Abstract Algebra Notes

Definition. A **map** $f : A \to B$ is a subset $f \subset A \times B$ such that for all $a \in A$, there exists a $b \in B$ such that b is unique with $(a, b) \in f$.

Definition. We write $f(a) = b$ if $(a, b) \in f$. A is the **domain** of f and B is the **codomain**.

Definition. A **binary operation** on A is a map $\star : A \times A \to A$ such that $\star(a_1, a_2) = a_1 \star a_2$ for $a_1, a_2 \in A$.

Definition. A binary operation $\star$ is **associative** on A if for all $a, b, c \in A$, $a \star (b \star c) = (a \star b) \star c$.

Definition. An element $e \in A$ is an **identity** element of $\star$ if for each $a \in A$, $e \star a = a \star e = a$.

Definition. An element $a \in A$ has an **inverse** under $\star$ if there exists a $b \in A$ such that $a \star b = b \star a = e$.

Definition. A set A with an associative binary operation $\star$ is a **group** if A has an identity element under $\star$ and every $a \in A$ has an inverse.

Definition

A group is a pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G such that

1. For all $a, b, c \in A$, $a \star (b \star c) = (a \star b) \star c$.
2. There exists an $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.
3. For all $a \in G$, there exists a $b \in G$ such that $a \star b = b \star a = e$.

Definition. A group $(G, \star)$ is **abelian** or commutative if for all $g, h \in G$, $g \star h = h \star g$.

Theorem

Let $(G, \star)$ be a group.

1. e is unique.
2. g^{-1} is unique.
3. $\forall g \in G, \left(g^{-1}\right)^{-1} = g$.
4. $\forall g, h \in G, (g \star h)^{-1} = h^{-1} \star g^{-1}$.

Proof

We may prove each part separately.

1. Suppose e, e' are identity elements. Then for all $a \in G$,

$$a \star e = e \star a = a \tag{i}$$
$$a \star e' = e' \star a = a \tag{ii}$$

By (i), $e' = e \star e'$ and by (ii), $e = e \star e'$. Therefore, $e = e'$.

2. Supposed $a \star b = b \star a = e$, then

$$\begin{aligned} b &= b \star e \\ &= b \star (a \star a^{-1}) \\ &= (b \star a) \star a^{-1} \\ &= e \star a^{-1} \\ &= a^{-1} \end{aligned}$$

Thus, $b = a^{-1}$.

3. $g^{-1} \star \left(g^{-1}\right)^{-1} = e = g^{-1} \star g$. By (ii), $g = \left(g^{-1}\right)^{-1}$.

4. Consider $(a \star b) \star (b^{-1} \star a^{-1})$.

$$\begin{aligned} (a \star b) \star (b^{-1} \star a^{-1}) &= a \star (b \star b^{-1}) \star a^{-1} \\ &= a \star e \star a^{-1} \\ &= a \star a^{-1} \\ &= e \end{aligned}$$

Thus, $(b^{-1} \star a^{-1}) = (a \star b)^{-1}$.

Definition. Let $[n] = \{1, 2, \ldots, n\}$. The **symmetric group** denoted S_n of degree n is the set of all bijections on $[n]$ under the operation of composition.

$$S_n = \{\sigma : [n] \to [n] \mid \sigma \text{ is a bijection}\}$$

Definition. The **order** of $(G, \star)$ is the number of elements in G denoted $|G|$.

Definition. Let $n \geq 2$. The **dihedral group** of index n is the group of all symmetries of a regular polygon P_n with n vertices in the Euclidean plane.

Symmetries of P_n consist of rotations and reflections.

Choose a vertex v. Let L_0 be the line from the center of P_n through v. Let L_k be L_0 rotated by $\frac{\pi k}{n}$ for $1 \leq k \leq n$. Let σ_k be a reflection about L_k. Let ρ_k be a rotation about $\frac{2\pi k}{n}$, $1 \leq k \leq n$.

Definition. A subset $S \subseteq G$ of a group $(G, \star)$ is a set of **generators**, denoted $\langle S \rangle = G$, if and only if every element of G can be written as a finite product of elements of S and their inverses.

Definition. Any equation satisfied by generators is called a **relation**.

Definition. A **presentation** of G, denoted $\langle S \mid R \rangle$, is a set of generators of G and relations such that any other relation can be derived by those given.

Example.

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

Definition. The cycles $\sigma = (\sigma_1 \; \sigma_2 \; \dots \; \sigma_n)$ and $\tau = (\tau_1 \; \tau_2 \; \dots \; \tau_n)$ are **disjoint** if $\sigma_i \neq \tau_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

Definition. A cycle of length 2 is called a **transposition**.

Definition. An expression of the form $(a_1 \; a_2 \; \dots \; a_m)$ is called a **cycle of length m** or an **m-cycle**.

Proposition. Let $\alpha = (a_1 \; a_2 \; \dots \; a_m)$ and $\beta = (b_1 \; b_2 \; \dots \; b_n)$. If $a_i \neq b_j$ for any i, j, then $\alpha\beta = \beta\alpha$.

Proposition. Every permutation can be written as a product of disjoint cycles.

Proposition. A cycle of length n has order n.

Proposition. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be disjoint cycles. Then,

$$|\alpha_1 \alpha_2 \dots \alpha_n| = \operatorname{lcm}(|\alpha_1|, |\alpha_2|, \dots, |\alpha_n|)$$

Proposition. Every permutation is S_n is a product of 2-cycles (which are not necessarily disjoint).

Proposition. If $\alpha = \beta_1 \beta_2 \dots \beta_r = \gamma_1 \gamma_2 \dots \gamma_s$ where β_i, γ_j are transpositions, then r and s have the same parity.

Definition. If r and s are both odd, α is called an **odd permutation**. If r and s are both even, α is called an **even permutation**.

Definition. The set of even permutations in S_n form a group called the **alternating group**, denoted A_n.

Note. $|A_n| = \frac{n!}{2}$ for $n > 1$.

> **Definition**
>
> Let $(G, \star)$ and $(G', *)$ be groups. A map of sets $\varphi : G \to G'$ is a **group homomorphism** if for all $a, b \in G$,
>
> $$\varphi(a \star b) = \varphi(a) * \varphi(b)$$

Example. The following are two very simple examples of homomorphisms.

Trivial Homomorphism

$$\varphi : G \to G', \varphi(g) = e, \forall g \in G$$

Identity Homomorphism

$$\varphi : G \to G', \varphi(g) = g, \forall g \in G$$

Definition. If $\varphi : G \to G'$ is a homomorphism, the **domain** of φ is $\mathrm{Dom}(\varphi) = G$, the **codomain** of φ is $\mathrm{Codom}(\varphi) = G'$, the **range** or **image** of φ is $\varphi(G) = \{\varphi(g) : g \in G\} \subseteq G'$ denoted $\mathrm{Range}(\varphi)$ or $\mathrm{Im}(\varphi)$.

> **Definition**
>
> A homomorphism which is bijective is called an **isomorphism**.

$\varphi : G \to G'$ is an isomorphism if and only if there exists $\psi : G' \to G$ such that ψ is a homomorphism and $\varphi \circ \psi = 1_{G'}$, $\psi \circ \varphi = 1_G$, i.e. ψ is an inverse homomorphism to φ. We say G is isomorphic to G' by $G \cong G'$ or $\phi : G \xrightarrow{\sim} G'$.

> **Definition**
>
> Let $(G, \star)$ be a group. A subset $H \subseteq G$ is a **subgroup** if $(H, *)$ is also a group.

If $H \neq \emptyset$ and $H \subseteq G$, $H \leq G$ or H is a subgroup of G if and only if

1. H is closed under $\star$ ($\forall h_1, h_2 \in H, h_1 \star h_2 \in H$).
2. H is closed under inverses ($h \in H \Rightarrow h^{-1} \in H$).

Note. The following is notation for arbitrary and abelian groups.

$$x \star y \to xy \text{ for arbitrary } G, x + y \text{ for abelian } G$$
$$e \to 1 \text{ for arbitrary } G, 0 \text{ for abelian } G$$

For an arbitrary subset $A \subseteq G$, and $g \in G$,

$$gA = \{ga : a \in A\} \qquad Ag = \{ag : a \in A\} \qquad gAg^{-1} = \{gag^{-1} : a \in A\}$$

> **Theorem** (Subgroup Criterion)
>
> Let $\emptyset \neq H \subseteq G$, $H \leq G$ if and only if $\forall x, y \in H$, $xy^{-1} \in H$.

Definition. Let $A \subseteq G$ be any subset. The **centralizer** of A in G is $C_G(A) = \{g \in G : gag^{-1} = a\}$ and it is the set of elements in G which commute with all elements of A.

Proposition. $C_G(A) \leq G$

Proof. First we show that the centralizer is not empty. $1a = a1 = a$, $\forall a \in A \Rightarrow 1 \in C_G(A)$ $\Rightarrow C_G(A) \neq 0$ so the centralizer of A is not empty. Let $x, y \in C_G(A)$. We want to show that $xy^{-1} \in C_G(A)$ or that $xy^{-1} \in C_G(A)$. We do this by showing that $\left(xy^{-1}\right) a \left(xy^{-1}\right)^{-1} = a$.

$$\begin{aligned}
\left(xy^{-1}\right) a \left(xy^{-1}\right)^{-1} &= xy^{-1}ayx^{-1} \\
&= x\left(y^{-1}ay\right)x^{-1} \\
&= xax^{-1} && (y \in C_G(A)) \\
&= a && (x \in C_G(A))
\end{aligned}$$

Since this subset satisfies the Subgroup Criterion, the centralizer $C_G(A)$ is a subgroup of G.

Definition. The **center** of a group G is denoted $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$. $Z(G) = C_G(G) \leq G$. $Z(G)$ is the set of elements of G which commute with all elements in G. If G is abelian, $Z(G) = G$.

Definition. The **normalizer** of A in G is $N_G(A) = \{g \in G : gAg^{-1} = A\}$ or $\{g \in G : gag^{-1} = a' \in A\}$.

Proposition. $C_G(A) \leq N_G(A) \leq G$

Definition. A **group action** of a group G on a set A is a map $G \times A \to A$ such that $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a), \forall g_1, g_2 \in G, \forall a \in A$ and $1 \cdot a = a, \forall a \in A$. It is denoted $G \circlearrowleft A$.

Definition. Suppose $G \circlearrowleft A$, the stabilizer of $a \in A$ in G is $G_a = \{g \in G : g \cdot a = a\}$. $G_a \leq G$.

Definition

An **equivalence relation** $\mathcal{E}$ on a set S is a subset $\mathcal{E} \subseteq S \times S$ which is reflexive, symmetric, and transitive. We write $(a, b) \in \mathcal{E} \Leftrightarrow a \; \mathcal{E} \; b$ or $a \sim b$.

1. $a \sim a$
2. $a \sim b \Leftrightarrow b \sim a$
3. $a \sim b, b \sim c \Rightarrow a \sim c$

Definition. The **equivalence class** of $a \in S$ is $[a] = \{b \in S : a \sim b\}$

Definition. The **quotient set** of S under $\sim$ is $S/{\sim} = \{[a] : a \in S\}$.

Example. $\mathbb{Q} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}/{\sim}, (a, b) \sim (c, d) \Rightarrow ad = bc.$

Definition. The quotient set comes equipped with the **projection map** $\pi : S \to S/{\sim}$ where $a \mapsto [a] = \pi(a)$. This map is surjective by definition.

Definition

A group G' is a **quotient group** of a group G if

1. $G' = G/{\sim}$, G' is the quotient set of G under an equivalence relation $\sim$.
2. The projection map $\pi : G \to G' = G/{\sim}$ is a group homomorphism.

Definition. Let $\varphi : G \to G'$ be a homomorphism and let $g' \in G'$. The **fiber** over g' is $\varphi^{-1}(g') = \{g \in G : \varphi(g) = g'\}$.

Proposition

All quotient groups come from subgroups.

Proof

Let $\varphi : G \to G'$ be a homomorphism, then φ induces an equivalence relation on G. Let $x \sim y \Leftrightarrow \varphi(x) = \varphi(y)$. But φ is a group homomorphism, so $\varphi(x) = \varphi(y) \Leftrightarrow \varphi(x)\varphi(y)^{-1} = 1_{G'} \Leftrightarrow \varphi(x)\varphi(y^{-1}) = 1 \Leftrightarrow \varphi(xy^{-1}) = 1$. So $x \sim y \Leftrightarrow \varphi(xy^{-1}) = 1$. Let $K = \{g \in G : \varphi(g) = 1\}$. Then $x \sim y \Leftrightarrow xy^{-1} \in K$. Recall $K = \text{Ker}(\varphi) \leq G$.

Let G' be a quotient group of G. Then $x \sim y \Leftrightarrow [x] = [y] \Leftrightarrow \pi(x) = \pi(y)$ where $\pi : G \to G'$ is the projection. But $\pi(x) = \pi(y) \Leftrightarrow xy^{-1} \in \text{Ker}(\varphi)$.

Definition. The **right coset** of a subgroup H of a group G by the element $x \in G$ is $Hx = \{hx : h \in H\}$. The **left coset**, denoted xH is denoted similarly.

Proposition. Let $\varphi : G \to G'$ be a homomorphism and $K = \text{Ker}(\varphi)$. Then $xKx^{-1} \subseteq K, \forall x \in G$.

Proof. We must show $\varphi(xkx^{-1}) = 1_{G'}$ for $x \in G, k \in K$. Then, $\varphi(xkx^{-1}) = \varphi(x)\varphi(k)\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = 1_{G'}$.

Definition

The subgroup $N \leq G$ is **normal** if $xNx^{-1} \subseteq N$ for all $x \in G$. It is denoted $N \trianglelefteq G$.

Proposition. $\text{Ker}(\varphi) \trianglelefteq G$ for any homomorphism $\varphi : G \to G'$.

Theorem

Let $N \leq G$. Then the following are equivalent.

1. $N \trianglelefteq G$ $(xNx^{-1} \subseteq N, \forall x \in G)$
2. $xNx^{-1} = N$
3. $xN = Nx$
4. $\forall x, y \in G,\ xy^{-1} \in N \Leftrightarrow y^{-1}x \in N$

Proof

$(1) \Rightarrow (2)$ Assume $\forall x \in G$, $xNx^{-1} \subseteq N$. We want to show $xNx^{-1} = N$. We do this by showing $N \subseteq xNx^{-1}$. Let $x \in G$, $n_0 \in N$. We show $n_0 \in xNx^{-1}$. Note that $x \in G \Rightarrow x^{-1} \in G$. Thus, $x^{-1}N\left(x^{-1}\right)^{-1} \subseteq N$ since $N \trianglelefteq G$. Thus there exists n such that $x^{-1}nx = n_1 \in N$. $n_0 = x\left(x^{-1}n_0x\right)x^{-1} = xn_1x^{-1} \in xNx^{-1}$.

$(3) \Rightarrow (4)$ Assume $\forall x \in G, xN = Nx$. Let $x, y \in G$. We want to show $xy^{-1} \in N \Leftrightarrow y^{-1}x \in N$. So we must show this is true in both directions. Suppose $xy^{-1} \in N$. Then there exists an $n_1 \in N$ such that $xy^{-1} = n_1$. Thus, $x = n_1y \in Ny = yN$ by assumption. So $x \in yN$. Thus there exists $n_2 \in N$ such that $x = yn_2 \Rightarrow y^{-1}x = n_2 \in N$. Thus, $xy^{-1} \in N \Rightarrow y^{-1}x \in N$. Similarly, $y^{-1}x \in N \Rightarrow xy^{-1} \in N$.

Proposition. Let $H \leq G$. Then, $x \sim y \Leftrightarrow y^{-1}x \in H$ is an equivalence relation on G.

Proof. We want to show $\sim$ is reflexive, symmetric, and transitive.

1. $x \sim x$: $x^{-1}x = 1 \in H$
2. $x \sim y \Rightarrow y \sim x$: $x \sim y \Leftrightarrow y^{-1}x \in H \Rightarrow x^{-1}y \in H \Leftrightarrow y \sim x$
3. $x \sim y, y \sim z \Rightarrow x \sim z$: $y^{-1}x \in H, z^{-1}y \in H \Rightarrow (z^{-1}y)(y^{-1}x) = z^{-1}x \in H \Leftrightarrow x \sim z$

Thus, $\sim$ is an equivalence relation on G.

Any subgroup gives an equivalence relation.

Definition. An equivalence relation on a set S is the same as a **partition** of S. $P = \{A_1, A_2, \ldots\}$, $A_i \subseteq S$ such that $S \cup_{i \in \mathbb{N}} A_i$, $A_i \cap A_j = \emptyset$, $i \neq j$. $a \sim b \Leftrightarrow a, b \in A_i$.

Proposition. For $H \leq G$, $x \sim y \Leftrightarrow y^{-1}x \in H \Leftrightarrow xH = yH$ $(Hx = Hy)$.

Proof. Suppose $y^{-1}x \in H$. We want to show that $xH = yH$ or $xH \subseteq yH$ and $yH \subseteq xH$. $y^{-1}x \in H$ implies that there exists a $h_1 \in H$ such that $y^{-1}x = h_1$. Thus, $x = yh_1 \Rightarrow x \in yH$. $y^{-1}x \in H \Leftrightarrow x^{-1}y \in H$ which implies that there exists a $h_2 \in H$ such that $x^{-1}y = h_2 \Rightarrow y = xh_2 \in xH$.

Note. $[x] = xH$.

Proposition. For $N \leq G$, let $G/N = \{xN : x \in G\}$. Define $xN \cdot yN = (xy)N$. Then G/N is a group if and only if $N \trianglelefteq G$.

$G/N = G/\!\sim (x \sim y \Leftrightarrow xN = yN)$

Every quotient group is G/N for some N.

$\pi : G \to G/\!\sim$, $\text{Ker}(\pi) \trianglelefteq G$, $G/\!\sim = G/\text{Ker}(\pi)$.

Proposition. If $H \leq G$ and G is abelian, then $H \trianglelefteq G$.

If G is a group and $\sim$ is an equivalence relation on G, then the quotient set $G/\sim$ is a quotient group if and only if the projection map $\pi : G \to G/\sim$, $\pi(x) = [x]$ is a homomorphism.

If $N \trianglelefteq G$, then G/N is a quotient group, where $G/N = \{xN : x \in G\}$ and $xN \cdot yN = (xy)N$.

These notions of quotient groups are equivalent.

Proposition. If $\sim$ is an equivalence relation and $G/\sim$ is a quotient group, then there exists a homomorphism $\pi : G \to G/\sim$ and $\text{Ker}(\pi) \trianglelefteq G$.

Proof. $x \sim y \Leftrightarrow \pi(x) = \pi(y) \Leftrightarrow \pi(y^{-1}x) = 1 \Leftrightarrow y^{-1}x \in \text{Ker}(\pi) \Leftrightarrow x\text{Ker}(\pi) = y\text{Ker}(\pi)$.

If $N \trianglelefteq G$, define $x \sim y \Leftrightarrow xN = yN \Leftrightarrow y^{-1}x \in N$. Then, $G/\sim = G/N$, $[x] = xN$, $\pi : G \to G/N$, $\pi(x) = xN$, $\text{Ker}(\pi) = N$.

Proposition. Every subgroup of an abelian group is a normal subgroup.

Definition. $S^n \subseteq \mathbb{R}^{n+1}$, $S^n = \{(x_1, x_2, \ldots, x_{n+1}) : \sum x_i^2 = 1\}$

For $H \leq G$, the relation $x \sim y \Leftrightarrow xH = yH \Leftrightarrow y^{-1}x \in H$ is an equivalence relation and thus partitions G into equivalence classes.

$$G = \bigcup_{x \in G} [x],\ [x] \cap [y] = \emptyset,\ [x] \neq [y]$$

$$G = \bigcup_{x \in G} xH,\ xH \cap yH = \emptyset,\ x \nsim y$$

Proposition. Let $H \leq G$. The number of right cosets of H equals the number of left cosets of H.

Proof. Let $R = \{Hx : x \in G\}$ and $L = \{xH : x \in G\}$. We construct a bijection $L \to R$. Define $f : R \to L$ by $f(Hx) = x^{-1}H$, and define $g : L \to R$ by $g(xH) = Hx^{-1}$. Then f and g are mutually inverse. Hence $R \leftrightarrow L$.

Definition. The number of distinct left cosets of H in G is called the **index** of H in G, and is denoted $[G : H]$.

> **Theorem** (Lagrange's Theorem)
> If H is a subgroup of G, $|G| = |H|[G : H]$.

Corollary. In a finite group, the order of every element divides the order of the group.

Corollary. A group of prime order is cyclic.

Corollary. Let G be a finite group and let $a \in G$. Then, $a^{|G|} = 1$.

Let $\varphi : G \to G'$ be a homomorphism. How far is φ from an isomorphism? How can φ fail to be an isomorphism?

1. φ could fail to be injective. ($\text{Ker}(\varphi) \neq \{1\}$)

2. φ could fail to be surjective.

Theorem (First Isomorphism Theorem)

Let $\varphi : G \to G'$ be a homomorphism. Then $\text{Ker}(\varphi) \trianglelefteq G$, $\text{Im}(\varphi) \leq G'$ and

$$G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$$

Proposition. There exists an isomorphism $\theta : G/\text{Ker}(\varphi) \to \text{Im}(\varphi)$ such that

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"] \arrow[dr, phantom, "\circlearrowright"] & G' \\
G/\text{Ker}(\varphi) \arrow[r, "\theta"] & \text{Im}(\varphi) \arrow[u, hook, "\iota"']
\end{tikzcd}$$

The curved arrow in the middle means the diagram is commutative, i.e. $\varphi = \iota \cdot \theta \cdot \pi$. The curved arrow means it is injective.

Proof. Define $\theta : G/\text{Ker}(\varphi) \to \text{Im}(\varphi)$ by $\theta(x\text{Ker}(\varphi)) = \varphi(x)$.

First we show that θ is well-defined. Suppose $x\text{Ker}(\varphi) = y\text{Ker}(\varphi)$. Then,

$$\begin{aligned}
x\text{Ker}(\varphi) = y\text{Ker}(\varphi) &\Leftrightarrow y^{-1}x\text{Ker}(\varphi) = \text{Ker}(\varphi) \\
&\Leftrightarrow y^{-1}x \in \text{Ker}(\varphi) \\
&\Leftrightarrow \varphi(y^{-1}x) = 1 \\
&\Leftrightarrow \varphi(y)^{-1}\varphi(x) = 1 \\
&\Leftrightarrow \varphi(x) = \varphi(y) \\
&\Leftrightarrow \theta(x\text{Ker}(\varphi)) = \theta(y\text{Ker}(\varphi))
\end{aligned}$$

Thus, θ is well-defined.

Then, we show that θ is a homomorphism. Let $K = \text{Ker}(\varphi)$.

$$\begin{aligned}
\theta(xKyK) &= \theta(xyK) \\
&= \varphi(xy) \\
&= \varphi(x)\varphi(y) \\
&= \theta(xK)\theta(yK)
\end{aligned}$$

Thus, θ is a homomorphism.

Then, we show that θ is injective.

$$\begin{aligned}\theta(xK) = \theta(yK) &\Leftrightarrow \varphi(x) = \varphi(y)\\ &\Leftrightarrow \varphi(y)^{-1}\varphi(x) = 1\\ &\Leftrightarrow \varphi(y^{-1}x) = 1\\ &\Leftrightarrow y^{-1}x \in K\\ &\Leftrightarrow xK = yK\end{aligned}$$

Thus, θ is injective.

Then, we show that θ is surjective. Let $y \in \text{Im}(\varphi)$. There exists $xK \in G/K$ such that $\theta(xK) = y$. We know there exists an $x \in G$ such that $\varphi(x) = y$. $\theta(xK) = \varphi(x) = y$. Thus, θ is surjective and θ is an isomorphism.

Proposition. Let $a \in G$. If $|a| = \infty$, then $\langle a\rangle \cong (\mathbb{Z}, +)$. If $|a| = n$, then $\langle a\rangle = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Proof. Consider $\mathbb{Z} \xrightarrow{\pi} G$ defined by $\pi(k) = a^k$.

Definition. Let $(A, \star)$ and $(B, *)$ be groups. The **direct product** or **direct sum** of A and B is $A \oplus B = \{(a, b) : a \in A, b \in B\}$ where $(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 * b_2) \in A \oplus B$.

Definition. In a group G, define $a \sim b \Leftrightarrow \exists x \in G$ such that $b = xax^{-1}$. This is an equivalence relation and a and b are **conjugates**.

Definition. For any $x \in G$, the **inner automorphism** of G induced by x is $T_x : G \to G$ defined by $T_x(g) = xgx^{-1}$.

Definition. The set of all inner automorphisms of G is a group, called the **inner automorphism group**, and is denoted $\text{Inn}(G) = \{T_x : G \to G \mid x \in G\}$.

Proposition. $G/Z(G) \cong \text{Inn}(G)$

Proof. Consider $\psi : G \to \text{Inn}(G)$ defined by $x \mapsto T_x$. Then, ψ is surjective, i.e. $\text{Im}(\psi) = \text{Inn}(G)$. We then determine the kernel of the homomorphism.

$$\begin{aligned}\text{Ker}(\psi) &= \{x \in G : \psi(x) = 1_G\}\\ &= \{x \in G : T_x(g) = g,\ \forall g \in G\}\\ &= \{x \in G : xgx^{-1} = g,\ \forall g \in G\}\\ &= \{x \in G : xg = gx,\ \forall g \in G\}\\ &= Z(G)\end{aligned}$$

By the first isomorphism theorem, $G/Z(G) \cong \text{Inn}(G)$.

Theorem (Third Isomorphism Theorem)

Let G be a group. Let $A \trianglelefteq G$, $B \trianglelefteq G$. If $A \subseteq B$, then $A \trianglelefteq B$, $B/A \trianglelefteq G/A$, and

$$(G/A)/(B/A) \cong (G/B)$$

Proof

First we establish $A \trianglelefteq B$. $A \leq B$ because $A \leq G$ and $A \subseteq B$.

$$A \trianglelefteq B \Leftrightarrow bAb^{-1} \subseteq A, \ \forall b \in B$$

$$A \trianglelefteq G \Leftrightarrow xAx^{-1} \subseteq A, \ \forall x \in G$$

But $B \subseteq G$ so $b \in G$. Thus, $bAb^{-1} \subseteq A, \forall b \in B$ and $A \trianglelefteq B$. Thus, $A \trianglelefteq B$ and we may construct B/A.

We first show $B/A \leq G/A$. It is closed under multiplication since $(b_1A)(b_2A) = (b_1b_2)A \in B/A$ because B is a group. It is also closed under inverses since $(bA)^{-1} = b^{-1}A \in B/A$.

We then show $B/A \trianglelefteq G/A$ by showing $x(B/A)x^{-1} \subseteq B/A, \forall x \in G/A$. Let $x \in G/A \Leftrightarrow yA$, $y \in G$. We want to show $(yA)(B/A)(yA)^{-1} \subseteq B/A$. Let $z \in (yA)(B/A)(yA)^{-1}$. Then, there exist $a_1, a_2 \in A$, $b_1 \in B$ such that

$$\begin{aligned} z &= (ya_1)(b_1A)(y^{-1}a_2) \\ &= y(a_1b_1)Ay^{-1}a_2 \\ &= y(a_1b_1)y^{-1}Aa_2 \end{aligned}$$

We know $a_2 \in A \Rightarrow Aa_2 = A$ and $A \subseteq B \Rightarrow a_1 \in A \subseteq B \Rightarrow a_1 \in A \Rightarrow a_1b_1 \in B$. Thus, there exists $b_2 \in B$ such that $a_1b_1 = b_2$. We substitute these in to get

$$z = yb_2y^{-1}A$$

We know $B \trianglelefteq G \Rightarrow yBy^{-1} \subseteq B$. Thus, there exists a $b_3 \in B$ such that $yb_2y^{-1} = b_3 \in B$. We then get $z = b_3A$. Since $z = b_3A \in B/A$, $B/A \trianglelefteq G/A$.

Now we prove $(G/A)/(B/A) \cong (G/B)$. We define the homomorphism $\omega : G/A \to G/B$ such that $\omega(xA) = xB$. We show that ω is well-defined. If $xA = yA$, then

$$\begin{aligned} xA = yA &\Leftrightarrow y^{-1}x \in A \subseteq B \\ &\Rightarrow y^{-1}x \in B \\ &\Leftrightarrow xB = yB \\ &\Leftrightarrow \omega(xA) = \omega(yA) \end{aligned}$$

We may then determine the kernel and image of the homomorphism.

$$\text{Im}(\omega) = \{xB : x \in G\} = G/B$$

$$\text{Ker}(\omega) = \{xA : \omega(xA) = B\} = \{xA : xB = B\} = \{xA : x \in B\} = B/A$$

By the first isomorphism theorem, $(G/A)/\text{Ker}(\omega) \cong \text{Im}(\omega)$ so $(G/A)/(B/A) \cong (G/B)$.

Proposition. There is an isomorphism $\theta : (G/A)/(B/A) \to G/B$ such that this diagram commutes.

$$\begin{tikzcd}
 & G/A \arrow[dr, "\sigma"] \arrow[dd, "\omega"] & \\
G \arrow[ur, "\pi"] \arrow[dr, "\rho"'] & & (G/A)/(B/A) \arrow[dl, "\theta"] \\
 & G/B &
\end{tikzcd}$$

Theorem (Second Isomorphism Theorem)

Let G be a group, $A \leq G$, and $N \trianglelefteq G$. Then $AN \leq G$, $N \trianglelefteq AN$, and $A \cap N \trianglelefteq A$. Also,

$$(AN)/N \cong A/(A \cap N)$$

Proof

Let $\varphi : A \to AN/N$ such that $a \mapsto aN$. Then by the first isomorphism theorem, $(AN)/N \cong A/(A \cap N)$.

Example. We look at an example of the third isomorphism theorem. Let $G = \mathbb{Z}$, $A = 12\mathbb{Z}$, and $B = 4\mathbb{Z}$. We observe that $A \trianglelefteq B \trianglelefteq G$ so the conditions for the third isomorphism theorem are satisfied.

$$G/A = \mathbb{Z}/12\mathbb{Z} = \{0, 1, \ldots, 11\} (\text{mod } 12)$$

$$B/A = 4\mathbb{Z}/12\mathbb{Z} = \{0, 4, 8\} (\text{mod } 12)$$

$$(G/A)/(B/A) = \{0, 1, 2, 3\} (\text{mod } 4) = \mathbb{Z}/4\mathbb{Z}$$

$$(\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$$

Example. We look at an example of the second isomorphism theorem. Let $G = \mathbb{Z}$, $N = 12\mathbb{Z}$, and $A = 8\mathbb{Z}$.

$$A \cap N = \{0, (2)\,4, (4)\,8, \ldots\} = 24\mathbb{Z}$$

$$AN = \{0, (4)\,, (8)\,, \ldots\} = 4\mathbb{Z}$$

$$AN/A = 4\mathbb{Z}/12\mathbb{Z} = \{0, 4, 8\} (\text{mod } 12)$$

$$A/(A \cap N) = 8\mathbb{Z}/24\mathbb{Z} = \{0, 8, 16\} (\text{mod } 24)$$

$$AN/N \cong \mathbb{Z}/3\mathbb{Z} \cong A/(A \cap N)$$

Definition

A ring $(R, +, \cdot)$ is a set together with two binary operations, called addition and multiplication respectively, satisfying the following three axioms.

(a) The set $(R, +)$ together with addition is an abelian group.

(b) The binary operation $\cdot$ is associative on R.

(c) The distributive law holds in R; for all $a, b, c \in R$,

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Definition. The ring R is **commutative** if multiplication is commutative.

Definition. The ring R has an **identity**, or **unity** or contains a 1 if there is an element $1 \in R$ such that for all $a \in R$, $1 \cdot a = a \cdot 1 = a$.

Note. By abuse of notation, multiplication $\cdot$ may be denoted by simple juxtaposition, i.e. $a \cdot b = ab$.

Note. For a ring with 1, the condition of commutativity under addition is redundant. Note that for any $a, b \in R$,

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$$
$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b$$

Therefore, $a + b + a + b = a + a + b + b$ and therefore $a + b = b + a$. Thus R is abelian.

Definition. A ring with identity is a **division ring** if every nonzero element has a multiplicative inverse.

Definition

A **field** is a commutative division ring.

Example. The following are two very simple examples of rings.

The Zero Ring

Let $R = \{0\}$. Then R is a ring and is called the zero ring.

Trivial Rings

For any abelian group $(G, +)$, consider the ring $(G, +, \cdot)$, where multiplication is given by $a \cdot b = 0$ for any $a, b \in G$.

Proposition. Let R be a ring, and $a, b \in R$.

(a) $0a = a0 = 0$

(b) $(-a)b = a(-b) = -(ab)$, where $-(a)$ is the additive inverse of a.

(c) $(-a)(-b) = ab$

(d) If R has identity 1, then it is unique and $-a = (-1)a$.

Definition. A nonzero element element a of a ring R is a **zero divisor** if there is a nonzero $0 \neq b \in R$ such that $ab = 0$ or $ba = 0$.

Definition. Let R be a ring with identity. An element a of R is a **unit** if it has a multiplicative inverse, i.e. there is some $b \in R$ such that $ab = ba = 1$. The set of units of R is denoted $R^\times$.

Definition

An **integral domain** is a commutative ring with identity which has no zero divisors.

Proposition. Let R be an integral domain, and let $a, b, c \in R$. If $ab = ac$, then $a = 0$ or $b = c$.

Definition. Let R be a commutative ring with 1. For any $a_0, a_1, \ldots, a_n \in R$, the expression

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

is a **polynomial** in R with coefficients $a_0, a_1, \ldots, a_n$. If $a_n \neq 0$, then $p(x)$ has **degree** n. The set of all polynomials in R is denoted $R[x]$ or R adjoin x. $R[x]$ is a ring (called the ring of polynomials in R in one variable) under ”usual” addition and multiplication. Let $p(x) = a_0 + a_1x + \ldots + a_nx^n$ and $q(x) = b_0 + b_1x + \ldots + b_mx^m$, and without loss of generality $n > m$. Then,

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$$

where $b_k = 0$ for $k > m$ and

$$p(x)q(x) = \sum_{k=0}^{m+n} (\sum_{i+j=k} a_ib_j)x^k$$

Note. Polynomials are not determined by their values

The following is a formal construction of the ring of polynomials in R.

Let R be a commutative ring with 1. $R[x]$ is the set of all tuples $p(x) = (a_0, a_1, \ldots, a_n) \in R^\infty = \prod_{i \in \mathbb{N}} R = \oplus_{i \in \mathbb{N}} R$, i.e. $a_k \in R$ where $\exists n \in \mathbb{N}$ such that $a_k = 0$ for $k > n$. The smallest such n is the degree of $p(x)$. If $p = (a_0, a_1, \ldots, a_n, 0, \ldots)$ and $q = (b_0, b_1, \ldots, b_m, 0, \ldots)$, then

$$p + q = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, 0, \ldots)$$

$$pq = (c_0, c_1, \ldots, c_k, 0, \ldots),\ c_k = \sum_{i+j=k} a_ib_j$$

Definition. Let R be any ring $M_n(R) = \{n \times n$ matrices with entries in $R\}$, $A = (a_{ij})$, $B = (b_{ij})$, $(A + B)_{ij} = a_{ij} + b_{ij}$, $A \cdot B = C$, $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$. This is the ring of **$n \times n$ matrices over R** or with entries in R. If R has 1, then

$$I = \begin{bmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \end{bmatrix} = 1 \in M_n(R)$$

Definition. $GL_n(R)$ is the group of units of $M_n(R)$ and is called the **general linear group**.

Definition. Let R be commutative with 1. Let $G = \{g_1, \ldots, g_n\}$ be a finite group. The **group ring** RG of G with coefficients in R is the set of all formal sums

$$a_1g_1 + a_2g_2 + \ldots + a_ng_n$$

where $a_i \in R$,

$$(a_1g_1 + \ldots + a_ng_n) + (b_1g_1 + \ldots + b_ng_n) = (a_1 + b_1)g_1 + \ldots + (a_n + b_n)g_n$$
$$(a_1g_1 + \ldots + a_ng_n) \cdot (b_1g_1 + \ldots + b_ng_n) = c_1g_1 + \ldots + c_ng_n, \text{ where } c_k = \sum_{g_ig_j = g_k} a_ib_j$$

Note. $1 \cdot g_i = g_i$, $a_i \cdot 1 = a_i$, $(a_ig_i)(b_jg_j) = (a_ib_j)(g_ig_j)$

Example. $G = S_4$, $R = \mathbb{Z}$.

$$x = 2(1\,2) + (2\,3) + 7(1\,2\,4) \qquad\qquad y = 3(1) + 2(2\,3)$$

$$\begin{aligned} x + y &= 3(1) + 2(1\,2) + 3(2\,3) + 7(1\,2\,4) \\ xy &= 6(1\,2) + 4(1\,2)(2\,3) + 3(2\,3) + 2(1) + 21(1\,2\,4) + 14(1\,2\,4)(2\,3) \\ &= 2(1) + 6(1\,2) + 3(2\,3) + 4(1\,2\,3) + 21(1\,2\,4) + 14(1\,2\,3\,4) \end{aligned}$$

Definition

A **subring** S of a ring $(R, +, \cdot)$ is a subgroup $S \leq (R, +)$ which is closed under the multiplicative structure of R.

Proposition. A subset S of the ring R is a subring if and only if S is closed under subtraction and multiplication.

Proof. This follows immediately from the fact that a subset H of an abelian group G is a subgroup if and only if H is closed under subtraction.

Definition. The **center** of a ring A is the set of elements $a \in A$ such that $ax = xa$ for all $x \in A$. The center of A is a subring of A.

Definition

Let R and S be rings. A **ring homomorphism** is a map of sets $\varphi : R \to S$ such that for all $a, b \in R$,

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

Definition. The **kernel** of the homomorphism $\varphi : R \to S$ is given by

$$\text{Ker}(\varphi) = \{r \in R : \varphi(r) = 0 \in S\}$$

Definition. A **ring isomorphism** is a bijective homomorphism.

Definition

A subring I of R is a **left ideal** of R if I is closed under left multiplication by elements from R, i.e. $rI \subseteq I$ for all $r \in R$. Similarly, I is a **right ideal** of R if I is closed under right multiplication by elements of R, i.e. $Ir \subseteq I$ for all $r \in R$. A subring which is both a left and right ideal is called a **two sided ideal**, or simply **ideal**.

Definition

The **quotient ring** R/I of the ring R by the ideal $I \subseteq R$ is the quotient group of cosets R/I under the operations

$$(r+I)+(s+I)=(r+s)+I \qquad (r+I)\cdot(s+I)=(r\cdot s)+I$$

a for all $r, s \in R$.

Proposition. For any ring R and ideal I, R/I is a ring.

Proposition. If I is any ideal of R, the map $\varphi : R \to R/I$ defined by $r \mapsto r+I$ is a surjective ring homomorphism with kernel I.

Theorem (First Isomorphism Theorem for Rings)**.** If $\varphi : R \to S$ is homomorphism of rings, then $\operatorname{Ker}(\varphi)$ is an ideal of R, $\operatorname{Im}(\varphi)$ is a subring of S, and

$$R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$$

Theorem (Second Isomorphism Theorem for Rings)**.** Let R be a ring, A a subring and B an ideal of R. Then $A+B=\{a+b : a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and

$$(A+B)/B \cong A/(A \cap B)$$

Theorem (Third Isomorphism Theorem for Rings)**.** Let I and J be ideals of the ring R such that $I \subseteq J$. Then J/I is an ideal of R/I and

$$(R/I)(J/I) \cong (R/J)$$

Theorem (Fourth Isomorphism Theorem for Rings)**.** Let I be an ideal of R. The correspondence

$$A \longleftrightarrow A/I$$

is an inclusion preserving bijection between the subring A of R containing I and the set of subrings of R/I. Further, a subring A containing I is an ideal of R if and only if A/I is an ideal of R/I.

Definition

Let $A \subseteq R$ be a subset. Then the **ideal generated by** A is the smallest ideal of R containing A, and is denoted (A).

Note. In this context, "smallest" means all other ideals containing A also contain (A). In other words, $A \subseteq J \implies (A) \subseteq J$.

Proposition. (A) is the intersection of all ideal I containing A, or

$$(A) = \bigcap_{A \subseteq I} I$$

Proof. R is an ideal of itself containing A and the intersection of nonempty ideals is an ideal. By definition the intersection contains A. Therefore, $\bigcap_{A\subseteq I} I$ is an ideal containing A. Since (A) is the smallest ideal containing A, $(A) \subseteq \bigcap_{A\subseteq I} I$.

On the other hand, suppose $x \in \bigcap_{A\subseteq I} I$. Then for any ideal I containing A, $x \in I$. But (A) is an ideal containing A. Thus $x \in (A)$. Therefore, $\bigcap_{A\subseteq I} I \subseteq (A)$. Thus, $(A) = \bigcap_{A\subseteq I} I$.

Proposition. If R is commutative, then

$$(A) = RA = AR$$

where

$$RA = \{r_1a_1 + r_2a_2 + \ldots + r_na_n : r_i \in R, a_i \in A, n \in \mathbb{Z}\}$$

and AR is define similarly.

Definition. An ideal generated by a single element is called a **principal ideal**.

Definition. An ideal generated by a finite set is called a **finitely generated ideal**.

Definition. An ideal I of a ring R is **proper** if it is a proper subset, i.e. $I \neq R$ and $I \subsetneq R$.

Definition. A proper ideal M of a ring R is **maximal** if whenever I is an ideal of R and $M \subseteq I \subseteq R$, then $M = I$ or $M = R$.

Example. Consider $(x-4) \in \mathbb{R}[x]$.

$$(x-4) = (\{x-4\}) = \{f(x)(x-4) : f \in \mathbb{R}[x]\}$$

We claim $(x-4)$ is maximal in $\mathbb{R}[x]$. Suppose $(x-4) \subsetneq I \subseteq R$. We want to show $I = R = \mathbb{R}[x]$. There exists $f(x) \in I$ with $f(x) \notin (x-4)$. Recall polynomial long division. $\forall f(x), g(x) \in \mathbb{R}[x], \exists q(x), r(x) \in \mathbb{R}[x]$ such that

$$f(x) = q(x)g(x) + r(x), \deg r(x) < \deg g(x)$$

In our case, $g(x) = (x-4)$, with $\deg r(x) < 1$. This implies that $r(x) = r \in \mathbb{R}$ so we can rewrite our expression as

$$f(x) = q(x)(x-4) + r$$

Since $(x-4) \subsetneq I$, we know $x-4 \in I$ and $q(x)(x-4) \in I$. Since I is a subring, $f(x) - q(x)(x-4) = r \in I$. Since $f(x) \notin (x-4)$ and $q(x)(x-4) \in (x-4)$, $r \neq 0$. Since $0 \neq r \in \mathbb{R}$, r is a unit in $\mathbb{R}[x]$. If $r \in I$ is a unit, then $I = R$ because r being a unit $\implies u^{-1} \in R \implies u^{-1}u \in I \implies 1 \in I \implies \forall r \in R, r1 \in I \implies I = R$. Therefore, $I = \mathbb{R}[x]$ and $(x-4)$ is maximal.

Definition. A proper ideal P of a commutative ring R is **prime** if $ab \in P$ implies $a \in P$ or $b \in P$ for any $a, b \in R$.

Example. Consider $2\mathbb{Z} \subseteq \mathbb{Z}$. We claim $2\mathbb{Z}$ is a prime ideal. Let $a, b \in \mathbb{Z}$. Suppose $ab \in 2\mathbb{Z}$. Then a or b is even, i.e. $a \in 2\mathbb{Z}$ or $b \in 2\mathbb{Z}$. Therefore, $2\mathbb{Z}$ is prime.

Alternate Proof: $ab \in 2\mathbb{Z} \Leftrightarrow \exists n \in \mathbb{Z}$ such that $ab = 2n$. Using prime factorization, there exist primes $p_1, \dots, p_l, q_1, \dots, q_s$ such that $a = p_1 \dots p_l$ and $b = q_1 \dots q_s$. Thus, $p_1 \dots p_l q_1 \dots q_s = 2n$ and there exists i or j such that $p_i = 2$ or $q_j = 2$. Thus, $a \in 2\mathbb{Z}$ or $b \in 2\mathbb{Z}$ and $2\mathbb{Z}$ is prime.

Theorem

Let R be a commutative ring with identity and let $A \subseteq R$ be an ideal. Then R/A is an integral domain if and only if A is prime.

Proof

Suppose R/A is an integral domain. Let $a, b \in R$ and suppose that $ab \in A$. We must show $a \in A$ or $b \in A$. We compute $(a + A)(b + A) = ab + A = A = 0 + A$, which is the additive identity in R/A. But R/A is an integral domain so $a + A = A$ or $b + A = A$. Therefore, $a \in A$ or $b \in A$.

Conversely, supposed that A is prime and let $a + A, b + A \in R/A$ such that $(a + A)(b + A) = ab + A = A$. Then $ab \in A$. But A is prime so $a \in A$ or $b \in A$. Thus, $a + A = 0 \in R/A$ or $b + A = 0 \in R/A$ and R/A is an integral domain.

Theorem

Let R be a commutative ring with identity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Proof

Suppose R/A is a field. Let B be an ideal of R that properly contains A, $A \subsetneq B \subseteq R$. We want to show that $B = R$. There exists $b \in B$ such that $b \notin A$. Then $b + A$ is a nonzero element of R/A. But R/A is a field, hence $b + A$ must have a multiplicative inverse, i.e. there exists $c \in R$ such that $(b + A)(c + A) = bc + A = 1 + A$. Therefore, $1 - bc \in A \subsetneq B$. But $bc \in B$ since B is an ideal so $(1 - bc) + bc = 1 \in B$. Since $1 \in B$, $B = R$.

Conversely, suppose that A is maximal. We want to show that R/A is a field. Since R is commutative and has an identity, R/A is also commutative and has an identity. We want to show that every nonzero element of R/A has a multiplicative inverse. Every nonzero element of R/A is of the form $b + A$, $b \in R - A$. Choose and fix such an element b. Consider the subset $B \subseteq R$ such that

$$B = \{br + a : r \in R, a \in A\}$$

We want to show that B is an ideal of R properly containing A. Since

$$(br + a) - (br' + a') = b(r - r') + (a - a') \in B$$

we know that B is a subgroup of $(R, +)$. We also know that is it closed under multiplication since

$$(br + a)(br' + a') = brbr' + bra' + br'a + aa' = b(rbr' + ra' + r'a) + (aa') \in B$$

so B is a subring. Also for any $s \in R$,

$$s(br + a) = sbr + sa = b(sr) + (sa)$$

Because A is an ideal, $sa \in A$ so B is an ideal of R. Also for any $a \in A$, $a = b0 + a \in B$ and $b = b1 + 0 \in B - A$ so B is an ideal that properly contains A. However, A is maximal so $B = R$. Because R contains 1, there exists $c \in R$ and $a' \in A$ such that $1 = bc + a'$. If we consider the coset of R/A this element is in, we see that $1 + A = bc + a' + A$. Since $a' \in A$, we can rewrite our equation as $1 + A = (b + A)(c + A)$. Therefore, for any $b + A \in R/A$, there exists a multiplicative inverse and R/A is a field.

Proposition. In a commutative ring R with identity, every maximal ideal is prime.

Definition. A **norm** N on the integral domain R is a map of set $N : R \to \mathbb{N} \cup \{0\}$. If $N(a) > 0$, $\forall a \in R$, we say N is a **positive norm**.

Note. Some texts require for nonzero $a, b \in R$, $N(a) \leq N(ab)$. Also, it is not required that $N(a + b) \leq N(a) + N(b)$ or $N(ab) \leq N(a)N(b)$.

Definition. The integral domain R is called a **Euclidean domain** if there is a norm N on R such that if $a, b \in R$, $b \neq 0$, then $\exists q, r \in R$ such that $a = qb + r$ where $r = 0$ or $N(r) < N(b)$. Here, q is the **quotient** and r is the **remainder**.

Definition. The **Euclidean algorithm** for two elements a, b in a Euclidean domain R is a list of divisions

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\dots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

where r_n is the last nonzero remainder. Such an r_n exists as $N(r_1) > N(r_2) > \ldots > N(r_n) \geq 0$ is a decreasing sequence of nonnegative integers.

Example. If K is a field, then $K[x]$ is a Euclidean domain with norm $N(f(x)) = \deg(f(x))$. The division algorithm is polynomial long divison. Let $f, g \in \mathbb{Z}_5[x]$, $f = 3x^4 + x^3 + 2x^2 + 1$, and $g = x^2 + 4x + 2$. Then we have $3x^4 + x^3 + 2x^2 + 1 = (3x^2 + 4x)(x^2 + 4x + 2) + (2x + 1)$.

Example. Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $ii = -1$, with norm $N(a + bi) = a^2 + b^2$.

Definition. Let $a, b \in R$, $b \neq 0$. Then a is a **multiple** of b if $a = qb$ for some $q \in R$. We also say b **divides** a or b is a **divisor** of a, or $b|a$.

Definition. The **greatest common divisor** of a and b is a nonzero element $d \in R$ such that

1. $d|a$ and $d|b$.
2. If $c|a$ and $c|b$, then $c|d$.

Note. Suppose $d|d'$ and $d'|d$. Then $d' = qd$ and $d = q'd'$. This becomes $d = q'qd$ or $(1 - qq')d = 0$. Since this is an integral domain, either $d = 0$ or $qq' = 1$, meaning q and q' are units. Thus, GCDs are unique only up to units.

Proposition. If $0 \neq a, b \in R$ and $(a, b) = (d)$, then $d = \gcd(a, b)$.

Definition. An integral domain such that every ideal generated by two elements is principal is called a **Bezout domain**.

Proposition. Let R be an integral domain. If $(d) = (d')$ then there exists a unit $u \in R$ such that $d' = ud$.

Proposition. Let R be a Euclidean domain and $0 \neq a, b \in R$. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm. Then $d = \gcd(a, b)$ and $(d) = (a, b)$.

Proposition. If $(d) = (a, b)$, then there exists $x, y \in R$ such that $d = ax + by$.

Proposition. Consider $R = \mathbb{Z}$. If $ax + by = c$, then $c \in (d)$ so c is a multiple of $\gcd(a, b)$.

Proposition. Every ideal in a Euclidean domain is principal.

Proof. Let $I \subseteq R$ be an ideal and R a Euclidean domain with norm N. If $I = \{0\}$, then $I = (0)$ is principal. Otherwise, consider $\{N(a) : a \neq 0, a \in I\} \subseteq \mathbb{N} \cup \{0\}$ as a subset of nonnegative integers. This set has a least element. Let $d \neq 0$, $d \in I$ be an element of minimal norm. We show $(d) = I$. First, $d \in I$ implies that $rd \in I$ for all $r \in R$ so $(d) \subseteq I$. We show $I \subseteq (d)$. Let $a \in I$. Since R is a Euclidean domain, there exists q and r such that $a = qd + r$, with $r = 0$ or $N(r) < N(d)$. But d has minimal norm so $r = 0$. Thus, $a = qd$ and $a \in (d)$. Therefore, $I = (d)$ and I is principal.

Definition. A **principal ideal domain** is an integral domain such that every ideal is principal.

Proposition. Every Euclidean domain is a PID. This containment is proper, i.e. not every PID is a Euclidean domain.

Example. $\mathbb{Z}$ is a PID. Every ideal is a subring, hence a subgroup, and hence is cyclic.

Proposition. Let R be a PID, $I \subseteq R$ a nonzero ideal. If I is prime, then I is maximal.

Proof. Suppose $I \subseteq J \subseteq R$ for some ideal J. We show $I = J$ or $J = R$. Since R is a PID, I and J are principal, so there exists $a, b \in R$ such that $I = (a)$ and $J = (b)$. First, $I \subseteq J$, i.e. $(a) \subseteq (b)$ so $a \in (b)$ and there exists $x \in R$ such that $a = bx$. Thus, $bx \in (a) = I$. But I is prime, hence $b \in (a)$ or $x \in (a)$. If $b \in (a)$, then $(b) \subseteq (a)$ and $(a) = (b)$, i.e. $I = J$. If $x \in (a)$, there exists $y \in R$ such that $x = ay$. Then $x = ay = bxy = xby$. Thus, $x(by - 1) = 0$. Since R is an integral domain, $x = 0$ or $by - 1 = 0$. If $x = 0$, then $I = 0$ but $I \neq 0$ by assumption. Thus, $1 = by$ and b is a unit. Thus, $(b) = R$, i.e. $J = R$. Therefore, I is maximal.

Proposition. If $R[x]$ is a PID, then R is a field.

Proof. Since $R \subseteq R[x]$, R is also an integral domain. Note that $R[x]/(x) \cong R$ so (x) is prime. Thus, (x) is maximal since $R[x]$ is a PID. Thus, $R[x]/(x)$ is a field. But $R[x]/(x) \cong R$ so R is a field.

Theorem (Ascending Chain Condition). In a PID, any strictly ascending chain of ideals is finite in length, i.e. $I_1 \subsetneq I_2 \subsetneq \ldots$ must be finite.

Proof. Let $I = \cup_n \in \mathbb{N} I_n$. This is an ideal. We are in a PID, hence I is principal, i.e. there exists $b \in R$ such that $I = (b)$. Thus, $b \in I = \cup_n \in \mathbb{N} I_n$. So there exists $k \in \mathbb{N}$ such that $b \in I_k$. Thus, $I_1, I_2, \ldots, I_{k-1} \subseteq I_k$ and $I_{k+1} \subseteq I_k$. Thus our chain is finite.

Definition. Let R be an integral domain.

1. Let $r \in R$, $r \neq 0$, and r be not a unit. We say r is **irreducible** in R if $r = ab$ implies a or b is a unit in R. Otherwise, r is **reducible**.
2. An element $0 \neq p \in R$ is called **prime** if (p) is a prime ideal of R, i.e. p is not a unit and $p|ab$ implies $p|a$ or $p|b$.
3. a and b are **associate in** R if there exists a unit $u \in R$ such that $a = ub$.

Proposition. In an integral domain, prime elements are irreducible.

Proof. Let $p \in R$ and (p) be prime. Suppose $p = ab$ where $a, b \in R$. We want to show that a or b is a unit. Note that $p \in (p)$ so $ab \in (p)$ and either $a \in (p)$ or $b \in (p)$. Without loss of generality, let $a \in (p)$. Then there exists $r \in R$ such that $a = pr$. Thus, $p = ab = prb$ so $p(1 - rb) = 0$. Since $p \neq 0$ by assumption, $1 = rb$ since R is an integral domain so b is a unit.

Note. Irreducible elements are not necessarily prime.

Example. Consider $3 \in \mathbb{Z}[\sqrt{-5}]$. Suppose we can factor 3. Let $3 = a(1+b\sqrt{-5})(1+c\sqrt{-5})$. Expanding gives $a(1-5bc)+5abc\sqrt{-5}$ so $abc = 0$ and $a - 5abc = 3$. Thus $a = 3$ and $bc = 0$. This means that $1 = (1+b\sqrt{-5})(1+c\sqrt{-5}) = 1 - 5bc + bc\sqrt{-5}$ and $5bc = bc\sqrt{-5}$ so 3 is not irreducible. However, note that $3|(1+\sqrt{-5})(1-\sqrt{-5})$. Another way to see this is by using norms where $N(a+b\sqrt{-5}) = a^2+5b^2$ and $N(3) = 9 = f^2+5g^2$.

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

Proof. The forward direction is trivial so we prove the reverse direction. Let $p \in R$ be irreducible. We want to show that (p) is prime. But in a PID, maximal ideals are prime so we show that (p) is maximal. Suppose $(p) \subseteq M \subseteq R$. Since R is a PID, there exists $m \in R$ such that $M = (m)$. This means that $p \in (m)$ and there exists $r \in R$ such that $p = mr$. But p is irreducible so m or r is a unit in R. Thus, $(m) = R$ or $(m) = (p)$ so (p) is maximal and therefore prime.

Definition. A **unique factorization domain** is an integral domain R such that for a nonzero nonunit r,

1. There exists irreducible elements $p_1, \ldots, p_n \in R$ such that $r = p_1 p_2 \ldots p_n$.
2. If $r = q_1 q_2 \ldots q_m$ for irreducible q_i, then $m = n$ and there exists $\sigma \in S_n$ such that p_i and $q_{\sigma(i)}$ are associate. The p_i are not necessarily distinct.

Example. The following are examples and non-examples of UFDs.

1. Fields are UFDs.
2. If R is a UFD, then $R[x]$ is a UFD.
3. $\mathbb{Z}[2i]$ is not a UFD. Note that $4 = 2 \cdot 2 = (2i)(-2i)$ and $i \notin \mathbb{Z}[2i] = \{a + b2i : a, b \in \mathbb{Z}\}$.

Proposition. PIDs are UFDs.

Proof. Let $r \in R$ be a nonzero nonunit. If r is irreducible then we are done. Otherwise, $r = r_1 r_2$. If r_i is irreducible, we are done. Otherwise, $r = r_{11} r_{12} \ldots$. We then have $(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq \ldots$. This is an ascending chain of ideals in a PID. Thus, there exists $n \in \mathbb{N}$ such that $I_m = I_n$ for $m \geq n$. Then $r = r_1 \ldots r_{1\ldots 1}$. Uniqueness can be proved by induction on n.

Corollary (Fundamental Theorem of Arithmetic)**.** $\mathbb{Z}$ is a UFD.

Note. There is a chain of proper containment of types of rings as follows.

$$\begin{aligned} \text{field} &\subsetneq \text{Euclidean domain: } \mathbb{Z} \\ &\subsetneq \text{principal ideal domain: } \mathbb{Z}[(1+\sqrt{-19})/2] \\ &\subsetneq \text{unique factorization domain: } \mathbb{Z}[x] \\ &\subsetneq \text{integral domain: } \mathbb{Z}[\sqrt{-5}] \\ &\subsetneq \text{commutative ring with 1: } \mathbb{Z}_6 \end{aligned}$$