# Algebra

This is mainly from introductory level Youtube Video by Michael Penn `https://www.youtube.com/watch?v=c6i6edrthFM&list=PL22w63XsKjqxaZ-v5N4AprggFkQXgkNoP&index=9`.

## 1 Introduction

***Definition:* 1.1: Relation**

A relation on a set $A$ is a subset $R \subset A \times A$. Write $(x, y) \in R$ as $xRy$, $(x, y) \notin R$ as $x \not R y$.

**Example:** $A$ =any set, $R$ is equality. $(x, y) \in R \Leftrightarrow x = y$, $R = \{(a, a) : a \in A\}$.
If $A = \{1, 2, 3\}$, $R = \{(1, 1), (2, 2), (3, 3)\}$

**Example:** $A = \{1, 2, 3\}$, $R$ is less than or equal.
Then $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$

**Example:** $A = \mathbb{N}$, $R$ is divides. $(m, n) \in R \Leftrightarrow m|n$, *i.e.* $\exists d \in \mathbb{N}$ s.t. $n = md$.
Then $(1, n) \in R$, since $1|n$ for any $n$, $(2, 10) \in R$, since $2|10$.

***Definition:* 1.2: Equivalence Relation**

A relation $R \subset A \times A$ is an equivalence relation if it has the following properties

1. Reflexivity: $(a, a) \in R$, $\forall a \in A$
2. Symmetry: $(a, b) \in R \Rightarrow (b, a) \in R$
3. Transitivity: $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$

**Example:** $R$ is equality. $(a, b) \in R \Leftrightarrow a = b$ is an equivalence relation.

**Example:** $R$ is nothing. $\forall a, b \in A, (a, b) \in R$. $R = A \times A$ is an equivalence relation.

**Example:** $A = C^1(\mathbb{R})$ (all differentiable functions on $\mathbb{R}$). $fRg \Leftrightarrow f' = g =$ is an equivalence relation.

***Definition:* 1.3: Equivalence Class**

Given an equivalence relation $R \subset A \times A$. The equivalence class of $a \in A$ is $[a] = \{b \in A : (a, b) \in R\}$.

**Example:** $R$ is equality. $[a] = \{b \in A : a = b\} = \{a\}$

**Example:** $R$ is nothing. $[a] = \{b \in A : (a, b) \in R = A \times A\} = A$

**Example:** $A = C^1(\mathbb{R})$. $[f] = \{g \in A : f' = g'\} = \{g \in A : (f - g)' = 0\} = \{f + c : c \in \mathbb{R}\}$.

**Definition: 1.4: Power Set**

Given a set $A$. $\mathcal{P}(A) = \{B : B \subset A\}$ is the power set of $A$.

**Definition: 1.5: Partition**

$P \subset \mathcal{P}(A)$ is a partition of $A$ if

1. $\bigcup_{X \in P} X = A$
2. If $X \neq Y$, then $X \cap Y = \emptyset$

**Example:** $A = \{1, 2, 3, 4, 5, 6\}$, $P = \{\{1\}, \{2, 3, 4\}, \{5, 6\}\}$ is a partition.

**Example:** $A = \mathbb{Z}$, $P = \{\{3k\}, \{3k + 1\}, \{3k + 2\}\}$ is a partition.

**Theorem: 1.1:**

There is a one-to-one correspondence between partitions of $A$ and equivalence relations on $A$.

*Proof.*

1. Suppose $P$ is a partition of $A$. Define a relation $R \subset A \times A$ s.t. $(a, b) \in R \Leftrightarrow a, b \in X \in P$. We need to check that $R$ is an equivalence relation.

   **Reflexivity:** $(a, a) \in R$, because $a \in X$ for some $X \in P$, since $\bigcup_{X \in P} X = A$ and $a \in A$.

   **Symmetry:** Suppose $(a, b) \in R$, then $a, b \in X \in P$. This is the same as $b, a \in X \in P$, thus $(b, a) \in R$

   **Transitivity:** Suppose $(a, b) \in R$ and $(b, c) \in R$, then $a, b \in X \in P$ and $b, c \in Y \in P$. But $X \cap Y = \emptyset$ if $X \neq Y$, thus $X = Y$. $a, c \in X \in P$, so $(a, c) \in R$

2. Suppose $R \subset A \times A$ is an equivalence relation. Let $P = \{[a] : a \in A\}$

   Suppose $a \in A$, $(a, a) \in R$. $a \in [a] = \bigcup_{[a] \in P} [a] \Rightarrow A \subset \bigcup_{[a] \in P} [a]$ and by definition $\bigcup_{[a] \in P} [a] \subset A$, thus $A = \bigcup_{[a] \in P} [a]$

   Take $a, b \in A$. Consider $[a] \cap [b]$. Suppose $x \in [a] \cap [b]$. Then $x \in [a]$ and $x \in [b]$. Then $(a, x) \in R$ and $(b, x) \in R$. By transitivity $(a, b) \in R$, $[a] = [b]$

□

**Definition: 1.6: Binary Operation**

Given a set $S$, a binary operation on $S$ ia a function $* : S \times S \to S$, write $*(a, b) = a * b$. The following properties may or may not hold.

1. Associativity: $a * (b * c) = (a * b) * c$
2. Commutativity: $a * b = b * a$

**Example:** $(\mathbb{N}, +)$, $+$ is associative and commutative.

**Example:** $(\mathbb{Z}, +)$, $+$ is associative and commutative, with identity and inverse.

**Example:** $M_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n}\}$, $*$ is matrix multiplication. Then $*$ is associative, but not commutative. If $*$ is the commutator $[\cdot, \cdot]$, $A * B = [A, B] = AB - BA$, then $*$ is neither associative nor commutative.

## 2 Groups

**Definition: 2.1: Groups**

A group is a set $G$ together with a binary operation $*$ s.t.

1. Closure: If $a, b \in G$, then $a * b \in G$
2. Identity: $\exists e \in G$ s.t. $\forall a \in G$, $a * e = a = e * a$
3. Inverse: $\exists a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$
4. Associative: $\forall a, b, c \in G$, $a * (b * c) = (a * b) * c$

**Example:** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are groups under addition.

**Example:** $(\{\pm 1\}, \cdot)$, $(\mathbb{Q}^\times, \cdot)$ where $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $GL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n \times n} : \det(A) \neq 0\}$ are groups are groups under multiplication.

**Definition: 2.2: Integer Modulo $n$ Groups**

Let $\mathbb{Z}_n$ be the set of all equivalence classes mod $n$. $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$. Define $[x]+[y] = [x+y]$. Then $(\mathbb{Z}_n, +)$ forms a group with identity $[0]$.

**Example:** $(\mathbb{Z}_6, +)$ is a group, but $(\mathbb{Z}_6, \cdot)$ where $\cdot : [x][y] \to [xy]$ is not a group, because 2,3,4 do not have an inverse.

**Definition: 2.3: Group of Units**

Given $n \in \mathbb{N}$, the group of units $U_n = \{[m]_n : \gcd(m, n) = 1\}$ with operation $[x][y] = [xy]$. $U_n$ is a group.

*Proof.*

1. Closure: Suppose $\gcd(x, n) = \gcd(y, n) = 1$, then $\gcd(xy, n) = 1$. So $[x], [y] \in U_n \Rightarrow [xy] \in U_n$.
2. Identity: $[1] \in U_n$ since $\gcd(1, n) = 1$ for any $n$.
3. Inverse: If $[a] \in U_n$, then $\gcd(a, n) = 1$. Thus $\exists x, y \in \mathbb{Z}$ s.t. $ax + ny = 1$ and $\gcd(x, n) = 1$. $[a][x] = 1$.
4. Associativity: From associativity of multiplication in $\mathbb{Z}$

□

**Example:** $U_6 = \{1, 5\}$.
**Example:** $U_5 = \{1, 2, 3, 4, 5\}$

**Definition: 2.4: Dihedral Groups**

$$\begin{aligned} D_n &= \{\text{rigid motions of regular n-gons}\} \\ &= \{e, r, ..., r^{n-1}, s, sr, ..., sr^{n-1}\}, \text{ where } r = \text{rotation by } \frac{2\pi}{n}, s = \text{reflection through a vertex} \\ &= \langle r, s : r^n = s^2 = e, rs = sr^{n-1} \rangle \text{ in generator representation} \end{aligned}$$

**Example:** $n = 3$, $D_3$ is the rigid motion on equilateral triangles. $r$ =rotation counter clockwise by $\frac{2\pi}{3}$. $r^2$ =rotation by $\frac{4\pi}{3}$. $r^3 = e$, $s$ =reflection through a vertex

For an $n$-gon, we can rotate by $\frac{2\pi k}{n}$ for $0 \leq k < n-1$, with a total of $n$ rotations, and $n$ total reflections through $n$ vertices.

**Example:** $n = 6$, $rsr^4sr^3 = sr^5r^4sr^3 = sr^9sr^3 = sr^3sr^3 = e$, since $sr^3$ is a reflection.

***Theorem:* 2.1:**

$r^k s = sr^{n-k}$ for all $1 \leq k \leq n-1$.

*Proof.* **Base case:** $rs = sr^{n-1}$ by definition.
**Induction Hypothesis:** Suppose $r^k s = sr^{n-k}$
**Induction Step:** $r^{k+1}s = r^k rs \overset{\text{Base case}}{=} r^k sr^{n-1} \overset{\text{IH}}{=} sr^{n-k}r^{n-1} = sr^{2n-(k+1)} = sr^{n-(k+1)}$ □

***Definition:* 2.5: Permutation Group**

Given a set $X$, define $S_X = \{f : X \to X : f \text{ a bijection}\}$. $S_X$ forms a group with operation given by composition of functions. $S_X$ is called the permutation group of $X$.
If $X = \{1, 2, ..., n\}$, we write $S_X = S_n$.

*Proof.*

1. Closure: $\forall f, g \in S_X$, $f \circ g : X \to X$ is a bijection, $f \circ g \in S_X$
2. Associativity: $\forall f, g, h \in S_X$, $f \circ (g \circ h)(x) = f(g(h(x))) = f \circ (g \circ h)(x)$
3. Identity: $\text{id} : X \to X$, $\text{id}(x) = x$. Then $\text{id} \circ f = f$ for $f \in S_X$
4. Inverse: Given a function $f : X \to X$, $f$ is a bijection $\Leftrightarrow$ $f$ has an inverse. Thus $\forall f \in S_X$, $f^{-1} \in S_X$

□

**Example:** $n = 3$, $S_3$ has 6 elements, and in cycle notation, we write $S_3 = \{1, (12), (13), (23), (123), (132)\}$, where $(123)(2) = 3$, $(123)(3) = 1$, $(132)(3) = 2$.

**Example:** Composing cycles

1. $(1352)(243) = (13)(245)$. 1 is sent to 1 by $(243)$, then to 3 by $(1352)$. We then look at 3, 3 is sent to 2 by $(243)$, then sent to 1 by $(1352)$
2. $(2974)(164) = (162974)$
3. $(1325)^{-1} = (1523)$ (just write in reverse order)

***Theorem:* 2.2: Basic Properties of Groups**

Given a group $G$,

1. The identity is unique
2. Inverses are unique
3. $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$
4. If $ab = ac$, then $b = c$. Similarly, if $ba = ca$, then $b = c$

*Proof.*

1. Suppose $e_1, e_2 \in G$ are both identities, $e_1 \overset{e_2 \text{ is identity}}{=} e_1e_2 \overset{e_1 \text{ is identity}}{=} e_2$
2. Suppose $a \in G$ with inverses $b$ and $c$. *i.e.* $ab = e = ba$, $ac = e = ba$.
   Then $b = be \overset{e=ac}{=} b(ac) \overset{\text{associativity}}{=} (ba)c \overset{ba=e}{=} ec = c$

3. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$ and $(ab)(ab)^{-1} = e$. Thus $(ab)^{-1} = b^{-1}a^{-1}$, since inverses are unique.

4. $ab = ac$, then $a^{-1}(ab) = a^{-1}(ac)$. By associativity, $b = c$.

□

**_Definition:_ 2.6: Abelian Group**

A group $G$ is abelian, if it is commutative. *i.e.* $\forall a, b \in G$, $ab = ba$.

**_Definition:_ 2.7: Order of a Group**

$G$ has order $n$ if $|G| = n$. *i.e.* $G$ has $n$ elements. $n$ can be infinite.

**_Definition:_ 2.8: Order of an Element**

$g \in G$ has order $m$ if $m$ is the smallest natural number s.t. $g^m = e$. Write $|g| = \mathrm{ord}(g) = n$.

## 2.1 Subgroups

**_Definition:_ 2.9: Subgroups**

Given a group $G$, a subset $H \subset G$ is a subgroup if $H$ is a group. Write $H \leq G$.

**Example:** Suppose $H \leq \mathbb{Z}$ under addition, $H \neq \{0\}$.
Let $n \in H$ be the smallest positive number, $m \in H$ be any other element. We can write $m = nq + r$, $0 \leq r < n$. $r = m - n - \cdots - n \in H$, thus $r = 0$.
*i.e.* any element $m \in H$ is a multiple of $n \in H$, the smallest positive element.
Thus we can write $H = n\mathbb{Z} = \{nk : k\mathbb{Z}\}$. *i.e.* The subgroups of $\mathbb{Z}$ must be of the form $n\mathbb{Z} \leq \mathbb{Z}$.

**Example:** $G$ any group, $\{e\} \leq G$, $G \leq G$ are the trivial subgroups.

**Example:** $\mathbb{C}^\times = \{a + bi : a, b \in \mathbb{R} \text{ not both zero}\}$, $\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$. $S^1 \leq \mathbb{C}^\times$, where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$

**Example:** $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$, where $SL(n, \mathbb{R}) = \{A \in \mathbb{R}^{n \times n}, \det A = 1\}$

**_Theorem:_ 2.3: Subgroup Test**

Suppose $G$ is a group. $H \subset G$ non-empty. Then $H \leq G \Leftrightarrow \forall x, y \in H$, $xy^{-1} \in H$

*Proof.* $(\Rightarrow)$ Suppose $H \leq G$. Let $x, y \in H$. Then $y^{-1} \in H$, since $H$ is a group. By closure property, $xy^{-1} \in H$.

$(\Leftarrow)$ Suppose $\forall x, y \in H$, $xy^{-1} \in H$.

1. Identity: Set $y = x$, then $xy^{-1} = xx^{-1} = e$, since $x \in G$, $G$ is a group. Thus $e \in H$.

2. Inverse: Suppose $a \in H$. Let $x = e, y = a \in H$. $xy^{-1} = ea^{-1} = a^{-1} \in H$.

3. Closure: Suppose $a, b \in H$, then $b^{-1} \in H$. Let $x = a$, $y = b^{-1}$. $xy^{-1} = a(b^{-1})^{-1} = ab \in H$

Thus $H \leq G$. □

**Definition: 2.10: Centralizer**

Let $H \leq G$. The centralizer of $H$ is

$$C(H) = \{g \in G : gh = hg, \forall h \in H\}$$

$C(H) \leq G$

*Proof.* Suppose $x, y \in C(H)$, we want to show $xy^{-1} \in C(H)$.

Notice that $gh = hg$ for all $h \in H$. Left and right multiply by $g^{-1}$, we get $g^{-1}ghg^{-1} = g^{-1}hgg^{-1}$. Thus $hg^{-1} = g^{-1}h$.

Let $h \in H$, $(xy^{-1})h \overset{\text{associativity}}{=} x(y^{-1}h) \overset{hg^{-1}=g^{-1}h}{=} xhy^{-1} \overset{gh=hg}{=} h(xy^{-1})$

Thus $xy^{-1} \in C(H)$, $C(H) \leq G$ □

**Definition: 2.11: Conjugate Subgroup**

Let $H \leq G$. The conjugate subgroup is $g^{-1}Hg = \{g^{-1}hg : h \in H\} \leq G$.

*Proof.* Suppose $x \in g^{-1}Hg$ and $y \in g^{-1}Hg$. Then $x = g^{-1}hg$, $y = g^{-1}\hat{h}g$ for $h, \hat{h} \in H$.

Then $y^{-1} = g^{-1}\hat{h}^{-1}g$. $xy^{-1} = g^{-1}hgg^{-1}\hat{h}^{-1}g = g^{-1}h\hat{h}^{-1}g \in g^{-1}Hg$. □

**Definition: 2.12: Center**

Given a group $G$, the center of $G$ is $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$. $Z(G) \leq G$.
*i.e.* $g \in Z(G) \Leftrightarrow gx = xg, \forall x \in G \Leftrightarrow xgx^{-1} = g, \forall x \in G$

*Proof.* Let $x, y \in Z(G)$. Then $gxg^{-1} = x$, $\forall x \in G$, and $gyg^{-1} = y, \forall y \in G$
Then $xy^{-1} = gxg^{-1}(gyg^{-1})^{-1} = gxg^{-1}gy^{-1}g^{-1} = g(xy^{-1})g^{-1}$, Thus $xy^{-1} \in Z(G)$.
By Theorem 2.3, $Z(G) \leq G$. □

**Example:** Find the center of $D_4 = \langle r, s : r^4 = s^2 = e, rs = sr^3\rangle$

*Proof.* If $x \in Z(D_4)$, then $rx = xr$ and $sx = xs$, thus $x = r^3xr$ and $x = s^{-1}xs = sxs$
Suppose $x$ is a rotation, $x = r^k$, $0 \leq k \leq 3$.
Then $r^3xr = r^3r^kr = r^{k+4} = r^kr^4 = r^k = x$, so any rotation commutes with $x$.
$sxs = sr^ks \overset{\text{By Theorem 2.1}}{=} ssr^{4-k} = r^{4-k} = x = r^k$. Then $r^{2k} = e$, $2k \equiv 0 \mod 4$, $k$ is even.
Thus $x = r^0$ or $r^2$.
Suppose $x$ is a reflection, $x = sr^k$, $0 \leq k \leq 3$.
Then $r^3xr = r^3sr^kr \overset{\text{By Theorem 2.1}}{=} srr^kr = sr^{k+2} = x = sr^2$. Then $r^{k+2} = r$, $r^2 = e$. Impossible.

In summary: if $x$ is a reflection, it cannot be in the center. Only rotations in $Z(D_4)$ are $e$ and $r^2$.

Thus $Z(D_4) = \{e, r^2\} = \langle r^2\rangle$. □

## 2.2 Types of Groups

### 2.2.1 Cyclic Groups

**Definition: 2.13: Cyclic Subgroups**

Given any group $G$ and element $a \in G$, the cyclic subgroup of $G$ generated by $a$ is $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

*Proof.* Suppose $x, y \in \langle a \rangle$. Then $x = a^m$, $y = a^n$ for $m, n \in \mathbb{Z}$
Then $xy^{-1} = a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle$, since $m - n \in \mathbb{Z}$.
Thus $\langle a \rangle \leq G$ by Theorem 2.3. □

**Theorem: 2.4:**

$\langle a \rangle$ is the smallest subgroup of $G$ containing $a$.

*Proof.* We want to show that for any $H \leq G$ with $a \in H$, $\langle a \rangle \subset H$.
Suppose $H \leq G$ with $a \in H$, then $a^n \in H$, $\forall n \in \mathbb{Z}$, because subgroups are closed under the operation.

Thus $\langle a \rangle \subset H$ and $\langle a \rangle \leq H$. □

**Example:** $(\mathbb{Z}, +)$, $\langle 5 \rangle = \{5n : n \in \mathbb{Z}\} = 5\mathbb{Z} \leq \mathbb{Z}$

**Example:** $\mathbb{Z}_{12}$, $\langle 4 \rangle = \{0, 4, 8\} \leq \mathbb{Z}_{12}$, $\langle 5 \rangle = \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}$

**Example:** $U_8 = \{1, 3, 5, 7\}$, $\langle 3 \rangle = \{1, 3\}$, $\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$

Figure 1: Lattice Diagram for $U_8$

$$\begin{tikzcd}[arrows=-]
 & U_8 \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle 3 \rangle \arrow[dr] & \langle 5 \rangle \arrow[d] & \langle 7 \rangle \arrow[dl] \\
 & \{1\} &
\end{tikzcd}$$

**Example:** $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, $\langle r \rangle = \{e, r, r^2, r^3\}$, $\langle r^2 \rangle = \{e, r^2\}$, $\langle s \rangle = \{e, s\}$, $\langle s, r \rangle = \{e, sr\}$

**Example:** $S_5 =$ all bijections of $\{1, 2, 3, 4, 5\}$. $\langle (123) \rangle = \{1, (123), (132)\}$

**Definition: 2.14: Cyclic Groups**

A group $G$ is a cyclic group if $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ for some $g \in G$.

**Theorem: 2.5:**

Every cyclic group is abelian

*Proof.* Suppose $G = \langle g \rangle$. Take $x, y \in G . x = g^m, y = g^n$ for $m, n \in \mathbb{Z}$.
Then, $xy = g^m g^n = g^{m+n} = g^n g^m = yx$. Thus the cyclic group is abelian. □

**Example:** Cyclic groups: $\mathbb{Z} = \langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\}$. $\mathbb{Z}_n = \langle 1 \rangle$.
$U_6 = \{1, 5\} = \langle 5 \rangle$. $U_9 = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle$
All non-abelian groups are not cyclic.
$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ is abelian, but not cyclic. $\langle (1,0) \rangle = \{(1,0), (0,0)\}$, $\langle (0,1) \rangle = \{(0,1), (0,0)\}$, $\langle (1,1) \rangle = \{(1,1), (0,0)\}$

***Theorem:* 2.6:**

Every subgroup of a cyclic group is cyclic.

*Proof.* Suppose $G = \langle g \rangle$, $H \leq G = \langle g \rangle$.
Let $S = \{a \in \mathbb{N} : g^a \in H\} \subset \mathbb{N}$, so it has a minimal element $m \in S$, $g^m \in H$.
Take $g^n \in H$. Perform division algorithm with $m$ and $n$. $n = mq + r$, $0 \leq r < m - 1$.
$g^n = g^{mq+r} = (g^m)^q g^r$. Then $g^r = g^n (g^m)^{-q} \in H$. This means that $r = 0$. Otherwise, $m$ is not the minimal.
Thus, $g^n = (g^m)^q g^r = (g^m)^q \in \langle g^m \rangle$.
Then $H \subset \langle g^m \rangle$.
Since $g^m \in H$, $\langle g^m \rangle \leq H$ by Theorem 2.4, Thus $H = \langle g^m \rangle$ $\square$

***Lemma:* 2.1:**

Suppose $G = \langle g \rangle$ with $|G| = n$ or equivalently $|g| = n$. Then $g^k = e \Leftrightarrow n | k$

*Proof.* ($\Leftarrow$) Suppose $n|k$, then $k = nd$ for $d \in \mathbb{N}$. $g^k = g^{nd} = (g^n)^d = e^d = e$

($\Rightarrow$) Suppose $g^k = e$. Perform division with $n$ and $k$. $k = nq + r$, $0 \leq r < n - 1$.
Then $e = g^k = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$. Thus $r = 0$, $k = nq$, $n|k$. $\square$

***Theorem:* 2.7: Element Order in Cyclic Group**

Let $G = \langle g \rangle$ with $|G| = |g| = n$. If $x = g^k$, then $|x| = \frac{n}{\gcd(n,k)}$.

*Proof.* Let $m = |x|$. By Definition 2.8, $x^m = (g^k)^m = e$. Thus $g^{km} = e$. By Lemma 2.1, $n | km$, or equivalently $\frac{n}{\gcd(n,k)} = \frac{km}{\gcd(n,k)}$.
But $\frac{n}{\gcd(n,k)}$ and $\frac{k}{\gcd(n,k)}$ are relevantly prime. Thus $\frac{m}{\gcd(n,k)} | m$
Notice $x^{\frac{n}{\gcd(n,k)}} = (g^k)^{\frac{n}{\gcd(n,k)}} = (g^n)^{\frac{k}{\gcd(n,k)}} = e$.
By Lemma 2.1, $m | \frac{n}{\gcd(n,k)}$.
Thus $m = \frac{n}{\gcd(n,k)}$ $\square$

**Corollary 1.** *If $G = \langle g \rangle$ with $|G| = n|g|$, then $G = \langle g^m \rangle \Leftrightarrow gcd(m,n) = 1$.*

**Corollary 2.** $\mathbb{Z}_n = \langle m \rangle \Leftrightarrow gcd(m,n) = 1$.

**Example:** $\mathbb{Z}_9 = \langle 1 \rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 8 \rangle$
For $p$ prime, $\mathbb{Z}_p = \langle m \rangle$, $\forall m \in [1, p-1]$.

### 2.2.2 Alternating Groups

**Definition: 2.15: k-cycle and Transposition**

A k-cycle is a permutation $(a_1a_2...a_k)$, $a_i \in \{1, ..., n\}$. A 2-cycle is known as a transposition.

**Theorem: 2.8:**

Any k-cycle can be written as a product of transpositions.

*Proof.* $(a_1a_2...a_{k-1}a_k) = (a_1a_2)(a_2a_3)...(a_{k-1}a_k)$. □

*Remark* 1. The composition is not unique. *e.g.* $(123) = (12)(13) = (12)(23)(23)(13)$

**Lemma: 2.2:**

If $\tau_1, ..., \tau_n \in S_n$ are transpositions with $\tau_1 \cdots \tau_r = 1$, then $r$ is even.

*Proof.* Note $r = 1$ is impossible. So we assume $r \geq 2$.

**Induction Hypothesis:** Assume that for $k \leq r$ if $\tau_1, ..., \tau_k \in S_n$ are transpositions with $\tau_1 \cdots \tau_k = 1$, then $k$ is even.

**Induction Step:** We can write the final two transpositions $\tau_{r-1}\tau_r = \begin{cases} (ab)(ab) = (1) \\ (bc)(ab) = (ac)(bc) \\ (cd)(ab) = (ab)(cd) \\ (ac)(ab) = (ab)(bc) \end{cases}$.

Using this we can move the last appearance of $a$ to the left. Suppose $a$ appears in $\tau_r$, we can move it left until

1. The resulting final appearance of $a$ is $(ab')$ and it encounters its inverse. $\tau'_{k-1}\tau_k = (1)$. Then $\tau_1 \cdots \tau_r = \tau'_1 \cdots \tau'_{r-2} = (1)$. $r-2$ is even by IH, thus $r$ is even.
2. The first occurrence of $a$ moves all the way to the left, $(1) = \tau_1 \cdots \tau_r = (ab)'\tau'_2 \cdots \tau'_r$. Then $\tau'_2 \cdots \tau'_r$ fixes $a$, and $(1) = \tau_1 \cdots \tau_r = (ab)'\tau'_2 \cdots \tau'_r$ sends $a$ to $b$, contradiction that $(1)$ is identity.

Thus we only have the first case, and $r$ must be even. □

**Theorem: 2.9:**

If $\tau_1 \cdots \tau_m$ and $\tau'_1 \cdots \tau'_n$ are transpositions s.t. $\tau_1 \cdots \tau_m = \tau'_1 \cdots \tau'_n$, then $m \equiv n \mod 2$.

*Proof.* Note $\forall \tau = (ab)$, $\tau^2 = 1$, thus $\tau^{-1} = \tau$.
Then right multiply both sides of the given equation by $(\tau'_1 \cdots \tau'_n)^{-1}$, we get $\tau_1 \cdots \tau_m (\tau'_n)^{-1} \cdots \tau'_1 = (1)$. Thus $(m+n) \equiv 0 \mod 2$, *i.e.* $m \equiv n \mod 2$. □

**Definition: 2.16: Even/Odd Cycles**

$\sigma \in S_n$ is said to be even/odd if it can be written as a product of an even/odd number of transpositions. $(a_1...a_k)$ is even if $k$ is odd, odd if $k$ is even, because $(a_1...a_k) = (a_1a_2) \cdots (a_{k-1}a_k)$ contains $k-1$ transpositions.

**Definition: 2.17: Alternating Group**

Define the alternating group $A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$. $A_n \leq S_n$

*Proof.* Suppose $\mu, \sigma \in A_n$. Then $\mu = \tau_1 \cdots \tau_{2k}$, $\sigma = \tau'_1 \cdots \tau'_{2m}$ for $k, m \in \mathbb{N}$. Then $\sigma^{-1} = \tau'_{2m} \cdots \tau'_1$. $\mu\sigma^{-1} = \tau_1 \cdots \tau_{2k}\tau'_{2m} \cdots \tau'_1$ has a total of $2(k+m)$ transpositions. Thus $\mu\sigma^{-1} \in A_n$. By Theorem 2.3, $A_n \leq S_n$. □

**Theorem: 2.10:**

$$|A_n| = \frac{n!}{2}$$

*Proof.* $S_n \setminus A_n = \{\text{odd permutations}\}$. Then $S_n$ is the disjoint union of $A_n$ and $S_n \setminus A_n$.

Consider $\phi : A_n \to S_n \setminus A_n$ s.t. $\phi(\sigma) = (12)\sigma$. We want to show that $\phi$ is a bijection.

1. Injective: $\phi(\sigma_1) = \phi(\sigma_2)$, $(12)\sigma = (12)\sigma$, then $\sigma_1 = \sigma_2$
2. Surjective: Let $\mu \in S_n \setminus A_n$. Then $\mu = \tau_1 \cdots \tau_{2k-1} = (12)(12)\tau_1 \cdots \tau_{2k-1}$
   Note that $(12)\tau_1 \cdots \tau_{2k-1} \in A_n$ as a even permutation, $\phi((12)\tau_1 \cdots \tau_{2k-1}) = \tau_1 \cdots \tau_{2k-1} = \mu$.

Thus $\phi$ is bijective. $|A_n| = |S_n \setminus A_n|$. $n! = |S_n| = |A_n| + |S_n \setminus A_n| = 2|A_n|$. Then $|A_n| = \frac{n!}{2}$ □

**Example:** Show that $A_{10}$ has an element of order 15.

*Proof.* Let $\sigma = (123)(45678) \in A_{10}$. $(123)$ has order 3, $(45678)$ has order 5. Then $|\sigma| = \text{lcm}(3,5) = 15$. □

### 2.2.3 Quaternion Group

**Definition: 2.18: Quaternion Group**

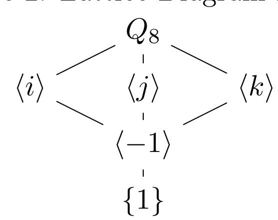
The Quaternion Group is $Q_8 = \{\pm 1, \pm i, \pm j, \pm j\}$ with the following operations:

- $id = 1$
- $(-1)^2 = 1$
- $i^2 = j^2 = k^2 = 1$
- $ij = k$, $ji = -k$
- $jk = i$, $kj = -i$
- $ki = j$, $ik = -j$

Note: $i \to j \to k \to i$ gives the positive orientation.

Cyclic subgroups of $Q_8$ are $\langle -1 \rangle = \{1, -1\}$, $\langle i \rangle = \langle -i \rangle = \{1, i, -1, -i\}$, $\langle j \rangle = \langle -j \rangle = \{1, j, -1, -j\}$, $\langle k \rangle = \langle -k \rangle = \{1, k, -1, -k\}$.

Figure 2: Lattice Diagram for $Q_8$



### 2.3 Cosets and Lagrange's Theorem

**_Definition:_ 2.19: Cosets**

Suppose $G$ is a group and $H \leq G$. Then the left coset of $H$ in $G$ with representative $g \in G$ is $gH = \{gh : h \in H\}$. The right coset of $H$ in $G$ with representative $g \in G$ is $Hg = \{hg : h \in H\}$.
**Note:** Cosets are not necessarily subgroups.

**Example:** $4\mathbb{Z} \leq \mathbb{Z}$
The coset with 0 is $0 + 4\mathbb{Z} = \{0 + 4n : n \in \mathbb{Z}\} = 4\mathbb{Z}$.
The coset with 1 is $1 + 4\mathbb{Z} = \{1 + 4n : n \in \mathbb{Z}\} = \{..., -3, 1, 5, 9...\}$.
The coset with 2 is $2 + 4\mathbb{Z} = \{2 + 4n : n \in \mathbb{Z}\} = \{..., -2, 2, 6, 10...\}$.
The coset with 3 is $3 + 4\mathbb{Z} = \{3 + 4n : n \in \mathbb{Z}\} = \{..., -1, 3, 7, 11...\}$.
$\mathbb{Z} = 4\mathbb{Z} \cup (1 + 4\mathbb{Z}) \cup (2 + 4\mathbb{Z}) \cup (3 + 4\mathbb{Z})$.

**Example:** $\langle 2 \rangle = \{0, 2, 4, 6\} \leq \mathbb{Z}_8$
$0 + \langle 2 \rangle = \{0, 2, 4, 6\} = 2 + \langle 2 \rangle = 4 + \langle 2 \rangle = 6 + \langle 2 \rangle = \langle 2 \rangle$
$1 + \langle 2 \rangle = \{1, 3, 5, 7\} = 3 + \langle 2 \rangle = 5 + \langle 2 \rangle = 7 + \langle 2 \rangle$
$\mathbb{Z}_8 = \langle 2 \rangle \cup (1 + \langle 2 \rangle)$.

**Example:** $\langle i \rangle = \{1, i, -1, -i\} \leq Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$
$i\langle i \rangle = \{i, -1, -i, 1\} = \langle i \rangle$, $j\langle i \rangle = \{j, -k, -j, k\}$
$Q_8 = \langle i \rangle \cup (j\langle i \rangle)$.

**Example:** $\langle 5 \rangle = \{1, 5\} \leq U_{12} = \{1, 5, 7, 11\}$
$7\langle 5 \rangle = \{7, 11\}$
$U_{12} = \langle 5 \rangle \cup (7\langle 5 \rangle)$.

**Example:** $H = \{e, r^2, s, sr^2\} \leq D_4 = \{e, r, r^2, r^3, sr, sr^2, sr^3\}$
$eH = r^2H = sH = (sr^2)H = H$, $rH = \{r, r^3, rs, rsr^2\} = \{r, r^3, sr^3, sr\}$ (By Theorem 2.1)
$D_4 = H \cup (rH)$.

**Example:** $\langle (12) \rangle = \{(1), (12)\} \leq S_3 = \{(1), (12), (13), (23), (123), (132)\}$
$(123)\langle (12) \rangle = \{(123), (13)\}$, $(132)\langle (12) \rangle = \{(132), (23)\}$
$S_3 = \langle (12) \rangle \cup ((123)\langle (12) \rangle) \cup ((132)\langle (12) \rangle)$.

**_Lemma:_ 2.3: Coset Partition**

Distinct left cosets of $H$ in $G$ partition $G$.

*Proof.* Suppose $x \in g_1H \cap g_2H$. Then $x = g_1h = g_2h'$ for $h, h' \in H$.
Then $g_1 = g_2h'h^{-1} \in g_2H$. Thus $g_1h'' = g_2(h'h^{-1}h'') \in g_2H$, so $g_1H \subset g_2H$.
Similarly, we get $g_2H \subset g_1H$. Thus $g_1H = g_2H$. So different cosets are disjoint. *i.e.* $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.

Suppose $g \in G$, then $g = ge \in gH$. Thus any element $g \in G$ must live in some coset. *i.e.* Distinct left cosets of $H$ in $G$ partition $G$. □

**_Lemma:_ 2.4:**

$|H| = |gH|$ for any $g \in G$.

*Proof.* Consider $\phi : H \to gH$ s.t. $\phi(h) = gh$
Injective: suppose $\phi(h) = \phi(h')$, then $gh = gh'$, meaning that $h = h'$.
Surjective: let $x \in gH$. By Definition 2.19, $x = gh$ for $h \in H$. $\phi(h) = gh = x$.
Thus $\phi$ is bijective, $|H| = |gH|$. □

**Theorem: 2.11: Lagrange's Theorem**

Let $G$ be a finite group with $H \leq G$. Then $|G| = |H|[G : H]$, where $[G : H]$ is the number of cosets of $H$ in $G$. Thus $|H|\,|\,|G|$. $[G : H]$ is also called the index of $H$ in $G$.

*Proof.* Suppose $|G| = n$ and $g_1H, ..., g_kH$ is a complete list of left cosets of $H$ in $G$.
By Lemma 2.3, $G = g_1H \cup g_2H \cup \cdots \cup g_kH$ with $g_iH \cap g_jH = \emptyset$ for $i \neq j$.
Then $|G| = \sum_{i=1}^{k} |g_iH| \overset{\text{By Lemma 2.4}}{=} \sum_{i=1}^{k} |H| = k|H|$. $k = [G : H] \in \mathbb{Z}$. Thus $|G| = |H|[G : H]$ and $|H|\,|\,|G|$. □

**Corollary 3.** *If $G$ is a finite group, Then*

1. $\forall g \in H$, $|g|\,|\,|G|$
2. *If $|G| = p$ a prime, then the only subgroups are $G$ and $\{e\}$*
3. *If $|G| = p$, $G$ is cyclic.*

*Proof.*
1. Since $\langle g \rangle \subset G$ by Theorem 2.4, and $|g| = |\langle g \rangle|$ which divides $|G|$ by Theorem 2.11.
2. A prime number can only be divided by 1 and itself
3. Choose $g \neq e \in G$, $\{e\} \neq \langle g \rangle \leq G$, then $\langle g \rangle = G$ by previous.

□

**Lemma: 2.5: Coset Equality**

Let $G$ be a group, $H \leq G$ and $g_1, g_2 \in G$. Then the following are equivalent:
1. $g_1H = g_2H$
2. $Hg_1^{-1} = Hg_2^{-1}$
3. $g_1H \subset g_2H$
4. $g_1 \in g_2H$
5. $g_1^{-1}g_2 \in H$

*Proof.* $(1 \Rightarrow 2)$ Suppose $g_1H = g_2H$.
Let $x \in Hg_1^{-1}$, then $x = hg_1^{-1}$ for some $h \in H$.
$x^{-1} = g_1h^{-1} \in g_1H = g_2H$, thus $x^{-1} = g_2\hat{h}$ for some $\hat{h} \in H$, then $x = (x^{-1})^{-1} = \hat{h}^{-1}g_2^{-1} \in Hg_2^{-1}$.
Thus $Hg_1^{-1} \subset Hg_2^{-1}$.
Similarly, we can show that $Hg_2^{-1} \subset Hg_1^{-1}$. Thus $Hg_1^{-1} = Hg_2^{-1}$.

$(2 \Rightarrow 3)$ Suppose $Hg_1^{-1} = Hg_2^{-1}$.
Let $x \in g_1H$, then $x = g_1h$ for some $h \in H$.
$x^{-1} = h^{-1}g_1^{-1} \in Hg_1^{-1} = Hg_2^{-1}$. Thus $x^{-1} = \hat{h}g_2^{-1}$ for some $\hat{h} \in H$. Then $x = (x^{-1})^{-1} = g_2\hat{h}^{-}1 \in g_2H$.
Thus $g_1H \subset g_2H$.

$(3 \Rightarrow 4)$ Suppose $g_1H \subset g_2H$.
Then $\forall x \in g_1H$, $x \in g_2H$.
$g_1 = g_1e \in g_1H$ so $g_1 \in g_2H$.

$(4 \Rightarrow 5)$ Suppose $g_1 \in g_2H$.
Then $g_1 = g_2h$ for some $h \in H$, then $g_2^{-1}g_1 = h$. Thus $g_1^{-1}g_2 = h^{-1} \in H$.

$(5 \Rightarrow 1)$ Suppose $g_1^{-1}g_2 \in H$.
Then $g_1^{-1}g_2 = h$ for some $h \in H$. $g_2 = g_1h \in g_1H$. By Lemma 2.3, $g_1H = g_2H$. □

### 2.4 Group Isomorphism

**_Definition:_ 2.20: Isomorphism**

Two groups $(G, \cdot)$ and $(H, \circ)$ are isomorphic if there is a bijection $\phi : G \to H$ s.t. $\phi(xy) = \phi(x) \circ \phi(y)$, for all $x, y \in G$. $\phi$ is called an isomorphism. Write $G \cong H$.

**Example:** Show that $(\mathbb{Z}_2, +) \cong \{\{\pm 1\}, \cdot\}$.

*Proof.* Let $\phi : \mathbb{Z}_2 \to \{\pm 1\}$ s.t. $\phi(0) = 1$, $\phi(1) = -1$.
$\phi(0 + 0) = \phi(0) = 1 = 1 \cdot 1 = \phi(0)\phi(0)$
$\phi(0 + 1) = \phi(1) = -1 = 1(-1) = \phi(0)\phi(1)$
$\phi(1 + 0)$ is by commutativity of Abelian groups. $\phi(1 + 1) = \phi(0) = 1 = (-1)(-1) = \phi(1)\phi(1)$

Thus $\mathbb{Z}_2 \cong \{\pm 1\}$ □

**Example:** Show that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

*Proof.* Let $\phi : \mathbb{R} \to \mathbb{R}^+$ s.t. $\phi(x) = e^x$
Injective: $\phi(x) = \phi(y) \Rightarrow e^x = e^y \Rightarrow x = y$
Surjective: Let $y \in \mathbb{R}^+$, $\ln y \in \mathbb{R}$. Set $x = \ln y$, $\phi(x) = e^{\ln y} = y$.
$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$ □

**Example:** Show that $U_5 \cong U_{10}$.

*Proof.* $U_5 = \{1, 2, 3, 4\} = \langle 3 \rangle$, $U_{10} = \{1, 3, 7, 9\} = \langle 7 \rangle$ (Any generator works.)
Let $\phi : U_5 \to U_{10}$ s.t. $\phi(3^k) = 7^k$, *i.e.* $\phi(1) = 1$, $\phi(3) = 7$, $\phi(4) = 9$, $\phi(2) = 3$
$\phi(3^k 3^l) = \phi(3^{k+l}) = 7^{k+l} = 7^k 7^l = \phi(3^k)\phi(3^l)$ □

**_Theorem:_ 2.12: Properties of Isomorphism**

Let $\phi : G \to H$ be an isomorphism. Then
1. $\phi^{-1} : H \to G$ is an isomorphism
2. $|G| = |H|$
3. If $G$ is abelian, then so is $H$
4. If $G$ is cyclic, then so is $H$
5. If $G$ has a subgroup of order $n$, then so does $H$

*Proof.* 1. $\phi$ is bijective, so $\phi^{-1}$ exists.
Suppose $u, v \in H$, $\exists x, y \in G$ s.t. $\phi(x) = u$, $\phi(y) = v$
$\phi^{-1}(uv) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(u)\phi^{-1}(v)$

2. By definition of bijections

3. Suppose $G$ is abelian.
   Let $u, v \in H$, $u = \phi(x)$, $v = \phi(y)$, $x, y \in G$
   $uv = \phi(x)\phi(y) = \phi(xy) \overset{G \text{is abelian}}{=} \phi(yx) = \phi(y)\phi(x) = vu$
   Thus $H$ is abelian.

4. Suppose $G$ is cyclic. $G = \langle g \rangle$.
   Let $u \in H$. $u = \phi(x)$ for some $x \in G = \langle g \rangle$. Then $x = g^n$ for some $n \in \mathbb{Z}$.
   Then $u = \phi(g^n) = (\phi(g))^n \in \langle \phi(g) \rangle$
   Thus $H \leq \langle \phi(g) \rangle \leq H$, $H = \langle \phi(g) \rangle$ is cyclic.

5. Suppose $K \leq G$ with $|K| = n$
   Consider $\phi(K) \subset H$ with $|\phi(K)| = n$.
   Let $x, y \in \phi(K)$. Then $x = \phi(k_1)$, $y = \phi(k_2)$ for some $k_1, k_2 \in K$. $k_1 k_2^{-1} \in K$, because $K$ is a subgroup.
   $xy^{-1} = \phi(k_1)\phi(k_2)^{-1} = \phi(k_1 k_2^{-1}) \in \phi(K)$
   By Theorem 2.3, $\phi(K) \leq H$.

□

### 2.4.1 Classification of Cyclic Groups

**Theorem: 2.13: Infinite Cyclic Groups**

If $G = \langle g \rangle$ with $|G| = \infty$, then $G \cong \mathbb{Z}$.

*Proof.* Consider $\phi : \mathbb{Z} \to G$ s.t. $\phi(n) = g^n$
$\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$

Injective: suppose $\phi(m) = \phi(n)$ with $m \geq n$. Then $g^m = g^n \Rightarrow g^{m-n} = e$.
If $m = n$, then done, $\phi$ is injective.
If $m > n$, then let $k = m - n > 0$. $\langle g \rangle = \{e, g, ..., g^{k-1}\}$ is finite, because $g^k = e$.

Surjective: suppose $x \in G = \langle g \rangle$, $x = g^n$ for some $n \in \mathbb{Z}$, then $\phi(n) = x$. □

**Theorem: 2.14: Finite Cyclic Groups**

Suppose $G = \langle g \rangle$ with $|G| = n$. Then $G \cong \mathbb{Z}_n$.

*Proof.* Consider $\phi : \mathbb{Z}_n \to G$ with $\phi(m) = g^m$ for $0 \leq m \leq n - 1$
Suppose $m \equiv m' \mod n$, then $m - m' = kn$ for some integer $k$. $\phi(m - m') = \phi(kn) \Rightarrow g^{m-m'} = (g^n)^k = e$.
Thus $g^m = g^{m'}$, $\phi(m) = \phi(m')$. So the map $\phi$ is well-defined.

Suppose $l, m \in \mathbb{Z}_n$. Then $\phi(l + m) = g^{l+m} = g^l g^m = \phi(l)\phi(m)$

Surjective: Suppose $x \in G = \langle g \rangle$. $x = g^m$ for $0 \leq m \leq n - 1$, then $\phi(m) = g^m = x$.

Injective: Suppose $l, m \in \mathbb{Z}_n$. $\phi(l) = \phi(m)$ means $l = m$, $g^{l-m} = e$.
If $l \neq m$, then $l - m \in \{1, ..., n - 1\}$, $|g| = |\langle g \rangle| < n$, which is a contradiction. Thus $l = m$.

Thus $\phi$ is bijective and $G \cong \mathbb{Z}_n$ □

*Remark* 2. In summary:

1. All infinite cyclic groups are isomorphic to $\mathbb{Z}$
2. All finite cyclic groups are isomorphic to $\mathbb{Z}_n$ for some $n$

### 2.4.2 Cayley's Theorem

***Theorem:* 2.15: Cayley's Theorem**

Every group is isomorphic to a permutation group.

*Proof.* For $g \in G$, define $\lambda_g : G \to G$ s.t. $\lambda_g(x) = gx$

We firstly show that $\lambda_g$ is a bijection, *i.e.* $\lambda_g \in S_g$
Injective: $\lambda_g(x) = \lambda_g(y) \Rightarrow gx = gy \Rightarrow x = y$
Surjective: Suppose $y \in G$, $g^{-1}y \in G$, $\lambda_g(g^{-1}y) = gg^{-1}y = y$
Thus $\lambda_g$ is a bijection and a permutation on $G$.

Let $H = \{\lambda_g : g \in G\}$. We show that $H$ is a group.

1. Associativity: is from associativity of function composition.
2. Closure: because $\forall g, h \in G$, $gh \in G$, then for all $\lambda_g, \lambda_h \in H$, $(\lambda_g \circ \lambda_h)(x) = ghx = \lambda_{gh}(x)$, and thus $\lambda_g \circ \lambda_h = \lambda_{gh} \in H$
3. Identity: $(\lambda_g \circ \lambda_e)(x) = gex = gx = \lambda_g(x)$, thus $\lambda_g \circ \lambda_e = \lambda_g$. $\lambda_e$ is the identity
4. Inverses: $(\lambda_g \circ \lambda_{g^{-1}})(x) = gg^{-1}x = x = ex = \lambda_e(x)$. Thus $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e$. $\lambda_{g^{-1}} = (\lambda_g)^{-1}$.

Now we show that $G \cong H$
Consider $\phi : G \to H$, $\phi(g) = \lambda_g$
$\phi(gh) = \lambda_{gh}$. Thus $\phi(gh)(x) = \lambda_{gh}(x) = ghx = (\lambda_g \circ \lambda_h)(x) = \phi(g)(x)\phi(h)(x)$. So $\phi(gh) = \phi(g)\phi(h)$.
Injective: Suppose $\phi(g) = \phi(h)$. *i.e.* $\lambda_g = \lambda_h$, then $\lambda_g(x) = \lambda_h(x), \forall x \Rightarrow gx = hx, \forall x \Rightarrow g = h$
Surjective: from definition of $\phi$.

Thus $G \cong H$ $\square$

**Corollary 4.** *If $|G| = n$, then there is a subgroup $H \subset S_n$ s.t. $G \cong H$.*

**Example:** Find a subgroup $H \leq S_3$ s.t. $\mathbb{Z}_3 \cong H$.

*Proof.* Consider $S_{\mathbb{Z}_3}$ = all permutation $\{0,1,2\} \to \{0,1,2\}$. $S_{\mathbb{Z}_3} = S_3$.
Define $\phi : \mathbb{Z}_3 \to H = \{\lambda_g : g \in \mathbb{Z}_3\}$.
$\lambda_0 : \mathbb{Z}_3 \to \mathbb{Z}_3$ s.t. $\lambda_0(x) = 0 + x$. This is the identity (0).
$\lambda_1 : \mathbb{Z}_3 \to \mathbb{Z}_3$ s.t. $\lambda_1(x) = 1 + x$. This is the 3-cycle (012).
$\lambda_2 : \mathbb{Z}_3 \to \mathbb{Z}_3$ s.t. $\lambda_2(x) = 2 + x$. This is the 3-cycle (021).
Thus $H = \{(0), (012), (021)\} \leq S_3$ and $\mathbb{Z}_3 \cong H$. $\square$

## 2.5 Group Products and Quotients

***Definition:* 2.21: External Direct Product**

Given groups $G_1, G_2$. Their external direct product is $G_1 \times G_2$. The respective group operations are componentwise.

**Example:** $\mathbb{Z}_5 \times \mathbb{Z} = \{m \in \mathbb{Z}_5, n \in \mathbb{Z}\}$.

**Example:** $\mathbb{R}^\times \times \mathbb{Z}_3 = \{(x, m) : x \in \mathbb{R}^\times, m \in \mathbb{Z}_3\}$ with $(x, n) * (y, m) = (xy, n + m)$

***Theorem:*** **2.16: Property of External Direct Product**

Let $(x, y) \in G_1 \times G_2$ with $|x| = r$, $|y| = s$, then $|(x, y)| = \text{lcm}(r, s)$.

*Proof.* Set $l = \text{lcm}(r, s)$, then $l = ra = sb$ for some $a, b \in \mathbb{N}$.
$(x, y)^l = (x^l, y^l) = ((x^r)^a, (y^s)^b) = (e_1^a, e_2^b) = (e_1, e_2)$. Thus $|(x, y)||l$
Set $l' = |(x, y)|$, then $(x, y)^{l'} = (e_1, e_2) \Rightarrow (x^{l'}, y^{l'}) = (e_1, e_2)$, so $x^{l'} = e_1$, $y^{l'} = e_2$. $r|l'$ and $s|l'$.
Thus $l = \text{lcm}(r, s)|l' = |(x, y)|$
Then $|(x, y)| = \text{lcm}(r, s)$ □

***Theorem:*** **2.17:**

$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \gcd(m, n) = 1$

*Proof.* ($\Rightarrow$) Suppose $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$. Assume $d = \gcd(m, n) > 1$
Take $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Then if we sum $(a, b)$ $\frac{mn}{d}$ times, we have $(a, b) + \cdots + (a, b) = (\frac{mn}{d}a, \frac{mn}{d}b) = (m(\frac{n}{d})a, n(\frac{m}{d}b)) = (0, 0)$.
But this shows that $|(a, b)||\frac{mn}{d}$ and thus $|(a, b)| < mn$ for any $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$.
Thus $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic. Contradiction.
Therefore $\gcd(m, n) = 1$.

($\Leftarrow$) Suppose $\gcd(m, n) = 1$, $|1| = m$ in $\mathbb{Z}_m$, $|1| = n$ in $\mathbb{Z}_n$.
Then $|(1, 1)| = \text{lcm}(m, n) = mn$ by Theorem 2.16.
Thus $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (1, 1) \rangle$ has order $mn$. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ by Theorem 2.14. □

***Definition:*** **2.22: Internal Direct Product**

Suppose $G$ is a group with $H, K \leq G$ s.t.
1. $G = HK = \{hk : h \in H, k \in K\}$
2. $H \cap K = \{e\}$
3. $hk = kh$, $\forall h \in H, k \in K$

Then $G$ is the internal direct product of $H$ and $K$.

***Theorem:*** **2.18: Isomorphism of Direct Products**

If $G$ is the internal direct product of $H$ and $K$, then $G \cong H \times K$.

*Proof.* We want to find a bijective map $\phi : G \to H \times K$, that satisfy the isomorphism property (Definition 2.20).

Let $\phi : G \to H \times K$. Take $g \in G$, write $g = hk$, $\phi(g) = (h, k)$.

We firstly show that $\phi$ is well defined.
Suppose $g = hk = h'k'$, then $h'^{-1}h = k'k^{-1}$. $h'^{-1}h \in H$ and $k'k^{-1} \in K$. Then both sides in $H \cap K = \{e\}$.
$h'^{-1}h = e \Rightarrow h = h'$. Similarly, $k = k'$.

Let $g, g' \in G$, $g = hk$, $g' = h'k'$. $\phi(gg') = \phi(hkh'k') \overset{by property 3}{=} \phi(hh'kk') = (hh', kk') = (h, k)(h', k') = \phi(g)\phi(g')$.

Injective: $\phi(g) = \phi(g')$, $g = hk$, $g' = h'k'$, then $(h,k) = (h',k')$, Thus $h' = h$, $k' = k$, $g = g'$.
Surjective: Take $(h,k) \in H \times K$. Let $hk \in G$, $\phi(hk) = (h,k)$, $\square$

**Example:** Find groups that are isomorphic to $U_{12} = \{1, 5, 7, 11\}$.
Note $\langle 5\rangle = \{1,5\} \leq U_{12}$, and $\langle 7\rangle = \{1,7\} \leq U_{12}$, $5 \cdot 7 \equiv 11 \mod 12$.
Then $U_{12} = \langle 5\rangle\langle 7\rangle \cong \langle 5\rangle \times \langle 7\rangle \overset{\text{By Theorem 2.18}}{\cong} \mathbb{Z}_2 \times \mathbb{Z}_2$.

**Example:** Find groups that are isomorphic to $D_6 = \langle r, s : r^6 = s^2 = e, rs = sr^5\rangle$ $(r^3 s = sr^3)$
$H = \langle r^3\rangle \cong \mathbb{Z}_2$, $K = \langle s, r^3\rangle = \{e, r^2, r^4, s, sr^2, sr^4\} \cong D_3$.
Note that $r = r^7 = r^3 \cdot r^4$, $D_6 = HK$, Thus $D_6 \overset{\text{By Theorem 2.18}}{\cong} H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

***Definition:* 2.23: Normal Subgroup**

Given a group $G$, we say $N \leq G$ is normal if $gN = Ng, \forall g \in G$. Equivalently, $gNg^{-1} = N, \forall g \in G \Leftrightarrow gng^{-1} \in N, \forall g \in G, n \in N$.
Write $N \trianglelefteq G$.

***Theorem:* 2.19:**

Every subgroup of an abelian group is normal.

*Proof.* Let $G$ be an abelian group, $H \leq G$.
Take $h \in H$, $g \in G$. $ghg^{-1} \overset{\text{abelian}}{=} gg^{-1}h = h \in H$. Thus $H \trianglelefteq G$. $\square$

**Example:** Find the normal subgroups of $D_3 = \langle r, s\rangle = \{e, r, r^2, s, sr, sr^2\}$
We only need to consider the generator subgroups of $\langle r\rangle$ and $\langle s\rangle$.
For $\langle r\rangle = \{e, r, r^2\}$. $s\langle r\rangle = \{s, sr, sr^2\}$, $\langle r\rangle s = \{s, rs = sr^2, r^2 s = sr\}$, thus $\langle r\rangle \trianglelefteq D_3$
For $\langle s\rangle = \{e, s\}$, $r\langle s\rangle = \{r, rs\} = \{r, sr^2\}$, $\langle s\rangle r = \{r, sr\} \neq r\langle s\rangle$. Thus $\langle s\rangle$ is not a normal subgroup of $D_3$.

***Definition:* 2.24: Left Cosets**

For any subgroup $H \leq G$, denote the set of left cosets $G/H = \{gH : g \in G\}$. By Theorem 2.11, $|G/H| = [G : H] = \frac{|G|}{|H|}$.

***Theorem:* 2.20: Quotient Groups**

If $N \trianglelefteq G$, then $G/N$ forms a group known as the quotient group with $(xN)(yN) = (xy)N$.

*Proof.* Suppose $N \trianglelefteq G$. Let $x_1, x_2, y_1, y_2 \in G$ s.t. $x_1 N = x_2 N$ $(x_1 x_2^{-1} \in N)$ and $y_1 N = y_2 N$ $(y_1 y_2^{-1} \in N)$. Then

$$\begin{aligned}
(x_1 N)(y_1 N) &= (x_1 y_1)N \\
&= (x_1 y_1 y_1^{-1} y_2)N \text{ (since } y_1^{-1} y_2 \in N) \\
&= (x_1 y_2)N = N(x_1 y_2) \text{ (By Definition 2.23)} \\
&= N(x_2 x_1^{-1} x_1 y_2) \text{ (since } x_2 x_1^{-1} \in N) \\
&= N(x_2 y_2) = (x_2 y_2)N
\end{aligned}$$

Thus $(x_1N)(y_1N) = (x_2N)(y_2n)$. The operation is well defined.

Check that $G/N$ is indeed a group:

1. Identity: $eN = N$, $(xN)(eN) = (xe)N = xN$
2. Inverse: $(xN)^{-1} = x^{-1}N$ (Only when $N$ is normal)
3. Associative: $((xN)(yN))zN = xyzN = (xN)((yN)(zN))$ (Only when $N$ is normal)
4. Closed since $G$ is closed.

Thus $G/N$ is a group. $\square$

**Example:** Find the quotient group of $D_3 = \{e, r, r^2, s, sr, sr^2\}$ by $\langle r\rangle = \{e, r, r^2\}$.
Note that $s\langle r\rangle = \langle r\rangle s$, $\langle r\rangle \trianglelefteq D_3$
By Theorem 2.11, $|D_3/\langle r\rangle| = [D_3 : \langle r\rangle] = \frac{|D_3|}{|\langle r\rangle|} = 2$.
$D_3/\langle r\rangle = \{\langle r\rangle, s\langle r\rangle\} \cong \mathbb{Z}_2$. ($\langle r\rangle \to 0$, $s\langle r\rangle \to 1$)

**Example:** Find the quotient groups of $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} = \langle i, j\rangle$.
Firstly, we consider $\langle i\rangle = \{1, i, -1, -i\}$ Note that $j\langle i\rangle = \langle i\rangle j = \{j, -k, -j, k\}$. Thus $\langle i\rangle \trianglelefteq Q_8$
$Q_8/\langle i\rangle = \{\langle i\rangle, j\langle i\rangle\} \cong \mathbb{Z}_2$. The quotient groups by $\langle j\rangle$ and $\langle k\rangle$ are similar.
Then, we consider $\langle -1\rangle = \{1, -1\} \trianglelefteq Q_8$
$Q_8/\langle -1\rangle = \{\langle -1\rangle, i\langle -1\rangle, j\langle -1\rangle, k\langle -1\rangle\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, because each of the non-identity element has order 2.
$\langle 1\rangle \to (0,0)$, $i\langle 1\rangle \to (1,0)$, $j\langle 1\rangle \to (0,1)$, $k\langle 1\rangle \to (1,1)$.

***Theorem:* 2.21:**

$Z(G) \trianglelefteq G$. If $G/Z(G)$ is cyclic, then $G$ is abelian.

*Proof.* Firstly, we show that $Z(G) \trianglelefteq G$
Let $g \in G$, $gZ(G) = \{gx : x \in Z(G)\} \overset{\text{By Definition 2.12}}{=} \{xg : x \in Z(G)\} = Z(G)g$
Thus by Definition 2.23, $Z(G) \trianglelefteq G$.

Assume $G/Z(G) = \langle xZ(G)\rangle$. By Theorem 2.3, $G = \bigcup_{n=0}^{\infty} x^n Z(G)$.
Take $a, b \in G$, $a = x^n Z(G) = x^n y$, $b = x^m Z(G) = x^m z$ for some $m, n \in \mathbb{Z}$, $m, n \geq 0$, $y, z \in Z(G)$.
$ab = x^n y x^m z \overset{\text{By Definition 2.12}}{=} x^n x^m yz = x^{n+m} zy = x^m x^n zy = x^m z x^n y = ba$.
Thus $G$ is abelian. $\square$

### 2.6 Group Homomorphism

***Definition:* 2.25: Group Homomorphism**

Suppose $G$ and $H$ are groups. A map $\phi : G \to H$ is called a homomorphism if $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

**Example:** $\phi : \mathbb{Z} \to G$ s.t. $\phi(n) = g^n$. $G$ any group. $g \in G$ fixed. Then $\phi$ is a homomorphism. $\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$.

**Example:** $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^\times$, $\phi(A) = \det A$ is a homomorphism. $\phi(AB) = \det(AB) = \det A \det B = \phi(A)\phi(B)$.

**Example:** $\phi : \mathbb{R} \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$. $\phi(x) = e^{ix}$ is a homomorphism. $\phi(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = \phi(x)\phi(y)$.

***Theorem:* 2.22: Properties of Homomorphism**

Let $\phi : G_1 \to G_2$ be a homomorphism. Then

1. $\phi(e_1) = e_2$
2. $\forall x \in G$, $\phi(x^{-1}) = (\phi(x))^{-1}$
3. If $H_1 \leq G_1$, then $\phi(H_1) \leq G_2$
4. If $H_2 \leq G_2$, then $\phi^{-1}(H_2) \leq G_1$. If $H_2 \trianglelefteq G_2$, then $\phi^{-1}(H_2) \trianglelefteq G_1$.

*Proof.*

1. Let $x \in G_1$, $e_1 x = x$. Since $\phi$ is a homomorphism, $\phi(e_1 x) = \phi(x) = \phi(e_1)\phi(x)$. Then $\phi(e_1) = \phi(x)(\phi(x))^{-1} = e_2$
2. $e_1 = xx^{-1}$. $e_2 \overset{\text{By 1.}}{=} \phi(e_1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Thus $\phi(x^{-1}) = (\phi(x))^{-1}$
3. Let $x, y \in H_1$, then By Theorem 2.3, $xy^{-1} \in H_1$. $\phi(x) \in \phi(H_1)$, $\phi(y) \in \phi(H_1)$, $(\phi(y))^{-1} = \phi(y^{-1}) \in \phi(H_1)$.
   Then $\phi(x)(\phi(y))^{-1} = \phi(xy^{-1}) \in \phi(H_1)$. Thus $\phi(H_1) \leq G_2$.
4. Suppose $H_2 \leq G$. Let $x, y \in \phi^{-1}(H_2)$, $\phi(x), \phi(y) \in H_2$. Then $\phi(x)(\phi(y))^{-1} = \phi(xy^{-1}) \in H_2$
   $\Rightarrow xy^{-1} \in \phi^{-1}(H_2)$. By Theorem 2.3, $\phi^{-1}(H_2) \leq G_1$.

   Suppose $H_2 \trianglelefteq G_2$. Take $n \in \phi^{-1}(H_2)$, $\phi(n) \in H_2$, $x \in G_1$. $\phi(xnx^{-1}) = \phi(x)\phi(n)\phi(x)^{-1} \in H_2$ because $H_2 \trianglelefteq G_2$.
   Thus $xnx^{-1} \in \phi^{-1}(H_2)$, $\phi^{-1}(H_2) \trianglelefteq G_1$.

$\square$

*Remark* 3. $H_1 \trianglelefteq G_1 \not\Rightarrow \phi(H_1) \trianglelefteq G_2$. *e.g.* $\phi : \mathbb{Z} \to D_n$. $\phi(m) = s^m$. $\mathbb{Z} \trianglelefteq \mathbb{Z}$, but $\phi(\mathbb{Z}) = \langle s \rangle$ is not normal in $D_n$.

***Lemma:* 2.6:**

If $\phi : G \to H$ is a homomorphism, then $|\phi(x)| \,\big|\, |x|$, $\forall x \in G$.

*Proof.* Suppose $\phi : G \to H$ is a homomorphism.
Take $x \in G$ s.t. $|x| = n < \infty$. $x^n = e_G \in G$, $(\phi(x))^n = \phi(x^n) = \phi(e_G) = e_H \in H$
Let $m = |\phi(x)|$. Perform division algorithm $n = mq + r$, $0 \leq r < m$. $n - mq = r$.
$(\phi(x))^r = \phi(x)^n[\phi(x)^m]^{-q} = e_H$. Thus $r = 0$ and $m|n$. $\square$

***Lemma:* 2.7:**

If $C_n = \langle x : x^n = e \rangle \cong \mathbb{Z}_n = \langle 1 \rangle$, then $|x^m| = |\langle x^m \rangle| = \frac{n}{\gcd(m,n)}$. $|m| = \frac{n}{\gcd(m,n)}$ in $\mathbb{Z}_n$

*Proof.* Follows Theorem 2.7. $\square$

**Example:** Find all homomorphism $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$

*Proof.* We find the map of the generator $\phi(1)$.
By Lemma 2.6, $|\phi(1)| \,\big|\, |1| = 24$. Thus $|\phi(1)| \in \{1, 2, 3, 4, 6, 8, 12\}$

In $\mathbb{Z}_{18}$, we want to find $m$ s.t. $|m| = \frac{18}{\gcd(m,18)}$ is in $\{1,2,3,4,6,8,12\}$.
$|1| = |5| = |7| = |11| = |13| = |17| = 18$
$|2| = |4| = |8| = |10| = |14| = |16| = 9$, not possible
$|3| = |15| = 6$, $\phi(1) = 3$ and $\phi(1) = 15$
$|6| = |12| = 3$, $\phi(1) = 6$ and $\phi(1) = 12$
$|9| = 2$, $\phi(1) = 9$.

$\phi(1) = 0$ mapping the identity is also a homomorphism. $\square$

**_Definition:_ 2.26: Kernel**

Given $\phi G_1 \to G_2$ a homomorphism, the kernel of $\phi$ is $\text{Ker}(\phi) = \{x \in G_1 : \phi(x) = e_2\} = \phi^{-1}(e_2)$.

**Example:** $\phi : \mathbb{Z} \to \mathbb{Z}_5$, $\phi(n) = [n]$. Then $\text{Ker}(\phi) = \{n \in \mathbb{Z} : \phi(n) = [0]\} = 5\mathbb{Z}$.

**Example:** $\phi : \mathbb{R} \to \mathbb{C}^{\times}$, $\phi(x) = e^{2\pi i x}$. Then $\text{Ker}(\phi) = \{x \in \mathbb{R} : e^{2\pi i x} = 1\} = \mathbb{Z}$.

**_Theorem:_ 2.23:**

For a homomorphism $\phi : G_1 \to G_2$, $\text{Ker}(\phi) \trianglelefteq G_1$.

*Proof.* Firstly, we show that $\text{Ker}(\phi) \leq G_1$.
Let $x, y \in \text{Ker}(\phi)$, $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_2 e_2^{-1} = e_2$. Thus $xy^{-1} \in \text{Ker}(\phi)$. By Theorem 2.3, $\text{Ker}(\phi) \leq G_1$.

Let $x \in G_1$, $n \in \text{Ker}(\phi)$, $\phi(xnx^{-1}) = \phi(x)\phi(n)\phi(x)^{-1} = \phi(x)e_2\phi(x)^{-1} = \phi(x)\phi(x)^{-1} = e_2$.
Thus $xnx^{-1} \in \text{Ker}(\phi)$, $\text{Ker}(\phi) \trianglelefteq G_1$. $\square$

**_Theorem:_ 2.24: Inverse Homomorphism**

$\psi : G \to G$ defined by $\psi(x) = x^{-1}$ is a homomorphism $\Leftrightarrow$ $G$ is abelian.

*Proof.* ($\Leftarrow$) Suppose $G$ is abelian.
Let $x, y \in G$, $xy = yx$
$\psi(xy) = (xy)^{-1} = y^{-1}x^{-1} \overset{\text{abelian}}{=} x^{-1}y^{-1} = \psi(x)\psi(y)$. Thus $\psi$ is a homomorphism.

($\Rightarrow$) Suppose $\psi(x) = x^{-1}$ is a homomorphism.
Let $x, y \in G$. $\psi(xy) = \psi(x)\psi(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1} \Rightarrow y^{-1}x^{-1} = x^{-1}y^{-1} \Rightarrow xy = yx$. $G$ is abelian. $\square$

## 2.7 Isomorphism Theorems for Groups

### 2.7.1 First Isomorphism Theorem

**Theorem: 2.25: First Isomorphism Theorem**

If $\phi : G \to H$ is a homomorphism and $\pi : G \to G/\text{Ker}(\phi)$, then there exists a unique isomorphism $\psi : G/\text{Ker}(\phi) \to Im(\phi) \leq H$ s.t. $\psi\pi = \phi$.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & Im(\phi) \leq H \\ G/\text{Ker}(\phi) \arrow[ur, "\psi"'] & \end{tikzcd}$$

*Proof.* Let $\psi : G/\text{Ker}(\phi) \to H$ s.t. $\psi(x\text{Ker}(\phi)) = \phi(x) \in Im(\phi) \leq H$.

Well defined: Suppose $x\text{Ker}(\phi) = y\text{Ker}(\phi)$, thus $xy^{-1} \in \text{Ker}(\phi)$. $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e$. Thus $\psi(x\text{Ker}(\phi)) = \phi(x) = \phi(y) = \psi(y\text{Ker}(\phi))$

Homomorphism:
$\psi((x\text{Ker}(\phi))(y\text{Ker}(\phi))) \overset{\text{Definition 2.20}}{=} \psi(xy\text{Ker}(\phi)) \overset{\text{Definition of } \psi}{=} \phi(xy) = \phi(x)\phi(y) = \psi(x\text{Ker}(\phi)\psi(y\text{Ker}(\phi))$

Injective: Suppose $x\text{Ker}(\phi) \in \text{Ker}(\psi)$, then $\psi(x\text{Ker}(\phi)) = e = \phi(x)$. Thus $x \in \text{Ker}(\phi)$, $x\text{Ker}(\phi) = e\text{Ker}(\phi) = \text{Ker}(\phi)$. Thus $\text{Ker}(\psi) = \{\text{Ker}(\phi)\}$. Kernal is trivial and $\psi$ is injective.

Surjective: suppose $y \in Im(\phi)$, there exists $x \in G$ s.t. $\phi(x) = y$, then $\psi(x\text{Ker}(\phi)) = \phi(x) = y$

Thus $\psi : G/\text{Ker}(\phi) \to H$ is an isomorphism.

Note that $\pi(x) = x\text{Ker}(\phi)$. Then $\psi(x\text{Ker}(\phi)) = \psi(\pi(x)) = \phi(x)$. Thus $\psi\pi = \phi$.

Suppose $\bar{\psi} : G/\text{Ker}(\phi) \to H$ s.t. $\bar{\psi}\pi = \phi$. Take $x\text{Ker}(\phi) \in G/\text{Ker}(\phi)$. Then $\bar{\psi}(x\text{Ker}(\phi)) = \bar{\psi}(\pi(x)) = \phi(x) = \psi(\pi(x)) = \psi(x\text{Ker}(\phi))$. $\square$

**Definition: 2.27: Group of Automorphisms and Inner Automorphisms**

Let $G$ be a group.
The automorphism group of $G$ is $Aut(G) = \{\phi : G \to G : \phi \text{ is an isomorphism}\}$.
The inner automorphism group of $G$ is $Inn(G) = \{I_g : G \to G : I_g(x) = gxg^{-1}\}$.
$Aut(G)$ forms a group with function composition and $Inn(G) \leq Aut(G)$.

*Proof.* For $Aut(G)$, the identity is $id : G \to G$ s.t. $id(g) = g$.
Inverse: if $\phi : G \to G$ is an isomorphism, then $\phi^{-1} : G \to G$ is also a well-defined isomorphism. $\phi \in Aut(G) \Leftrightarrow \phi^{-1} \in Aut(G)$.
Associativity follows associativity of function compositions.
Closure: composition of automorphisms is still an automorphism.

Show that $Inn(G) \leq Aut(G)$:
Let $I_x, I_y \in Inn(G)$. Note $I_y \circ I_{y^{-1}}(g) = y(y^{-1}gy)y^{-1} = g$, so $(I_y)^{-1} = I_{y^{-1}}$.
$I_x \circ (I_y)^{-1}(g) = I_x \circ I_{y^{-1}}(g) = x(y^{-1}gy)x^{-1} = (xy^{-1})g(yx^{-1}) = (xy^{-1})g(xy^{-1})^{-1} = I_{xy^{-1}}(g)$
Thus $I_x \circ (I_y)^{-1} = I_{xy^{-1}} \in Inn(G)$. By Theorem 2.3, $Inn(G) \leq Aut(G)$. $\square$

**Theorem: 2.26:**

$G/Z(G) \cong Inn(G)$

*Proof.* Define $\phi : G \to Inn(G) \leq Aut(G)$. $\phi(g) = I_g$, where $I_g(x) = gxg^{-1}$.

Homomorphism: Let $x \in G$, $\phi(gh)(x) = I_{gh}(x) = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = I_g(I_h(x)) = I_g \circ I_h(x)$.

Surjectivity is obvious by definition of the function.

Consider the kernel. Ker$(\phi) = \{g \in G : \phi(g) = I_g = id\}$. $I_g(x) = gxg^{-1} = x$, $\forall x \in G \Leftrightarrow gx = xg$ which follows Definition 2.12.

By Theorem 2.25, $G/Z(G) \cong Inn(G)$. □

**Example:** $\phi : \mathbb{Z} \to \mathbb{Z}_n$ s.t. $\phi(m) = [m] = \{k \in \mathbb{Z} : k \equiv m \mod n\}$
Surjective: $\forall 0 \leq m \leq n-1$, $\phi(m) = [m]$
Homomorphism: $\phi(m_1 + m_2) = [m_1 + m_2] = [m_1] + [m_2] = \phi(m_1) + \phi(m_2)$
Ker$(\phi) = \{m \in \mathbb{Z} : [m] = [0]\} = n\mathbb{Z}$
By Theorem 2.25, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

**Example:** $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2$ s.t. $\phi([m]_4) = [m]_2$
Well Defined: Suppose $[m_1]_4 = [m_2]_4$, then $[m_1 - m_2]_4 = [0]_4 \Rightarrow m_1 - m_2 \equiv 0 \mod 4 \equiv 0 \mod 2$. Then, $[m_1 - m_2]_2 = [0]_2$. $\phi(m_1) = [m_1]_2 = [m_2]_2 = \phi(m_2)$.
Homomorphism: $\phi([m_1]_4 + [m_2]_4) = \phi([m_1 + m_2]_4) = [m_1 + m_2]_2 = [m_1]_2 + [m_2]_2 = \phi([m_1]_4) + \phi([m_2]_4)$.
Surjective: $\phi([0]_4) = [0]_2$, $\phi([1]_4) = [1]_2$
Ker$(\phi) = \{[m]_4 : \phi([m]_4) = [m]_2 = [0]_2\} = \{[0]_4, [2]_4\} = 2\mathbb{Z}_4 \cong \mathbb{Z}_2$.
By Theorem 2.25, $\mathbb{Z}_4/2\mathbb{Z}_4 \cong \mathbb{Z}_4/\mathbb{Z}_2 \cong \mathbb{Z}_2$.

**Example:** $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{15}$.

The order of elements of $\mathbb{Z}_{15}$ $\begin{cases} 1 : [0]_{15} \\ 3 : [5]_{15}, [10]_{15} \\ 5 : [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15} \\ 15 : \text{all other elements} \end{cases}$

If $\phi([1]_6) = [0]_{15}$. Then Ker$(\phi) = \mathbb{Z}_6$, $Im(\phi) = \{[0]_{15}\}$. $\mathbb{Z}_6/\mathbb{Z}_6 \cong \{[0]_{15}\} \leq \mathbb{Z}_15$.
If $\phi([1]_6) = [5]_{15}$. Then $\phi([0]_6) = \phi([3]_6) = [0]_{15}$, $\phi([1]_6) = \phi([4]_6) = [5]_{15}$, $\phi([2]_6) = \phi([5]_6) = [10]_{15}$
Ker$(\phi) = \{[0]_6, [3]_6\} = \langle [3]_6 \rangle \cong \mathbb{Z}_2$. $Im(\phi) = \{[0]_{15}, [5]_{15}, [10]_{15}\} = \langle [5]_{15} \rangle \cong \mathbb{Z}_3$
By Theorem 2.25, $\mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_6/\langle [3]_6 \rangle \cong \langle [5]_{15} \rangle \cong \mathbb{Z}_3$.

**Example:** $D_n = \langle r, s : r^n = s^2 = e, rs = sr^{n-1} \rangle$, $\phi : D_n \to \mathbb{Z}_2$ s.t. $\phi(r) = 0$, $\phi(s) = 1$.
$\phi(r^n) = n\phi(r) = 0$, $\phi(s^2) = \phi(e) = 0 = \phi(s) + \phi(s) = 1 + 1$.
$1 = \phi(s) + \phi(r) = \phi(sr) = \phi(sr^{n-1}) = \phi(s) + (n-1)\phi(r)$.
Ker$(\phi) = \langle r \rangle$, $\phi(r^k) = k\phi(r) = 0$, $\phi(sr^k) = \phi(s) + k\phi(r) = 1$, and $D_n/\langle r \rangle \cong \mathbb{Z}_2$ by Theorem 2.25.

**Example:** $\phi : D_n \to \mathbb{Z}_n$ s.t. $\phi(r) = 1$, $\phi(s) = 0$.
$\phi(rs) = \phi(r) + \phi(s) = 1 + 0 = 1$, $\phi(sr^{n-1}) = \phi(s) + (n-1)\phi(r) = n - 1$
Note $rs = sr^{n-1}$, but $\phi(rs) \neq \phi(sr^{n-1})$ unless $n = 2$, so $\phi$ is not a homomorphism in general.

**Example:** $\phi : D_{2n} \to \mathbb{Z}_2$ s.t. $\phi(r) = 1$, $\phi(s) = 0$
$0 = 2n = 2n\phi(r) = \phi(r^{2n}) = \phi(e) = 0$, and $1 = \phi(r) + \phi(s) = \phi(rs) = \phi(sr^{2n-1}) = \phi(s) + (2n-1)\phi(r) = 2n - 1 \mod 2 = 1$

$\text{Ker}(\phi) = \{e, r^{2k}, sr^{2k}\}$ for $0 \le k \le n-1$, $\text{Ker}(\phi) = \langle s, r^2 \rangle \cong D_n$.
By Theorem 2.25, $D_{2n}/\langle s, r^2 \rangle \cong D_{2n}/D_n \cong \mathbb{Z}_2$.

**Example:** $\phi : D_6 \to S_6$ s.t. $\phi(r) = (123456)$, $\phi(s) = (16)(25)(34)$
$\phi(r^6) = (123456)^6 = (1) = \phi(e)$, $\phi(s^2) = ((16)(25)(34))^2 = (16)^2(25)^2(34)^2 = e = \phi(e)$
$\phi(rs) = (123456)(16)(25)(34) = (1)(26)(35)(4) = (26)(35)$
$\phi(sr^5) = (16)(25)(34)(123456)^5 = (16)(25)(34)(165432) = (26)(35)$
Then $Im(\phi) = \langle (123456), (16)(25)(34) \rangle$
Note that $|r| = 6 = |(123456)|$, $\phi(r^n) \ne e$ for $n = 1, 2, 3, 4, 5$. Thus $\text{Ker}(\phi) = \{e\}$.

*Remark* 4. We can similarly construct homomorphism $\phi : D_n \to S_n$

**Example:** $\phi : S_n \to \mathbb{Z}_2$, $\phi(\sigma) = \begin{cases} 0, \sigma \text{ is even} \\ 1, \sigma \text{ is odd} \end{cases}$
It is easy to check that $\phi$ is homomorphism by Definition 2.16.
$\text{Ker}(\phi) = \{\sigma \in S_n : \sigma \text{ even}\} = A_n$.
By Theorem 2.25, $S_n/A_n \cong \mathbb{Z}_2$.

**Example:** $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^\times$ s.t. $\phi(A) = \det(A)$.
$\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$.
$\text{Ker}(\phi) = \{A \in GL_2(\mathbb{R}) : \phi(A) = \det(A) = 1\} = SL_2(\mathbb{R})$.
By Theorem 2.25, $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \cong \mathbb{R}^\times$.

**Example:** Define $gl_2(\mathbb{R}) = \{A \in \mathbb{R}^{2\times 2}\}$, $sl_2(\mathbb{R}) = \{A \in gl_2(\mathbb{R}) : \text{Tr}(A) = 0\}$.
Define $\phi : gl_2(\mathbb{R}) \to \mathbb{R}$ s.t. $\phi(A) = \text{Tr}(A)$. $\phi(A + B) = \text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B) = \phi(A) + \phi(B)$.
$\text{Ker}(\phi) = \{A \in gl_2(\mathbb{R}) : \text{Tr}(A) = 0\} = sl_2(\mathbb{R})$.
By Theorem 2.25, $gl_2(\mathbb{R})/sl_2(\mathbb{R}) \cong \mathbb{R}$.

**Example:** $\phi : gl_2(\mathbb{R}) \to sl_2(\mathbb{R})$, $\phi \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-d & b \\ c & d-a \end{bmatrix}$.
$\text{Ker}(\phi) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \phi \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a-d & b \\ c & d-a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R} \right\} \cong \mathbb{R}$.
By Theorem 2.25, $gl_2(\mathbb{R})/\mathbb{R} \cong sl_2(\mathbb{R})$.

**Example:** Homomorphisms for $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$

1. $\phi : \mathbb{Z} \to \mathbb{R}^\times$
   (a) $\phi(1) = 1$, $\phi(n) = 1^n = 1$, $\text{Ker}(\phi) = \mathbb{Z}$, $Im(\phi) = 1$, $\mathbb{Z}/\mathbb{Z} \cong \{1\} \le \mathbb{R}^\times$
   (b) $\phi(1) = -1$, $\phi(n) = (-1)^n$. $\text{Ker}(\phi) = 2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\} \le \mathbb{R}^\times$
   (c) $\phi(1) = a$, $\phi(n) = a^n$, $a \in \mathbb{R}^\times \setminus \{\pm 1\}$. $\text{Ker}(\phi) = \{0\}$, $\mathbb{Z} \cong \{\pm a^n : n \in \mathbb{Z}\}$
2. $\phi : \mathbb{R} \to \mathbb{R}^\times_+$, $\phi(x) = 2^x$. $\text{Ker}(\phi) = \{0\}$. $Im(\phi) = \mathbb{R}^\times_+$, $\mathbb{R} \cong \mathbb{R}^\times_+$
3. $\phi : \mathbb{Z} \to \mathbb{C}$, $\phi(n) = i^n$. $Im(\phi) = \{1, i, -1, -i\}$. $\text{Ker}(\phi) = \{n \in \mathbb{Z} : i^n = 1\} = 4\mathbb{Z}$. $\mathbb{Z}/4\mathbb{Z} \cong \langle i \rangle$.
4. $\phi : \mathbb{Z} \to \mathbb{C}^\times$. $\phi(m) = e^{\frac{2\pi i m}{n}}$. $\text{Ker}(\phi) = \{m : e^{\frac{2\pi i m}{n}}\} = n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \cong \{1, \omega_n, ..., \omega_n^{n-1}\} = \langle \omega_n \rangle \cong \mathbb{Z}_n \le \mathbb{C}^\times$, where $\omega_n = e^{\frac{2\pi i}{n}}$
5. $\phi : \mathbb{Z} \to \mathbb{C}$, $\phi(n) = (2i)^n$. $\text{Ker}(\phi) = \{0\}$. $Im(\phi) = \{(2i)^n : n \in \mathbb{Z}\} \le \mathbb{C}^\times$. $\mathbb{Z} \cong \{(2i)^n : n \in \mathbb{Z}\}$.
6. $\phi : \mathbb{R} \to \mathbb{C}^\times$, $\phi(x) = e^{2\pi i x}$. $Im(\phi) = \{z \in \mathbb{C}^\times : |z| = 1\} = S^1$. $\text{Ker}(\phi) = \{x \in \mathbb{R} : e^{2\pi i x} = 1\} = \mathbb{Z}$. $\mathbb{R}/\mathbb{Z} \cong S^1$

**Example:** $\phi : Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ s.t. $\phi(\pm 1) = (0,0)$, $\phi(\pm i) = (1,0)$, $\phi(\pm j) = (0,1)$, $\phi(\pm k) = (1,1)$. $\text{Ker}(\phi) = \{\pm 1\} = \langle -1 \rangle$. $Q_8/\langle -1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

**Example:** $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. $\langle 2 \rangle = \{1, 2, 4, 8\} \cong \langle 7 \rangle = \{1, 7, 4, 13\} \cong \mathbb{Z}_4$, $\langle 4 \rangle = \{1, 4\} \cong \mathbb{Z}_2$.
$U_{15} = \langle 2 \rangle \langle 11 \rangle$
Define $\phi : \mathbb{Z} \times \mathbb{Z} \to U_{15}$ s.t. $\phi(m,n) = 2^m 11^n$. $\text{Ker}(\phi) = 4\mathbb{Z} \times 2\mathbb{Z}$. Thus $(\mathbb{Z} \times \mathbb{Z})/(4\mathbb{Z} \times 2\mathbb{Z}) \cong U_{15} \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

### 2.7.2 Second Isomorphism Theorem

***Theorem:* 2.27: Second Isomorphism Theorem**

Let $H \leq G$ and $N \trianglelefteq G$, then

1. $HN \leq G$
2. $H \cap N \trianglelefteq H$, $N \trianglelefteq HN$
3. $H/(H \cap N) \cong HN/N$

*Proof.*

1. Let $x, y \in HN$, *i.e.* $x = h_1 n_1$, $y = h_2 n_2$ for $h_1, h_2 \in H$, $n_1, n_2 \in N$
   Since $N \trianglelefteq G$, $gN = Ng$ $\forall g \in G$, then $gn = n'g$ for some $n, n' \in N$.
   $xy^{-1} = (h_1 n_1)(h_2 n_2)^{-1} = h_1(n_1 n_2^{-1})h_2^{-1} \overset{\text{Definition 2.23}}{=} h_1 h_2^{-1} \hat{n}$ for some $\hat{n} \in N$.
   Thus $xy^{-1} \in HN$. $HN \leq G$ by Theorem 2.3.

2. $H \cap N \trianglelefteq H$ can be shown in 3. We show $N \trianglelefteq HN$ here.
   Let $n \in N$, $x = hn'$ for $h \in H$, $n' \in N$
   $xnx^{-1} = h(n'nn'^{-1})h^{-1} = h\hat{n}h^{-1}$ for $\hat{n} = n'nn'^{-1} \in N$. Thus $xnx^{-1} = h\hat{n}h^{-1} \in N$, because $h \in G$, $\hat{h} \in N$ and $N \trianglelefteq G$.

3. Define $\phi : H \to HN/N$ s.t. $\phi(h) = hN$.
   $\phi(xy) = xyN \overset{\text{By Definition 2.20}}{=} (xN)(yN) = \phi(x)\phi(y)$

   Surjective: Suppose $xN \in HN/N$, *i.e.* $x \in HN$, then $x = hn$ where $h \in H$, $n \in N$.

   Injective: Note $xN = (hn)N = hN$, $\phi(h) = hN = xN$, thus $\phi$ is injective.

   $\text{Ker}(\phi) = \{h \in H : \phi(h) = eN = N\}$. Note if $h \in \text{Ker}(\phi)$, then $\phi(h) = hN$. Thus $h \in N \Rightarrow h \in H \cap N$. *i.e.* $\text{Ker}(\phi) \subset H \cap N$.

   Suppose $x \in H \cap N$, then $x \in H$ and $x \in N$. Then $xN = N$. Thus $\phi(x) = xN = N$, $x \in \text{Ker}(\phi)$. Then $H \cap N \subset \text{Ker}(\phi)$. Thus $\text{Ker}(\phi) = H \cap N$.

   By Theorem 2.25, $H/(H \cap N) \cong HN/N$.

Since $\text{Ker}(\phi) = H \cap N$, by Theorem 2.23, $H \cap N \trianglelefteq H$. □

**Example:** Let $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $N = n\mathbb{Z}$. $H + N = m\mathbb{Z} + n\mathbb{Z} = \{mx + ny : x, y \in \mathbb{Z}\} = \gcd(m,n)\mathbb{Z}$.
$H \cap N = \{a \in \mathbb{Z} : a = mx \text{ and } a = ny\} = \text{lcm}(m,n)\mathbb{Z}$.
Let $d = \gcd(m,n)$, $l = \text{lcm}(m,n)$
By Theorem 2.27, $m\mathbb{Z}/l\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$.
Consider $\phi : d\mathbb{Z} \to \mathbb{Z}_{n/d}$, $\phi(dx) = [x]$. $\text{Ker}(\phi) = \{dx \in d\mathbb{Z} : \phi(dx) = 0\} = \{dx \in d\mathbb{Z} : [x] = 0\} = n\mathbb{Z}$
Then by Theorem 2.25, $d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{n/d}$.
Thus $\mathbb{Z}_{n/d} \cong d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}_{l/m}$.
Then $\frac{n}{d} = |\mathbb{Z}_{n/d}| = |\mathbb{Z}_{l/m}| = \frac{l}{m} \Rightarrow \frac{m}{\gcd(m,n)} = \frac{\text{lcm})m,n}{n}$. $\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$.

### 2.7.3 Third Isomorphism Theorem

**Theorem: 2.28: Third Isomorphism Theorem**

Let $N \trianglelefteq H \trianglelefteq G$, then $(G/N)/(H/N) \cong G/H$

*Proof.* Define $\phi : G/N \to G/H$ s.t. $\phi(gN) = gH$.

Well defined: suppose $gN = g'N$, then $g(g')^{-1} \in N \leq H$. Thus $g(g')^{-1} \in H$. By Lemma 2.5, $gH = g'H$. Therefore, $\phi(gN) = \phi(g'N)$.

Homomorphism: $\phi((gN)(g'N)) = \phi(gg'N) = gg'H = (gH)(g'H) = \phi(gN)\phi(g'N)$

Surjective: Let $gH \in G/H$. Then $gN \in G/N$ since $N \trianglelefteq H$. Then $\phi(gN) = gH$.

Let $gN \in \mathrm{Ker}(\phi) = \{gN \in G/N : \phi(gN) = gH = H\}$. Then $g \in H$, $gN \in H/N$. Thus $\mathrm{Ker}(\phi) \subset H/N$
Let $hN \in H/N$. Then $hN \in G/N$, since $h \in G$. $\phi(hN) = hH = H$. Thus $hN \in \mathrm{Ker}(\phi)$. $H/N \subset \mathrm{Ker}(\phi)$
Thus $H/N = \mathrm{Ker}(\phi)$. By Theorem 2.25, $(G/N)/(H/N) \cong G/H$. $\square$

**Example:** Let $G = \mathbb{Z}$, $H = m\mathbb{Z}$, $N = mn\mathbb{Z}$, $N \trianglelefteq H \trianglelefteq G$

$$\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z} = G/H \overset{\text{By Theorem 2.28}}{\cong} (G/N)/(H/N) = (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}_{mn}/\langle m\rangle$$

Consider $\phi : m\mathbb{Z} \to \mathbb{Z}_{mn}$, $\phi(mx) = [mx]$. $Im(\phi) = \langle [m]\rangle \leq \mathbb{Z}_{mn}$. $\mathrm{Ker}(\phi) = mn\mathbb{Z}$.
By Theorem 2.25, $m\mathbb{Z}/mn\mathbb{Z} \cong \langle [m]\rangle \leq \mathbb{Z}_{mn}$.

**Theorem: 2.29:**

$\mathbb{Z}_n/\langle m\rangle \cong \mathbb{Z}_{\gcd(m,n)}$

*Proof.* We want to show $\langle m\rangle = \langle \gcd(m,n)\rangle$.
Let $d = \gcd(m,n)$

($\leq$) $d|m$, so $m = dk$ for some $k \in \mathbb{N}$, $\langle m\rangle = \{mx : x \in \mathbb{Z}\} = \{dkx : x \in \mathbb{Z}\} \leq \langle d\rangle$

($\geq$) By extended Euclidean algorithm, write $d = ma + nb$ for $a, b \in \mathbb{Z}$. Inside $\mathbb{Z}_n$, $d = ma$ for $a \in \mathbb{Z}$, $\langle d\rangle = \langle m\rangle$. $\square$

# 3 Rings

**Definition: 3.1: Ring**

A set $R$ together with operations $(+, \cdot)$ is called a ring if
1. $(R, +)$ is an abelian group with identity 0.
2. $(ab)c = a(bc)$, $\forall a, b, c \in R$
3. $a(b + c) = ab + ac$
4. $(a + b)c = ac + bc$

*Remark* 5. In the context of rings, identity, inverses, and commutativity specifically refer to the ones for multiplication. We don't necessarily need identity, inverses or commutativity for a ring.

**Example:** $\mathbb{Z}$: identiy=1, commutative, $\pm 1$ are the only integers with inverses.

**Example:** $2\mathbb{Z}$: no identiy, commutative, no inverses.

**Example:** $\mathbb{Z}_n$: identity=1, commutative, $m^{-1} \in \mathbb{Z}_n$ exists $\Leftrightarrow \gcd(m, n) = 1$.

**Example:** $\mathbb{R}^{n\times n}$: identity=$I_n$, not commutative, $A^{-1}$ exists $\Leftrightarrow \det(A) \neq 0$.

**Example:** $\mathbb{Z}[x] = \{a_0 + a_1x + \cdots a_nx^n : n \geq 0, a_i \in \mathbb{Z}\}$, identity=1, commutative, only $\pm 1$ have inverses.

**Definition: 3.2: Zero Divisors**

If $a, b \neq 0 \in R$ and $ab = 0$, then $a$ and $b$ are the zero divisors of $R$.

**Definition: 3.3: Unit**

$a \in R$ is a unit if $\exists b \in R$ s.t. $ab = 1_R$.

**Example:** $\mathbb{Z}_{12}$. Units: $1, 5, 7, 11$ (they are not zero divisors). Zero divisors: $2, 3, 4, 6, 8, 9, 10$

**Theorem: 3.1: Units and Zero Divisors of $\mathbb{Z}_n$**

$m \in \mathbb{Z}_n$ is a unit $\Leftrightarrow \gcd(m, n) = 1$
$m \in \mathbb{Z}_n$ is a zero divisor $\Leftrightarrow \gcd(m, n) \neq 1$

*Proof.* Units:
($\Rightarrow$) Suppose $m \in \mathbb{Z}_n$ is a unit, then $\exists x \in \mathbb{Z}_n$ s.t. $mx = 1 \Leftrightarrow mx \equiv 1 \mod n \Leftrightarrow n|(mx - 1)$, so $\exists y \in \mathbb{Z}$ s.t. $mx - ny = 1$. Thus $\gcd(m, n)|1$, $\gcd(m, n) = 1$.
($\Leftarrow$) Suppose $\gcd(m, n) = 1$, then $\exists x, y \in \mathbb{Z}$, $mx + ny = 1$, $mx - 1 = -ny$, so $n|mx - 1$, $mx \equiv 1 \mod n$, then $mx = 1 \in \mathbb{Z}_n$.

Zero divisors:
($\Rightarrow$) Suppose that $m \in \mathbb{Z}_n$ is a zero divisor. Assume $\gcd(m, n) = 1$
Then $m$ is a unit by previous statement, $\exists a \neq 0 \in \mathbb{Z}_n$ with $ma = 0 \in \mathbb{Z}_n$, *i.e.* $n|ma$.
$\gcd(m, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ s.t. $mx + ny = 1$. $\Rightarrow (ma)x + (na)y = a$. Since $n|ma$, then $n|(ma)x + n(ay)$, thus $n|a$. $a \equiv 0 \mod n$, $a = 0 \in \mathbb{Z}_n$. Contradiction. Thus $\gcd(m, n) \neq 1$.
($\Leftarrow$) Suppose $m = 0 \in \mathbb{Z}_n$ with $\gcd(m, n) = d \neq 1$. Then $\exists a \in \mathbb{Z}$ with $1 < a < n$ and $ad = n$. (If $a = 1$,

$d = n = m$, similar for $a = n$.)
Find $x, y \in \mathbb{Z}$ with $mx + ny = d$, $amx + any = ad = n$. By commutativity of $\mathbb{Z}_n$, $(ax)m = n(1 - ay) \equiv 0 \mod n$. Thus $(ax)m = 0 \in \mathbb{Z}_n$. $m$ is zero divisor. ☐

***Theorem:* 3.2: Units and Zero Divisors of $\mathbb{R}^{2\times 2}$**

$A \in \mathbb{R}^{2\times 2}$ is a unit $\Leftrightarrow \det A \neq 0$
$A \in \mathbb{R}^{2\times 2}$ is a zero divisor $\Leftrightarrow \det A = 0$

*Proof.* The first statement follows the invertibility of matrices.

Consider the second statement:
($\Rightarrow$) Suppose $A \in \mathbb{R}^{2\times 2}$ is a zero divisor $A \neq 0$ and $\exists B \neq 0$ s.t. $AB = 0$.
Assume $\det A \neq 0$, $A$ has an inverse $A^{-1}$, then $A^{-1}AB = A^{-1}0 = 0$. Then $B = 0$. Contradiction. Thus $A$ does not have an inverse, $\det A = 0$
($\Leftarrow$) Suppose $A \neq 0$, but $\det A = 0$. Then $\exists v \neq 0 \in Nul(A)$. Let $B = (v\ v) \neq 0$. $AB = A(v\ v) = (Av\ Av) = (0\ 0) = 0$. $A$ is a zero divisor. ☐

***Theorem:* 3.3:**

If $a \in R$ is a unit, then it is not a zero divisor.
If $a \in R$ is a zero divisor, then it is not a unit.

*Proof.* Suppose $a \in R$ is a unit and $b \in R$ with $ab = 0$. $b = (a^{-1}a)b = a^{-1}ab = a^{-1}0 = 0$. Thus $b$ has to be 0, and $a$ is not a zero divisor.
The second statement is true by contrapositive. ☐

***Lemma:* 3.1: Identities with -1**

$(-1)^2 = 1$
$-a = (-1)a = a(-1)$

*Proof.* $(-1)^2 + (-1) = (-1)(-1) + (-1)1 = (-1)(-1+1) = (-1)0 = 0$. Thus $(-1)^2$ and $(-1)$ are additive inverse. By uniqueness of inverses, $(-1)^2 = 1$.

$a + (-1)a = 1a + (-1)a = (1-1)a = 0$. And $a + a(-1) = a(1) + a(-1) = a(1-1) = 0$. ☐

***Theorem:* 3.4:**

If $R$ is a ring with 1, $u \in R$ is a unit, then so is $-u$.

*Proof.* Take $u^{-1} \in R$ s.t. $uu^{-1} = 1$. $(-u)(-u^{-1}) = u(-1)(-1)u^{-1} \overset{\text{By Lemma 3.1}}{=} uu^{-1} = 1$.
Thus $(-u)^{-1} = -u^{-1}$ ☐

***Definition:* 3.4: Nilpotent**

$x \in R$ is nilpotent if $x^m = 0$ for some $m \in \mathbb{N}$.

**Example:** In $\mathbb{Z}_4$, $2^2 = 4 = 0$, 2 is a nilpotent element.

**Theorem: 3.5: Properties of Nilpotents**

If $x$ is nilpotent, then
1. $x = 0$ or $x$ is a zero divisor.
2. If $R$ is a ring with 1, $1 + x \in R$ is a unit.

*Proof.* 1. Suppose $x \neq 0$. Let $x \in \mathbb{N}$ s.t. $x^m = 0$ and $m = 0$ is the smallest, then $x^m = x(x^{m-1}) = 0$, but $x \neq 0$ and $x^{m-1} \neq 0$. Both are zero divisors by Definition 3.2.

2. Let $m \in \mathbb{N}$ s.t. $x^m = 0$ and $m$ is minimum. Then $1 = 1 + x^m = (1 + x)(1 - x + \cdots + (-1)^{m-1}x^{m-1})$ Therefore $(1 + x)^{-1} = (1 - x + \cdots + (-1)^{m-1}x^{m-1})$ exists in $R$. By Definition 3.3, $1 + x$ is a unit.

□

## 3.1 Types of Rings

**Definition: 3.5: Ring with 1**

If $R$ has a multiplication identity $1 \in R$, then $R$ is a ring with 1.

**Example:** $\mathbb{R}^{n\times n}$, $f : \mathbb{R} \to \mathbb{R}$, $\mathbb{Z}_n$.

**Definition: 3.6: Commutative Ring**

If $ab = ba$, $\forall a, b \in R$, then $R$ is a commutative ring.

**Example:** $n\mathbb{Z}$, $x\mathbb{Z}[x] = \{a_1x + a_2x^2 + \cdots + a_nx^n\}$, $\mathbb{Z}_n$.

**Definition: 3.7: Integral Domain**

If $R$ is commutative with 1 and $ab = 0 \Rightarrow a = 0$ or $b = 0$, then $R$ is an integral domain.

*Remark* 6. $R$ is an integral domain if it is a commutative ring with 1 and has no zero divisors.

**Example:** $\mathbb{Z}$, $\mathbb{Z}[x]$.

**Definition: 3.8: Division Ring**

If $a^{-1}$ exists for all $a \neq 0 \in R$, then $R$ is a division ring.

**Example:** Quaternion Ring $H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1\}$.

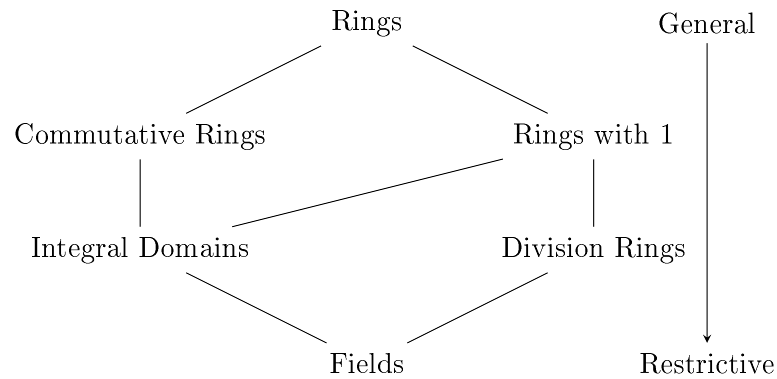
**Definition: 3.9: Field**

A commutative division ring is a field.

**Example:** $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

**Theorem: 3.6: Classification of $\mathbb{Z}_n$**

If $n$ is comoposite, then $\mathbb{Z}_n$ is a commutative ring with 1 and not an integral domain.
If $p$ is a prime, then $\mathbb{Z}_p$ is a finite field.




*Proof.* Note: $\mathbb{Z}_n$ is definitely a commutative ring with 1.

If $n$ is composite, then $n = ab$ with $1 < a, b < n$. $a \neq 0 \in \mathbb{Z}_n$, $b \neq 0 \in \mathbb{Z}_n$, but $ab = 0 \in \mathbb{Z}_n$, thus $\mathbb{Z}_n$ is not integral domain.

$\mathbb{Z}_p$ is integral domain: Suppose $a, b \in \mathbb{Z}_p$ with $ab = 0 \in \mathbb{Z}_p$. $ab \equiv 0 \mod p$, then $p|ab$. Since $p$ is a prime, then $p|a$ or $p|b$. Thus $a = 0 \in \mathbb{Z}_p$ or $b = 0 \in \mathbb{Z}_p$.
$\mathbb{Z}_p$ is a field (check inverse): Let $a \neq 0 \in \mathbb{Z}_p$. Then $\gcd(a, p) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ s.t. $ax + py = 1$, $ax \equiv 1 \mod p$, $a^{-1} = x \in \mathbb{Z}_p$. $\square$

**_Theorem:_ 3.7: Quaternion Ring**

$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1\}$ is a division ring.

*Proof.* It is easy to see that $1 + (0i + bj + 0k) \in H$ is the identity. We want to find the inverse.

Consider $(a + bi + cj + dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$.
Then $(a+bi+cj+dk)(a+bi+cj+dk)^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a+bi+cj+dk)(a-bi-cj-dk) = \frac{1}{a^2+b^2+c^2+d^2}(a^2 + b^2 + c^2 + d^2 + (ab - ab + cd - cd)i + (-bd + bd + ac - ac)j + (ad - ad + bc - bc)k) = 1$. $\square$

**_Theorem:_ 3.8:**

Let $R$ be a commutative ring with 1. Then $R$ is an integral domain $\Leftrightarrow \forall a \neq 0 \in R$, with $ab = ac$, then $b = c$.

*Proof.* $(\Rightarrow)$ Suppose $R$ is an integral domain, and $a \neq 0 \in R$ , $ab = ac$
Subtract both sides by $ac$, $ab - ac = 0 \overset{\text{Associativity}}{\Rightarrow} a(b - c) = 0$. Since $a \neq 0$ and $R$ is an integral domain, we have $b - c = 0$, *i.e.* $b = c$.

$(\Leftarrow)$ Suppose $a \neq 0 \in R$ and $b \in R$ s.t. $ab = 0$. We want to show that $b = 0$
$ab = 0 = a \cdot 0$ *i.e.* $a(b - 0) = 0$. Since $a \neq 0$, $b = 0$. Thus $R$ is an integral domain. $\square$

**_Theorem:_ 3.9: Finite Integral Domain**

Every finite integral domain is a field.

*Proof.* Consider $R^* = \{r \in R : r \neq 0\} = R \setminus \{0\}$. Define $\lambda_a : R^* \to R^*$, $a \neq 0$ s.t. $\lambda_a(b) = ab$.
Injective: Suppose $\lambda_a(b) = \lambda_a(c)$, *i.e.* $ab = ac$. Since $R$ is an integral domain, by Theorem 3.8. $b = c$.
Note: Injection on finite sets $\Rightarrow$ Bijective $\Rightarrow$ Surjective.

Then $1 \in R^* \Rightarrow \exists b \in R^*$ s.t. $\lambda_a(b) = ab = 1$, $b = a^{-1}$. Every non-zero element has an inverse, then it is a field. □

**Definition: 3.10: Boolean Ring**

$R$ is a boolean ring if $a^2 = a$ for all $a \in R$.

**Theorem: 3.10:**

All Boolean Rings are commutative.

*Proof.* Let $x, y \in R$.

$$\begin{aligned}(x+y) = (x+y)^2 &= x^2 + y^2 + xy + yx \\ &= x + y + xy + yx \text{ (By Definition 3.10)}\end{aligned}$$

Thus $xy + yx = 0$, $xy = -yx \Rightarrow xy = (xy)^2 = (-yx)^2 = (-1)^2(yx)^2 = yx$ □

**Example:** Given $X$ a non-empty set, $\mathcal{P}(X)$ is a boolean ring with $+ = \cup$, $\cdot = \cap$.

**Theorem: 3.11: Gaussian Integers**

The Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is an integral domain.

*Proof.* Let $z = a + bi, w = c + di \in \mathbb{Z}[i]$. Suppose $zw = 0$.
$0 = (a+bi)(c+di) = (a-bi)(a+bi)(c+di)(c-di) = (a^2+b^2)(c^2+d^2)$
We need $a^2 + b^2 = 0$ or $c^2 + d^2 = 0$.
Since $\mathbb{Z}$ is an integral domain, then $a^2 + b^2 = 0 \Rightarrow a = 0$ and $b = 0$. Similarly, $c^2 + d^2 = 0 \Rightarrow c = 0$ and $d = 0$. Thus, $z = 0$ or $w = 0$. By Definition 3.7, $\mathbb{Z}[i]$ is an integral domain. □

**Definition: 3.11: Characteristic of a Ring**

The least $n \in \mathbb{N}$ s.t. $\forall r \in R$, $nr = (r + \cdots + r) = 0$ is the charactersitic of $R$. Write $\text{char}(R) = n$. If no such $n$ exists, then $\text{char}(R) = 0$.

**Example:** $\text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = \text{char}(\mathbb{Z}[x]) = 0$

**Theorem: 3.12: Characteristic of $\mathbb{Z}_n$**

$\text{char}(\mathbb{Z}_n) = n$

*Proof.* For all $a \in \mathbb{Z}_n$, $na = 0 \in \mathbb{Z}_n$, thus $\text{char}(\mathbb{Z}_n) \leq n$
Suppose $\text{char}(\mathbb{Z}_n) = m$, $m = m \cdot 1 = 0 \in \mathbb{Z}_n$. $m \equiv 0 \mod n$, $n|m$. Thus $\text{char}(\mathbb{Z}_n) = m \neq n$
Thus $\text{char}(\mathbb{Z}_n) = n$. □

**Lemma: 3.2: Characteristic of Ring with 1**

Let $R$ be a ring with 1. If $n \in \mathbb{N}$ is the least number s.t. $n \cdot 1 = 0$, then $\text{char}(R) = n$

*Proof.* $n \cdot r = (r + \cdots + r) = r \cdot 1 + \cdots + r \cdot 1 = r(1 + \cdot + 1) = rn = r \cdot 0 = 0$. □

**Example:** $2\mathbb{Z}_6 = \{0, 2, 4\}$. $\text{char}(2\mathbb{Z}_6) = 3$.

***Theorem:* 3.13: Characteristic of Integral Domains**

If $R$ is an integral domain, then $\text{char}(R)$ is prime or $\text{char}(R) = 0$.

*Proof.* Use the contrapositive. If $\text{char}(R) = n$ is composite, then $R$ is not an integral domain.
Suppose $n = \text{char}(R)$ with $n = ab$ $(a, b > 1)$. $0 = n \cdot 1 = (ab)1 = (a1)(b1)$. By Lemma 3.2, otherwise $n = a$ or $n = b$. Then $a1 \neq 0$ and $b1 \neq 0$. Thus $R$ is not an integral domain. $\square$

***Theorem:* 3.14: Characteristic of Prime Commutative Ring with 1**

Suppose $R$ is a commutative ring with 1 with $\text{char}(R) = p$ a prime, then $\forall a, b \in R$, $(a+b)^p = a^p + b^p$.

*Proof.* By binomial theorem, $(a+b)^p = \displaystyle\sum_{k=0}^{p} \binom{p}{k}_R a^k b^{p-k} = b^p + \sum_{k=1}^{p-1} \binom{p}{k}_R a^k b^{p-k} + a^p$, where $\binom{p}{k}_R = \underbrace{(1 + \cdots + 1)}_{\binom{p}{k} \text{ times in } R}$.
For $k \in [1, p-1]$, $\binom{p}{k} = \frac{p!}{(p-k)!k!} = p\frac{(p-1)\cdots(p-k+1)}{k!}$ is a multiple of $p$. Thus $\binom{p}{k}_R = 0_R$. $\square$

## 3.2 Ring Homomorphism

***Definition:* 3.12: Ring Homomorphism and Isomorphism**

Let $R, S$ be rings. $\phi : R \to S$ is a ring homomorphism if $\forall a, b \in R$, $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.
If $\phi$ is bijective, then $\phi$ is an ismorphism.
$\text{Ker}(\phi) = \{a \in R : \phi(a) = 0_S\}$.

**Example:** $\phi : \mathbb{Z} \to \mathbb{Z}_n$ s.t. $\phi(m) = [m]$.
Homomorphism: Let $m_1, m_2 \in \mathbb{Z}$, $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$ from Group Homomorphism.
$\phi(m_1 m_2) = [m_1 m_2] = [m_1][m_2] = \phi(m_1)\phi(m_2)$.
$\text{Ker}(\phi) = n\mathbb{Z}$ from group homomorphism.

**Example:** $\phi : \mathbb{C} \to \mathbb{R}^{2\times 2}$ s.t. $\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

Homomorphism: $\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(a+bi) + \phi(c+di)$

$\phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(a+bi)\phi(c+di)$
$\text{Ker}(\phi) = \{a+bi : \phi(a+bi) = 0\} = \{0\}$.
Thus $\phi$ is injective. $\mathbb{C} \cong Im(\phi) = \left\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R}\right\} \subset \mathbb{R}^{2\times 2}$

**Example:** $\phi : \mathbb{Q}[x] \to \mathbb{R}$ s.t. $\phi(p(x)) = p(\sqrt{2})$.
$\phi(x^3 + x^2 - 3) = (\sqrt{2})^3 + (\sqrt{2})^2 - 3 = 2\sqrt{2} - 1$. $Im(\phi) = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field.
Homomorphism: Let $p(x), q(x) \in \mathbb{Q}[x]$. $\phi(p(x)+q(x)) = p(\sqrt{2}) + q(\sqrt{2}) = \phi(p(x)) + \phi(q(x))$

$\phi(p(x)q(x)) = p(\sqrt{2})q(\sqrt{2}) = \phi(p(x))\phi(q(x))$
$\text{Ker}(\phi) = \{p(x) \in \mathbb{Q}[x] : p(\sqrt{2}) = 0\}$. If $p(x) \in \text{Ker}(\phi)$, then $\sqrt{2}$ is a root of $p(x)$.

$$\begin{aligned} p(x) &= (x - \sqrt{2})q(x) \text{ over } \mathbb{R}[x] \\ &= (x^2 - 2)\tilde{q}(x) \text{ over } \mathbb{Q}[x] \end{aligned}$$

Thus $\text{Ker}(\phi) = \{(x^2 - 2)f(x) : f(x) \in \mathbb{Q}[x]\} = (x^2 - 2)\mathbb{Q}[x]$.

**Example:** $\phi : \mathbb{R}[x] \to \mathbb{C}$ s.t. $\phi(f(x)) = f(i)$.
$\phi(x^4 + x^3 - 3x^2 + 2) = i^4 + i^3 - 3i^2 + 2 = 6 - i$, $Im(\phi) = \{a + bi : a, b \in \mathbb{R}\}$.
Homomorphism: $\phi(f(x) + g(x)) = f(i) + g(i) = \phi(f(x)) + \phi(g(x))$
$\phi(f(x)g(x)) = f(i)g(i) = \phi(f(x))\phi(g(x))$
$\text{Ker}(phi) = \{f(x) \in \mathbb{R}[x] : f(i) = 0\}$

$$\begin{aligned} f(x) &= (x - i)g(x) \in \mathbb{C}[x] \\ &= (x^2 + 1)h(x) \in \mathbb{R}[x] \end{aligned}$$

Thus $\text{Ker}(\phi) = (x^2 + 1)\mathbb{R}[x]$.

***Theorem:* 3.15: Identities under Ring Homomorphism**

If $\phi : R \to S$ is a ring homomorphism, then
1. $\phi(0) = 0$
2. If $1_R \in R$, $1_S \in S$ and $\phi$ is onto, then $\phi(1_R) = 1_S$

*Proof.* $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$, thus $\phi(0) = 0$.

Take $a \in R$ s.t. $\phi(a) = 1_S$. $\phi(1_R) = \phi(1_R)1_S = \phi(1_R)\phi(a) = \phi(1_R a) = \phi(a) = 1_S$. □

**Example:** $2\mathbb{Z} \cong 3\mathbb{Z}$ as groups, but not rings.

*Proof.* As groups, $\phi : \mathbb{Z} \to n\mathbb{Z}$ s.t. $\phi(m) = mn$ is a homomorphism with $\text{Ker}(\phi) = \{0\}$ and surjective. $2\mathbb{Z} \cong \mathbb{Z} \cong 3\mathbb{Z}$.

As rings, suppose $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$ is a homomorphism.
$\phi(2) \in 3\mathbb{Z}$, thus $\phi(2) = 3n$ for $n \in \mathbb{Z}$. $\phi(4) = \phi(2 + 2) = \phi(2) + \phi(2) = 6n$.
But $\phi(4) = \phi(2 \cdot 2) = \phi(2)\phi(2) = 9n^2$. $6n = 9n^2$ gives $n = \frac{2}{3} \notin \mathbb{Z}$. Contradiction, so there is no ring homomorphism $2\mathbb{Z} \to 3\mathbb{Z}$. □

**Example:** $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[\sqrt{3}]$ as group but not as fields.

*Proof.* As groups, define $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ as $\phi(a + b\sqrt{2}) = a + b\sqrt{3}$. $\phi$ is a well-defined homomorphism under addtion.

Suppose $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ is a field isomorphism. $\phi(\sqrt{2}) = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$.
Then $\phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}$.
Also $\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) \overset{\text{By Theorem 3.15}}{=} 1 + 1 = 2$.
So we need $(a^2 + 3b^2) + 2ab\sqrt{3} = 2$. This gives $a = 0, b = \pm\sqrt{\frac{2}{3}}$ or $a = \pm\sqrt{2}, b = 0$. Both are not in $\mathbb{Q}$. Thus there is no field homomorphism $\mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$. □

**Example:** Find ring homomorphisms $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, where for $\mathbb{Z} \times \mathbb{Z}$, both addition and multiplication are component-wise.

*Proof.* Note that $\mathbb{Z} \times \mathbb{Z}$ has 2 generators $(1,0)$ and $(0,1)$.
Suppose $\phi(1,0) = m$ and $\phi(0,1) = n$. Then $\phi(0,0) = \phi((1,0)(0,1)) = mn = 0 \Rightarrow m = 0$ or $n = 0$.
$\phi(a,b) = \phi(a(1,0) + b(0,1)) = a\phi(1,0) + b\phi(0,1) = am + bn$
Case 1: $m = 0$, $\phi(a,b) = bn$, then $\text{Ker}(\phi) = \mathbb{Z} \times \{0\}$, $Im(\mathbb{Z}) = n\mathbb{Z}$.
Case 2: $n = 0$, $\phi(a,b) = am$, then $\text{Ker}(\phi) = \{0\} \times \mathbb{Z}$, $Im(\mathbb{Z}) = m\mathbb{Z}$. □

**Example:** Let $\phi : \mathbb{R}^{2\times 2} \to \mathbb{R}$, which of $\phi(A) = A_{11}$, $\phi(A) = \det(A)$, $\phi(A) = \text{Tr}(A)$ makes $\phi$ a ring homomorphism?

*Proof.* Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$

$\phi(A) = A_{11}$, $\phi(A+B) = a + x = \phi(A) + \phi(B)$, thus a group homomorphism, but $\phi(AB) = ax + bz \neq ax = \phi(A)\phi(B)$, thus not a ring homomorphism.

$\phi(A) = \det(A)$, $\phi(AB) = \det(AB) = \det A \det B = \phi(A)\phi(B)$, thus a group homomorphism, but $\phi(A + B) = (a+x)(d+w) - (b+y)(c+z) \neq (ad - bc) + (xw - yz) = \phi(A) + \phi(B)$, thus not a ring homomorphism.

$\phi(A) = \text{Tr}(A)$, $\phi(A + B) = a + d + x + w = \phi(A) + \phi(B)$, thus a group homomorphism, but $\phi(AB) = ax + bz + cy + dw \neq (a + d)(x + w) = \phi(A)\phi(B)$, thus not a ring homomorphism. □

### 3.3 Ideal

**Definition: 3.13: Subring**

Let $R$ be a ring, a subring $S$ of $R$ is $S \subset R$ that satisfies ring properties.

**Theorem: 3.16: Subring Test**

Let $R$ be a ring, $S \subset R$ is a subring if $\forall a, b \in S$, $a - b \in S$ and $ab \in S$.

**Definition: 3.14: Cosets of Rings**

Let $R$ be a ring and $S \subset R$ be a subring. The cosets of $r \in R$ is $r + S = \{r + s : s \in S\}$.

Note $S, R$ are abelian, thus $S \trianglelefteq R$. $(R/S, +)$, where $R/S = \{r + S : r \in R\}$, is an abelian group.

For $(R/S, +)$ to be a ring, we need $(a + S)(b + S) = ab + S$ for all $a, b \in R$. *i.e.* For all $s, s' \in S$, we need $(a + s)(b + s') = ab + as' + sb + ss' \in ab + S$. Therefore, we need $as' + sb \in S \Rightarrow as' \in S$ and $sb \in S$.

**Definition: 3.15: Ideal**

Let $I \subset R$ be a subring.
1. $I$ is a right ideal if $\forall r \in R$, $i \in I$, $ir \in I$. (absorbs multiplication from right)
2. $I$ is a left ideal if $\forall r \in R$, $i \in I$, $ri \in I$. (absorbs multiplication from left)
3. $I$ is an ideal if it is a right ideal and a left ideal.

**Theorem: 3.17: Quotient Ring**

If $I \subset R$ is an ideal, then $R/I = \{r + I : r \in R\}$ is a ring.

*Proof.* $R/I$ is an abelian group because $R, I$ are abelian groups and $I \trianglelefteq R$.

We now show that the multiplication is well defined. Let $a, a', b, b' \in R$ with $a+I = a'+I$ and $b+I = b'+I$. $a - a' \in I$ and $b - b' \in I$.
Then $(a - a')b \in I$ by Definition 3.15, $ab - ab' \in I \Rightarrow ab + I = a'b + I$
Similarly, $a'(b - b') \in I \Rightarrow a'b - a'b' \in I \Rightarrow a'b + I = a'b' + I$. Thus $(a + I)(b + I) = ab + I = a'b' + I = (a' + I)(b' + I)$. $\square$

**_Definition:_ 3.16: Principal Ideal**

Suppose $R$ is a commutative ring with 1 and $a \in R$, then the principal ideal of $R$ generated by $a$ is $(a) = \{ra : r \in R\} = Ra \overset{\text{Commutative}}{=} \{ar : r \in R\}$.

*Proof.* We show that $(a) \subset R$ is indeed an ideal for any $a$.
Suppose $i \in (a)$ and $r \in R$, then by Definition 3.16, $i = ar'$ for some $r' \in R$.
Note $ir = (ar)r' = a(rr') \in (a)$. $\square$

**Example:** In $\mathbb{Z}$: $(3) = \{3n : n \in \mathbb{Z}\} = 3\mathbb{Z}$ is the principal ideal generated by 3.

**Example:** In $\mathbb{Z}_{15}$, $(2) = \{2n : n \in \mathbb{Z}\} = \{0, 2, 4, 6, 8, 10, 12, 14, 1, 3, 5, 7, 9, 11, 13\} = \mathbb{Z}_{15}$ is the ideal generated by a unit 2. $(5) = \{5n : n \in \mathbb{Z}_{15}\} = \{0, 5, 10\}$

**_Theorem:_ 3.18:**

$(a) = R \Leftrightarrow a \in R$ is a unit.

*Proof.* $(\Rightarrow)$ Suppose $a \in R$ with $(a) = R$, then $1 \in (a)$. Thus, exists $r \in R$ s.t. $ar = 1$. By Definition 3.3,$a$ is a unit.

$(\Leftarrow)$ Suppose $a \in R$ is a unit, there exists $r \in R$ s.t. $ar = 1$. Then $1 \in (a)$. For $b \in R$, $b = b(1) \in (a)$ Thus $R \subset (a)$, and $R = (a)$. $\square$

**_Theorem:_ 3.19: Principal Ideals of $\mathbb{Z}$**

Every ideal of $\mathbb{Z}$ is a principal ideal.

*Proof.* Suppose $I \subset \mathbb{Z}$ is an ideal, and take $n \in I$ to be the smallest non-negative element. (Note, if $n = 0$, then $I = \{0\}$ is the trivial ideal.)
We show that $I = (n)$.
Firstly, $(n) \subset I$ by definition.
Suppose $m \in I$, use division algorithm with $m$ and $n$. $m = nq + r$ where $0 \le r < n$. $r = m - nq \in I$ since $m \in I, n \in I$, and $nq \in I$. Thus $r = 0$, $m = nq$, $m \in (n)$. Therefore $I \subset (n)$ and $I = (n)$. $\square$

**_Theorem:_ 3.20:**

Let $\phi : R \to S$ be a ring homomorphism, then $\text{Ker}(\phi)$ is an ideal.

*Proof.* let $a, b \in \text{Ker}(\phi)$.
$\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0$, then $a - b \in \text{Ker}(\phi)$.

$\phi(ab) = \phi(a)\phi(b) = 0 \cdot 0 = 0$, $ab \in \text{Ker}(\phi)$.
Thus $\text{Ker}(\phi)$ is a subring by Theorem 3.16.

Suppose $a \in \text{Ker}(\phi)$, $r \in R$.
$\phi(ar) = \phi(a)\phi(r) = \phi(a)0 = 0$. $\phi(ra) = \phi(r)\phi(a) = 0\phi(a) = 0$
Thus $ar, ra \in \text{Ker}(\phi)$, and $\text{Ker}(\phi)$ is an ideal by Definition 3.15. $\square$

***Theorem:* 3.21:**

Let $\phi : R \to S$ be a homomorphism. If $J \subset S$ is an ideal, then $\phi^{-1}(J) = \{a \in R : \phi(a) \in J\} \subset R$ is an ideal.

*Proof.* Suppose $a, b \in \phi^{-1}(J)$, then $\phi(a) \in J$, $\phi(b) \in J$.
$\phi(a - b) = \phi(a) - \phi(b) \in J$, because $J$ is a subring, then $a - b \in \phi^{-1}(J)$
$\phi(ab) = \phi(a)\phi(b) \in J$, thus $ab = \phi^{-1}(\phi(a)\phi(b)) \in \phi^{-1}(J)$
By Theorem 3.16, $\phi^{-1}(J)$ is a subring of $R$.

Let $a \in \phi^{-1}(J)$, $r \in R$. $\phi(ar) = \phi(a)\phi(r) \in J$, since $J$ is an ideal. $ar \in \phi^{-1}(J)$. Similarly $\phi(ra) = \phi(r)\phi(a) \in J$. $ra \in \phi^{-1}(J)$.
Thus $\phi^{-1}(J)$ is an ideal. $\square$

***Definition:* 3.17: Prime Ideal**

An ideal $P \subset R$ is a prime ideal if $ab \in P \Leftrightarrow a \in P$ or $b \in P$. (This is the generalization of prime numbers.)

***Definition:* 3.18: Maximal Ideal**

An ideal $M \subset R$ is a maximal ideal if for any ideal $I \subset R$ with $M \subset I \subset R$, we have $I = M$ or $I = R$.

***Theorem:* 3.22:**

If $R$ is a commutative ring with 1. Then $P \subset R$ is a prime ideal $\Leftrightarrow R/P$ is an integral domain.

*Proof.* ($\Rightarrow$) Suppose $P$ is a prime ideal and $(a+P)(b+P) = 0+P \in R/P$. Then $ab+P = 0+P$ and thus $ab \in P$ by Definition 3.15.
Since $P$ is prime ideal, $a \in P$ or $b \in P$, then $a + P = 0 + P$ or $b + P = 0 + P$. Thus $R/P$ is an integral domain by Definition 3.7.

($\Leftarrow$) Suppose that $R/P$ is an integral domain and $ab \in P$. We want to show that $a \in P$ or $b \in P$.
Since $ab \in P$, $ab + P = 0 + P \in R/P$, thus $(a + P)(b + P) = 0 + P$. This gives either $a + P = 0 + P$ or $b + P = 0 + P$. Therefore, $a \in P$ or $b \in P$. $P \subset R$ is a prime ideal. $\square$

***Theorem:* 3.23:**

If $R$ is a commutative ring with 1. Then $M \subset R$ is a maximal ideal $\Leftrightarrow R/M$ is a field.

*Proof.* ($\Rightarrow$) Suppose $M \subset R$ is a maximal ideal and $a + M \in R/M$ with $a \notin M$.
Consider $\langle 0 + M\rangle \subset \langle a + M\rangle \subset R/M$. Note $\langle a + M\rangle = I/M$, where $M \subset I \subset R$. $a \in I$ and $a \notin M$ means $M \neq I$.

Then $I = R$ because $M$ is maximal. Then $\langle a+M\rangle = R/M$, $1+M \in \langle a+M\rangle$. Then there exists $b \in R$ s.t. $(a+M)(b+M) = (1+M)$. Inverse exsists, $R/M$ is a field.

($\Leftarrow$) Suppose $R/M$ is a field. Take $I \subset R$, $M \subsetneq I \subset R$. We want to show that $I = R$.
Since $M \subsetneq I$, there exists $a \in I$ s.t. $a \notin M$, then $M \subsetneq \langle a, M\rangle \subset I \subset R$, since $a + M \neq 0 + M \in R/M$.
Then there exists $b \in R$ s.t. $(a+M)(b+M) = 1+M$, so inverse of $a+M$ exists. $1+M \in \langle a, M\rangle \subset I$.
Thus $I = R$ by Theorem 3.18, since the unit is in $I$. $\square$

**Example:** Which are ideals in $\mathbb{Z}[x]$?

1. $I = \{p(x) : p(x) = xq(x) + 2k, k \in \mathbb{Z}, q(x) \in \mathbb{Z}[x]\}$, polynomials with even constant terms.
2. $I = \{p(x) : p(x) = x^2q(x) + 2kx + l, k, l \in \mathbb{Z}, q(x) \in \mathbb{Z}[x]\}$, polynomials with even coefficients for $x$.
3. $I = \{p(x) \in \mathbb{Z}[x] : p'(0) = 0\}$

*Proof.*

1. Let $p_1(x) = xq_1(x) + 2k_1 \in I$, $p_2(x) = xq_2(x) + 2k_2 \in I$. Then $p_1(x) - p_2(x) = x(q_1 - q_2) + 2(k_1 - k_2) \in I$
   $p_1p_2 = (xq_1 + 2k_1)(xq_2 + 2k_2) = x^2q_1q_2 + 2x(k_1q_2 + k_2q_1) + 4k_1k_2 \in I$. Thus $I$ is a subring by Theorem 3.16
   Take $f(x) = xg(x) + l \in \mathbb{Z}[x]$ with $l \in \mathbb{Z}$, then $p(x)f(x) = x^2qg + 2xkg + lxq + 2kl \in I$. Thus $I$ is an ideal.
2. Let $p_1(x) = x^2q_1(x) + 2k_1x + l_1 \in I$, $p_2(x) = x^2q_2(x) + 2k_2x + l_2 \in I$. Then $p_1(x) - p_2(x) \in I$
   $p_1p_2 = (x^2q_1 + 2k_1x + l_1)(x^2q_2 + 2k_2x + l_2) = x^2(x^2q_1q_2 + l_1q_2 + l_2q_1 + 4k_1k_2) + 2(k_1l_2 + k_2l_1) + l_1l_2 \in I$.
   Thus $I$ is a subring by Theorem 3.16
   Take $f(x) = x^2g + mx + n \in \mathbb{Z}[x]$ with $l \in \mathbb{Z}$, then $p(x)f(x) = x^2(x^2gq + nq + mg + 2km) + (lm + 2kn)x + ln \notin I$, since $lm + 2kn$ is not even when $l = m = 1$. Thus $I$ is not an ideal.
3. Let $p(x), q(x) \in I$. Then $p'(0) = q'(0) = 0$. $(p-q)'|_{x=0} = p'(0) - q'(0) = 0$. $(pq)'|_{x=0} = p'(0)q(0) + p(0)q'(0) = 0$ Thus $I$ is a subring by Theorem 3.16
   Take $f(x) \in \mathbb{Z}[x]$ with $l \in \mathbb{Z}$, then $(fp)'|_{x=0} = f'(0)p(0) + f(0)p'(0) = f'(0)p(0) \neq 0$. Thus $I$ is not an ideal.

For the third case, if we have $I = \{p(x) \in \mathbb{Z}[x] : p'(0) = 0, p(0) = 0\}$. Then $I$ is an ideal. $\square$

***Theorem:* 3.24: Smallest Enclosing Ideal**

Let $I, J \subset R$ be ideals. $I + J$ is the smallest ideal containing $I$ and $J$.

*Proof.* $I + J = \{i + j : i \in I, j \in J\}$. Let $a, b \in I, J$, then $a = i + j$, $b = i' + j'$ for $i, i' \in I$, $j, j' \in J$.
Then $b - a = (i' - i) + (j' - j) \in I + J$, $ab = (i+j)(i'+j') = ii' + ij' + jj' + ji'$. Since $ii' + ij' \in I$ and $ji' + jj' \in J$ by Definition 3.15. Then $ab \in I + J$. $I + J$ is a subring by Theorem 3.16.

Let $a \in I$, $x \in R$, $a = i + j$ for $i \in I$, $j \in J$. $ax = (i+j)x = ix + jx \in I + J$, since $ix \in I$, $jx \in J$. $xa = xi + xj \in I + J$. Since $i \in I \Rightarrow i + 0 = I + J, 0 \in J$, then $I \subset I + J$. Similarly, $J \subset I + J$.

Suppose $K \subset R$ an ideal s.t. $I \subset K$ and $J \subset K$.
Let $a \in I + J$, $a = i + j$ for $i \in I$, $j \in J$. Then $i \in K$ and $j \in K$, thus $a \in K$. $I + J \subset K$. $\square$

### 3.4 Isomorphism Theorems for Rings

**_Theorem:_ 3.25: First Isomorphism Theorem for Rings**

Let $\phi : R \to S$ be a ring homomorphism. Then there is a unique ismorphism $\psi : R/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$ s.t. $\psi(r + \mathrm{Ker}(\phi)) \cong Im(\phi)$.

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, "\pi"'] & Im(\phi) \subset S \\
R/\mathrm{Ker}(\phi) \arrow[ur, "\psi"'] &
\end{tikzcd}$$

*Proof.* Define $\psi : R/\mathrm{Ker}(\phi) \to Im(\phi)$ s.t. $\psi(r + \mathrm{Ker}(\phi)) = \phi(r)$

Well-defined: Suppose that $r + \mathrm{Ker}(\phi) = r' + \mathrm{Ker}(\phi)$, then $r - r' \in \mathrm{Ker}(\phi)$.
$\phi(r + \mathrm{Ker}(\phi)) = \phi(r) = \phi(r) + 0 = \phi(r) + \phi(r' - r) = \phi(r + r' - r) = \phi(r') = \psi(r' + \mathrm{Ker}(\phi))$

Ring Homomorphism: $\psi(a + \mathrm{Ker}(\phi) + b + \mathrm{Ker}(\phi)) = \psi(a + b + \mathrm{Ker}(\phi)) = \phi(a + b) = \phi(a) + \phi(b) = \psi(a + \mathrm{Ker}(\phi)) + \psi(b + \mathrm{Ker}(\phi))$
$\psi((a + \mathrm{Ker}(\phi))(b + \mathrm{Ker}(\phi))) = \psi(ab + \mathrm{Ker}(\phi)) = \phi(ab) = \phi(a)\phi(b) = \psi(a + \mathrm{Ker}(\phi))\psi(b + \mathrm{Ker}(\phi))$

Injective: Suppose $r + \mathrm{Ker}(\phi) \in \mathrm{Ker}(\phi)$, $\psi(r + \mathrm{Ker}(\phi)) = 0 = \phi(r)$. Thus $r \in \mathrm{Ker}(\phi)$, $r + \mathrm{Ker}(\phi) = 0 + \mathrm{Ker}(\phi)$. $\mathrm{Ker}(\psi) = \{0 + \mathrm{Ker}(\phi)\}$, $\psi$ is injective.

Surjective: Suppose $\phi(r) \in Im(\phi)$, then $\psi(r + \mathrm{Ker}(\phi)) = \phi(r)$

Uniqueness: Suppose $\bar{\psi}(r + \mathrm{Ker}(\phi)) = \phi(r) = \psi(r + \mathrm{Ker}(\phi))$. Thus $\bar{\psi} = \psi$. $\square$

**Example:** $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \subset \mathbb{R}^{2\times 2}$. Show that $I = \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$ is an ideal for $R$ and $R/I \cong \mathbb{R} \times \mathbb{R}$.

*Proof.* Let $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, $B = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$
Then $A - B = \begin{bmatrix} a - x & b - y \\ 0 & c - z \end{bmatrix} \in R$ and $AB = \begin{bmatrix} ax & ay + bz \\ 0 & cz \end{bmatrix} \in R$. Therefore, $R$ is a ring by Theorem 3.16.

Let $I_1 = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$, $I_2 = \begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix}$
Then $I_1 - I_2 = \begin{bmatrix} 0 & x - y \\ 0 & 0 \end{bmatrix} \in I$ and $I_1 I_2 = \begin{bmatrix} 0 & xy \\ 0 & 0 \end{bmatrix} \in I$. Therefore, $I$ is a subring of $R$ by Theorem 3.16.

To show that $I$ is an ideal of $R$. Consider $AI_1$ and $I_1A$.
$AI_1 = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & xc \\ 0 & 0 \end{bmatrix} \in I$, $I_1 A = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 0 & xc \\ 0 & 0 \end{bmatrix} \in I$

Consider $\phi : R \to \mathbb{R} \times \mathbb{R}$ s.t. $\phi \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = (a, c)$.
Then $\phi(A + B) = (a + x, c + z) = (a, c) + (x, z) = \phi(A) + \phi(B)$, and $\phi(AB) = (ax, cz) = (a, c)(x, z) = \phi(A)\phi(B)$. Thus $\phi$ is a ring homomorphism.
$\mathrm{Ker}(\phi) = \{A \in R : \phi(A) = (a, c) = (0, 0)\}$, so we need $a = c = 0$. $\mathrm{Ker}(\phi) = I$, and $I$ is an ideal. Thus by Theorem 3.25, $R/I \cong \mathbb{R} \times \mathbb{R}$. $\square$

**Example:** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $(3) = 3\mathbb{Z}[i] = \{3a + 3bi : a, b \in \mathbb{Z}\}$. Show that $3\mathbb{Z}[i] \subset \mathbb{Z}[i]$ is a maximal ideal.

*Proof.* Let $\phi : \mathbb{Z}[i] \to \mathbb{Z}_3[i]$ s.t. $\phi(a + bi) = [a + bi]_3 = [a]_3 + [b]_3 i$. $\phi$ is a homomorphism.
$\text{Ker}(\phi) = \{a + bi : \phi(a + bi) = [a]_3 + [b]_3 i = [0]_3 + [0]_3 i\}$. Thus $a \equiv 0 \mod 3$ and $b \equiv 0 \mod 3$. $a = 3m$, $b = 3n$ for some $m, n \in \mathbb{Z}$. Then, $a + bi \in 3\mathbb{Z}[i] = (3)$. By Theorem 3.25, $\mathbb{Z}[i]/(3) \cong \mathbb{Z}_3[i]$.

Note: $\mathbb{Z}_3[i] = \{0, 1, 2, i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i\}$ is a field since inverses exist for all elements. Thus $(3) \subset \mathbb{Z}[i]$ is maximal by Theorem 3.23. □

***Theorem:* 3.26: Second Isomorphism Theorem for Rings**

Let $I \subset R$ be a subring and $J \subset R$ be an ideal. Then

1. $I \cap J \subset I$ is an ideal
2. $I/(I \cap J) \cong (I + J)/J$

*Proof.*

1. Suppose $a \in I \cap J$ and $b \in I$, we want to show that $ab \in I \cap J$ and $ba \in I \cap J$.
   Note $a \in I \cap J$ means $a \in I$ and $I \in J$, $b \in J \subset R$. Then $ab \in J$ since $J \subset R$ is an ideal. $ab \in I$ since $I \subset R$ is a subring. Thus $ab \in I \cap J$.
   Similarly, we have $ba \in I \cap J$, thus $I \cap J \subset I$ is an ideal.

2. Define $\phi : I \to (I + J)/J$ s.t. $\phi(a) = a + J$
   Homomorphism: $\phi(a + b) = (a + b) + J = (a + J) + (b + J) = \phi(a) + \phi(b)$
   $\phi(ab) = ab + J = (a + J)(b + J) = \phi(a)\phi(b)$

   Surjective: Let $a + J$ s.t. $a \in I + J$, (then $a + J \in (I + J)/J$) *i.e.* $a = i + j$ for $i \in I$, $j \in J$. Then $a + J = i + j + J = i + J$. Therefore, $\exists i \in I$ s.t. $\phi(i) = i + J = a + J$, thus surjective.

   Find kernel: Suppose $a \in I \cap J$, *i.e.* $a \in I$ and $a \in J$. $\phi(a) = a + J \overset{a \in J}{=} 0 + J$. Thus $a \in \text{Ker}(\phi) \Rightarrow I \cap J \subset \text{Ker}(\phi)$.
   Suppose $a \in \text{Ker}(\phi) \subset I$, then $a \in I$, and $\phi(a) = a + J = 0 + J$. Then $a \in J$, thus $a \in I \cap J$. So $\text{Ker}(\phi) \subset I \cap J$.
   Therefore, $\text{Ker}(\phi) = I \cap J$, $I/(I \cap J) \cong (I + J)/J$ by Theorem 3.25.

□

## 3.5 Polynomial Rings

***Definition:* 3.19: Polynomial Rings**

Suppose $R$ is a commutative ring with 1, $p(x) = a_0 + a_1 x + \cdots + a_n x_n^n$ with $a_i \in R$ is a polynomial over $R$ with indeterminate $x$

1. $a_n \neq 0$ is called the leading coefficient of $p(x)$
2. $\deg(p(x)) = n$
3. If $a_n = 1$, then $p(x)$ is monic
4. The set of all polynomials is denoted $R[x]$

***Theorem:* 3.27:**

$R[x]$ is a commutative ring with 1.

*Proof.* Let $p(x) = a_0 + a_1x + \cdots a_nx^n$, $q(x) = b_0 + b_1x + \cdots b_mx^m$.
$pq = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$, where $c_k = \sum_{l=0}^{k} a_{k-l}b_l$.
$qp = \hat{c}_0 + \hat{c}_1x + \cdots + \hat{c}_{m+n}x^{m+n}$, where $\hat{c}_k = \sum_{l=0}^{k} a_l b_{k-l} \overset{\text{set } l=k-l}{=} \sum_{l'=0}^{k} a_{l'}b_{k-l'} = c_k$.
Thus $qp = pq$, multiplication is commutative. ☐

**Theorem: 3.28:**

If $R$ is an integral domain, then so is $R[x]$.

*Proof.* Contrapositive: if $R[x]$ is not is integral domain, then $R$ is not an integral domain.
Let $p(x) = a_0 + a_1x + \cdots a_nx^n$, $q(x) = b_0 + b_1x + \cdots b_mx^m$, with $a_n \neq 0$, $b_m \neq 0$.
Suppose $R[x]$ is not an integral domain, then we have $p(x) \neq 0$, $q(x) \neq 0$, but $p(x)q(x) = 0$, *i.e.* $a_nb_m = \text{coeff}_{x^{n+m}}(pq) = 0$.
Then $\exists a_n, b_m \in R$ s.t. $a_n \neq 0$, $b_m \neq 0$, but $a_nb_m = 0$. We have a zero divisor, thus $R$ is not an integral domain. ☐

*Remark* 7.

1. If $K$ is a field, $K[x]$ is not a field. $p(x) = x$ does not have an inverse.
2. If $K$ is a field $K[[x]] = \left\{\sum_{n=0}^{\infty} a_nx^n : a_n \in R\right\}$ is a field. $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$, so $(1-x)\sum_{n=0}^{\infty} x^n = 1$. And we can show that every element has an inverse.
3. If $K$ is a field, $K[x, x^{-1}] = \left\{\sum_{n=-N}^{M} a_nx^n : a_n \in R\right\}$ (Laurent polynomials) is not a field.

### 3.5.1 Division Algorithm

**Theorem: 3.29: Division Algorithm for Polynomials**

Let $K$ be a field and $f(x), g(x) \in K[x]$. Then there are unique $q(x), r(x)$ s.t. $f(x) = g(x)q(x) + r(x)$, where $0 \leq \deg(r(x)) < \deg(g(x))$

*Proof.* Let $f(x), g(x)$ be polynomials s.t. $\deg(f(x)) = n$, $\deg(g(x)) = m$. Assume $m \leq n$, otherwise, $f(x) = 0g(x) + r(x)$ a trivial case.

We do induction on $n = m + k$.
**Base Case:** $k = 0$, $m = n$, $f(x) = a_nx^n + \cdots + a_0$, $g(x) = b_nx^n + \cdots + b_0$, $a_n \neq 0, b_n \neq 0$.
Then $f(x) = \frac{a_n}{b_n}g(x) + \left[f(x) - \frac{a_n}{b_n}g(x)\right]$. $r(x) = f(x) - \frac{a_n}{b_n}g(x) = \left(a_{n-1} - \frac{a_n}{b_n}b_{n-1}\right)x^{n-1} + \cdots$, $\deg(r(x)) < n$
**Induction Hypothesis:** Assume for all $p(x)$ with degree $< n$, we can do the division algorithm.
**Induction Step:** Consider $\hat{f}(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x) = (a_nx^n + \cdots) - \frac{a_n}{b_m}x^{n-m}(b_mx^m + \cdots) = \left(a_n - \frac{a_n}{b_m}b_m\right)x^n + \hat{a}_{n-1}x^{n-1} + \cdots + \hat{a}_0 = \hat{a}_{n-1}x_{n-1} + \cdots + \hat{a}_0$ has degree $< n$.
Apply IH to $\hat{f}(x)$ and $g(x)$, $\hat{f} = g\hat{q} + r$ with $0 \leq \deg(\hat{r}) < m$.
$f(x) = \hat{f} + \frac{a_n}{b_m}x^{n-m}g = g\hat{q} + \hat{r} + \frac{a_n}{b_m}x^{n-m}g = g\left(\hat{q} + \frac{a_n}{b_m}x^{n-m}\right) + \hat{r}$.
Let $q = \hat{q} + \frac{a_n}{b_m}x^{n-m}$, $r = \hat{r}$, then $f = gq + r$ where $0 \leq \deg(r) < m$.

Uniqueness: Suppose $f = gq_1 + r_1 = gq_2 + r_2$, $0 \leq \deg r_i < \deg g$
Then $0 = g(q_1 - q_2) + (r_1 - r_2)$, $r_2 - r_1 = g(q_1 - q_2)$, $\deg(r_2 - r1) < \deg(g) \leq \deg(g(q_1 - q_2))$.
Thus, $r_1 = r_2$, and $q_1 = q_2$. The factorization is unique. $\square$

**Definition: 3.20: GCD of Polynomials**

Let $K$ be a field, $d(x) \in K[x]$ is the gcd of $f(x), g(x) \in K[x]$ if $d(x)|f(x)$ and $d(x)|g(x)$ and if $\hat{d}(x)|f(x)$ and $\hat{d}(x)|g(x)$, then $\hat{d}(x)|d(x)$. If $\gcd(f, g) = 1$, then $f$ and $g$ are relatively prime.

**Theorem: 3.30: Bezout's Identity**

If $d(x) = \gcd(f, g)$, then $\exists a(x), b(x) \in K[x]$ s.t. $a(x)f(x) + b(x)g(x) = d(x)$

*Proof.* Consider the set $S = \{p(x)f(x) + q(x)g(x) : p(x), q(x) \in K[x]\}$.
Suppose $u(x), v(x) \in S$, both monic with the smallest degree, then $u(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $v(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Note $u(x) - v(x) \in S$, $u(x) - v(x) = (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_0 - b_0)$, $\deg(u - v) \leq n - 1 < \deg(u) = n$, thus $u(x) - v(x) = 0$, $u = v$. *i.e.* There is a unique polynomial in $S$ which is monic with the smallest degree.

Let $d(x) = a(x)f(x) + b(x)g(x) \in S$ be the monic polynomial with min degree. We show that $d(x)|f(x)$ and $d(x)|g(x)$.
Use Theorem 3.29 on $f$ and $g$, $f(x) = d(x)q(x) + r(x)$, $0 \leq \deg(r) < \deg(d)$.
$r(x) = f(x) - d(x)q(x) = f(x) - (a(x)f(x) + b(x)g(x))q(x) = (1 - a(x)q(x))f(x) - b(x)q(x)g(x) \in S$. Thus $r(x) = 0$, $d(x)|f(x)$. Similarly $d(x)|g(x)$.

Suppose $\hat{d}(x) \in K[x]$ s.t. $\hat{d}(x)|f(x)$ and $\hat{d}(x)|g(x)$. Then $f(x) = \hat{d}(x)u(x)$ and $g(x) = \hat{d}(x)v(x)$.
Thus $d(x) = a(x)u(x)\hat{d}(x) + b(x)v(x)\hat{d}(x) = (a(x)u(x) + b(x)v(x))\hat{d}(x)$. $\hat{d}(x)|d(x)$ $\square$

**Example:** Find $a(x)$ and $b(x)$ s.t. $a(x)f(x) + b(x)g(x) = \gcd(f(x), g(x))$, where $f(x) = x^4 - 2x^3 - 3x - 2$, $g(x) = x^3 + 4x^2 + 4x + 1$
In $\mathbb{Q}[x]$, $f(x) = (x - 4)g(x) + (10x^2 + 12x + 2)$, $g(x) = \left(\frac{1}{10}x + \frac{7}{25}\right)(10x^2 + 12x + 2) + \frac{11}{25}(x + 1)$
Note that $(x + 1)|(10x^2 + 12x + 2)$, so $(x + 1)|g(x)$ and $(x + 1)|f(x)$ is the gcd.

$$\begin{aligned}
x + 1 &= \frac{25}{11}g(x) - \frac{25}{11}\left(\frac{1}{10}x + \frac{7}{25}\right)(10x^2 + 12x + 2) \\
&= \frac{25}{11}g(x) - \frac{25}{11}\left(\frac{1}{10}x + \frac{7}{25}\right)(f(x) - (x - 4)g(x)) \\
&= \left(\frac{5x^2}{22} - \frac{3x}{11} - \frac{3}{11}\right)g(x) + \left(-\frac{5}{22}x - \frac{7}{11}\right)f(x)
\end{aligned}$$

Thus $a(x) = (\frac{5x^2}{22} - \frac{3x}{11} - \frac{3}{11}$, $b(x) = -\frac{5}{22}x - \frac{7}{11}$

In $\mathbb{Z}_2[x]$, $f(x) = x^4 + x$, $g(x) = x^3 + 1$, $f(x) = xg(x)$.
Thus $g(x)|f(x)$, $\gcd(f, g) = g = x^3 + 1$.

In $\mathbb{Z}_{11}[x]$, we start with $f(x) = (x - 4)g(x) + (10x^2 + 12x + 2)$. Reduce in $\mathbb{Z}_{11}$, we get $f(x) = (x - 4)g(x) + (-x^2 + x + 2)$
Note $g(x) = (-x^2 + x + 2)(-x - 5)$. Thus $\gcd(f, g) = -x^2 + x + 2$
$-x^2 + x + 2 = f(x) - (x - 4)g(x)$

### 3.5.2 Irreducible Polynomials

***Definition:* 3.21: Irreducible Polynomials**

We say a non constant polynomial $f(x) \in K[x]$ is irreducible if it cannot be written as $f(x) = g(x)h(x)$ with $\deg(g), \deg(h) < \deg(f)$.

***Theorem:* 3.31:**

$p(x) \in K[x]$ is irreducible $\Leftrightarrow K[x]/(p(x))$ is a field. $(p(x))$ is the principal ideal generated by $p(x)$.

*Proof.* ($\Rightarrow$) Suppose $p(x) \in K[x]$ is irreducible. Consider an ideal $I \subset K[x]$, where $(p(x)) \subsetneq I \subset K[x]$.
Take $f(x) \in I \setminus (p(x))$. $p(x)$ is irreducible and $f(x)$ is not a multiple of $p(x)$, otherwise $f(x) \in (p(x))$. Thus $\gcd(f, p) = 1$.
By Theorem 3.30, $\exists a(x), b(x) \in K[x]$ s.t. $a(x)f(x) + b(x)p(x) = 1$
Note $f(x) \in I$, $p(x) \in I$. By Definition 3.15, $1 \in I$. By Theorem 3.18, $I = K[x]$. Thus $(p(x))$ is maximal by Definition 3.18. And by Theorem 3.23, $K[x]/(p(x))$ is a field.

($\Leftarrow$) Suppose $K[x]/(p(x))$ is a field, then $(p(x))$ is a maximal ideal by Theorem 3.23.
Suppose $p(x) = f(x)g(x)$, then $p(x) \in (f(x))$, $(p(x)) \subset (f(x)) \subset K[x]$.
Case 1: $(p(x)) = (f(x))$, then $f(x) = p(x)h(x)$, $\deg(f) = \deg(p)$, $p(x) = \text{const} f(x)$. $p(x)$ is irreducible.
Case 2: $(f(x)) = K[x]$. Then $f(x)$ is a unit in $K[x]$. $f(x) = \alpha$ is a constant. $\deg(f) = 0$. Thus $\deg(g) = \deg(p)$. $p$ is irreducible. $\square$

**Example:** Show that $\mathbb{C}$ is a field.

*Proof.* $\phi : \mathbb{R}[x] \to \mathbb{C}$ s.t. $\phi(f(x)) = f(i)$ is a homomorphism with $\text{Ker}(\phi) = (x^2 + 1)$. $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. Thus $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ is a field by Theorem 3.25 and 3.31. $\square$

**Example:** Show that $\mathbb{Q}(\sqrt{2})$ is a field.

*Proof.* $\phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ s.t. $\phi(f(x)) = f(\sqrt{2})$ is a homomorphism, $\text{Ker}(\phi) = (x^2 - 2)$. $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$. Thus $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$ is a field. $\square$

**Example:** Show that $\mathbb{Z}[x]/(x^2 + x + 1)$ is a field.

*Proof.* $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. The field has order $2^2 = 4$. $\square$

***Lemma:* 3.3:**

Let $p(x) \in \mathbb{Q}[x]$, then $p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n)$ with $\gcd(r, s) = 1$, $\gcd(\{a_i\}) = 1$.

*Proof.* Let $p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n$ for $b_i, c_i \in \mathbb{Z}$, $p(x) \in \mathbb{Q}[x]$.
We can write $p(x) = \frac{1}{c_0 \cdots c_n}(d_0 + d_1 x + \cdots d_n x^n)$, where $d_i = \frac{c_0 \cdots c_n}{c_i} b_i$.
Let $d = \gcd(d_0, ..., d_n)$, then $d_0 = da_0$, $d_n = da_n$ with $\gcd(a_0, ..., a_n) = 1$
$p(x) = \frac{1}{c_0 \cdots c_n}(da_0 + da_1 x + \cdots + da_n x^n) = \frac{d}{c_0 \cdots c_n}(a_0 + a_1 x + \cdots + a_n x^n) = \frac{r}{s}(a_0 + a_1 x + \cdots a_n x^n)$ by reducing the fractions. $\square$

**Lemma: 3.4: Gauss Lemma**

Let $p(x) \in \mathbb{Z}[x]$ be monic that factors $p(x) = \alpha(x)\beta(x) \in \mathbb{Q}[x]$ with $\deg(\alpha), \deg(\beta) < \deg(p)$. Then $\exists a(x), b(x) \in \mathbb{Z}[x]$ s.t. $a(x), b(x)$ are monic with $\deg(a) = \deg(\alpha)$, $\deg(b) = \deg(\beta)$ and $p(x) = a(x)b(x)$.

*Proof.* Suppose $p(x) = \alpha(x)\beta(x)$, $\alpha(x), \beta(x) \in \mathbb{Q}[x]$. By Lemma 3.3, $\alpha(x) = \frac{c_1}{d_1}(a_0 + \cdots + a_m x^m)$. Similarly, $\beta(x) = \frac{c_2}{d_2}(a_0 + \cdots + a_n x^n)$.
Let $\alpha_1(x) = (a_0 + \cdots + a_m x^m)$, $\beta_1(x) = (a_0 + \cdots + a_n x^n)$, $c = c_1c_2$, $d = d_1d_2$. Then $p(x) = \alpha(x)\beta(x) = \frac{c_1c_2}{d_1d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x)$. Thus $c\alpha_1(x)\beta_1(x) = dp(x)$.

Case 1: $d = 1$. $\alpha_1(x)\beta_1(x) \in \mathbb{Z}[x]$. $1 \overset{p(x) \text{ is monic}}{=} \text{coeff}_{x^{m+n}} p(x) = c a_m b_n$
If $c = 1$, $a_m = b_n = 1$, $a(x) = \alpha_1(x)$, $b(x) = \beta_1(x)$, or $a_m = b_n = -1$, $a(x) = -\alpha_1(x)$, $b(x) = -\beta_1(x)$.
If $c = -1$, $a_m = 1$, $b_n = -1$, $a(x) = \alpha_1(x)$, $b(x) = -\beta_1(x)$, or $a_m = -1$, $b_n = 1$, $a(x) = -\alpha_1(x)$, $b(x) = \beta_1(x)$.

Case 2: $d \neq 1$. Pick a prime s.t. $p|d$ and $p \nmid c$. Take $a_l$ with $p \nmid a_l$, $b_k$ with $p \nmid b_k$.
Set $\hat{\alpha}(x) \equiv \alpha_1(x) \mod \mathbb{Z}_p[x]$, $\hat{\beta}(x) \equiv \beta_1(x) \mod \mathbb{Z}_p[x]$. Then $\hat{\alpha}(x) \neq 0$ and $\hat{\beta}(x) \neq 0$.
$\hat{\alpha}(x)\hat{\beta}(x) \equiv \alpha_1(x)\beta_1(x) \mod \mathbb{Z}_p[x] \equiv \frac{d}{c}p(x) \mod \mathbb{Z}_p[x] \equiv 0 \mod \mathbb{Z}_p[x]$ since $p|d$.
Contradiction, because $\mathbb{Z}_p[x]$ is an integral domain. Thus $d \neq 1$ is not possible. $\square$

**Theorem: 3.32: Einstein's Criterion**

Let $p$ be a prime and $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$. If $p|a_i$ for $i \in \{0, ..., n-1\}$, but $p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}[x]$.

*Proof.* Assume $f(x) = a_0 + a_1 x + \cdots a_n x^n = (b_0 + \cdots + b_r x^r)(c_0 + \cdots + c_s x^s)$.
$p^2 \nmid a_0$ with $a_0 = b_0 c_0$ means $p \nmid b_0$ or $p \nmid c_0$. WLOG, we assume $p \nmid b_0$, but $p|c_0$.
$p \nmid a_n$ with $a_n = b_r c_s$ means $p \nmid b_r$ and $p \nmid c_s$.
Let $m$ be the minimal integer s.t. $p \nmid c_m$ and consider $a_m = \underbrace{b_0 c_m}_{\text{not divisible by } p} + \underbrace{b_1 a_{m-1} + \cdots + b_m c_0}_{\text{divisible by } p}$. Then $p \nmid a_m$.
By the constraints (the minimal integer s.t. $p \nmid a_m$ should be $n$), $a_m = a_n$, thus $m = n$.
$\deg(c_0 + \cdots + c_s x^s) = \deg(f(x))$. Thus there is no factorization. $f(x)$ is irreducible. $\square$

**Example:** $3x^6 + 25x^5 - 20x^2 + 15x - 10$ is irreducible with $p = 5$.

**Example:** $5x^3 + 14x^2 - 7x + 7$ is irreducible with $p = 7$.

## 3.6 Integral Domains

**Theorem: 3.33:**

Every ideal in $K[x]$ is a principal ideal. $K[x]$ is a PID (Principal Ideal Domain).

*Proof.* Suppose $I \subset K[x]$ is an ideal. Take $p(x) \in I$ s.t. $p(x)$ is monic, and $\deg(p(x))$ is minimal over all polynomials of positive degree. $(p(x)) \subset I$.
Let $f(x) \in I$. Do division algorithm with $f(x)$ and $p(x)$, $f(x) = p(x)q(x) + r(x)$ with $0 \leq \deg(r) < \deg(p)$.
Thus $\deg(r) = 0$, because $p(x)$ is minimal degree.
Case 1: $r(x) = 0$, $f(x) \in (p(x))$, $I \subset (p(x))$. Then $(p(x)) = I$. $I$ is principal ideal.
Case 2: $\alpha \neq 0 \in K$. Then $(p(x)) = (\alpha) = K[x] = I$. $I$ is a principal ideal. $\square$

**Example:** $\mathbb{Z}[x]$ is not a PID.

*Proof.* We find an ideal $I$ that is not principal.
Let $I = (x, 2) = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 2a_0 : a_i \in \mathbb{Z}\}$.
Suppose $p(x) \in \mathbb{Z}[x]$ with $(p(x)) = I = (x, 2)$, then $2 \in (p(x))$, $2 = p(x)f(x)$ for some $f(x) \in \mathbb{Z}[x]$.
Then $\deg(p) = \deg(f) = 0$. $p(x) = 1$ or $p(x) = 2$. But $p(x) \neq 1$, otherwise $(p(x)) = (1) = \mathbb{Z}[x]$.
Thus $p(x) = 2$, $I = (2)$, but $x \notin I$, since $x$ is not necessarily a multiple of 2. Contradiction. Thus $I$ is not principal. □

### 3.6.1 Field of Fractions

We can think of $\mathbb{Q}$ as a set of symbols $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$, where $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.

***Theorem:* 3.34: Field of Fractions**

Let $D$ be any integral domain. $S = \{(a, b) : a, b \in D, b \neq 0\}$. $\sim \subset S \times S$ s.t. $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ is an equivalence relation. The equivalence classes are $[a, b] = \{(c, d) \in S : (a, b) \sim (c, d)\}$. Define $F_D = \{[a, b] : a, b \in D, b \neq 0\}$.
$F_D$ is a field (the field of fraction of $D$). It is the unique smallest field s.t. $D$ can be embedded in $F_D$.

*Proof.* Firstly, we show that $\sim$ is an equivalence relation.

1. Reflexivity: $(a, b) \sim (b, a)$, because $ab = ab$
2. Symmetry: If $(a, b) \sim (c, d)$, then $ad = bc$, $bc = ad \Rightarrow (c, d) \sim (a, b)$
3. Transitivity: If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$. Then $adcf = bcde$, $af = be$, $(a, b) \sim (e, f)$.

Now we show that $F_D$ is a field.
We define the addtion $[a, b] + [c, d] = [ad + bc, bd]$. We check that the addition is well-defined:
Suppose $[a, b] = [\hat{a}, \hat{b}]$, $[c, d] = [\hat{c}, \hat{d}]$. *i.e.* $a\hat{b} = \hat{a}b$, $c\hat{d} = \hat{c}d$.
$[a, b] + [c, d] = [ad + bc, bd]$, $[\hat{a}, \hat{b}] + [\hat{c}, \hat{d}] = [\hat{a}\hat{d} + \hat{b}\hat{c}, \hat{b}\hat{d}]$.
$(ad + bc)(\hat{b}\hat{d}) = ad\hat{b}\hat{d} + bc\hat{b}\hat{d} = a\hat{b}d\hat{d} + c\hat{d}b\hat{b} \stackrel{\text{Equivalence} of [a,b]=[\hat{a},\hat{b}]}{=} \hat{a}bd\hat{d} + \hat{c}db\hat{b} = bd(\hat{a}\hat{d} + \hat{c}\hat{b})$. Thus addition is well-defined.
We define the multiplication $[a, b][c, d] = [ac, bd]$. It is also easy to check that the multiplication is well defined.
$F_D$ is abelian, additive identity is $[0, d]$, invserse of $[a, b]$ is $[-a, b]$. Multiplication is associative, distributive, commutative and identity is $[a, a]$, with inverse of $[a, b]$ being $[b, a]$ for $a \neq 0$.

Now we show that we can embed $D$ in $F_D$.
Consider $I : D \to F_D$ s.t. $I(a) = [a, 1]$.
Homomorphism: $I(a, b) = [a + b, 1] = [a, 1] + [b, 1] = I(a) + I(b)$
$I(ab) = [ab, 1] = [a, 1][b, 1] = I(a)I(b)$
Injective: Suppose $a \in \text{Ker}(I)$, *i.e.* $I(a) = 0$. Then $[a, 1] = [0, 1] \Rightarrow a = 0$. Thus $\text{Ker}(I) = 0$.
Thus $I$ is an injective ring homomorphism.

We now show that $F_D$ is the smallest such field.
Suppose $\exists K$ a field s.t. $D$ is embedded in $K$. *i.e.* $\exists \phi : D \to K$ an injective field homomorphism. We want to find $\psi : F_D \to K$ s.t. $\phi = \psi \circ I$.
Set $\psi([a, b]) = \phi(a)\phi(b)^{-1}$. With $a, b \in D$, $\phi(a), \phi(b) \in K$.

Homomorphism:
$\psi([a,b]+[c,d]) = \psi([ad+bc, bd]) = \phi(ad+bc)\phi(bd)^{-1} = (\phi(a)\phi(d)+\phi(b)\phi(c))\phi(b)^{-1}\phi(d)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \psi([a,b]) + \psi([c,d])$.
$\psi([a,b][c,d]) = \psi([ac, bd]) = \phi(ac)\phi(bd)^{-1} = \phi(a)\phi(b)^{-1}\phi(c)\phi(d)^{-1} = \psi([a,b])\psi([c,d])$
Injective: Suppose $[a,b] \in \text{Ker}(\psi)$. $\psi([a,b]) = \phi(a)\phi(b)^{-1} = 0$, but $\phi(b)^{-1} \neq 0$. Thus $\phi(a) = 0$. $a = 0$. $\text{Ker}(\psi) = \{[0,b]\} = \{[0,1]\}$ is trivial. $\psi$ is injective field homomorphism.

Now we show that $\phi = \psi \circ I$, $\psi \circ I(a) = \psi([a,1]) = \phi(a)\phi(1)^{-1} = \phi(a)$. Thus $\phi = \psi \circ I$. $\square$

***Definition:* 3.22: Irreducibles and Primes**

Let $R$ be a commutative ring with 1, $D$ be an integral domain. Let $a, b \in R$.
1. $a|b$ if $\exists c \in R$ s.t. $b = ac$
2. $a$ and $b$ are associates if there exists a unit $u$ s.t. $a = ub$
3. A non-unit $p \in D$ is irreducible if when $p = ab$, $a$ or $b$ is a unit
4. $p$ is prime if $p|ab \Rightarrow p|a$ or $p|b$

**Example:** $R = \langle x^2, y^2, xy \rangle \subset \mathbb{Q}[x,y]$.
Note: $R = \mathbb{Q}[x,y]^{\mathbb{Z}_2}$ is $\mathbb{Q}[x,y]$ under the group action of $\mathbb{Z}_2$. $\mathbb{Z}_2(x) = -x$, $\mathbb{Z}_2(y) = -y$.
$x^2, y^2, xy$ are irreducible in $R$, but $xy$ is not prime. $xy | x^2y^2$, but $xy \nmid x$ and $xy \nmid y$.

***Definition:* 3.23: $\mathbb{Z}[i\sqrt{3}]$ and Norm**

Consider the ring $\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\}$. We can associate a norm function $N : \mathbb{Z}[i\sqrt{3}] \to \mathbb{N}$ s.t. $N(a + bi\sqrt{3}) = a^2 + 3b^2$ with the following properties:
1. $N(x) = 0 \Leftrightarrow x = 0$
2. $N(xy) = N(x)N(y)$
3. $u$ is a unit $\Leftrightarrow N(u) = 1$
4. If $N(x)$ is a prime, $x$ is irreducible.

*Proof.* We show that $N(x)$ is a well-defined norm function.

1. $(\Rightarrow)$ Let $x = a + bi\sqrt{3}$. If $N(x) = 0$, $a^2 + 3b^2 = 0$. Since $a^2 \geq 0, b^2 \geq 0$, we have $a = b = 0$, $x = 0$. $(\Leftarrow)$ trivial.
2. Let $x = a + bi\sqrt{3}$, $y = c + di\sqrt{3}$. $xy = (ac - 3bd) + (ad + bc)i\sqrt{3}$.
   $N(xy) = (ac - 3bd)^2 + 3(ad + bc)^2 = (a^2 + 3b^2)(c^2 + 3d^2) = N(x)N(y)$
3. $(\Rightarrow)$ Suppose $u$ is a unit. $\exists u^{-1} \in \mathbb{Z}[i\sqrt{3}]$ s.t. $uu^{-1} = 1$. $N(uu^{-1}) = 1 \overset{\text{By 2.}}{=} N(u)N(u^{-1})$.
   But $N(u), N(u^{-1}) \in \mathbb{N}$, then $N(u) = N(u)^{-1} = 1$
   $(\Leftarrow)$ Suppose $N(u) = 1$, $u = a + bi\sqrt{3}$. $N(u) = a^2 + 3b^2$. If $b^2 > 0$, $N(u) > 1$. Thus $b^2 = 0$, $b = 0$, and $a^2 = 1$, $a = \pm 1$. $u = \pm 1$, both are units.
4. Suppose $x = yz$. Then $N(x) = N(y)N(z)$. If $N(x)$ is prime. WLOG, $N(y) = 1$, $N(x) = N(z)$, $y$ is a unit, $x$ is irreducible.

We now show that $(1 + i\sqrt{3})$ is irreducible but not a prime in $\mathbb{Z}[i\sqrt{3}]$.
Suppose $1 + i\sqrt{3} = xy$, $N(x)N(y) = N(1 + i\sqrt{3}) = 4$.
Case 1: $x$ or $y$ is a unit, then $1 + i\sqrt{3}$ is irreducible.
Case 2: $x$ and $y$ are not unit, then $N(x) = N(y) = 2$, but $a^2 + 3b^2 = 2$ has no solution in natural numbers. Contradiction. This case is impossible.

$(1+i\sqrt{3})(1-i\sqrt{3}) = 4 = 2\cdot 2$
Thus $(1+i\sqrt{3})|4 \Rightarrow (1+i\sqrt{3})|2\cdot 2$, but $(1+i\sqrt{3}) \not| 2$, thus it is not a prime. $\square$

### 3.6.2 Unique Factorization Domain

**Definition: 3.24: Unique Factorization Domain**

An integral domain $D$ is a unique factorization domain (UFD) if

1. Every non-zero non-unit element can be written as the product of irreducibles.
2. If $a = p_1\cdots p_r = q_1\cdots q_s$ with $p_i, q_j$ irreducible, then $r = s$ and $\exists\sigma\in S_r$ with $p_i = q_{\sigma(i)}u_i$, $u_i$ a unit. *i.e.* $p_i$ and $q_{\sigma(i)}$ are associates.

**Example:** $\mathbb{Z}$ is a UFD by the fundamental theorem of arithmetic.
$30 = 2\cdot 3\cdot 5 = 2(-3)(-5)$, but $(-3) = (-1)3$, where $(-1)$ is a unit. $\{2,3,5\}$ is the same as $\{2,-3,-5\}$ up to a unit.

**Example:** $\mathbb{Z}[i]$, $K[x]$ are UFD.

**Example:** $\mathbb{Z}[i\sqrt{3}]$ is not a UFD.
Consider $4 = 2\cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$.
For $\mathbb{Z}[i\sqrt{3}]$ to be a UFD, we need $2 = (1+i\sqrt{3})u$, where $u$ is a unit.
Let $u = a+bi\sqrt{3}\in\mathbb{Z}[i\sqrt{3}]$. $u^{-1} = \frac{a-bi\sqrt{3}}{a^2+3b^2}\in\mathbb{Z}[i\sqrt{3}]$.
We need $\frac{a}{a^2+3b^2}\in\mathbb{Z}$, $b=0$, $\frac{a}{a^2} = \frac{1}{a} = \mathbb{Z}$, then $a=\pm 1$. $u = \pm 1$, which is impossible, because $2\neq 1+i\sqrt{3}$.

**Example:** $\mathbb{Z}[\sqrt{5}]$ is not a UFD.
Consider $4 = 2\cdot 2 = (1+\sqrt{5})(-1+\sqrt{5})$.
We need $2 = u(1+\sqrt{5})$. Let $u = a+b\sqrt{5}$. $2 = (1+\sqrt{5})(a+b\sqrt{5}) = a+5b+(a+b)\sqrt{5}$. $\begin{cases} a+5b=2 \\ a+b=0\end{cases} \Rightarrow \begin{cases} a = -\frac{1}{2} \\ b = \frac{1}{2}\end{cases}$, $a,b\notin\mathbb{Z}$.

**Definition: 3.25: Primitive and Content**

Let $D$ be an integral domain, $F$ be a field of fraction. Let $p(x) = a_nx^n+\cdots a_0\in D[x]$. Define the content of $p(x)$ to be $\text{cont}(p(x)) = \gcd(a_0,...,a_n)$.
$p(x)$ is primitive if $\text{cont}(p(x)) = 1$.

**Lemma: 3.5:**

1. If $f(x), g(x)\in D[x]$ are primitive, then so is $f(x)g(x)$
2. $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$
3. Suppose $p(x)\in D[x]$ with $p(x) = f(x)g(x)\in F(x)$, then $\exists\hat{f}(x),\hat{g}(x)\in D[x]$ s.t. $p = \hat{f}\hat{g}$

**Corollary 5.** *$p(x)$ is irreducible in $D[x]$ $\Leftrightarrow$ $p(x)$ is irreducible in $F[x]$.*

**Theorem: 3.35:**

$D$ is a UFD $\Leftrightarrow$ $D[x]$ is a UFD.

### 3.6.3 Principal Ideal Domain

***Definition:* 3.26: Principal Ideal Domain**

An integral domain is called a principal ideal domain (PID) if every ideal is principal.

**Example:** $\mathbb{Z}$, $K[x]$ are PIDs.

***Lemma:* 3.6: Properties of PID**

Let $D$ be a PID with $a, b \in D$, then

1. $a|b \Leftrightarrow \langle b\rangle \subset \langle a\rangle$
2. $a$ and $b$ are associates $\Leftrightarrow \langle a\rangle = \langle b\rangle$
3. $a$ is a unit $\Leftrightarrow \langle a\rangle = D$

*Proof.*

1. $(\Rightarrow)$ Suppose $a|b$, then $b = ar$ for $r \in D$. Suppose $x \in \langle b\rangle$, then $x = by$ for $y \in D$. Then $x = ary \in \langle a\rangle$. Thus $\langle b\rangle \subset \langle a\rangle$

   $(\Leftarrow)$ Suppose $\langle b\rangle \subset \langle a\rangle$, then $b \in \langle a\rangle$, $b = ar$ for some $r \in D$, thus $a|b$.

2. $(\Rightarrow)$ Suppose $a, b$ are associates, by Definition 3.22, there exists unit $u \in D$ s.t. $a = ub$. thus $b|a$. By 1, $\langle a\rangle \subset \langle b\rangle$. Also $au^{-1} = b$, $u^{-1}$ is a unit, then $a|b$, $\langle b\rangle \subset \langle a\rangle$. Therefore $\langle a\rangle = \langle b\rangle$.

   $(\Leftarrow)$ Suppose $\langle a\rangle = \langle b\rangle$. Then $\langle a\rangle \subset \langle b\rangle \Rightarrow a|b$, $b = ax$; $\langle b\rangle \subset \langle a\rangle \Rightarrow b|a$, $a = yb$. Therefore $a = yax = axy$. $1 = xy$, $x$ is a unit. $a$ and $b$ are associates.

3. $(\Rightarrow)$ Suppose $a$ is a unit, $a^{-1}$ exists. Take $x \in D$ and $x = x \cdot 1 = xa^{-1}a \in \langle a\rangle$. $D \subset \langle a\rangle \subset D$, thus $\langle a\rangle = D$

   $(\Leftarrow)$ Suppose $D = \langle a\rangle$. In particular $1 \in \langle a\rangle$. Then $\exists b \in D$ s.t. $ab = 1$, $a$ is a unit.

□

***Theorem:* 3.36:**

Let $D$ be a PID and $0 \neq \langle p\rangle \subset D$, then $\langle p\rangle$ is a maximal ideal $\Leftrightarrow p$ is irreducible.

*Proof.* $(\Rightarrow)$ Suppose $\langle p\rangle$ is a maximal ideal and $p = ab$.
Then $a|p$. By Lemma 3.6, $\langle p\rangle \subset \langle a\rangle \subset D$.
By Definition 3.18, either $\langle p\rangle = \langle a\rangle$ or $\langle a\rangle = D$.
If $\langle p\rangle = \langle a\rangle$, then $p$ and $a$ are associates by Lemma 3.6, $b$ is a unit.
If $\langle a\rangle = D$, then $a$ is a unit.
Thus $p$ is irreducible by Definition 3.22.

$(\Leftarrow)$ Suppose $p$ is irreducible.
Consider $a \in D$ with $\langle p\rangle \subset \langle a\rangle \subset D \overset{\text{By Lemma 3.6}}{\Rightarrow} a|p \Rightarrow p = ab$ for some $b \in D$.
But $p$ is irreducible, then $a$ is a unit or $b$ is a unit.
If $a$ is a unit, $\langle a\rangle = D$
If $b$ is a unit, $p$ and $a$ are associates, $\langle p\rangle = \langle a\rangle$.
By Definition 3.18, $\langle p\rangle$ is maximial. □

**Corollary 6.** *Let $D$ be a PID. If $p \in D$ is irreducible, then it is prime. In general prime$\subset$irreducible.*

*Proof.* Suppose $p$ is irreducible and $p|ab$.
Then $ab = pr$ for some $r \in D$. By Theorem 3.36, $ab \in \langle p \rangle$
Then $\langle p \rangle$ is a prime ideal by Definition 3.17. This means that $a \in \langle p \rangle$, $p|a$ or $b \in \langle p \rangle$, $p|b$.
By Definition 3.22, $p$ is a prime. □

**Definition: 3.27: Accending Chain Condition (Noetherian Ring)**

A ring satisfies the accending chain condition if for every set of ideals $\{I_j\}_{j=1}^{\infty}$ s.t. $I_1 \subset I_2 \subset \cdots$, there exists $N \in \mathbb{N}$ s.t. $I_n \geq I_N$ for all $n \geq N$. These rings are called Noetherian Rings.

**Lemma: 3.7:**

Every PID satisfies Accending Chain Condition.

*Proof.* Let $D$ be a PID, and $\{I_j\}_{j=1}^{\infty}$ be a set of ideals s.t $I_1 \subset I_2 \subset \cdots$.
Let $I = \bigcup\limits_{j=1}^{\infty} I_j$. We show that $I$ is an ideal.
Subring: Suppose $a, b \in I$, $\exists k, l$ s.t. $a \in I_k$, $b \in I_l$. $a, b \in I_{\max(l,k)}$. Then $a - b, ab \in I_{\max(l,k)} \subset I$. Thus $I$ is a subring by Theorem 3.16.
Ideal: Suppose $a \in I$ and $r \in D$, then $a \in I_k$ for some $k$, $ra \in I_k \subset I$, $I$ is then an ideal.

By Definition 3.26, every ideal is principal. Thus $I = (a)$ for some $a \in D$. $a \in I = \bigcup\limits_{j=1}^{\infty} I_j$. Thus $a \in I_N$ for some $N \in \mathbb{N}$.
Therefore $I = (a) \subset I_N \subset I_{N+1} \subset \cdots \subset I$. Then $I_N = I_{N+1} = \cdots = I$. □

**Theorem: 3.37:**

Every PID is a UFD.

*Proof.* We show that factorization is possible and is unique in PIDs.

Let $D$ be a PID.

Factorization: Suppose $a \in D$ is a non-zero non-unit element.
We can write $a = a_1 b_1$ where $a_1$ is not an unit. We can iteratively factor $a_k$ and write $a_k = a_{k+1} b_{k+1}$, where $a_{k+1}$ is not a unit.
Then we form a divisibility chain $a_1|a$, $a_2|a_1$,..., $a_{k+1}|a_k$. Thus $\langle a \rangle \subset \langle a_1 \rangle \subset \cdots \subset \langle a_k \rangle \subset \cdots$ by Definition 3.26.
By Lemma 3.7, $\exists N$ s.t. $\langle a_N \rangle = \langle a_{N+1} \rangle = \cdots = \langle a_n \rangle$ for all $n \geq N$.
By Lemma 3.6, $a_N$ and $a_n$ are associates for all $n \geq N$. Thus $a_N = pu$ for $p$ irreducible and $u$ unit.
Then $a = p_1 x_1$ for some irreducible $p_1$. Iterate on $x_k = p_{k+1} x_{k+1}$ where $p_{k+1}$ irreducible.
$\langle x_1 \rangle \subset \cdots \subset \langle x_N \rangle = \langle x_{N+1} \rangle$. $x_N$ is irreducible. Set $x_N = p_{N+1}$. Then $a = p_1 \cdots p_{N+1}$ where $p_i$ are irreducible.

Uniqueness: Suppose $a = p_1 \cdots p_r = q_1 \cdots q_s$. We show taht $r = s$ and $p_i = u_j q_j$.
Assume $r < s$. $p_1 | a \Rightarrow p_1 | q_1 \cdots q_s$, then $p_1 | q_j$ for some $j$. Reorder s.t. $p_1 | q_1$. $q_1 = u_1 p_1$ s.t. $u_1$ is a unit, since $q_1$ is irreducible.
Then $p_1(p_2 \cdots p_r) = p_1(u_2 q_2 \cdots q_s)$. Iterate and we get $u_1 \cdots u_r q_{r+1} \cdots q_s = 1$. This means that $q_{r+1} \cdots q_s = 1$, which is a contradiction. □

### 3.6.4 Euclidean Domain

***Definition:* 3.28: Euclidean Domain**

An integral domain $D$ is known as a Euclidean domain if $\exists N : D \to \mathbb{N}$ (norm function) s.t.

1. If $0 \neq a, b \in D$, then $N(a) \leq N(ab)$
2. If $a, b \in D$ with $b \neq 0$, there exists $q, r \in D$ s.t. $a = bq + r$ with $r = 0$ or $N(r) < N(b)$

**Example:** $\mathbb{Z}$ with $N(m) = |m|$, $K[x]$ with $N(f(x)) = \deg(f)$ are Euclidean domains.

**Example:** Show that the Gaussian Integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a Euclidean domain.

*Proof.* Define $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$. If $\alpha = a + bi$, $N(\alpha) = a^2 + b^2$

We show that the two properties in Definition 3.28 are satisfied.

Let $0 \neq \alpha, \beta \in \mathbb{Z}[i]$. $N(\alpha\beta) = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta) \geq N(\alpha)$, since $N(x) \geq 1$ for any $x \neq 0 \in \mathbb{Z}[i]$.

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Write $\alpha = a + bi$, $\beta = c + di$. Then $\beta^{-1} = \frac{c-di}{c^2+d^2}$

$$\begin{aligned}
\alpha\beta^{-1} &= (a + bi)\frac{c - di}{c^2 + d^2} = \frac{1}{c^2 + d^2}((ac + bd) + (bc - ad)i) \\
&= (q_1 + r_1) + (q_2 + r_2)i, \text{ where } -\frac{1}{2} \leq r_1, r_2 \leq \frac{1}{2}, q_1, q_2 \in \mathbb{Z} \\
&= (q_1 + q_2 i) + (r_1 + r_2 i)
\end{aligned}$$

Let $\gamma = q_1 + q_2 i \in \mathbb{Z}[i]$. $\alpha = \beta\gamma + \beta(r_1 + r_2 i)$. Since $\alpha, \beta, \gamma \in \mathbb{Z}[i]$, then $\rho = \beta(r_1 + r_2 i) \in \mathbb{Z}[i]$ (Rings are closed under addition and multiplication)

$N(\rho) = \beta\bar{\beta}(r_1 + r_2 i)(r_1 - r_2 i) = N(\beta)(r_1^2 + r_2^2) \overset{-\frac{1}{2} \leq r_1, r_2 \leq \frac{1}{2}}{\leq} \frac{1}{2}N(\beta) < N(\beta)$

Thus $\mathbb{Z}[i]$ is a Euclidean domain. □

***Theorem:* 3.38:**

If $D$ is a Euclidean domain, then it is a PID.

*Proof.* Let $I \subset D$ be an ideal. We want to show that $I = (a)$, *i.e.* $I$ is principal.
Take $b \in I$ s.t. $N(b)$ is minimal among all elements from $I$, $\langle b \rangle \subset I$.
Take $a \in I$, find $q, r$ with $a = bq + r$ where $r = 0$ or $N(r) < N(b)$.
Note that $N(r) < N(b)$ is not possible, otherwise $N(b)$ is not minimal.
Therefore $r = a - bq = 0 \in I$. $a = bq \in \langle b \rangle$. $I \subset \langle b \rangle$. Therefore $I = \langle b \rangle$. $I$ is principal. □

### 3.6.5 Summary of Integral Domains

Commutative Ring with 1 $\supsetneq$ Integral domain $\supsetneq$ UFD $\supsetneq$ PID $\supsetneq$ Euclidean Domain $\supsetneq$ Field.

**Example:**

1. Commutative Ring with 1: $\mathbb{Z}_{12}$, $3 \cdot 4 = 0 \in \mathbb{Z}_{12}$, thus not an Integral domain
2. $\mathbb{Z}[i\sqrt{5}]$: $6 = 2 \cdot 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$, factorization is not unique, thus not a UFD
3. $\mathbb{Z}[x]$: $\langle x, 2\rangle$ is not principal. $\mathbb{Q}[x, y]$, $\langle x, y\rangle$ not principal. Thus not PID.
4. $\mathbb{Z}[\frac{1}{2}(1 + i\sqrt{19})]$ is a PID but not Euclidean domain
5. $\mathbb{Z}$, $K[x]$ are Euclidean domain, but not fields
6. $\mathbb{Q}$, $\mathbb{R}$, $F_D$, $\mathbb{Z}_p$ are fields.

In commutative ring with 1, we always have prime$\Rightarrow$irreducible.

Starting from UFD, we have prime$\Leftrightarrow$irreducible.

Note: in field, there is no irreducible or prime. Every element is a unit.

# 4 Fields

Consider $\mathbb{Z}_2[x]/(x^2+x+1)$, $x^2+x+1$ is irreducible in $\mathbb{Z}_2[x]$. $\mathbb{Z}_2[x]/(x^2+x+1)$ is a field.
Define $\mathbb{Z}_2(\alpha) = \{a + b\alpha : a, b \in \mathbb{Z}_2, \alpha^2 = \alpha + 1\}$, where $\alpha$ is the root of $x^2+x+1$.
$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha+1\}$. $\mathrm{char}(\mathbb{Z}_2(\alpha)) = 2$, *i.e.* $\forall x \in \mathbb{Z}_2(\alpha)$, $x + x = 0$
Sometimes, we write $\mathbb{Z}_2(\alpha) = F_{2^2} = F_4$. It is a finite field of order 4.

**Facts:** Every finite field is of order $p^r$ for some prime $p$ and charactersitic of $p$. There is only one finite field up to isomorphism of any given order, $F_{p^r}$. To construct $F_{p^r}$, we find an irreducible degree $r$ polynomial $f(x) \in \mathbb{Z}_p[x]$, then $F_{p^r} \cong \mathbb{Z}_p[x]/(f(x))$.