = \{e\}$, and $G = \langle a\rangle\langle b\rangle$.
and so we have

$$G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

by the Characterization of Direct Products.

19 October 28th

Group Actions and Representations
Definition:
A **representation** of a group G is a group homomorphism, $\rho : G \to \mathrm{Perm}(S)$ for some set S.
An injective representation is called **faithful**.

When $\rho : G \to \mathrm{Perm}(S)$ is faithful, we sometimes identity G with the isomorphic group $\rho(G) \leq \mathrm{Perm}(G)$.
An **action** of a group G on a set S is a function $* : G \times S \to S$, where for $a \in G$ and $x \in S$, we write $*(a, x)$ as $a * x$ or sometimes just as ax, such that

1. $ex = x$ for all $x \in S$ and
2. $a(bx) = (ab)x$ for all $a, b \in G$ and $x \in S$.

Note that there is a natural bijective correspondence between the set of all group actions of G on S and the set of all representations $\rho : G \to \mathrm{Perm}(S)$.
The action and its corresponding representation are related by

$$a + x = \rho(a)(x)$$

for $a \in G$ and $x \in S$.
Example:
When G acts on itself by left multiplication. (So $a * x = ax$ for all $a, x \in G$), the corresponding representation $\rho : G \to \mathrm{Perm}(G)$ is given by $\rho(a)(x) = ax$, that is $\rho(a) = l_a$, where $l_a : G \to G$ is given by $l_a(x) = ax$.
This representation is faithful (since for $a, b \in G$, if $l_a = l_b$, then $l_a(x) = l_b(x)$ for all $x \in G$. So $a = a \cdot e = l_a(e) = l_b(e) = be = b$)
This was used in the proof of Cayley's Theorem.
Example:
When G acts on itself by conjugation, that is when

$$a * x = axa^{-1}$$

The corresponding representation $\rho : G \to \mathrm{Perm}(G)$ is given by $\rho(a)(x) = axa^{-1} = C_a(x)$, that is $\rho(a) = C_a$, where $C_a : G \to G$ is given by $C_a(x) = axa^{-1}$
We have

$$\mathrm{Im}(\rho) = \rho(G) = \mathrm{Inn}(G)$$

and $\mathrm{Ker}(\rho) = Z(G)$
So we have $Z(G) \trianglelefteq G$ and $G/Z(G) \cong \mathrm{Inn}(G)$
Example:
Let R be a commutative ring with 1.
When $GL_n(R)$ acts on R^n by matrix multiplication. The corresponding representation $\rho : GL_n(R) \to \mathrm{Perm}(R^n)$ is given by $\rho(A)(x) = Ax = L_A(x)$ where $L_A : R^n \to R^n$ is given by $L_A(x) = Ax$, so we have $\rho(A) = L_A$. This representation is faithful (and we often identify a matrix A with its associated linear map $\rho(A) = L_A$)
Definition:
Let G be a group which acts on a set S.
When $a \in G$, the fixed set of a is the set

$$\mathrm{Fix}(a) = \mathrm{Fix}_G(a) = \{x \in S | ax = x\} \subseteq S$$

For $x \in S$, the orbit of x is the set

$$\mathrm{Orb}(x) = \mathrm{Orb}_G(x) = \{ax | a \in G\} \subseteq S$$

For $x \in S$, the stabilizer of x is the subgroup

$$\mathrm{Stab}(x) = \mathrm{Stab}_G(x) = \{a \in G | ax = x\} \leq G$$

Note that $\mathrm{Stab}(x) \leq G$ because $e \in \mathrm{Stab}(x)$ since $e \cdot x = x$.
If $a, b \in \mathrm{Stab}(x)$, so $ax = x$ and $bx = x$.
Then $(ab)(x) = a(bx) = ax = x$.
So that $a, b \in \mathrm{Stab}(x)$, and if $a \in \mathrm{Stab}(x)$, so $ax = x$.
Then $a^{-1}x = a^{-1}(ax) = (a^{-1}a)x = ex = x$
So that $a^{-1} \in \mathrm{Stab}(x)$
Example:
When $SO_2(\mathbb{R}) = \{R_\theta | \theta \in \mathbb{R}\}$ acts on $\mathbb{R}^2$, for $u \in \mathbb{R}^2$

$$\begin{aligned} \mathrm{Orb}(u) &= \{Au | A \in SO_2(\mathbb{R})\} \\ &= \{x \in \mathbb{R}^2 | |x| = |u|\} \end{aligned}$$

When $SO_{n+1}(\mathbb{R})$ acts on $\mathbb{R}^{n+1}$, and $e_{n+1} = (0, \ldots, 0, 1)^T$

$$\begin{aligned} \mathrm{Orb}(e_{n+1}) &= \{Ae_{n+1} | A \in SO_{n+1}(\mathbb{R})\} \\ &= \mathbb{S}^n = \{u \in \mathbb{R}^{n+1} | |u| = 1\} \end{aligned}$$

(Since Ae_{n+1} is the last column of A, which can be any unit vector and

$$\begin{aligned} &\mathrm{Stab}(e_{n+1}) \\ =&\{A \in SO_{n+1}(\mathbb{R}) | Ae_{n+1} = e_{n+1}\} \\ =&\left\{ \left[\begin{array}{c|c} B & 0 \\ \hline 0 & 1 \end{array} \right] | B \in SO_n(\mathbb{R}) \right\} \end{aligned}$$

)
Example:
When G is a group and $H \leq G$ and H acts on G by right-multiplication, that is $h * x = xh$ for $h \in H$ and $x \in G$, the orbit of an element $a \in G$ is

$$\begin{aligned} \mathrm{Orb}(a) &= \{ah | h \in H\} \\ &= aH \end{aligned}$$

20 October 30th

A **representation** of G is a group homomorphism $\rho : G \to \mathrm{Perm}(S)$ for some set S.
An action of G on S is a map $* : G \times S \to S$, where we write $*(a, x)$ as $a * x$ and sometimes as ax such that

$$ex = x \text{ for all } x \in S$$

$a(bx) = (ab)x$ for all $a, b \in G, x \in S$.
These are the same thing:

$$\rho(a)(x) = a * x$$

$$\mathrm{Fix}(a) = \{x \in S | ax = x\}, \mathrm{Orb}(x) = \{ax | a \in G\}, \mathrm{Stab}(x) = \{a \in G | ax = x\}$$

When a group G acts on a set S, we can define an equivalence relation $\sim$ on S by

$$\begin{aligned} x \sim y &\iff y = a \cdot x \text{ for some } a \in G \\ &\iff y \in \mathrm{Orb}(x) \end{aligned}$$

This is an equivalence relation because

$$x \sim x$$

Since $x = ex \in \mathrm{Orb}(x)$
If $x \sim y$, say $y = ax$, then

$$\begin{aligned} a^{-1}y = a^{-1}(ax) &= \left(a^{-1}a\right)x \\ = ex &= x \end{aligned}$$

So $y \sim x$.
And if $x \sim y$ and $y \sim z$
Say $y = a \cdot x$ and $z = b \cdot y$, then $z = by = b(ax) = (ba)x$
So $x \sim z$.
Note that, using this equivalence relation,

$$\begin{aligned} [x] &= \{y \in S | x \sim y\} \\ &= \{y \in S | y = a \cdot x \text{ for some } a \in G\} \\ &= \{ax | a \in G\} \\ &= \mathrm{Orb}(x) \end{aligned}$$

We write $S/\sim$ as S/G.
So

$$\begin{aligned} S/G &= \{[x] | x \in S\} \\ &= \{\text{Orb}(x) | x \in S\} \end{aligned}$$

and S is the disjoint union of the disjoint orbits.
Examples:
When $H \leq G$ and H acts on G by right multiplication, so $h * a = ah$ for $a \in G, h \in H$
We have $\text{Orb}(a) = \{ah | h \in H\} = aH$
In this case, our new notation G/H agrees with our previous notation

$$G/H = \{aH | a \in G\}$$

(When H acts on G by left multiplication, so $h * a = ha$ for $h \in H, a \in G$, our new and old notations do not agree)
Theorem (The Orbit / Stabilizer Theorem)
Let G be a fintie group which acts on a set S. For each $x \in S$,

$$|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |G|$$

Proof:
Let $x \in S$, let $H = \text{Stab}(x) \leq G$.
We know (from Lagrange's Theorem)

$$|G| = |G/H| \cdot |H|$$

We need to show that

$$|\text{Orb}(x)| = |G/H| = |G/\text{Stab}(x)|$$

Define $F : G/H \to \text{Orb}(x)$ by $F(aH) = ax$ for $a \in G$.
Note that F is well-defined, because, for $a, b \in G$, if $aH = bH$, then $b^{-1}a \in H = \text{Stab}(x)$.
So $(b^{-1}a)(x) = x$
Hence, $ax = bx$.
F is clearly surjective. Note that F is injective because for $a, b \in G$. If $F(aH) = F(bH)$, then $ax = bx$.
So $b^{-1}ax = x$.
Hence, $b^{-1}a \in \text{Stab}(x) = H$.
Hence, $aH = bH$.
Theorem (Burnside's Counting Lemma or
The Cauchy-Frobenius Counting Lemma)
Let G be a finite group which acts on a finite set S.
Then

$$|S/G| = \frac{1}{|G|} \sum_{a \in G} |\text{Fix}(a)|$$

Proof:
Let $T = \{(a,x)|a \in G, x \in S, ax = x\}$
Then $|T| = \sum_{a\in G} |\{x \in S|ax = x\}| = \sum_{a \in G} |\text{Fix}(a)|$ and

$$\begin{aligned}|T| &= \sum_{x\in S} |\{a \in G|ax = x\}| \\ &= \sum_{x\in S} |\text{Stab(x)}| \\ &= \sum_{x \in S} \frac{|G|}{|\text{Orb}(x)|} \\ &= \sum_{A\in S/G} \sum_{x\in S} \frac{|G|}{|A|} \\ &= \sum_{A \in S/G} |G| \\ &= |G||S/G|\end{aligned}$$

Thus, $|G||S/G| = \sum_{a\in G} |\text{Fix}(a)|$
Example:
Find the number of ways to colour the 6 vertices of a regular hexagon using 3 colours, up to equivalence under symmetry under the natural action of D_6.
Example:
Find the number of ways to colour the 8 vertices of a cube, up to symmetry under the group of rotations in $SO_3(\mathbb{R})$ of the cube, using 2 colours.
Solution:
Let G be the group of rotations of the cube and let S be the set of all possible 2^8 colourings of the vertices (ignoring symmetry).
G acts on S and we need to find $|S/G|$.
A picture here, refer to the photos.
If we fix a vertex x, then under the action of G, on the 8 vertices of the cube

$$|G| = |\text{Stab}(x)| \cdot |\text{Orb}(x)|$$

We have $|\text{Orb}(x)| = 8$ and $|\text{Stab}(x)| = 3$. Hence, $|G| = 24$.
Pictures here. Refer to the photos.

21 November 1st

The table below comes with accompanying pictures. Refer to photos.

Type of A	# of such A	$\lvert\text{Fix}(A)\rvert$
I	1	2^8
$R_{V,\pm\frac{2\pi}{3}}$	8	2^4
$R_{E,\pi}$	6	2^4
$R_{F,\pm\frac{\pi}{2}}$	6	2^2
$R_{F,\pi}$	3	2^4

Thus, we have

$$\begin{aligned}
|S/G| &= \frac{1}{|G|}\sum_{A\in G}|\mathrm{Fix}(A)| \\
&= \frac{1}{24}\left(1\cdot 2^8 + 8\cdot 2^4 + 6\cdot 2^4 + 6\cdot 2^2 + 3\cdot 2^4\right) \\
&= \frac{1}{3}\left(32+16+12+3+6\right) \\
&= 23
\end{aligned}$$

If we use n colours, we get

$$\begin{aligned}
|S/G| &= \frac{1}{24}\left(1\cdot n^8 + 8\cdot n^4 + 6n^4 + 6n^2 + 3n^4\right) \\
&= \frac{1}{24}\left(n^8 + 17n^4 + 6n^2\right)
\end{aligned}$$

In particular, $n^8 + 17n^4 + 6n^2 = 0 \mod 24$ for all $n \in \mathbb{Z}^+$.
Theorem (The Class Equation)
Let G be a finite group. Let m be the number of conjugacy classes in G.
(The conjugacy class of $x \in G$ is $Cl(x) = \{axa^{-1}|a \in G\}$)
Choose elements $x_1, \cdot, x_m$ with one from each conjugacy class.
Then

$$|G| = \sum_{k=1}^{m}|G/C(x_k)|$$

where $C(x_k) = \{a \in G|ax_k = x_k a\}$, which is the centralizer of x_k in G.
Proof:
When G acts on itself by conjugation, (so $a * x = axa^{-1}$) for $x \in G$,

$$\mathrm{Orb}(x) = \{axa^{-1}|a \in G\} = Cl(x)$$

and

$$\mathrm{Stab}(x) = \{a \in G|axa^{-1} = x\} = C(x) \leq G$$

By the Orbit / Stabilizer Theorem, $|G/\mathrm{Stab}(x)| = |\mathrm{Orb}(x)|$
Since G is the disjoint union of the orbits, (and we selected one element x_k from each orbit)

$$\begin{aligned}
|G| &= \sum_{k=1}^{m}|\mathrm{Orb}(x_k)| = \sum_{k=1}^{m}|G/\mathrm{Stab}(x_k)| \\
&= \sum_{k=1}^{m}|G/C(x_k)|
\end{aligned}$$

Theorem (Cauchy's Theorem)
Let G be a finite group with $|G| = n$.
Let p be a prime factor of n. Then G has an element of order p.
In fact, we shall prove that

$$|\{a \in G | |a| = p\}| = p - 1 \mod p(p-1)$$

Proof:
Let $m = |\{a \in G||a| = p\}|$
Note that $m = l - 1$ where

$$l = |\{a \in G | a^p = e\}|$$

Recall that m is a multiple of $\phi(p) = p - 1$.
So $m = 0 \mod p - 1$
So $m = p - 1 \mod p - 1$
It remains to show that $m = p - 1 \mod p$.
Let $S = \{(x_1, x_2, \ldots, x_p) \mid \text{each } x_k \in G \text{ and } \prod x_k = e\}$ and $\mathbb{Z}_p$ act on S by cyclic permutation, so

$$k * (x_1, x_2, \ldots, x_p) = (x_{k+1}, x_{k+2}, \ldots, x_p, x_1, x_k)$$

Then for $x = (x_1, \ldots, x_p) \in S$

$$|\text{Orb}(x)| = \begin{cases} 1 & \text{if } x = (a, a, \ldots, a) \text{ where } a \in G \text{ with } a^p = e \\ p & \text{otherwise} \end{cases}$$

Since S is the disjoint union of the orbits

$$|S| = 1 \cdot l + p \cdot t$$

So that $l = |s| \mod p$, but also we have

$$|S| = n^{p-1} = n = 0 \mod p$$

(Since we can choose $x_1, \ldots, x_{p-1} \in G$ arbitrarily and then $x_p = (x_1, x_2, \ldots, x_{p-1})^{-1}$ to get $\prod x_k = e$)
Hence,

$$l = 0 \mod p$$

So $m = l - 1 = -1 = p - 1 \mod p$ as required.

22 November 4th

Theorem (The Classification of Finite Abelian Groups)

1. Every finite abelian group is isomorphic to a unique group of the form $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_l}$ for some $l \geq 0$ ($l = 0$ gives the trivial group) and some $n_i \in \mathbb{Z}^+$ with $n_1|n_2, n_2|n_3, \ldots, n_{l-1}|n_l$.

2. Every finite abelian group is isomorphic to a unique group of the form $\mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \ldots \mathbb{Z}_{{p_m}^{k_m}}$ for some $m \geq 0$, and some primes $p_1, \ldots, p_m$ with $p_1 \leq p_2 \leq \cdots \leq p_m$ and some $k_i \in \mathbb{Z}^+$ with $k_i \geq k_{i+1}$ when $p_i = p_{i+1}$

   Recall that for $k, l \in \mathbb{Z}^+$, $\mathbb{Z}_k \times \mathbb{Z}_l \cong \mathbb{Z}_{kl} \iff \gcd(k, l) = 1$.

Preliminary Definitions
Definition:
A free abelian group of rank n is a group which is isomorphic to $\mathbb{Z}^n$.
Remark: In this chapter, we use additive notation for abelian groups.
Note that the rank of the abelian group is unique: $G \cong \mathbb{Z}^n$ and $G \cong \mathbb{Z}^m$ with $n, m \in \mathbb{Z}^+$, then we must have $n = m$.
Sketch Proof:
If $G \cong \mathbb{Z}^n$ and $G \cong \mathbb{Z}^m$, then we have $\mathbb{Z}^n \cong \mathbb{Z}^m$.
Let $\phi : \mathbb{Z}^n \to \mathbb{Z}^m$ be an isomorphism.
Note that ϕ restricts to an isomorphism, $\phi : 2\mathbb{Z}^n \to 2\mathbb{Z}^m$.
Verify that ϕ determines an isomorphism

$$\Phi : \mathbb{Z}^n/2\mathbb{Z}^n \to \mathbb{Z}^m/2\mathbb{Z}^m$$

Also, verify that $\mathbb{Z}^n/2\mathbb{Z}^n \cong (\mathbb{Z}_2)^n$.
It follows that

$$(\mathbb{Z}_2)^n \cong \mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}^m/2\mathbb{Z}^m \cong (\mathbb{Z}_2)^m$$

So

$$|\mathbb{Z}_2^n| = |\mathbb{Z}_2^m|$$

That is $2^n = 2^m$. Hence $n = m$.
Familiar Terminology:
Let G be an abelian group, and let $S \subseteq G$. A linear combination (over $\mathbb{Z}$) of elements in S is an element in G of the form

$$\sum_{i=1}^{l} t_i u_i$$

with $l \geq 0$, each $t_i \in \mathbb{Z}$, and each $u_i \in S$.
(If we want, we can require that the u_i are distinct.)
The span of S (over $\mathbb{Z}$) is the set of linear combination:

$$\langle S \rangle = \mathrm{Span}_{\mathbb{Z}}(S) = \{\sum_{i=1}^{l} t_i u_i | l \geq 0,\ \text{each } t_i \in \mathbb{Z},\ \text{each } u_i \in S\}$$

We say that S spans G (over $\mathbb{Z}$) with $G = \mathrm{Span}_{\mathbb{Z}}(S)$.

We say that S is linearly independent (over $\mathbb{Z}$), when for all $t_i \in \mathbb{Z}$ and $u_i \in S$ distinct, if $\sum_{i=1}^{l} t_i u_i$, then each $t_i = 0$.
We say that S is a basis for G (over $\mathbb{Z}$), when S is linearly independent and spans G.
An n-element ordered basis for G is an n-tuple, $(u_1, u_2, \ldots, u_n)$ of distinct elements in G such that $\{u_1, u_2, \ldots, u_n\}$ is a basis for G.
Side Note: Drop the repetition?
Note:
A group G is a free abelian group of rank n if and only if G has a basis with n (distinct) elements.
Sketch Proof:
If G is abelian, $G \cong \mathbb{Z}^n$ and $\phi : \mathbb{Z}^n \to G$ is an isomorphism, then for $u_k = \phi(e_k) = \phi(0, 0, 0, \ldots, 1, 0, \ldots, 0)$ (1 at k^{th} position.)
The set $\{u_1, \ldots, u_n\}$ is a basis with n distinct elements.
Conversely, if $\{u_1, \ldots, u_n\}$ is a basis for G with distinct elements, then the map $\phi : \mathbb{Z}^n \to G$ given by $\phi(t_1, \ldots, t_n) = \sum_{i=1}^{n} t_i u_i$ is an isomorphism.
Note:
When $(u_1, \ldots, u_n)$ is an ordered basis for the free abelian group G, we can obtain new basis by performing any of the following 3 operations

1. $u \mapsto \pm u_k$ (replace u_k by $\pm u_k$)
2. $u_k \leftrightarrow u_l$ (interchanging u_k with u_l)
3. $u \mapsto u_k + t u_l$ with $t \in \mathbb{Z}$ (replace u_k by u_k plus an integer multiple of u_l when $l \neq k$)

Side Note: Analogy to $k\vec{v}, k \in \mathbb{Z}$
Examples:

$$\left\{ \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 6 \\ 2 \end{pmatrix} \right\} \subseteq \mathbb{Z}^2$$

is linearly independent (over $\mathbb{Z}$).

$$H = \mathrm{Span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 3 \\ 6 \end{pmatrix}, \begin{pmatrix} 6 \\ 2 \end{pmatrix} \right\}$$

is a free abelian group of rank 2.
Proof Later?
Also, check picture.
Theorem (Classification of Subgroups and Quotient Groups of Finite Rank Abelian Group)
Let G be a free abelian group of rank n, let $H \leq G$. Then H is a free abelian group of rank at most n. In other words, $0 \leq r \leq n$. (with $r = 0$ giving the trivial group $H = \{0\}$ which consider to be a free group with empty basis), and there exists integers, $d_i, d_2, \ldots, d_r \in \mathbb{Z}^+$ with $d_1 | d_2, d_2 | d_3, \ldots, d_{r-1} | d_r$ such that

$$G/H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

23 November 6th

Sketch Proof:
To prove this, we shall show that there exists $\{u_1, u_2, \dots, u_n\}$ for G and there exist $d_1, d_2, \dots, d_r$ as above such that $\{d_1u_1, d_2u_2, \dots, d_ru_r\}$ is a basis for H with each $d_i \in \mathbb{Z}^+$ with $d_1|d_2, d_2|d_3, \dots, d_{r-1}|d_r$.
If we can find a basis $\{u_1, u_2, \dots, u_n\}$ for G and a basis $\{d_1u_1, \dots, d_ru_r\}$ for H. Then, as an exercise, verify that the map $\phi : G \to \mathbb{Z}_{d_1} \times \dots \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$ by $\phi\left(\sum_{i=1}^n t_iu_i\right) = (t_1, \dots, t_n)$ is a well-defined surjective group homomorphism with $\mathrm{Ker}(\phi) = H$.
So that we have

$$G/H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$

We shall prove that such bases for G and H exist by induction on n, the rank of G
When $n = 0$, (so $G = \{0\}$), there is nothing to prove.
Can start at $n = 1$, use the knowledge of cyclic group. Not necessary.
Let $n \geq 1$, (or $n \geq 2$) and suppose the theorem holds for all free abelian groups G_0 of rank $n-1$ and all subgroups $H_0 \leq G_0$.
Let G be a free abelian group of rank n and let $H \leq G$.
If $H = \{0\}$ is trivial, there is nothing to prove. (the empty set is a basis for $H = \{0\}$ and we take $r = 0$)
Suppose $H \neq \{0\}$, note that if $0 \neq a \in H$ and $\{v_1, \dots, v_n\}$ is any basis for G. Then when we write $a = \sum_{i=1}^n t_iv_i$ with each $t_i \in \mathbb{Z}$, at least one of the coefficients $t_i \neq 0$.
Choose d_1 to be the smallest positive integer (Main trick of the theorem!!) which is equal to one of the coefficients t_i in some linear combination $a = \sum_{i=1}^n t_iv_i$ for some $a \in H$ and for some basis $\{v_1, \dots, v_n\}$ for G.
Choose a particular basis $\{v_1, \dots, v_n\}$ for G and a particular element $a \in H$ of the form

$$a = d_1v_1 + t_2v_2 + \dots + t_nv_n \in H$$

Note: by our choice of d_1, $d_i|t_i$ for $2 \leq i \leq n$, since $2 \leq h \leq n$..
We can write

$$t_k = q \cdot d_1 + r$$

for $0 \leq r < d$.
Then we have

$$\begin{aligned} a &= d_1v_1 + t_2v_2 + \dots + (q \cdot d_1 + r)v_k + \dots + t_nv_n \\ &= d_1(v_1 + q \cdot v_k) + t_2v_2 + \dots + rv_k + \dots + t_nv_n \end{aligned}$$

So, we must have $r = 0$, (if $0 < r < d_1$, this would contradict our choice of d_1, since $\{v_1 + qv_k, v_2, v_3, \dots, v_n\}$ is another basis for G).
Write $t_k = q \cdot d_1$ for $2 \leq k \leq n$.
Then $a = d_1\left(v_1 + q_2v_2 + \dots + q_nv_n\right)$.

Let $u_1 = v_1 + q_2 v_2 + \cdots + q_n v_n$ (So $a = d_1 u_1 \in H$)
and note that $\{u_1, v_2, v_3, \ldots, v_n\}$ is another basis for G.
Let $G_0 = \mathrm{Span}_{\mathbb{Z}}\{v_2, v_3, \ldots, v_n\}$ which is a free abelian group with rank of $n-1$.
Let $H_0 = H \cap G_0 \leq G_0$.
We claim that every element $b \in H$, can be written uniquely in the form $b = t_1 d_1 u_1 + C$ with $t_1 \in \mathbb{Z}$, $c = H_0$.
Let $b \in H$, since $b \in G$, we can write b uniquely as $b = s_1 u_1 + s_2 v_2 + \ldots, s_n v_n$. (Since $\{u_1, u_2, \ldots, v_n\}$ is a basis for G).
Note that $d_1 | s_1$ using the same argument used above (writing $s_1 = q \cdot d + r$))
Since $d_i | s_i$, $s_1 u_1$ is a multiple of $d_u = a \in H$.
So $s_1 u_1 \in H$.
Hence

$$s_2 v_2 + \cdots + s_n v_n = b - s_1 u_1 \in H$$

We have $b = s_1 u_1 + c = t_1 d_1 u_1 + c$ with $c \in H$.
By the induction hypothesis, we can choose a basis $\{u_2 \ldots, u_n\}$ for G_0. And a basis $d_2 u_2, \ldots, d_r u_r$ for H_0 with $d_2 | d_3, d_3 | d_4, \ldots, d_{r-1} | d_r$
Also $c \in G_0 = \mathrm{Span}(\{v_2, \ldots, v_n\})$, so $c \in H_0$.
Thus, every $b \in H$ can be written uniquely in the form $b = t_1 d_1 u_1 + t_2 d_2 u_2 + \cdots + t_r d_r u_r$.
Thus, $\{d_1 u_1, \ldots, d_r u_r\}$ is a basis for H.
Finally, verify that $d_1 | d_2$.
Examples:
Let $G = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$
and let $H = \mathrm{Span}_{\mathbb{Z}}\{(3,6), (6,2)\}$
Note that H has the following bases

$$\{(3,6), (6,2)\}$$

$$\{(3,6), (6,2) + (3,6)\} = \{(3,6), (9,8)\}$$

$$\{(3,6) + 3(9,8), (9,8)\} = \{(30,30), (9,8)\} = \{1 \cdot (9,8), 30(1,1)\}$$

Also note that $\{(9,8), (1,1)\}$ is a basis for $G = \mathbb{Z} \times \mathbb{Z}$.
Since $(1,0) = (9,8) - 8(1,1)$ and $(0,1) = 9(1,1) - (9,8)$

$$\det \begin{pmatrix} 9 & 1 \\ 8 & 1 \end{pmatrix} = 1, \begin{pmatrix} 9 & 1 \\ 8 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ -8 & 9 \end{pmatrix}$$

It follows that $n = 2, r = 2$,

$$G/H \cong \mathbb{Z}_1 \times \mathbb{Z}_{30} \times \mathbb{Z}^0 \cong \mathbb{Z}_{30}$$

$H = \mathrm{Span}\{u_1, \ldots, u_k\}$
$A = (u_1 \ldots u_k) \in M_{n \times k}$
Row operations and column operations can convert A to the form
Picture here.

24 November 8th

Theorem: (Classification of Finite Abelian Groups)
Let G be a finite abelian group.

1. G is isomorphic to a unique group of the form
$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_l}$$
with $l \in \mathbb{Z}$ with $l \geq 0$ and each $n_i \in \mathbb{Z}$ with $n_i \geq z$ and $n_1 | n_2, \ldots, n_{l-1} | n_l$.

2. G is isomorphic to a unique group of the form
$$\mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \cdots \times \mathbb{Z}_{{p_m}^{k_m}}$$
where $m \in \mathbb{Z}$ with $m \geq 0$, each p_i is prime with $p_1 \leq p_2 \leq \cdots \leq p_m$, each $k_i \in \mathbb{Z}$ with $k_i \geq 1$ such that if $p_i = p_{i+1}$, then $k_i \leq k_{i+1}$.

Sketch Proof:
Let $n = |G|$ and say $G = \{a_1, \ldots, a_n\}$.
Define $\phi : \mathbb{Z}^n \to G$ by $\phi(t_1, \ldots, t_n) = \sum_{i=1}^n t_i a_i$.
Verify that ϕ is a surjective group homomorphism.
By the First Isomorphism Theorem,
$$G \cong \mathbb{Z}^n / H \text{ where } H = \text{Ker } \phi$$
By the previous theroem, we have
$$G \cong \mathbb{Z}^n / H \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \cdots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{n-r}$$
for some $0 \leq r \leq n$ and some $d_i \in \mathbb{Z}^+$
with some $d_i \in \mathbb{Z}^+$ with $d_1 | d_2, d_2 | d_3, \ldots, d_{r-1} | d_r$.
Note that we must have $n = r$ since G is finite.
So
$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \mathbb{Z}_{d_n}$$
Say $d_1 = d_2 = \cdots = d_k = 1$ and $d_{k+1} \geq 2$.
Then we can take $n_i = d_{k+i}$ for $i \leq i \leq l$ where $l = n - k$.
This puts G up to isomorphism, into the form in Part (1).
Verify that there is a bijective correspondence between the forms described in Parts (1) and (2).
Examples:

$$\begin{aligned}
&\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{60} \times \mathbb{Z}_{3600} \\
&= \mathbb{Z}_2 \times \mathbb{Z}_{2 \cdot 3} \times \mathbb{Z}_{2^2 . 3 . 5} \times \mathbb{Z}_{2^4 . 3^2 . 5^2} \\
&\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2} \\
&\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_{5^2}
\end{aligned}$$

and

$$
\begin{aligned}
&\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{5^2} \\
\cong\, &\mathbb{Z}_{2^1} \times (\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^1}) \times (\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{5^1}) \times (\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^4} \times \mathbb{Z}_{5^2}) \\
\cong\, &\mathbb{Z}_2 \times \mathbb{Z}_{2^2.3} \times \mathbb{Z}_{2^2.3^4.5^1} \times \mathbb{Z}_{2^3.3^4.5^2}
\end{aligned}
$$

Finally, we verify that the form of Part (2) is unique (up to isomorphism)
Let $G \cong \mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_1}^{k_2}} \times \cdots \times \mathbb{Z}_{{p_m}^{k_m}}$ as in Part (2).
We shall show that the prime powers ${p_i}^{k_i}$ are determined from the number of elements in G of each order.
Fix a prime p, let $n_k =$ the number of $a \in G$ with $|a|/p^k$. (That is $|a| \in \{1, p, p^2, \ldots, p^k\}$)
Let $a_k =$ the number of indices i such that $p_i = p$ and $k_i = k$.
Let $b_k =$ the number of indices i such that $p_i = p$ and $k_i \geq k$.
Recall that if $a_i \in \mathbb{Z}_{{p_i}^{k_i}}$. So $a = (a_1, \ldots, a_m) \in \mathbb{Z}_{{p_1}^{n_1}} \times \ldots \mathbb{Z}_{{p_m}^{k_m}}$, then $|a| = \operatorname{lcm}(|a_1|, \ldots, |a_m|)$
Side Note:
In $\mathbb{Z}_{p^k}$, there are $\phi(p) = p - 1$ elements a with $|a| = p$. So that there are p elements a with $|a| = 1$ or p
We have

$$
\begin{aligned}
n_1 &= \# \text{ of } a \in G \text{ such that } |a| = 1 \text{ or } p \\
&= p^{b_1}
\end{aligned}
$$

(there are p choices for each $\mathbb{Z}_{{p_i}^{k_i}}$ with $p_i = p, k_i \geq 1$)

$$
\begin{aligned}
n_2 &= \# \text{ of } a \in G \text{ such that } |a| = 1, p, \text{ or } p^2 \\
&= p^{a_1} \cdot p^{2b_2}
\end{aligned}
$$

(there are p choices for each $\mathbb{Z}_{{p_i}^{k_i}}$ with $p_i = p$, $k_i = 1$ and there are p^2 choices for each $\mathbb{Z}_{{p_i}^{k_i}}$ with $p_i = p, k_i \geq 2$)

$$n_3 = p^{a_1} p^{2a_2} p^{3b_3}$$

and so on, solution

$$n_k = p^{a_1} p^{2a_2} \ldots p^{(k-1)a_{k-1}} p^{kb_k}$$

Also, note that

$$a_k = b_k - b_{k+1}$$

It follows that

$$
\begin{aligned}
\frac{n_k}{n_{k-1}} &= \frac{p^{(k-1)a_{k-1}}p^{kb_k}}{p^{(k-1)b_{k-1}}} \\
&= \frac{p^{(k-1)a_{k-1}}p^{kb_k}}{p^{(k-1)(a_{k-1}+b_k)}} \\
&= p^{b_k}
\end{aligned}
$$

Hence

$$
\begin{aligned}
p^{a_k} &= p^{b_k - b_{k+1}} = p^{b_k}/p^{b_{k+1}} \\
&= \frac{n_k}{n_{k-1}} / \frac{n_{k+1}}{n_k} \\
&= \frac{{n_k}^2}{n_{k-1}n_{k+1}}
\end{aligned}
$$

$$
a_k = \log_p \left(\frac{{n_k}^2}{n_{k-1}n_{k+1}} \right)
$$

Fact (Gauss)

$$
U_2 \cong \mathbb{Z}_1, U_4 \cong \mathbb{Z}_2, U_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_2, U_{2^n} \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \text{ for } n \geq 3
$$

and

$$
U_{p^k} \cong \mathbb{Z}_{\phi(p^k)}
$$

where $\phi(p^k) = p^k - p^{k-1}$.

25 November 11th

Chapter 8 Rings
Definition:
A ring is a set R with an element $O \in R$ and two binary operations $+$ and $\times$ such that

1. $+$ is associative
2. $+$ is commutative
3. O is an additive identity
4. Every $a \in R$ has an additive inverse
5. $\times$ is associative
6. $\times$ is distributive over $+$ for all $a, b, c \in R$, $a(b+c) = ab+ac$ and $(a+b)c = ac + bc$.

R is commutative when $\times$ is commutative.
R has an identity (or R has a 1) when there is an element $1 \in R$ with $1 \neq 0$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.
When R has a 1 and $a \in R$, we say that a is invertible, or that a is a unit, when there exists $b \in R$ such that $ab = ba = 1$
A field is a commutative ring in which every non-zero element is invertible.
In any ring R, we have $0 \cdot a = 0$ for all a, (also $a \cdot 0 = 0$ for all $a \in R$).
Proof:
Let $a \in R$, then $0 \cdot a = (0 + 0)$ by property (3)
Then $= 0 \cdot a + 0 \cdot a$ by property (6)
By (4), we can choose $b \in R$ such that $0 \cdot a + b = 0$.
Then we have
$0 \cdot a = 0 \cdot a + 0 \cdot a$ (as above)
$0 \cdot a + b = (0 \cdot a + 0 \cdot b) + b = 0 \cdot a + (0 \cdot a + b)$ by (1)
$0 = 0 \cdot a + 0$ since $0 \cdot a + b = 0$.
$\therefore 0 = 0 \cdot a$ by (3).
Note that we do have additive cancellation:
If $a + b = a + c$ or if $b + a = c + a$, then $b = c$.
In general, we do not have multiplicative cancellation, ($ab = ac$ does not imply that $b = c$).
In a ring R, we say that a and b are zero divisors when $a \neq 0, b \neq 0, a \cdot b = 0$.
Example:
$\mathbb{Z}_6$ we have $2 \cdot 3 = 0$.
The multiplicative cancellation rule is as follows:
For all $a, b, c \in R$, if $ab = ac$, then either $a = 0$ or a is a zero divisor or $b = c$.
An **integral domain** is a commutative ring with 1 with no zero divisors.
In an integral domain, R, for all $a, b, c \in R$, if $ab = ac$, then either $a = 0$ or $b = c$.
Note that units are never zero divisors.
If u is a unit, say $uv = vu = 1$, then if we had $u \cdot b = 0$, then we would have

$$0 = v \cdot 0 = v(u \cdot b) = (vu) \cdot b = 1 \cdot b = b$$

Example:
In $\mathbb{Z}_n$, the units are the elements in $U_n = \{k \in \mathbb{Z}_n |\, \gcd(k, n) = 1\}$. All other elements are zero divisors. $0 \neq k \in \mathbb{Z}_n$, and $\gcd(k, n) \neq 1$, we can choose a prime p with $p|k$ and $p|n$. Then if we write $n = p \cdot l$, then $k \cdot l = 0$.
In $M_n(\mathbb{R})$, the units are the elements in

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) |\, \det(A) \neq 0\}$$

and all other non-zero elements are zero divisors since when $\det A = 0$, we can choose $0 \neq u \in \mathbb{R}^n$ such that $Au = 0$ and then $AB = 0$ where

$$B = (u, u, \ldots, u) \quad (\text{or } B\,(u, 0, 0, \ldots, 0))$$

If $\mathbb{F}$ is a field, all non-zero elements are units and $\mathbb{F}$ has no zero divisors.

If $\mathbb{F}$ is a field and R is a subring of $\mathbb{F}$ with $1 \in R$, then R is an integral domain.
Note:
If an element $a \in R$ has a left inverse and a right inverse, then these inverses are equal to each other, so a is invertible.
(If $ab = 1$ and $c \cdot a = 1$, then $c = c \cdot 1 = c\,(ab) = (ca)\,b = 1 \cdot b = b$)
Using addition and multiplication.
In the ring $C^0(\mathbb{R}, \mathbb{R}) = \{\text{continuous functions } f : \mathbb{R} \to \mathbb{R}\}$. The units are the functions $f : \mathbb{R} \to \mathbb{R}^*$ (the functions such that $f(x) \neq 0$ for all $x \in R$ and the inverse of f is the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \frac{1}{f(x)}$).
Exercise:
Verify that the zero divisors are the functions $f : \mathbb{R} \to \mathbb{R}$ such that for some $a < b$ we have $f(x) = 0$ for all $x \in [a, b]$.
A picture here.
Definition:
For a ring R with 1, the characteristic of R is

$$\text{char}(R) = \begin{cases} \text{the smallest } n \in \mathbb{Z}^+ \text{ for which } n \cdot 1 = 0 \\ 0 \quad \text{if no such } n \in \mathbb{Z}^+ \text{ exists} \end{cases}$$

Note:
If $\text{char}(R) = n \in \mathbb{Z}^+$, then we have $n \cdot a = 0$ for all $a \in R$, because

$$\begin{aligned} 0 = n \cdot a &= (1 + 1 + \cdots 1)\,a \\ &= (n \cdot 1)\,a = 0 \cdot a = 0 \end{aligned}$$

Exercise:
Verify that if R has no zero divisors, and if $\text{char}(R) = n \in \mathbb{Z}^+$, then n is prime.
Example:
$\text{char}\ \mathbb{Z} = \text{char}\ \mathbb{Q} = \text{char}\ \mathbb{R} = \text{char}\ \mathbb{C} = 0$ and $\text{char}\ \mathbb{Z}_p = p$.
Note:
When R is a ring and $S \subseteq R$ is a subset of R, S is a subring when

$$0 \in S, S \text{ closed under } +, -, \text{ and } \times$$

That is, for all $a, b \in S$, we have $a + b \in S, -a \in S,$ and $ab \in S$.

26 November 13th

Chapter 9: Ring Homomorphisms and Quotient Rings
Definition:
When R and S are rings, a **ring homomorphism** from R to S is a function $\phi : R \to S$ such that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in R$.

A **ring isomorphism** from R to S is a bijective ring homomorphism from R to S. We say that R and S are isomorphic (as rings), and we write $R \cong S$, when there exists a ring isomorphism $\phi : R \to S$.
Check that when ϕ is a homomorphism from R to S, we have $\phi(0) = 0$.
If R has a 1 and ϕ is surjective, then S has a 1 and $\phi(1) = 1$.
Examples:
$\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ given by $\phi(k) = (k, 0)$ is a (non-surjective) ring homomorphism and $\phi(1) = (1, 0)$ which is not equal to the identity element $(1, 1)$ in $\mathbb{Z} \times \mathbb{Z}$.
(Think about $\phi : \mathbb{Z} \to \mathbb{Z}[i]$ given by $\phi(1) = 1 = (1, 0)$ where $\mathbb{Z}[i] = \{(a, b)|a + ib|a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.)
Check also that when $K \subseteq R$ is a subring, $\phi(k) \subseteq S$ is a subring and when $L \subseteq S$ is a subring, $\phi^{-1}(L) \subseteq R$ is a subring.
In particular,

$$\text{Image}(\phi) = \phi(R) \subseteq S \text{ is a subring}$$

and

$$\text{Ker}(\phi) = \phi^{-1}(0) \subseteq R \text{ is a subring}$$

Check that ϕ is surjective $\iff$ Image$(\phi) = S$
and ϕ is injective $\iff$ Ker $\phi = \{0\}$.
Examples:
The subgroups of $\mathbb{Z}$ are of the form $\langle n \rangle = n\mathbb{Z}$ where $n \in \mathbb{N}$.
These are all subrings. Similarly, the subgroups of $\mathbb{Z}_n$ are the groups

$$\langle d \rangle = d\mathbb{Z}_n = \{dk|k \in \mathbb{Z}\}$$

where d is a positive divisor of n. These are also subrings.
In $\mathbb{Z}[i]$, the subgroup generated by $(2, 1) = 2 + i$ is

$$\langle 2 + i \rangle = \{k\,(2 + i)\,|k \in \mathbb{Z}\}$$

(which is a free abelian group).
Picture here.
Is this a subring of $\mathbb{Z}[i]$?
It is not because, for example

$$(2 + i)\,(2 + i) = 3 + 4i$$

The smallest subring of $\mathbb{Z}[i]$ which contains $(2, 1) = 2 + i$ is the ring

$$\text{Span}\{(2 + i), (-1 + 2i)\} = \langle 2 + i, -1 + 2i \rangle = (2 + i)\text{Span}\{1 + i\} = (2 + i)\mathbb{Z}[i]$$

(which is also a free abelian group under $+$)
(Verify this!)
Examples:
In $\mathbb{Q}$, the subgroup generated by $\frac{1}{2}$ is $\langle \frac{1}{2} \rangle = \frac{1}{2}\mathbb{Z} = \{\frac{k}{2}|k \in \mathbb{Z}\}$ and the smallest subring of $\mathbb{Q}$ which contains $\frac{1}{2}$ is

$$\left\{ \frac{k}{2^n} \middle| k \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

(Verify this!)

Quotient Rings

Note: When R is a ring and $A \subseteq R$ is a subring, A is also a subgroup under addition. And $+$ is commutative, so $A \trianglelefteq R$ so we can form the quotient group

$$R/A = \{r + A | r \in R\}$$

with the operation given by

$$(r + A) + (s + A) = (r + s) + A$$

When can we define a product operation by

$$(r + A) \cdot (s + A) = rs + A$$

to obtain a ring structure on R/A.

Exercise:

If A is closed under addition by ???

Theorem:

Let R be a ring and let $A \subseteq R$ be a subring. Then we can define a well-defined multiplication operation on the quotient group $R/A = \{r + A | r \in R\}$ by the formula $(r + A) \cdot (s + A) = rs + A$ if and only if A is closed under multiplication by elements in R, that $ar \in A$ and $ra \in A$ for all $a \in A$ and $r \in R$.

Proof:

To say that the operation

$$(r + A)(s + A) = rs + A$$

is well-defined means that for all $r_1, r_2, s_1, s_2 \in R$ if $r_1 + A = r_2 + A$ (equivalently $r_2 - r_1 \in A$) and $s_1 + A = s_2 + A$ (equivalently $s_2 - s_1 \in A$), then we must have $r_1 s_1 + A = r_2 s_2 + A$.

(Or equivalently $r_2 s_2 - r_1 s_1 \in A$)

Suppose the operation is well-defined, let $a \in A$ and $r \in R$. Then taking $r_1 = r_2 = r$ and $s_1 = 0$ and $s_2 = a$ so that $r_2 - r_1 = 0 \in A$ and $s_2 - s_1 = a \in A$, we have $r_2 s_2 - r_1 s_1 \in A$, that is $ra - r \cdot 0 = ra \in A$.

A similar argument shows that $a \cdot r \in A$.

Suppose, conversely that A is closed under elements in R.

Let $r_1, r_2, s_1, s_2 \in R$, with $r_2 - r_1 \in A$ and $s_2 - s_1 \in A$, say $r_2 - r_1 = a \in A$ and $s_2 - s_1 = b \in A$.

Then

$$\begin{aligned} r_2 s_2 - r_1 s_1 &= r_2 s_2 - (r_2 - a)(s_2 - b) \\ &= r_2 s_2 - (r_2 s_2 - r_2 b - a s_2 + ab) \\ &= r_2 b + a s_2 - ab \\ &\in A \end{aligned}$$

As long as the operation is closed, then it is well-defined.

27 November 15th

Theorem
If $A \subseteq R$ is a subring, then we can define an operation on $R/A = \{r + A | r \in R\}$ by $(r + A)(s + A) = (r \cdot s)A$ for $r, s \in R$ if and only if A is closed under multiplication (on the left and on the right) by elements in R.
In this case, $R|A$ is a ring under $(r+A)+(s+A) = (r+s)+A$ and $(r+A)\cdot(s+A) = (r \cdot s) + A$

$$\begin{aligned}
&(r + A)\left((s + A) + (t + A)\right) \\
=&(r + A)\left((s + t) + A\right) \\
=&r(s + t) + A \\
=&(rs + rt) + A \\
=&(rs + A) + (rt + A) \\
=&(r + A)(s + A) + (r + A)(t + A)
\end{aligned}$$

Definition:
An **ideal** in a ring R is a subring $A \subseteq R$ which is closed under multiplication by elements in R (that is, for all $a \in A, r \in R$, we have $ar \in A$ and $ra \in A$)
When $A \subseteq R$ is an ideal, the quotient $R/A = \{r + A | r \in R\}$ is called the quotient ring of R by A.
Check that the zero element in R/A is $0 + A = A$.
Check that if R has a 1, then so does R/A, and the identity in R/A is $1 + A$.
Check that if R has a 1 and $r \in R$ is a unit then $r + A$ is a unit in R/A with $(r + A)^{-1} = r^{-1} + A$.
Check that if R is commutative, then so is R/A.
Notation
When R is a ring and $U \subseteq R$ is a subset, we could write

$$\langle u \rangle = \mathrm{Span}_{\mathbb{Z}} U$$

to denote the smallest subgroup of R (under +) containing U.
We could write

$$[U]$$

to denote the smallest subring of R containing U, and we could write

$$\langle U \rangle = (U)$$

to denote the smallest ideal in R containing U.
When R is a subring of S, and $U \subseteq S$ is a subset, we could write

$$R[U]$$

to denote the smallest subring of S containing $R \cup U$ (that $R[U] = [R \cup U]$)

When F is a subfield of K and $U \subseteq K$, we could write $F(U)$ to denote the smallest subfield of K which contains $F \cup U$.
Examples:
For $\frac{1}{2} \in \mathbb{Q}$, we have

$$\left\langle \frac{1}{2} \right\rangle = \frac{1}{2} \cdot \mathbb{Z} = \{\frac{k}{2} | k \in \mathbb{Z}\}$$

$$\left[\frac{1}{2} \right] = \{\frac{k}{2^n} | k \in \mathbb{Z}, n \in \mathbb{Z}^+\}$$

$$\left(\frac{1}{2} \right) = \mathbb{Q}$$

More generally, if F is a field then the only ideals in F are $\{0\}$ and $\mathbb{F}$.
Examples:
For $2 + 1 \in \mathbb{Z}[i]$,

$$\langle 2+i \rangle = (2+i)\mathbb{Z} = \{(2+i)k | k \in \mathbb{Z}\}$$

$$[2+i] = \text{Span}\{2+i, -1+2i\}$$

$$(2+i) = [2+i] = \text{Span}\{2+i, -1+2i\}$$

Picture here.
Examples:
For $2 \in \mathbb{Z}[i]$

$$\langle 2i \rangle = 2i\mathbb{Z}$$

$$[2i] = \text{Span}_{\mathbb{Z}}\{2i, 4\}$$

Check if it is closed under multiplication

$$\begin{aligned} &(4k + i2l)(4m + i2n) \\ =&(16km - 4nl) + i(8kn + 8lm) \end{aligned}$$

$$(2i) = \text{Span}_{\mathbb{Z}}\{2i, 2\} = (2i)\mathbb{Z}[i] = 2(\mathbb{Z}[i]) = \{2k + i2l | k, l \in \mathbb{Z}\}$$

Example:
In $\mathbb{C}$,

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

$$\mathbb{Q}[i] = \{a + ib | a, b \in \mathbb{Q}\}$$

$$\mathbb{Q}(i) = \mathbb{Q}[i]$$

(since $\mathbb{Q}[i]$ is already a field, because when $a + ib \neq 0$, $\frac{1}{a+ib} = \frac{a}{a^2+b^2} + i\frac{-b}{a^2+b^2}$)
Theorem (The First Isomorphism Theorem)
When R and S are rings and $\phi : R \to S$ is a ring homomorphism, and $K = \text{Ker}\phi \subseteq R$, K is an ideal in R and $R/K \cong \phi(R)$.

Indeed, the map $\Phi : R/K \to \phi(R)$ given by $\Phi(r + K) = \phi(r)$ is as well defined ring isomorphism.
Proof:
Exercise.
Good practice!!
There are also second, and third Isomorphism Theorems.
Note:
We can perform the following operations on ideals in a ring R:
If $A, B \subseteq R$ are ideals, then so are the each of the followings:

1. $A \cap B$
2. $A + B = \{a + b | a \in A, b \in B\}$
3. $A \cdot B = \{\sum_{i=1}^{n} a_i \cdot b_i | n \in \mathbb{Z}^+, \text{ each } a_i \in A, \text{ each } b_i \in B\} \subseteq A \cap B$

$(a + b)r = ar + br$
$(\sum_{i=1}^{n} a_i b_i) \cdot r = \sum_{i=1}^{n} a_i (b_i r)$
In $\mathbb{Z}$, the subgroups are of the form $\langle n \rangle = n\mathbb{Z}$ with $n \in \mathbb{N}$.
These are also subrings and ideals.
Given $k, l \in \mathbb{Z}$ (or in $\mathbb{N}$), what are $\langle k \rangle \cap \langle l \rangle, \langle k \rangle + \langle l \rangle$ and $\langle k \rangle \langle l \rangle$

28 November 18th

Example:
Describe all ring homomorphisms $\phi : \mathbb{Z} \to R$ where R is a ring.
Solution:
If $\phi : \mathbb{Z} \to R$ is a ring homomorphism, then ϕ is also a group homomorphism (under $+$).
So ϕ is determined by the value $\phi(1) \in R$.
If $\phi(1) = a \in R$, then
for $k \in \mathbb{Z}$,

$$\phi(k \cdot 1) = k\phi(1) = ka$$

So we have $\phi = \phi_a$ where $\phi_a : \mathbb{Z} \to R$ given by $\phi_a(k) = k \cdot a$.
But also, for ϕ to be a ring homomorphism, we also need

$$a = \phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = a^2$$

Thus, we must have $\phi = \phi_a$ for some a in the ring with $a^2 = a$.
An element $a \in R$ with $a^2 = a$ is called **idempotent**.
Finally, note that if $a \in R$, with $a^2 = a$, then the map $\phi_a : \mathbb{Z} \to R$ given by $\phi_a(k) = k \cdot a$ is a ring homomorphism because

$$\phi_a(k + l) = (k + l)a = ka + la = \phi_a(k) + \phi_a(l)$$

and

$$\phi_a(k \cdot l) = (kl)a = kla^2 = (ka)(la) = \phi_a(k)\phi_a(l)$$

Exercise:
Describe ring homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to R, \phi : \mathbb{Z}_n \to R$ and $\phi : \mathbb{Z}_n \times \mathbb{Z}_m \to R$.
Example:
In $\mathbb{Z}_n$, the subgroups are of the form $\langle d \rangle = d \cdot \mathbb{Z}_n$ where $d|n$, and these subgroups are also subrings and ideals.
So the quotient $\mathbb{Z}_n/d \cdot \mathbb{Z}_n$ is a ring.
We can prove that when $d|n$, $\mathbb{Z}_n/d \cdot \mathbb{Z}_n \cong \mathbb{Z}_d$ as follows.
Define $\phi : \mathbb{Z}_n \to \mathbb{Z}_d$ by $\phi(k) = k$. (That is $\phi(k \mod n) = k \mod d$)
Then, ϕ is well-defined because if $k = l \mod n$, then $k = l \mod d$.
Also, ϕ is a ring homomorphism and ϕ is surjective.
By the Fisrt Isomorphism Theorem,

$$\mathbb{Z}_n/\mathrm{Ker}(\phi) \cong \mathbb{Z}_d$$

(as rings)
For $k \in \mathbb{Z}$, giving $k \in \mathbb{Z}_n$

$$\begin{aligned} k \in \mathrm{Ker}(\phi) &\iff \phi(k) = 0 \in \mathbb{Z}_d \\ &\iff k = 0 \in \mathbb{Z}_d \\ &\iff k = 0 \mod d \\ &\iff d|k \\ &\iff k \in d\mathbb{Z}_n \end{aligned}$$

Example:
Show that $2\mathbb{Z} \ncong 3\mathbb{Z}$ as rings.
Note that $2\mathbb{Z} \cong 3\mathbb{Z}$ as groups (both are infinite cyclic groups)
We can see that $2\mathbb{Z} \ncong 3\mathbb{Z}$ as rings because in $2\mathbb{Z}$ we have $2 + 2 = 4 = 2 \cdot 2$
But in $3\mathbb{Z}$, there is no element $a \in 3\mathbb{Z}$ such that $a + a = a \cdot a$ (that is $2a = a^2$)
Example:
Show that $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}]$.
Solution:
Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ by $\phi(f) = f(\sqrt{2})$.
Note that when $f \in \mathbb{Q}[x]$, if $f(\sqrt{2}) = A + B\sqrt{2}$
then $f(-\sqrt{2}) = A - B\sqrt{2}$ (with $A, B \in \mathbb{Q}$)
So if $f(\sqrt{2}) = 0$, then $f(-\sqrt{2}) = 0$.
So $(x - \sqrt{2})$ and $\big(x + \sqrt{2}\big)$ are factors of $f(x)$ (in $\mathbb{R}[x]$).
So $(x^2 - 2) = (x - \sqrt{2})(x + \sqrt{2})$ is a factor of $f(x)$ (in $\mathbb{R}[x]$ hence also in $\mathbb{Q}[x]$)
If $f(\sqrt{2}) = 0$, then $(x^2 - 2)$ is a factor of $f(x)$.
So we can write $f(x) = (x^2 - 2)g(x)$ for some $g \in \mathbb{Q}[x]$
Then $f(x) = (x^2 - 2)$ (the ideal geenrated by $x^2 - 2$)
Conversely, if $f \in (x^2 - 2)$, then (since $(x^2 - 2) = \{(x^2 - 2)g(x) | g \in \mathbb{Q}[x]\}$), we have $f(x) = (x^2 - 2)g(x)$ for some $g(x) \in \mathbb{Q}[x]$.

Hence, $f(\sqrt{2}) = 0$.
Side Note:
More generally, if $a \in R$ and R is commutative with 1, then $(a) = a \cdot R = \{ar | r \in R\}$.
$ar + as = a(r+s), ar \cdot as = a(ars), (a \cdot r)s = a(rs)$
Side Note ends
This shows that $\text{Ker}(\phi) = \{f \in \mathbb{Q}[x] | f(\sqrt{2}) = 0\} = (x^2 - 2)$
Since $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ is a surjective ring homomorphism with $\text{Ker}(\phi) = (x^2 - 2)$, it follows that

$$\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}]$$

Example:
Show that $\mathbb{Z}[i]/\langle 2+i \rangle \cong \mathbb{Z}_5$
Solution:

$$\begin{aligned}
\langle 2+i \rangle = (2+i)\mathbb{Z}[i] &= \{(2+i)(k+il) | k, l \in \mathbb{Z}\} \\
&= \{(2+i)k + (-1+2i)l | k, l \in \mathbb{Z}\} \\
&= \text{Span}_{\mathbb{Z}}\{(2+i), (-1+2i)\}
\end{aligned}$$

Picture here.
As a group, we saw (informally) that $\mathbb{Z}[i]/\text{Span}\{(2+i), (-1+2i)\} \cong \mathbb{Z}_5$
Cosets, shifting left or right.
$(1,1) + H$ is a generator.
To prove (rigorously) that $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$ as rings, we find a surjective ring homomorphism $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ with $\text{Ker}(\phi) = \langle 2+i \rangle$
Picture revised here.
Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ by $\phi(a+ib) = 2b - a (\text{mod } 5)$.
ϕ is clearly well-defined and surjective.
ϕ is a ring homomorphism because for $a, b, c, d \in \mathbb{Z}$,

$$\begin{aligned}
\phi\left((a+ib) + (c+id)\right) &= \phi\left((a+c) + i\left(b+d\right)\right) \\
&= 2(b+d) - (a+c) \\
&= (2b-a) + (2d-c) \\
&= \phi(a+ib) + \phi(c+id)
\end{aligned}$$

$$\begin{aligned}
\phi\left((a+ib)\left(c+id\right)\right) &= \phi((ac-bd) + i(ad+bc)) \\
&= 2(ad+bc) - (ac-bd) \\
&= 2ad + 2bc - ac + bd
\end{aligned}$$

$$
\begin{aligned}
\phi(a+ib)\cdot\phi(c+id) &= (2b-a)(2d-c) \\
&=
\end{aligned}
$$

29 November 20th

Example:
Show that $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$ as rings.
Solution:
Define $\phi : \mathbb{Z} \to \mathbb{Z}_5$ by $\phi(a+ib) = a - 2b = a + 3b \in \mathbb{Z}_5$
Then, ϕ is clearly well-defined and surjective
Note that ϕ is a ring homomorphism because for $a, b, c, d \in \mathbb{Z}$

$$
\begin{aligned}
\phi((a+ib)+(c+id)) &= \phi((a+c)+i(b+d)) \\
&= (a+c)+3(b+d) \\
&= (a+3b)+(c+3d) \\
&= \phi(a+ib)+\phi(c+id)
\end{aligned}
$$

and

$$
\begin{aligned}
\phi((a+ib)\cdot(c+id)) &= \phi((ac-bd)+i(ad+bc)) \\
&= (ac-bd)+3(ad+bc)
\end{aligned}
$$

$$
\begin{aligned}
\phi(a+ib)\cdot\phi(c+id) &= (a+3b)\cdot(c+3d) \\
&= ac+3ad+3bc+9bd \\
&= ac+3ad+3bc-bd \in \mathbb{Z}_5
\end{aligned}
$$

Since $9 = -1$
By the First Isomorphism Theorem,

$$\mathbb{Z}[i]/\mathrm{Ker}(\phi) \cong \mathbb{Z}_5$$

We claim that $\mathrm{Ker}\phi = (2+i)$
(Recall that when R is a commutative ring with 1 and $a \in R$, we have $(a) = a \cdot R = \{ar | r \in R\}$)
In $\mathbb{Z}[i]$,

$$
\begin{aligned}
(2+i) &= (2+i)\mathbb{Z}[i] \\
&= \{(2+i)(k+il) | k, l \in R\} \\
&= \{(2+i)k + (-1+2i)l | k, l \in \mathbb{Z}\} \\
&= \mathrm{Span}_{\mathbb{Z}}\{2+i, -1+2i\}
\end{aligned}
$$

If $a + ib \in (2 + i) = \mathrm{Span}_{\mathbb{Z}}\{2 + i, -1 + 2i\}$
say $a + ib = (2 + i)k + (-1 + 2i)l = (2k - l) + i(k + 2l)$

$$\begin{aligned} \phi(a + ib) &= a + 3b = (2k - l) + 3(k + 2l) \\ &= 5k + 5l = 0 \in \mathbb{Z}_5 \end{aligned}$$

$\phi(a + ib) = a + 3b \in \mathbb{Z}_5$
Suppose that $\phi(a + ib) = 0$, that is $a + 3b = 0 \in \mathbb{Z}_5$.
We need to show that there exist $k, l \in \mathbb{Z}$ such that

$$(a + ib) = (2 + i)k + (-1 + 2i)l = (2k - l) + i(k + 2l)$$

We need

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix}$$

That is

$$\begin{aligned} \begin{bmatrix} k \\ l \end{bmatrix} &= \frac{1}{5} \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \\ &= \begin{bmatrix} (2a + b)/5 \\ (-a + 2b)/5 \end{bmatrix} \end{aligned}$$

Since $a + 3b = 0 \mod 5$

$$\begin{aligned} 0 &= -(a + 3b) = (-a - 3b) \\ &= -a + 2b \mod 5 \end{aligned}$$

and

$$\begin{aligned} 0 &= 2(a + 3b) = 2a + 6b \\ &= 2a + b \mod 5 \end{aligned}$$

So the values k, l above lie in $\mathbb{Z}$.
Example:
Let R be a commutative ring with 1.
We define the evaluation map

$$\phi : R[x] \to \mathrm{Func}(R, R) = R^R$$

by $\phi(f) = f$
(So ϕ sends the polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$, where each $a_k \in R$, to the function $f : R \to R$ given by $f(x) = \sum_{k=0}^{n} a_k x^k$)
Example:
For $f(x) = x^2 + x \in \mathbb{Z}_2[x]$, we have $0 \neq f(X) \in \mathbb{Z}_2[x]$, but $f(x) = 0$ for all $x \in \mathbb{Z}_2$.

When R is commutative, ϕ is a ring homomorphism.
(When R is not commutative, its not in $R[x]$

$$(a+bx)(c+dx) = (ac) + (ad+bc)x + bdx^2$$

but in R^R

$$(a+bx)(c+dx) = ac + adx + bxc + bxdx$$

)
When $\mathbb{R}$ is an infinite field (or an infinite integral domain), the evaluation map ϕ is injective.
(For $f \in R[x]$, $\phi(f) = 0 \in R^R$, so $f(x) = 0$ for all $x \in R$)
We must have that $f = 0 \in R[x]$ since a non-zero polynomial of degree n can only have at most n roots.)
The image of ϕ in R^R is called the ring of polynomial functions on R.
If R is a finite field, then ϕ is not injective (Since $R[x]$ is infinite but R^R is finite.)
But, instead, ϕ is surjective:
Indeed, if $R = \{a_1, a_2, \ldots, a_n\}$, then given $b_1, b_2, \ldots, b_n \in R$
We can construct a polynomial function $R \to R$ with $f(a_i) = b_i$ for all i as follows.
For each $1 \le k \le n$, let

$$g_k(x) = \frac{\prod_{i \neq k}(x - a_i)}{\prod_{i \neq k}(a_k - a_i)}$$

Thus, $g_k(a_l) = \begin{cases} 1 \text{ if } l = k \\ 0 \text{ if } l \neq k \end{cases}$

$$\begin{aligned} &\sum_{k=1}^{n} b_k g_k(a_l) \\ =&\sum b_k \delta_{k,l} \\ =&b_l \end{aligned}$$

So we can take

$$f(x) = \sum_{k=1}^{n} b_k g_k(x)$$

We have the evaluation map $\phi : R[x] \to R^R$. The ring of the polynomial maps is

$$\phi(R[x]) \cong R[x]/\mathrm{Ker}(\phi)$$

When R is a finite field with $|R| = n$.
Show, as an exercise, that

$$\mathrm{Ker}\phi = (x^n - x)$$

(Since $R^* = R \setminus \{0\}$ is a group with $n-1$ elements.

So $x^{n-1} = 1$ for all $x \in R$ by Lagrange's Theorem.
Hence, $x^n = x$ for all $x \in R$.)
In algebraic geometry, we study **varieties**, when $S \subseteq \mathbb{F}[x_1, \ldots, x_n]$ with $\mathbb{F}$ a field.
The **variety** of S is

$$V(S) = \{x \in \mathbb{F}^n | f(x) = 0 \text{ for all } f \in S\}$$

When $f \in \mathbb{F}[x_1, \ldots, x_n]$, we write

$$V(\{f\}) = V(f)$$

Photos Here.
Given $X \subseteq \mathbb{F}^n$, the ideal of X is the ideal

$$I(X) = \{f \in \mathbb{F}[x_1, \ldots, x_n] | f(x) = 0 \text{ for all } x \in X\}$$

The ring of polynomial functions $A(X)$ on a variety X is the ring of functions $f : X \to \mathbb{R}$ such that there is a polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ for which $f(x) = p(x)$ for all $x \in X$.
We have the evaluation map

$$\phi : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^X = \{f : X \to F\}$$

$$\begin{aligned} A(X) &= \text{Image}(\phi) \\ &\cong \mathbb{F}[x_1, \ldots, x_n]/\text{Ker}\phi \end{aligned}$$

Show that $\text{Ker}\phi = I(X)$

30 November 22nd

When X is a set and $R = \mathcal{P}(x) = \{A | A \subseteq X\}$, we define

$$A + B = (A \cup B) \setminus (A \cap B)$$

$$A \cdot B = A \cap B$$

A picture here.
Chapter 10 Factorization in Commutative Rings
Example
Solve $ax + by = d = \gcd(a, b)$
If p is **irreducible**, then

$$p|ab \Rightarrow (p|a) \text{ or } p|b$$

$p_1 p_2 \ldots p_l = q_1 q_2 \ldots q_m$, $p_1 | q_i$ for some i.
Definition:

Let R be a commutative ring with 1. For $a, b \in R$, we say a **divides** b, or a is a **factor** of b, or b is a multiple of a, and we write $a|b$ when $b = ac$ for some $c \in R$.
For $a, b \in R$, we say that a and b are **associates** and we write $a \sim b$, when $a|b$ and $b|a$.
Exercise:
Verify each of the following:

1. $a|0$ for all a, and $0|a \iff a = 0$.
2. $1|a$ for all $a \in R$, and $a|1 \iff a$ is a unit.
3. $a|b \iff b \in (a) \iff (b) \subseteq (a)$
4. Association is an equivalence relation.
5. For $a, b \in R$, $a \sim b \iff (a) = (b)$
$\iff a$ and b have the same divisors and the same multiples

Definition:
In a commutative ring, R, with 1, a **principle ideal** is the ideal of the form

$$A = (a) = \{ar | r \in R\}$$

for some $a \in R$.
Exercise:
Show that when R is a commutative ring with 1 and $a, b \in R$, we have $(a)(b) = (ab)$.
Proof:

$$\begin{aligned}
(a)(b) &= \{\sum_{i=1}^{n} (a \cdot r_i)(b \cdot s_i) | r_i, s_i \in R\} \\
&= \{ab \left(\sum_{i=1}^{n} r_i s_i \right) | r_i, s_i \in R\} \\
&= \{ab \cdot t | t \in R\} = (ab)
\end{aligned}$$

Definition
Let R be a commutative ring with 1.

1. An element in a ring, $a \in R$, we say a is **reducible** when a is a non-zero, non-unit, such that $a = b \cdot c$ for some non-units $b, c \in R$.
2. For $a \in R$, we say that a is **irreducible** when a is a non-zero, non-unit and for all $b, c \in R$, if $a = b \cdot c$, then either b is a unit or c is a unit.
3. For $p \in R$, we say that p is **prime** when it has the property that for all $a \in R$, if $p|ab$, p is a non-zero, non-unit, then $p|a$ or $p|b$.

   (In integer, irreducible and prime are the same thing.)

Exercise:
Verify the following:
If R is a commutative ring with 1 and $a, b \in R$ with $a \sim b$,

$$\begin{aligned} a = 0 &\iff b = 0 \\ a \text{ is a unit} &\iff b \text{ is a unit} \\ a \text{ is reducible} &\iff b \text{ is reducible} \\ a \text{ is irreducible} &\iff b \text{ is irreducible} \\ a \text{ is a prime} &\iff b \text{ is a prime} \end{aligned}$$

If R is an integer domain (So R is commutative with 1 and R has no zero divisors), then every prime in R is irreducible.
Proof:
Let $p \in R$ be prime. (So for all $a, b \in R$, if $p|ab$, then $p|a$ or $p|b$)
Suppose $p = a \cdot b$, where $a, b \in R$. (We need to show that a is a unit or b is a unit)
Since $p = ab$, we have $p|ab$, so either $p|a$ or $p|b$.
Suppose $p|a$, say $a = p \cdot u$ where $u \in R$
Then $p = ab = p \cdot u \cdot b$
$\therefore p - pub = 0$
$\therefore p \cdot 1 - pub = 0$
$\therefore p(1 - ub) = 0$
Since R has no zero divisors and $p \neq 0$, $1 - ub = 0$.
Thus, $u \cdot b = 1$.
So b is a unit.
Similarly, if $p|b$, then a is a unit.
Example:
In $\mathbb{Z}_{12}$, the association classes are $\{0\}, \{1, 5, 7, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{6\}$.
The primes in $\mathbb{Z}_{12}$ are 2 and 3. (and their associates)
Multiplication table here. See picture.
and the reducible elements are

$$3, 4, 6$$

(and associates)
and the irreducible elements are

$$2$$

(and associates) (that is 10)
Note that 3 reduces as

$$3 = 3 \cdot 9 = 3 \cdot 3 \cdot 3 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = \dots$$

Definition:
A **Euclidean domain** (or ED) is an integral domain, R, together with a function, $N : R \setminus \{0\} \to \mathbb{N} = \{0, 1, 2, \dots\}$ (Called the Euclidean norm on R) such that for all $a, b \in R$ with $b \neq 0$)

There exist $q, r \in R$, such that $a = b \cdot q + r$ and either $r = 0$ or $N(r) < N(b)$
Examples:
$\mathbb{Z}$ is a ED with Euclidean norm given by $N(k) = |k|$.
When $\mathbb{F}$ is a field, $\mathbb{F}$ is a ED and any function $N : F \setminus \{0\} \to \mathbb{N}$ is a Euclidean norm.
When $\mathbb{F}$ is a field, the polynomial ring $\mathbb{F}[x]$ is a Euclidean domain with norm given by $N(f) = \deg(f)$.
Definition:
A **principal ideal domain** or PID is an integral domain in which every ideal is principal.
Every Euclidean domain is a principal ideal domain.

31 November 25th

$a|b$ when $b = ac$ for some c.
$a|b \iff b \in (a) \iff (b) \subseteq (a)$
$a \sim b$ when $a|b$ and $b|a \iff (a) = (b)$
We say that a is irreducible when a is a non-zero, non-unit and $a = b \cdot c \iff$ b is a unit or c is a unit
a is **prime** when a is a non-zero, non-unit and $a|bc \Rightarrow (a|b$ or $a|c)$
R is a Euclidean Domain when R is an integral domain with a function $N : R\ \{0\} \to \mathbb{N}$ (called a Euclidean Norm on R) such that for all $a, b \in R$, with $b \neq 0$. There exists a quotient remainder, $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.
R is a principal ideal domain when R is an integral domain and every ideal is a principal ideal. (For every ideal A in R, $A = \langle a \rangle$ for some $a \in R$).
Example:
$\mathbb{Z}, \mathbb{Z}_n, \mathbb{F}, \mathbb{F}[x]$
$\mathbb{Z}[x]$ is not a P.I.D.
For example,

$$\langle 2, x \rangle = \{f(x) = \sum_{k=0}^{n} c_k x^k | c_0 \text{ is even}\}$$

is not principal.
Example:
$F[x, y]$ is not a PID
For example,

$$\begin{aligned}\langle x, y \rangle &= \{f(x, y) = \sum c_{k,l} x^k y^l | c_{0,0} = 0\} \\ &= \{f \in F[x, y] | f(0, 0) = 0\}\end{aligned}$$

is not principal.
A **unique factorization domain**, or a U.F.D, is an integral domain R in which

1. Every non-zero, non-unit $a \in R$ can be written as a product

$$a = a_1 a_2 \dots a_l$$

where $l \in \mathbb{Z}^+$ and each a_i is irreducible.

2. For $a \in R$, if $a = a_1 a_2 \dots a_l = b_1 b_2 \dots b_m$ where $l, m \in \mathbb{Z}$ and each a_i and b_j is irreducible. Then $l = m$, and there is a permutation $\sigma \in S_l$ such that $a_k \sim b_{\sigma(k)}$ for all k. (Up to order and up to association.)

Example:
$\mathbb{Z}$ is a UFD when $\mathbb{F}$ is a field. $\mathbb{F}[x]$ is a UFD.
$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3}i | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ is not a UFD.
Example:

$$(1 + \sqrt{3}i)\left(1 - \sqrt{3}i\right) = 4 = 2 \cdot 2$$

and $1 \pm \sqrt{3}i$ and 2 are irreducible because if we define $N(u) = ||u||^2$ for $u \in \mathbb{Z}[\sqrt{3}i]$.
So $N(a + b\sqrt{3}i) = a^2 + 3b^2 \in \mathbb{N}$
Then $N(uv) = N(u) \cdot N(v)$.
So $u = 0 \iff N(u) = 0$
u is a unit $\iff N(u) = 1$.
If w is reducible with $w = u \cdot v$, with u, v non-units. Then $N(w)$ is composite with $N(w) = N(u)N(v)$
So if $1 \pm \sqrt{3}$ or 2 were reduced, they would necessarily factor into elements of norm 2, and there are no such elements in $\mathbb{Z}[\sqrt{3}i]$.
Also, $1 \pm \sqrt{3}i$ and 2 are not associates since association differ by multiplication by a unit and the only units are ± 1.
Our goal is to show that every Euclidean Domain (ED) is a principal ideal domain (PID), and that every PID is a UFD.
Theorem:
Every Euclidean Domain (ED) is a principal ideal domain (PID).
Proof:
Let R be a Euclidean Domain with $N : R \setminus \{0\} \to \mathbb{N}$.
Let A be an ideal in R.
If $A = \{0\}$, then $A = (0)$
Suppose $A \neq \{0\}$. Choose an element in the ideal, $0 \neq u \in A$ of smallest possible norm.
(Using Well-Ordering Property).
We claim that the ideal is generated by 1 element, $A = (a)$.
Since $a \in A$, we have $(a) \subseteq A$.
Write $b = q \cdot a + r$ with $r = 0$ or $N(r) < N(a)$.
Since $r = b - q \cdot a \in A$ as $b \in A$
We cannot have $N(r) < N(a)$ as we chose a to be the minimum.
So we must have $r = 0$.
Thus, $b = q \cdot a \in (a)$.

and so $A \subseteq (a)$.
Example:
Determine whether $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ is a PID but not a ED. (using any norm).
To prove that every PID is a UFD. We use two lemmas.
Definition:
A ring, R is called **Noetherian** when it has the property that for any ascending chain of ideals

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$$

in R, there exists $n \in \mathbb{Z}^+$ such that $A_k = A_n$ for all $k \geq n$.
Lemma I:
Every PID is Noetherian.
Proof:
Let $a_1, a_2, a_3 \in R$ with

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

Note that $\bigcup_{k=1}^{\infty}(a_k)$ is an ideal.
Choose $a \in R$ so that $\bigcup_{k=1}^{\infty}(a_k) = (a)$.
Since $a \in \bigcup_{k=1}^{\infty}(a_k)$, we have $a \in (a_n)$ for some $n \in \mathbb{Z}$.
Then, for $k \geq n$, we have $(a_k) \subseteq \bigcup_{j=0}^{\infty}(a_j) = (a) \subseteq (a_n) \subseteq (a_k)$
and so $(a_k) = (a_n)$.
Remind: In an integral domain, every prime element is irreducible.
Lemma II:
Let R be a PID. Let $a \in R$.

1. If a is irreducible then (a) is maximal amongst proper ideals. (This means that for $b \in R$, if $(a) \subseteq (b) \subseteq R$. (If and only if statement. Prove the other direction for yourself. Converse might need non-unit and non-zero?) Then, either $(b) = (a)$ or $(b) = R$.)

2. If a is irreducible, then a is prime.

Proof:
Let $a \in R$ be irreducible. Since a is a non-zero, non-unit. $(a) \neq \{0\}$ and $(a) \neq R$.
Let $b \in R$ with $(a) \subseteq (b) \subseteq R$.
Since $(a) \subseteq (b)$, we have $b|a$, say $a = b \cdot c$ with $c \in R$.
Since a is irreducible, either b is a unit or c is a unit.
If b is a unit, then $(b) = R$.
If c is a unit, then since $a = b \cdot c$, we have $a \sim b$.
So $(a) = (b)$.
Part 2 as an exercise.

32 November 27th

If R is a Euclidean Domain.
Every Euclidean Domain is a principal ideal domain.
Lemma II
Proof:
Let $a \in R$, a irreducible.
Let $b, c \in R$ with $a|bc$.
Suppose $a \not| b$, so $b \notin (a)$.
Then $(a) \subset (a) + (b) = \{ar + bs | r, s \in R\}$
Since a is irreducible, by Part (1), (a) is maximal amongst proper ideals in R.
So $(a) + (b) = R$.
In particular, $1 \in (a) + (b) = \{ar + bs | r, s \in R\}$
Say $1 = ar + bs$.
Then $c = c \cdot 1 = c(ar + bs) = a \cdot cr + bc \cdot s \in (a)$
As $a \in (a)$ and $bc \in (a)$ since $a|bc$.
Since $c \in (a)$, we have $a|c$.
Thus, a is prime.
Theorem:
Every PID is a UFD.
Proof:
Let R be a PID. Let $a \in R$ be a non-zero, non-unit.
We claim that a has an irreducible factor in R.
Let $a \in R$ be a non-zero, non-unit.
If a is irreducible, then we are done since $a|a$.
Suppose that a is reducible, say $a = a_1 b_1$ where a_1 and b_1 are non-units.
Note that $(a) \subset (a_1)$ indeed since $a_1 | a$, we have $(a) \subset (a_1)$ and since b_1 is not a unit.
a and a_1 are not associates.
(If we had $a \sim a_1$, say $a = a_1 \cdot u$ where u is a unit, then since $a = a_1 b_1$, so $a_1 u = a_1 b_1$, so $b_1 = u$ by cancellation.)
If, a_1 is irreducible, we are done. (since $a_1 | a$).
Suppose a_1 is reducible, say that $a_1 = a_2 b_2$ where a_2 and b_2 are non-units.
Note that as above, $(a_1) \subset (a_2)$.
If a_2 is irreducible, we are done, and otherwise we repeat the procedure above.
The procedure has to end afte finitely many steps because the ring is Noetherian. (by Lemma I).
and

$$(a) \subset (a_1) \subset (a_2) \subset \dots$$

We next claim that we can factor non-zero, non-units completely into irreducibles.
We can write $a = a_1 a_2 \dots a_l$ for some $l \in \mathbb{Z}^+$ and some irreducible elements $a_i \in R$.
If a is already irreducible, then there is nothing to prove. (Since $a|a$)

Suppose a is reducible, by our previous claim, we can choose an irreducible factor a_1 of a.
Say $a = a_1 \cdot b_1$.
Note that b_1 cannot be a unit. (Since if b_1 was a unit, we could have $a \sim a_1$, but a is reducible and a_1 is not.)
As above, we have

$$(a) \subset (b_1)$$

If b_1 is irreducible, we are done. (Taking $a_2 = b_1$)
Suppose that b_1 is reducible, choose an irreducible factor, a_2 of b_1 and write $b_1 = a_2 b_2$
As above, b_2 must be a non-unit.
And we have $(b_1) \subset (b_2)$, if b_2 is irreducible, we are done. (Taking $a_3 = b_2$ so $a = a_1 a_2 a_3$)
Otherwise, repeat.
The procedure must end after finitely many steps because R is Noetherian.
Finally, we claim that if $a = a_1 a_2 \dots a_l = b_1 b_2 \dots b_m$ where $l, m \in \mathbb{Z}^+$, and each a_i and each b_j is irreducible, then $l = m$. and after reordering the b_j, if necessary, we have $a_i = b_i$ for all $1 \leq i \leq l$.
Since a_1 is irreducible, by Lemma II, it is also prime.
Since $a_1 | a$, that is $a_1 | b_1 b_2 \dots b_m$, by the prime property and induction, we must have $a_i | b_j$ for some j.
After reordering, we can say that $a_1 | b_1$.
Because b_1 is irreducible, by the definition of irreducible, we cannot factor this into non-zero, non-units.
The only factors of b_1 are the units in R and the associates of b_1 in R.
Since a_1 is not a unit, and $a_1 | b_1$, $a_1 \sim b_1$, say $b_1 = a_1 \cdot u$ where u is a unit in R.
Then

$$\begin{aligned} a_1 a_2 \dots a_l &= b_1 b_2 \cdots b_m \\ &= a_1 u \cdot b_2 \cdot b_3 \dots b_m \end{aligned}$$

So $a_2 a_3 \dots a_l = u \cdot b_2 \cdot b_3 \dots b_m$
By cancellation, (and ub_2 is irreducible).
By a suitable induction hypothesis, the proof is done. $l = m$, after reordering, $a_i \sim b_i$ for $2 \leq i \leq l = m$.
Examples:
To study the problem of whether the ring

$$\mathbb{Z}[\sqrt{d}i] \text{ is a UFD}$$

where $d \in \mathbb{Z}^+$, it is useful to consider the , field norm on $\mathbb{Q}[\sqrt{d}i]$ given by $N(z) = ||z||^2$, that is $N(a + b\sqrt{d}i) = a^2 + db^2 \in \mathbb{Q}$
Note that for $z \in \mathbb{Q}[\sqrt{d}i]$ (or even for $z \in \mathbb{C}$, $z = 0 \iff N(z) = 0$)
For $z, w \in \mathbb{Q}[\sqrt{d}i]$ (or for $z, w \in \mathbb{C}$)

$$N(zw) = N(z) \cdot N(w)$$

For $z \in \mathbb{Z}[\sqrt{d}i]$, $N(z) \in \mathbb{N}$.
It follows that for $z \in \mathbb{Z}[\sqrt{d}i]$, z is a unit $\iff N(z) = 1$.
Examples:
We already used that above field norm to show that $\mathbb{Z}[\sqrt{3}i]$ is **not** a UFD.

$$(1+\sqrt{3}i)(1-\sqrt{3}i) = 4 = 2 \cdot 2$$

and $1 \pm \sqrt{3}i$ and 2 are irreducible.
And $1 \pm \sqrt{3}i$ and 2 are not associates.

$$1 \pm \sqrt{3}i \not\sim 2$$

.
Picture here.
Example:
Show that $\mathbb{Z}[\sqrt{2}i]$ is a ED (hence also a PID and UFD).
And the field norm

$$N(z) = ||z||^2$$

is also a Euclidean norm.
Solution:
Let $z, w \in \mathbb{Z}[\sqrt{2}i]$ with $w \neq 0$.

$$z = w \cdot q + r$$
$$N(r) < N(w)$$

We have $\frac{z}{w} \in \mathbb{Q}(\sqrt{2}i)$
Say $\frac{z}{w} = x + y \cdot \sqrt{2}i$ with $x, y \in \mathbb{Q}$,
Choose $a, b \in \mathbb{Z}$ with

$$|x-a| \leq \frac{1}{2}$$

and

$$|y-b| \leq \frac{1}{2}$$

Let $q = a + b\sqrt{2}i$, and $r = z - wq$.
Then

$$\begin{aligned}
N(r) = ||r||^2 &= ||z - wq||^2 \\
&= ||w||^2 ||\frac{z}{w} - q||^2 \\
&= ||w||^2 ||(x-a) + (y-b)\sqrt{2}i||^2 \\
&\leq ||w||^2 \left(||x-a||^2 + 2||y-b||\right) \\
&\leq ||w||^2 \left(\frac{1}{4} + \frac{2}{4}\right) \\
&= \frac{3}{4}||w||^2 \\
&= \frac{3}{4}N(w)^2
\end{aligned}$$

So $N(r) < N(w)$.
Exercise:
Show that $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ is a PID but not a ED.

33 November 29th

Example: $\mathbb{Z}[x]$ are $\mathbb{F}[x, y]$ are UFD's but not a PID's.
(The proof that $\mathbb{Z}[x]$ and $\mathbb{F}[x, y]$ are UFD's is at the end of the last chapter.)
Examples:
Show that $R = \mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ is a PID but not a ED.
Solution:
Suppose for a contradiction, that $R = \mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ is a ED with Euclidean norm $N : R \setminus \{0\} \to \mathbb{N}$.
Remark:
If all the non-zero elements in R were units, then R would be a field, so it would be a ED.
We can draw a picture of the ring.
Picture here.
Check that the only units in R are ± 1
Choose a non-zero, non-unit $a \in R$, $a \notin \{0, \pm 1\}$ of smallest possible Euclidean norm.
By the definition of a Euclidean norm for all $x \in R$, we can choose $q = q(x), r = r(x) \in R$ such that $x = q \cdot a + r$ with $r = 0$ or $N(r) < N(a)$.
Taking $x = 2$, we see that there exists

$$2 = qa + r$$

for some $q \in R$ and some r with $r = 0$ or $N(r) < N(a)$
By our choice of a, we must have $r \in \{0, \pm 1\}$, so $qa = 2 + r$ with $r \in \{0, \pm 1\}$, that is $q \cdot a \in \{1, 2, 3\}$
Since a divides one of the elements $1, 2, 3$, we must have

$$a = \pm 1, \pm 2, \pm 3$$

and $a \neq \pm 1$ so $a \in \{\pm 2, \pm 3\}$.
Taking $x = \frac{1+\sqrt{19}i}{2}$, we have

$$\frac{1+\sqrt{19}i}{2} = qa + r$$

for some $r \in \{0, \pm 1\}$.
So $qa = \frac{1+\sqrt{19}i}{2} - r$ for some $r \in \{0, \pm 1\}$, that is

$$q \cdot a \in \{\frac{-1+\sqrt{19}i}{2}, \frac{1+\sqrt{19}i}{2}, \frac{3+\sqrt{19}i}{2}\}$$

So a must have a factor of one of the elements

$$\frac{-1 \pm \sqrt{19}i}{2}, \frac{1+\sqrt{19}i}{2}, \frac{3+\sqrt{19}i}{2}$$

But $\pm 2, \pm 3$ are not factors (Since $||\frac{-1+\sqrt{19}i}{2}||^2 = ||\frac{1+\sqrt{19}}{2}||^2 = 5$ and $||\frac{3+\sqrt{19}i}{2}||^2 = 7$)
This gives the desired contradiction.
We sketch a proof that $R = \mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ is a PID.
Let A be any ideal in R.
If $A = \{0\}$, then $A = (0)$.
Suppose $A \neq \{0\}$
Choose a non-zero element $0 \neq a \in A$ of smallest possible field norm $||a||^2$.
We claim that $A = (a)$.
Since $a \in A$, we have $(a) \subseteq A$.
Let $b \in A$ be arbitrary.
Picture here.
By adding an integer multiple of a and $\frac{1+\sqrt{19}i}{2}a$ to b.
We obtain a point $c \in A$ which lies in the parallelogram with vertices at $0, a\frac{1+\sqrt{19}i}{2}a, \frac{3+\sqrt{19}i}{2}a$.
Also, $c - 0, c - a, c - \frac{1+\sqrt{19}i}{2}a$ and $c - \frac{3+\sqrt{19}i}{2}a \in A$.
By our choice of a, if c is not equal to one of these vertices, then

$$||c - v||^2 < ||a||^2$$

for all 4 vertices v.
If $c \neq v$ for any of the four v, then c must lie in the shaded region.
Picture here.
Thus, $2c \in A$ lies in the larger shaded region.
But all the points in the larger shaded region close to one of the points.

$$1 + \sqrt{19}i/2, 3 + \sqrt{19}i/2, 5 + \sqrt{19}i/2$$

to within a distance of $||a||$.
Picture here.
Thus, if c is not one of the vertices of the parallelogram, $2c$ would be equal to one of the point

$$\frac{1+\sqrt{19}i}{2}a, \frac{3+\sqrt{19}i}{2}a, \frac{5+\sqrt{19}i}{2}a$$

So that

$$c = \frac{1+\sqrt{19}i}{4}a, \frac{3+\sqrt{19}i}{4}a, \frac{5+\sqrt{19}i}{4}a$$

Play with these points to obtain a contradiction.
Note:
To study rings of the form $\mathbb{Z}[\sqrt{d}i]$ with $d \in \mathbb{Z}^+$, it is useful to make use of the "field norm".

In $\mathbb{Q}[\sqrt{d}i]$ given by $N(z) = ||z||^2$, that is

$$N(a + b\sqrt{d}i) = a^2 + db^2$$

To study rings $\mathbb{Z}[\sqrt{d}]$ where $d \in \mathbb{Z}^+$ (with d not a perfect square.)
It is useful to use the "field norm" in $\mathbb{Q}[\sqrt{d}]$ given by $N(a + b\sqrt{d}) = a^2 - db^2$ (or by $N(a + b\sqrt{d}) = |a^2 - db^2|$)

34 December 2nd

Remark:
In a ring, R,

$$a \sim b \iff (a) = (b)$$

$$a|b \iff (b) \subseteq (a)$$

m is irreducible, $\iff$ (m) is maximal amongst proper principal ideals.
P is prime $\iff$ $p|ab \Rightarrow p|a$ or $p|b$

$$(a)(b) = (ab) \subseteq (q) \Rightarrow ((a) \subseteq (p) \text{ or } (b) \subseteq (p))$$

Definition:
Let R be a commutative ring with 1.

1. For ideals A and B in Rsometimes we write $A|B$ when $B \subseteq A$.
2. For an ideal M in R, we say that M is maximal when it is maximal amongst all proper ideals, that is $M \subset R$ and for all ideals A in R.

   If $M \subseteq A \subseteq R$, then either $A = M$ or $A = R$.
3. For a proper ideal P in R, we say that P is prime when $P \subset R$ and for all ideals A, B in R.

   If $AB \subseteq P$, then either $A \subseteq P$ or $B \subseteq P$.

Note:
For an ideal P with a commutative ring with 1, P is prime ideal if and only if P has the property that for all $a, b \in R$, if $a \cdot b \in P$, then ($a \in P$ or $b \in P$).
Proof:
Suppose P be a prime ideal in R, let $a, b \in R$ with $a \cdot b \in P$.
Then

$$(a)(b) = (ab) \subseteq P$$

(Commutative used here)
So since P is prime, either $(a) \subseteq P$ or $(b) \subseteq P$.
If $(a) \subseteq P$, then $a \in P$ while if $(b) \subseteq P$, then $b \in P$.
Conversely, let P be any proper ideal and suppose that for all $a, b \in R$, if $ab \in P$, then ($a \in P$ or $b \in P$).
Let A and B be ideals in R with $AB \subseteq P$.

Suppose $A \not\subseteq P$ and choose $a \in A$ with $a \notin P$.
Let $b \in B$ be arbitrary.
Then $a \cdot b \in AB \subseteq P$.
Then either $a \in P$ or $b \in P$.
But $a \notin P$, so $b \in P$.
Thus, $B \subseteq P$ as required.
Theorem:
Let R be a commutative ring with 1.

1. For an ideal $M \in R$, M is maximal iff $R|M$ is a field.
2. For an ideal P in R, P is prime iff $R|P$ is an integral domain.

Proof:

1. Suppose M is maximal.

   Since $M \subset R$, we have $a \notin M$.

   So $1 + M \neq 0 + M$ in $R|M$.

   Since R is commutative, so is $R|M$, let $a \in R$ with $a \notin M$ so that $a+M \neq 0 + M \in R|M$.

   Since $a \notin M$, we have

   $$M \subset M + (a) = \{m + ar | r \in R, m \in M\}$$

   Because M is maximal, we have $M + (a) = R$.

   So in particular, $1 \in M + (a)$, so we can say

   $$1 = m + a \cdot r$$

   where $m \in M, r \in R$.

   Then, we have
   $$ar + M = 1 + M$$

   That is,
   $$(a + M)(r + M) = 1 + M$$

   and so $a + M$ is invertible (with inverse $r + M$).

   Suppose, conversely, that $R|M$ is a field.

   Since $0 + M \neq 1 + M$ in $R|M$.

   We have $1 \notin M$ so $M \subset R$.

   Let A be any ideal in R with $M \subset A$, we need to prove that $A = R$.

   Since $M \subset A$, we can choose $a \in A$ with $a \notin M$, then $a + M \neq 0 + M \in R|M$.

   So $a + M$ has an inverse in $R|M$.

Say

$$(a + M)(b + M) = 1 + M$$

where $b \in R$.

Then

$$ab + M = 1 + M$$

So $1 - ab = m$ for some $m \in M$, hence $1 = ab + m \in A$. (Since $a \in A$ so $a \cdot b \in A$ and $m \in M \subseteq A$)

Since $1 \in A$, we have $A = R$, as required.

2. Let P be an ideal in R.

   Suppose $R|P$ is an integral domain. (No zero divisors).

   Since $R|P$ is an integral domain,

   $$0 + P \neq 1 + P$$

   So $1 \notin P$.

   Hence $P \subset R$.

   Let $a, b \in R$ with $ab \in P$.

   Since $ab \in P$, $ab + P = 0 + P \in R|P$

   $$(a + P)(b + P) = 0 + P \in R|P$$

   Since $R|P$ has no zero divisors, we can say that either the element $a+P = 0 + P$ or $b + P = 0 + P$ in $R|P$.

   Hence, either $a \in P$ or $b \in P$.

   Thus, P is prime.

   Converse is left as a exercise.

Example:
When $\mathbb{F}$ is a field, and $f \in \mathbb{F}[x]$ is irreducible (in the polynomial ring $\mathbb{F}[x]$)
$\mathbb{F}[x]$ is a E.D. (Hence a PID)
Since f is irreducible,

$$(f) \text{ is maximal amongst proper principal ideals}$$

Hence among proper ideals, so (f) is a maximal ideal in $\mathbb{F}[x]$.
Thus, $\mathbb{F}[x]/\langle f \rangle$ is a field.
(If a is a root of $f(x)$ in a bigger field, then $\mathbb{F}(a) = \mathbb{F}[a] \cong \mathbb{F}[x]/(a)$)
Example:
Photo here.
$\mathbb{Z}[\sqrt{3}i]$ is not a UFD.
For example,

$$(1 + \sqrt{3}i)(1 - \sqrt{3}i) = 4 = 2 \cdot 2$$

and $1 \pm \sqrt{3}i$ and 2 are irreducible and $1 \pm \sqrt{3}i$ are not associates of 2.
But $\mathbb{Z}[\sqrt{3}i] \subseteq \mathbb{Z}[\frac{1+\sqrt{3}i}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{3}i}{2}]$ is a ED with Euclidean norm

$$N(z) = ||z||^2$$

In $\mathbb{Z}[\sqrt{3}i]$, we have $1 \pm \sqrt{3}i \sim 2$.
Example:
$\mathbb{Z}[\sqrt{5}i]$ is not a UFD

$$(1 + \sqrt{5}i)(1 - \sqrt{5}i) = 6 = 2 \cdot 3$$

2 is irreducible. (2) is maximal among principal proper ideals.
But

$$(2) \subset (2, 1 + \sqrt{5}i)$$

Verify that $\left(2, 1 + \sqrt{5}i\right)\left(2, 1 + \sqrt{5}i\right) = (2)$.