Math 110.1 Lecture Notes

Jhon Christian N. Rozano
University of the Philippines Diliman
jnrozano@up.edu.ph

December 20, 2022

Contents

1 First Half Semester

1.1 Friday, September 9: Division Algorithm and Modular Arithmetic

1.1.1 Division Algorithm

Definition 1.1.1. (Division Algorithm) Let $m, n \in \mathbb{Z}$ with $n > 0$. Then $\exists!\ q, r \in \mathbb{Z}$ such that $m = nq + r$ where $0 \leqslant r < n$ (m div $n = q$ and m mod $n = r$)

Remark 1.1.1. We call q the **quotient** and r the **remainder**.

Exercise 1.1.1. (Prove: Extended Division Algorithm) Let $m, n \in \mathbb{Z}$ with $n \neq 0$. Then $\exists!\ q, r \in \mathbb{Z}$ such that $m = nq + r$, where $0 \leqslant r < |n|$.

Proof. Let $m, n \in \mathbb{Z}$ with $n \neq 0$. By the Division Algorithm on $\mathbb{Z}$ applied to m and $|n| \in \mathbb{Z}^+$, $\exists!\ q, r \in \mathbb{Z}$ such that $m = |n|q + r$ with $0 \leqslant r < |n|$.

Case 1: If $n > 0$

If $n > 0$, then $|n| = n$. Hence $\exists!\ q, r \in \mathbb{Z}$ such that

$$m = |n|q + r = nq + r, \text{ with } 0 \leqslant r < |n|$$

Case 2: If $n < 0$

If $n < 0$, then $|n| = -n$. Hence $\exists! \; -q, r \in \mathbb{Z}$ such that

$$m = |n|q + r = -nq + r = n(-q) + r$$

Since $q \in \mathbb{Z}$ and is uniquely determined, then so is $-q$.

Definition 1.1.2. Let $m, n \in \mathbb{Z}$ with $n \neq 0$.

$$n \text{ divides } m (\text{notation: } n \mid m) \Leftrightarrow m = nk$$

for some $k \in \mathbb{Z}$.

Remark 1.1.2.
1. For every nonzero integer a, $a \mid 0$, and for every integer b, $1 \mid b$.
2. For $a \in \mathbb{Z}$, a and $-a$ have the same divisors.

Definition 1.1.3. Let n be a fixed positive integer and $a, b \in \mathbb{Z}$.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b) \Leftrightarrow a \bmod n = b \bmod n$$

Definition 1.1.4. (Greatest Common Divisor) Let a, b be integers not both zero. A positive integer d is called the **greatest common divisor** ($\gcd(a, b) = d$) of a and b if

1. $d \mid a$ and $d \mid b$, that is, d is a common divisor of a and b
2. $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \mid d$.

Definition 1.1.5. (Least Common Multiple) Let $a, b \in \mathbb{Z}^+$ and m be a positive integer. Then m is the **least common multiple** ($\operatorname{lcm}(a, b) = m$) of a and b if m satisfies the following:

1. $a \mid m$ and $b \mid m$, that is m is a multiple of both a and b;
2. $\forall c \in \mathbb{Z}$, if $a \mid c$ and $b \mid c$, then $m \mid c$.

Theorem 1.1.1. (Bézout's Identity) Let a, b be integers, not both zero, and $\gcd(a, b) = d$. Then $\exists u, v \in \mathbb{Z}$ such that $d = au + bv$.

Theorem 1.1.2. If $a, b, u, v \in \mathbb{Z}$, where a and b are not both zero, such that $au + bv = 1$, then $\gcd(a, b) = 1$.

Exercise 1.1.2. (Prove) If a and b are relatively prime, $c \in \mathbb{Z}$ and $a \mid bc$, then $a \mid c$.

Proof. Since a and b are relatively prime, let $\gcd(a,b) = 1, c \in \mathbb{Z}$ and $a \mid bc$. Thus, Theorem 1.1.2 implies that $1 = au + bv \ \exists\, u, v \in \mathbb{Z}$ and $bc = ak \ \exists \ k \in \mathbb{Z}$. Therefore, multiplying by c, we get $c = c(au + bv) = cau + bcv = cau + akv = a(cu + kv)$ where $c, u, k, v \in \mathbb{Z}$. Therefore, $a \mid c$. ■

Theorem 1.1.3. (Euclid's Lemma) Let $a, b \in \mathbb{Z}$. If p is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Exercise 1.1.3. (Prove) Let a, b be nonzero integers and $c \in \mathbb{Z}$. Suppose $a \mid c$ and $b \mid c$ and $\gcd(a,b) = d$. Then $ac \mid cd$.

Proof. Suppose $c = ak_1 \wedge c = bk_2$ for some $k_1, k_2 \in \mathbb{Z}$ and $d = au + bv$ for some $u, v \in \mathbb{Z}$ (by Bézout's identity). Thus, multiplying by c, $cd = c(au + bv) = cau + cbv = (bk_2)qu + (ak_1)bv = ab\underbrace{(k_2u + k_1v)}_{\in \mathbb{Z}}$ where $k_2u + k_1v \in \mathbb{Z}$. Therefore, $ab \mid cd$. ■

Theorem 1.1.4. If $a, b \in \mathbb{Z}^+$, then $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$

1.1.2 Equivalence Relation

Definition 1.1.6. (Relation) A **relation** R between sets A and B is any subset $R \subseteq A \times B$. A relation R on a set A is a subset of $A \times A$.

Definition 1.1.7. (Equivalence Relation) An **equivalence relation** E on a set A is a relation on A such that the following are satisfied for all $x, y, z \in A$:
1. (**reflexive**) $(x, x) \in E$;
2. (**symmetric**) $(x, y) \in E \Rightarrow (y, x) \in E$;
3. (**transitive**) $(x, y) \in E$ and $(y, z) \in E \Rightarrow (x, z) \in E$.

Definition 1.1.8. (Equivalence Class) Let E be an equivalence relation on A and let $a \in A$. Consider the set

$$[a]_E = \{x \in A \mid (x, a) \in E\}$$

The set $[a]_E$ is called the **equivalence class** of a with respect to E and a is called a **representative** of this class. We often denote by A/E the set of the equivalence classes with respect to E.

Remark 1.1.3.

1. The relation congruence modulo n is an equivalence relation on the set of integers.
2. If $a \equiv b \pmod{n}$ and $c \equiv \pmod{n}$, then
   (a) $a + c \equiv b + d \pmod{n}$
   (b) $ac \equiv bd \pmod{n}$

Exercise 1.1.4. Consider the relation $\sim$ on $\mathbb{Z}$ defined as follows:

$$a \sim b \text{ iff } 5 \mid (a - b)$$

a. Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.
b. Describe the equivalence classes of $\mathbb{Z}$ with respect to $\sim$.

Solution.

a. We show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

   i. (**reflexive**) Let $a \in \mathbb{Z}$

   $$5 \mid 0 = (a - a) \Rightarrow a \sim a$$

   ii. (**symmetric**) Let $a, b \in \mathbb{Z}$. Suppose $a \sim b \Leftrightarrow 5 \mid (a - b)$. Then, there exists $k \in Z$ such that $a - b = 5k$.

   $$\Rightarrow -(b - a) = 5k \Rightarrow b - a = 5(-k) \text{ where } (-k) \in \mathbb{Z} \Rightarrow 5 \mid (b - a) \Rightarrow b \sim a$$

   iii. (**transitive**) Let $a, b, c \in \mathbb{Z}$. Suppose $a \sim b \wedge b \sim c$. Thus $5 \mid (a - b)$ and $5 \mid (b - c)$. These imply that $a - b = 5k_1$ and $b - c = 5k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then $(a - b) + (b - c) = 5k_1 + 5k_2 \Rightarrow a - c = 5(k_1 + k_2)$ where $k_1 + k_2 \in \mathbb{Z}$. Thus, $5 \mid (a - c) \Rightarrow a \sim c$.

b. Let $a \in \mathbb{Z}$. Then,

$$\begin{aligned}
[a]_\sim &= \{x \in \mathbb{Z} \mid x \sim a\} = \{x \in \mathbb{Z} \mid 5 \mid (x - a)\} \\
&= \{x \in \mathbb{Z} \mid x - a = 5k \ \exists\, k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x = a + 5k, \exists\, k \in \mathbb{Z}\} \\
&= \{a + 5k \mid k \in \mathbb{Z}\}
\end{aligned}$$

$$\mathbb{Z}/_\sim = \{[0]_\sim, [1]_\sim, [2]_\sim, [3]_\sim, [4]_\sim\}$$

For the second part:

Exercise 1.1.5. Let $A = \mathbb{R}$. Consider the relation $\sim$ on A defined as follows:

$$a \sim b \text{ iff } ab > 0$$

1. Show that $\sim$ is not an equivalence relation on $\mathbb{R}$
2. Is $\sim$ an equivalence relation on $\mathbb{R}/\{0\}$? Justify your answer.

Solution.

1. Note that $0 \in \mathbb{R}$ and $0 \cdot 0 = 0 \not> 0$ $(0 \nsim 0)$, so $\sim$ is not reflexive. Since $\sim$ is not reflexive, it is not an equivalence relation.
2. Second part:
   i. (reflexive) Let $a \in \mathbb{R}^*$. We have $a \cdot a = a^2 > 0$. Therefore, $a \sim a$.
   ii. (symmetric) Let $a, b \in \mathbb{R}^*$ and $a \sim b \Rightarrow ab > 0$. Then $ba = ab > 0$. Therefore, $b \sim a$.
   iii. (transitive) Let $a, b, c \in \mathbb{R}^*$ and $a \sim b \wedge b \sim c$. Hence, $ab > 0$ and $bc > 0$. Therefore, their product is $(ab)(bc) < 0 \Rightarrow ab^2c > 0 \Rightarrow \dfrac{1}{b^2}(ab^2c) > \dfrac{1}{b^2} \cdot 0 \Rightarrow ac > 0 \Rightarrow a \sim c$

Therefore,
$[1]_\sim = \{x \in \mathbb{R}^* \mid x \sim 1\} = \{x \in \mathbb{R}^* \mid x = x \cdot 1 > 0\} = (0, +\infty)$
$[-1]_\sim = \{x \in \mathbb{R}^* \mid x \sim -1\} = \{x \in \mathbb{R}^* \mid -x = x(-1) > 0\} = \{x \in \mathbb{R}^* \mid x < 0\} = (-\infty, 0)$
$\mathbb{R}^*/_\sim = \{[1]_\sim, [-1]_\sim\}$

Theorem 1.1.5. Let n be a fixed positive integer and $a, b \in \mathbb{Z}$. Then $a \bmod n = b \bmod n$ if and only if $a \equiv b \pmod{n}$.

1.2 Friday, September 16: Binary Operations and Groups

1.2.1 Binary Operations

Definition 1.2.1. (Function) A **function** f from set A to set B (denoted by $f : A \to B$) is a relation between A and B such that each $a \in A$ appears as the first member of exactly one ordered pair $(a, b) \in f$, that is, f is a rule that assigns to each $a \in A$ exactly one $b \in B$. The element a is called a **preimage** of b under f, and b is called the **image** of a under f or the value of the function f at a and is usually denoted by $f(a)$.

Remark 1.2.1. Consider the function $f : A \to B$.

1. Then we have the following
   (a) $\operatorname{Dom} f = A$ (domain of f)
   (b) If $x_1, x_2 \in A$ and $x_1 = x_2$, then $f(x_1) = f(x_2)$. In this case, f is **well-defined**

2. The set B is called the codomain of f. The range of f is the set $f(A) = \{f(a) \mid a \in A\}$. If $B = A$, we say f is a function on A

Definition 1.2.2. (Binary Operation) A **binary operation** $*$ on a nonempty set S is a function

$$\begin{aligned} * : S \times S &\to S \\ (a, b) &\mapsto a * b \end{aligned}$$

Remark 1.2.2. To verify that $*$ is a binary operation on $S \neq \varnothing$:

1. **closure property**: $\forall (a, b) \in S \times S, a * b \in S$.
2. **uniqueness of the assigned element in** S: $\forall (a_1, b_1), (a_2, b_2) \in S \times S$, if $(a_1, b_1) = (a_2, b_2)$. then $a_1 * b_1 = a_2 * b_2$. This means that the operation $*$ is well-defined.

Exercise 1.2.1. Is $*$ defined by $a * b = ab - 1$ a binary operation on $\mathbb{Z}$? on $\mathbb{Z}^*$

Solution.

1. On $\mathbb{Z}$,
   i. Let $a, b \in \mathbb{Z}$. Then $a * b = ab - 1 \in \mathbb{Z}$. Therefore, $\mathbb{Z}$ is closed under $*$.
   ii. Let $a, b, c, d \in \mathbb{Z}$. Suppose $a = c$ and $b = d$. Then, $a * b = ab - 1 = cd - 1 = c * d$. Hence, $*$ is well-defined.

   Therefore, $*$ is a binary operation on $\mathbb{Z}$. ■
2. On $\mathbb{Z}^*$,
   i. Let $a = b = 1 \in \mathbb{Z}^*$

   $$a * b = 1 * 1 = 1 \cdot 1 - 1 = 0 \notin \mathbb{Z}^*$$

   Therefore, $*$ is not a binary operation on $\mathbb{Z}^*$. ■

Exercise 1.2.2. Let $R = \left\{(x, y) \in \mathbb{Z}^2 \mid |x| = |y|\right\}$. Define the operation $*$ on $\mathbb{Z}/R = \{[x]_R \mid x \in \mathbb{Z}\}$ by

$$[a] * [b] = [a + b]$$

where $[a], [b] \in \mathbb{Z}/R$. Show that $*$ is not well-defined.

Proof. Note that $\mathbb{Z}/R = [a] = \{a, -a\} = [-a]$. For instance, take $[2] = [-2]$ and $[3] = [3]$. Then,

$$[2] * [3] = [2 + 3] = [5] \neq [1] = [-2 + 3] = [-2] * [3]$$

Therefore, $*$ is not well-defined. ■

1.2.2 Groups

Definition 1.2.3. (Algebraic Structure) An **algebraic system** or **algebraic structure** is a nonempty set S with one or more binary operations defined on S.
Notation. $\langle S, * \rangle$ (a (binary) algebraic structure)

Definition 1.2.4. (Groups) $\langle G, * \rangle$ is
1. a **semigroup** if $*$ is associative, i.e., $\forall a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. a **monoid** if it is a semigroup and $\exists e \in G$ such that $\forall a \in G$, $a * e = a = e * a$.
3. a **group** if it is a monoid and $\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$.

Remark 1.2.3.
1. $a, b, c \in \langle G, * \rangle$, then $a * b * c$ makes sense by (G1)
2. e is the **identity element** for $*$ and a^{-1} is the **inverse** of a
3. A group G is **abelian** if its binary operation $*$ is commutative
4. Order of a group $G : |G|$

Exercise 1.2.3. $\langle 2\mathbb{Z}, \cdot \rangle$ Note: $(m\mathbb{Z} \mid m \in \mathbb{Z})$

Solution.
i. $2\mathbb{Z} \subseteq \mathbb{Z}$ and $\cdot$ is associative in $\mathbb{Z}$. Therefore, $\cdot$ is associative in $2\mathbb{Z}$.
ii. Note that 1 is an identity element in $\langle \mathbb{Z}, \cdot \rangle$, but $1 \notin 2\mathbb{Z}$.

Thus, $2\mathbb{Z} \subseteq \mathbb{Z}$ is a semigroup.

Let $m \in \mathbb{Z}$, consider $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ under multiplication.
Case 1: $m \notin \{-1, 0, 1\} \Rightarrow \langle m\mathbb{Z}, \cdot \rangle$ is a semigroup.
Case 2: $m \in \{1, -1\} \Rightarrow m\mathbb{Z} = Z : \langle \mathbb{Z}, \cdot \rangle$ is a monoid
Case 3: $m = 0 \Rightarrow m\mathbb{Z} = \{0\}$ under $\cdot$ is associative since $0 \cdot 0 = 0$ which implies $e = 0 \in \{0\}$. It also has an inverse since $0 * a^{-1} = e = 0 \Rightarrow a^{-1} = 0$. Moreover, $\cdot$ is commutative. Thus, $\langle \{0\}, \cdot \rangle$ is an **abelian group**.

Exercise 1.2.4. $\langle \mathbb{Z}, * \rangle$ where $*$ is defined by $a * b = a + b + 2, \forall a, b \in \mathbb{Z}$

Solution. Let $a, b, c \in \mathbb{Z}$
(G1) Note that

$$a*(b * c) = a*(b + c + 2) = a+(b + c + 2)+2 = a+b+c+4$$

and

$$(a*b)*c = (a+b+2)*c = a+b+2+c+2 = a+b+c+4$$

Therefore, $a*(b*c) = (a*b)*c$

(G2) $-2 \in \mathbb{Z}, \forall a \in \mathbb{Z}$

$$a*-2 = a+(-2)+2 = a = -2+a+2 = -2*a$$

Therefore, $e = -2$

(G3) $\forall a \in \mathbb{Z}$,

$$a*(-4-a) = a+(-4-a)+2 = -2 = -4-a+a+2 = (-4-a)*a$$

Take $a^{-1} = -4-a \in \mathbb{Z}$.

Moreover, $*$ is commutative: $\forall a, b \in \mathbb{Z}$

$$a*b = a+b+2 = b+a+2 = b*a$$

Thus, $\langle \mathbb{Z}, * \rangle$ is an abelian group.

Exercise 1.2.5. Let X be a non-empty set and $G = \{f \mid f : X \to X\}$ (f is a function on X). Consider $\langle G, \circ \rangle$, where $\circ$ is function composition.

Solution. Let $f_1, f_2 \in G$. Then $f_1 \circ f_2 : X \to X$ where $x \mapsto f_1(f_2(x)) = (f_1 \circ f_2)(x)$.
Let $f, g, h \in G$.

(G1) Let $x \in X$

$$\begin{aligned}[f \circ (g \circ h)](x) = f((g \circ h)(x)) &= f(g(h(x))) \\ &= (f \circ g)(h(x)) \\ &= [(f \circ g) \circ h](x)\end{aligned}$$

Therefore, $f \circ (g \circ h) = (f \circ g) \circ h$

(G2) $\forall x \in X$,

$$(f \circ \ \mathrm{id}(x)) = f(\mathrm{id}(x)) = f(x) = \ \mathrm{id}(f(x)) = (\mathrm{id} \circ f)(x)$$

Therefore, $f \circ \ \mathrm{id} = f = \ \mathrm{id} \circ f$

(G3) f might not have an inverse unless f is bijective. Moreover, $\circ$ is not always commutative. So $\langle G, \circ \rangle$ is a monoid.

Definition 1.2.5. (Euler's phi function) Let $n \in \mathbb{Z}^+$. The **Euler's phi function (or Euler's totient function)** $\phi(n)$ counts the positive intergers less than or equal to n that are relatively prime to n.

Remark 1.2.4.

1. Observe that $\phi(1) = 1$ and $|U(\mathbb{Z}_n)| = \phi(n)$
2. Let p be prime. Note that $\phi(p) = p - 1$. Moreover, if $k \geqslant 1$, then $\phi(p^k) = p^k - p^{k-1}$
3. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$
4. If $a^{-1}, b^{-1} \in G$ are inverses of $a, b \in G$, then
   a. $\left(a^{-1}\right)^{-1} = a$
   b. $(a * b)^{-1} = b^{-1} * a^{-1}$ (socks-shoes property)
5. The linear equations $a*x = b$ and $y*c = d$ have unique solutions x and y in G given respectively by $x = a^{-1} * b$ and $y = d * c^{-1}$

Theorem 1.2.1. Let $\langle G, * \rangle$ be a group and $a, b, c \in G$.

i. The identity element is unique
ii. The left and right cancellation laws hold, that is, $a * b = a * c$ implies $b = c$ and $b * a = c * a$ implies $b = c$
iii. For each $a \in G$, the inverse of a is unique

	Multiplicative Notation	Additive Notation
operation:	ab	$a + b$
identity:	e or 1	0
inverse:	a^{-1}	$-a$
exponents:	$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ factors}}$	$na = \underbrace{a + a + \dots a}_{n \text{ addends}}$
	$(a^m)^n = a^{mn} = a^{nm}$	$n(ma) = (nm)a = (mn)a$
	$a^m \cdot a^n = a^{m+n}$	$ma + na = (m+n)a$
	$a^{-n} = (a^n)^{-1} = \left(a^{-1}\right)^n$	$(-n)a = -(na) = n(-a)$
	$a^0 = e$	$0a = 0$
	$a^1 = a$	$1a = a$

Exercise 1.2.6. Complete the following Cayley table for the group $\langle \{e, a, b, c, d, *\rangle\}$.

$*$	e	a	b	c	d
e	e				
a		b			e
b		c	d	e	
c		d		a	b
d					

Solution.

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Corollary 1.2.1. In a Cayley table of a group, each element appears exactly one in each row and exactly once in each column.

Theorem 1.2.2. Let G be a group. Then G is abelian if and only if $\forall n \in \mathbb{Z}^+, \forall a, b \in G, (ab)^n = a^n b^n$

Proof.
($\Rightarrow$) By induction,
Base case: If $n = 1$,

$$ab = (ab)^1 = a^1 b^1 = ab$$

Assume that $n = k$ such that $(ab)^k = a^k b^k$. This holds when $k \in \mathbb{Z}^+$. Then

$$(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = a^k ab^k b = a^{k+1} b^{k+1}$$

Therefore, $(ab)^n = a^n b^n \, \forall n \in \mathbb{Z}^+, \forall a, b \in G$. ■
($\Leftarrow$) Suppose G is a group $\wedge \forall n \in \mathbb{Z}^+, \forall a, b \in G, (ab)^n = a^n b^n$. In particular, for $n = 2$,

$$\begin{aligned} (ab)^2 &= a^2 b^2 \\ (ab)(ab) &= aabb \\ a(ba)b &= aabb \\ ba &= ab \qquad \text{(by LCL and RCL)} \end{aligned}$$

Definition 1.2.6. (Order of an Element) The **order of an element** g in group G, denoted by $|g|$ or $\text{ord}(g)$, is the smallest positive integer n such that $g^n = e$ (in additive notation, this would be $ng = 0$). If no such integer exists, we say that g has **infinite order** (that is, $g^n \neq e, \forall n \in \mathbb{Z}^+$).

Exercise 1.2.7. Find the order of the following elements of a group.

$$\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in \mathrm{GL}(2, \mathbb{R})$$

Solution.

1. $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

   $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2 \Rightarrow$
   $\operatorname{ord}\left(\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\right) = 3$

2. $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^2$

   $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^3$

   Claim: $\forall n \in \mathbb{Z}^+$
   $$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$$
   Proof: Base Case. If $n = 1$,
   $$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$
   Assume that $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}$ is true for $k \geqslant 1$. Therefore,
   $$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ k+1 & 1 \end{bmatrix}$$
   Thus, $\forall n \in \mathbb{Z}^+ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$. The order of $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ is infinite.

Exercise 1.2.8. Complete the order of the following elements.

$$\begin{bmatrix} 2 & 0 & 0 \\ 4 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 2 & 0 & 3 \end{bmatrix} \in M_{2\times 3}(\mathbb{Z}_6)$$

Solution. In additive notation, find least $n \in \mathbb{Z}^+$

1. $n\begin{bmatrix} 2 & 0 & 0 \\ 4 & 0 & 0 \end{bmatrix} = \begin{bmatrix} n2 & 0 & 0 \\ n4 & 0 & 0 \end{bmatrix} = 0_{2\times 3} \in M_{2\times 3}(\mathbb{Z}_6)$. Thus, $n = 3$.
2. $n\begin{bmatrix} 0 & 1 & 0 \\ 2 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 0 & n & 0 \\ n2 & 0 & n3 \end{bmatrix} = 0_{2\times 3}$. Thus, $n = 6$.

1.3 Friday, September 23: Isomorphic Binary Structures and Subgroups

1.3.1 Isomorphic Binary Structures

Definition 1.3.1. (Bijective Functions) Let $f : X \to Y$. We say that

1. f is **one-to-one** (or is an **injection**) iff $(\forall x_1, x_2 \in X)(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$. Notation: $f : X \overset{1-1}{\to} Y$
2. f is **onto** Y (or is a **surjection**) iff $\{f(x) \mid x \in X\} = \operatorname{Ran} f = Y$, that is, $(\forall y \in Y)(\exists x \in X)(f(x) = y)$. Notation: $f :\overset{\text{onto}}{\to} Y$
3. f is **bijection** iff f is one-to-one and onto Y, that is, $(\forall y \in Y)(\exists! x \in X)(f(x) = y)$

Definition 1.3.2. (Isomorphism) Let $\langle S, *\rangle$ and $\langle S', *'\rangle$ be binary algebraic structures. A function $\phi : S \to S'$ is an **isomorphism** of S **with** S' if

1. ϕ is bijective and
2. $\forall x, y \in S, \phi(x * y) = \phi(x) *' \phi(y)$. This is the homomorphism property

Remark 1.3.1. The concept of isomorphism introduces the relation of being isomorphic on a collection S of binary structures. This relation is an equivalence relation, that is,

1. $\forall U \in S, U \cong U$
2. $\forall U, V \in S$ if $U \cong V$, then $V \cong U$
3. $\forall U, V, W \in S$, if $U \cong V$ and $V \cong W$, then $U \cong W$

Definition 1.3.3. (Automorphism) An isomorphism of a group with itself is an automorphism of the group.

Remark 1.3.2. The set of all automorphisms of a group G, denoted by $\operatorname{Aut}(G)$, forms a group under function composition.

Note that if an isomorphism ϕ exists, we say that S and S' are isomorphic binary structures ($S \cong S'$).

Theorem 1.3.1. (Isomorphism) Suppose ϕ is an isomorphism of a group $\langle G, * \rangle$ with $\langle G', *' \rangle$. Then,

1. $\phi(e_G) = e_{G'}$ where e_G is the identity element of G and $e_{G'}$ is the identity element of G'
2. $\phi(g^{-1}) = [\phi(g)]^{-1}, \forall g \in G$
3. If G is abelian, then so is G'

Exercise 1.3.1. Let $\langle G, * \rangle$ be a group and c be a fixed element of G. Show that $\iota : G \to G$ given by $\iota_c(g) = c * g * c^{-1}$ is an automorphism of G (ι_c is called the inner automorphism of G induced by c)

Solution. Show that ι_c is bijective.
First, we show that the function is one-to-one. Let $g_1, g_2 \in G \wedge$ suppose $\iota_c(g_1) = \iota_c(g_2)$. Then

$$\begin{aligned} c * g_1 * c^{-1} &= c * g_2 * c^{-1} \\ g_1 &= g_2 \qquad \text{LCL and RCL} \end{aligned}$$

Then, we show that it is onto. Let $g' \in G$. Then,

$$\begin{aligned} \iota_c\left(c^{-1} * g' * c\right) &= c * \left(c^{-1} * g' * c\right) * c^{-1} \\ &= \left(c * c^{-1}\right) * g' * \left(c * c^{-1}\right) \\ &= g' \end{aligned}$$

We show the homomorphism property. Let $g_1, g_2 \in G$.

$$\begin{aligned} \iota_c(g_1 * g_2) &= c * (g_1 * g_2) * c^{-1} \\ &= c * (g_1 * e * g_2) * c^{-1} \\ &= c * \left(g_1 * \left(c^{-1} * c\right) * g_2\right) * c^{-1} \\ &= \left(c * g_1 * c^{-1}\right) * \left(c * g_2 * c^{-1}\right) \\ &= \iota_c(g_1) * \iota_c(g_2) \end{aligned}$$

Therefore, ι is an automorphism.

Exercise 1.3.2. Show that the conjugation mapping $\phi : \mathbb{C}^* \to \mathbb{C}^*$ where $\phi(z) = \bar{z}$ is an automorphism of $\mathbb{C}^*$ (for $z \in \mathbb{C}^*, \bar{z} = a - bi$, where $z = a + bi$)

Solution. Let $x = a + bi, y = c + di \in \mathbb{C}^*$. We show the homomorphism property.

$$\phi(x \cdot y) = \phi(ac - bd + (bc + ad)i) = (ac - bd) - (bc + ad)i$$

and

$$\begin{aligned}\phi(x)\cdot\phi(y) = (a-bi)\cdot(c-di) &= (ac-bd)+(-bc-ad)i\\ &= (ac-bd)-(bc+ad)i\end{aligned}$$

Next, we show that ϕ is both one-to-one and onto. For one-to-one, suppose $\phi(a+bi)=\phi(c+di)$. Then,

$$a-bi = c-di \Rightarrow a=c \wedge b=d$$

Therefore,

$$a+bi=c+di$$

To show onto, let $a+bi\in\mathbb{C}^*$ ($a,b\in R$ not both zero). Then,

$$\phi(a-bi)=a-(-b)i=a+bi$$

Exercise 1.3.3. Let $S=\mathbb{R}\backslash\{-1\}$

1. Verify that $*$ defined by $a*b=a+b+ab, \forall a,b\in S$ is a binary operation
2. Show that $\langle S,*\rangle$ is an abelian group
3. Prove that $S\cong\mathbb{R}^*$

Solution.

1. Closure: Let $a,b\in S$. Note that $a*b=a+b+ab\in\mathbb{R}$ We will show that $a*b\neq -1$. Suppose, by contradiction, that $a*b=a+b+ab=-1$. Then,

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

This is a contradiction since $b\neq -1$. Therefore, $a*b\neq -1$. So $a*b\in\mathbb{R}/\{-1\}=S$.
Well-defined: Let $a,b,c,d\in S$. Suppose $a=c\wedge b=d$. Then,

$$a*b=a+b+ab=c+d+cd=c*d$$

2. $*$ is commutative. Let $a,b\in S=\mathbb{R}\backslash\{-1\}$.

$$a*b=a+b+ab=b+a+ba=b*a$$

(G1) $*$ is associative: Let $a,b,c\in S$.

$$\begin{aligned}(a*b)*c &= (a+b+ab)*c\\ &= (a+b+ab)+c+(a+b+ab)c\end{aligned}$$

$$\begin{aligned} &= a+b+ab+c+ac+bc+abc \\ a*(b*c) &= a*(b+c+bc) \\ &= a+(b+c+bc)+a(b+c+bc) \\ &= a+b+c+bc+ab+ac+abc \\ &= a+b+ab+c+ac+bc+abc \end{aligned}$$

(G2) Pre-proof: Find e such that $a*e=a, \forall a \in S$.

$$a = a*e = a+e+ae = a+(1+a)e \Rightarrow e=0$$

$0 \in S = \mathbb{R}\backslash\{-1\}, \forall a \in S$.

$$0*a = a*0 = a+0+0 = a$$

So, we take $e=0$.

(G3) Inverse: Pre-proof: Let $a \in S$. Find b such that

$$0 = a*b = a+b+ab = b(1+a)+a \Rightarrow \frac{-a}{1+a} = b$$

Proof. $\forall a \in S$

$$\begin{aligned} \frac{-a}{1+a}*a = a*\frac{-a}{1+a} &= a+\frac{-a}{1+a}+\frac{a(-a)}{1+a} \\ &= \frac{a(1+a)-a-a^2}{1+a} \\ &= \frac{a+a^2-a-a^2}{1+a} = 0 \end{aligned}$$

Show that $\frac{-a}{1+a} \in S = \mathbb{R}\backslash\{-1\}$.

$$\frac{-a}{1+a} \in \mathbb{R} \quad (-a \in S, 1+a \neq 0)$$

We show $\frac{-a}{1+a} \neq -1$. By contradiction, suppose $\frac{-a}{1+a} = -1$. Then

$$\begin{aligned} \frac{-a}{1+a} &= -1 \\ -a &= -(1+a) \\ -a &= -1-a \\ 0 &\neq -1 \text{ (a contradiction)} \end{aligned}$$

3. If $\phi : \mathbb{R}^* \to S$ is an isomorphism, then $\phi(1) = 0$ $(e_s = 0 \wedge e_{\mathbb{R}^*} = 1)$. We define $\phi : \mathbb{R}^* \to S$ which has a

map $x \mapsto x - 1$.
$\phi(x) = x - 1 \neq -1$ since $x \neq 0$. So $\phi(x) \in S$. ϕ is well-defined for $x = y \in \mathbb{R}^*$, $\phi(x) = x - 1 = y - 1 = \phi(y)$.

We show that ϕ is one-to-one: $\forall x, y \in \mathbb{R}^*$, suppose $\phi(x) = \phi(y)$. Then, $x - 1 = y - 1 \Leftrightarrow x = y$.

We show that ϕ is onto: Let $y \in S = \mathbb{R}\backslash\{-1\}$. Then,

$$\phi(\underbrace{y+1}_{\in\mathbb{R}^*}) = y + 1 - 1 = y$$

To show homomorphism property, let $x, y \in \mathbb{R}^*$. Then

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

and

$$\begin{aligned}\phi(x) * \phi(y) &= (x-1) * (y-1) = x - 1 + y - 1 + (x-1)(y-1) \\ &= x + y - 2 + xy - x - y + 1 = xy - 1 = \phi(xy)\end{aligned}$$

Exercise 1.3.4. Show: $\langle 2\mathbb{Z}, +\rangle \ncong \langle 2\mathbb{Z}, \cdot\rangle$

Proof. Note that $\langle 2\mathbb{Z}, +\rangle$ is an abelian group while $\langle 2\mathbb{Z}, \cdot\rangle$ is only a semigroup. Thus, $\langle 2\mathbb{Z}, \cdot\rangle$ does not have an identity element while $\langle 2\mathbb{Z}, +\rangle$ has. Therefore, $\langle 2\mathbb{Z}, +\rangle$. ■

1.3.2 Subgroup

A goal of (finite) group theory is to enumerate all finite groups of order n (up to isomorphism). Note that there is only group (up to isomorphism) of orders 1, 2, and 3. On the other hand, there are two groups (up to isomorphism) of order four.

Definition 1.3.4. Let $\langle G, *\rangle$ be a group and $\varnothing \neq H \subseteq G$. If $\langle H, *\rangle$ is also a group, we say that H is a subgroup of G. Notation: $H \leqslant G$.

Theorem 1.3.2. (3-step Subgroup Test) Let G be a group and $H \subseteq G$. Then $H \leqslant G$ iff

1. $e \in H$ (e identity element of G)
2. $\forall h_1, h_2 \in H, h_1h_2 \in H$
3. $\forall h \in H, h^{-1} \in H$

Theorem 1.3.3. (2-step Subgroup Test) Let G be a group and $H \subseteq G$. Then $H \leqslant G$ iff

1. $H \neq \varnothing$, and
2. $\forall a, b \in H, ab^{-1} \in H$

Exercise 1.3.5. Suppose $G = \{e, y, u, v, w, x, y, z\}$ is the group defined by the table below.

$*$	e	t	u	v	w	x	y	z
e	e	t	u	v	w	x	y	z
t	t	e	v	u	y	z	w	x
u	u	v	e	t	z	y	x	w
u	v	u	t	e	x	w	z	y
w	w	y	x	t	z	v	e	u
x	x	z	w	y	u	e	v	t
y	y	w	z	x	e	u	t	v
z	z	x	y	w	v	t	u	e

Is G an abelian group? Compute $C(a) = \{g \in G \mid ag = ga\}$ (centralizer of a in G), for every $a \in G$ and use this to find $Z(G) = \bigcap_{a \in G} C(a)$ (center of G).

Exercise 1.3.6. Let G be an abelian group with identity e. Show that the following are subgroups of G.

(a) $H_1 = \left\{x^2 \mid x \in G\right\}$
(b) $H_2 = \left\{x \in G \mid x^3 = e\right\}$

Proof. Using 3-step subgroup test.

- Let e be the identity element of G. Then $e = e^2 \in H_1$
- Let $x^2, y^2 \in H_1$ where $x, y \in G$. Then,

$$x^2 y^2 = (xy)^2 \quad (H_1 \subseteq G \text{ is abelian})$$

  Since $xy \in G$ (G is a group), $x^2y^2 \in H_1$.
- Let $x^2 \in H_1$. Since $x \in G, x^{-1} \in G$ (G is a group). Note that $(x^2)^{-1} = \left(x^{-1}\right)^2 \in H_1$.

Therefore, $H_1 \leqslant G$. ∎

Exercise 1.3.7. Suppose ϕ is an isomorphism of a group $\langle G, * \rangle$ with $\langle G', *' \rangle$.

1. Show that if G is abelian, then so is G'
2. Suppose $H \leqslant G$. Show that $\phi(H) = \{\phi(h) \mid h \in H\} \leqslant G'$

Solution.

(a) Let $x', y' \in G'$. Show $x' * y' = y' * x'$. Since ϕ is onto, $\exists x, y \in G$ such that $\phi(x) = x' \wedge \phi(y) = y'$

$$\begin{aligned} x' *' y' &= \phi(x) *' \phi(y) \\ &= \phi(x * y) \quad (\phi \text{ is isomorphism}) \\ &= \phi(y * x) \quad (G \text{ is abelian}) \\ &= \phi(y) *' \phi(x) \quad (\phi \text{ is isomorphism}) \\ &= y' * x' \end{aligned}$$

(b) Note that $\phi \subseteq G'$. Using 2-step subgroup test,

- Let e' be the identity element of G'. We know that $\phi(e) = e'$, where e is the identity element of G. Since $H \leqslant G, e \in H$. Hence, $e' = \phi(e) \in \phi(H)$
- Let $\phi(x), \phi(y) \in \phi(H)$ with $x, y \in H \leqslant G$. We show that $\phi(x) *' (\phi(y))^{-1} \in \phi(H)$

$$\begin{aligned} \phi(x) *' (\phi(y))^{-1} &= \phi(x) *' \phi(y^{-1}) \\ &= \phi(x * y^{-1}) \quad (\phi \text{ is an isomorphism }) \end{aligned}$$

Therefore, $\phi(x * y^{-1}) \in \phi(H)$

1.4 Friday, September 30: Cyclic Groups

We recall the definition of the order of an element g in group G.

Theorem 1.4.1. Let G be a group, $a \in G$ and $i \neq j$, with $i, j \in \mathbb{Z}$. If $a^i = a^j$, then a has finite order.

Remark 1.4.1. Let G be a group, $a \in G$ and $i \neq j$, with $i, j \in \mathbb{Z}$. If a has infinite order, then $a^i \neq a^j$ (that is, the elements a^k where $k \in \mathbb{Z}$ are all distinct).

Theorem 1.4.2. Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G, and is the smallest subgroup of G that contains a.

Definition 1.4.1. (Cyclic Subgroup) Let G be a group and $a \in G$. The subgroup $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is called the cyclic subgroup of G generated by a.

Remark 1.4.2. Let G be a group and $a \in G$.

1. $\langle a \rangle = \langle a^{-1} \rangle$

2. If G is an infinite group, $\langle a \rangle$, need not be infinite
3. Let $a, b, \in G$. If $a \in \langle b \rangle$, then $\langle a \rangle \subseteq \langle b \rangle$
4. The subgroup $\langle a \rangle$ is abelian

Definition 1.4.2. (Cyclic Group) A group G is called a cyclic group if $\exists a \in G$ such that $G = \langle a \rangle$. The element a is said to generate G or a is a generator of G.

Remark 1.4.3. Let $G = \langle a \rangle$ where $a \in G$.

- G is an abelian group
- a is of infinite order $\Rightarrow$ distinct powers of a are distinct elements and $G \cong \mathbb{Z}$
- $|a| = n \Rightarrow G = \left\{e, a, \dots, a^{n-1}\right\}, a^i = a^j$ if and only if $i \equiv j \pmod{n}$ and $G \cong \mathbb{Z}_n$
- every subgroup of G is cyclic

Exercise 1.4.1. Suppose $G = \{e, t, u, v, w, x, y, z\}$ is the group defined by the table below.

$*$	e	t	u	v	w	x	y	z
e	e	t	u	v	w	x	y	z
t	t	e	v	u	y	z	w	x
u	u	v	e	t	z	y	x	w
v	v	u	t	e	x	w	z	y
w	w	y	x	z	t	v	e	u
x	x	z	w	y	u	e	v	t
y	y	w	z	x	e	u	t	v
z	z	x	y	w	v	t	u	e

Find the elements of $\langle x \rangle$ and $\langle y \rangle$

Solution. We have the following

$$\langle x \rangle = \{e, x\}$$

and

$$\langle y \rangle = \{e, y, t, w\}$$

Exercise 1.4.2. Determine whether the following are cyclic groups

(a) $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$
(b) $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$

Solution.

(a) We will see what element generates the group. We have

$$\langle 1\rangle = \{1\}$$

$$\langle 3\rangle = \{1, 3, 9, 7\}$$

Since there is a generator. Then it is a cyclic group. Furthermore, this is also isomorphic to $\mathbb{Z}_4$

(b) Similarly,

$$\langle 1\rangle = \{1\}$$
$$\langle 3\rangle = \{1, 3\}$$
$$\langle 5\rangle = \{1, 5\}$$
$$\langle 7\rangle = \{1, 7\}$$

Since there is no generator, then this is not cyclic group. However, this group is isomorphic to V_4 (Klein-4 group)

Theorem 1.4.3. Let G be a group and $a \in G$. Suppose a has finite order n. Then,

i. $\langle a\rangle = \left\{e, a, a^2, a^3, \ldots, a^{n-1}\right\}$

ii. For $i, j \in \mathbb{Z}$, $a^i = a^j$ if and only if $i \equiv j \pmod{n}$

Remark 1.4.4. Let G be a group and $a \in G$.

1. Let $\langle a\rangle$ be a finite cyclic subgroup of G. Then $|a| = |\langle a\rangle|$
2. Suppose $|a| = n$ for some $n \in \mathbb{Z}^+$, and $k \in \mathbb{Z}$. Then $a^k = e$ if and only if $n \mid k$
3. If a is of infinite order, then

$$\langle a\rangle = \left\{\ldots, a^{-2}, a^{-1}, e, a^1, a^2, \ldots\right\}$$

Theorem 1.4.4. Every subgoup of a cyclic group is cyclic.

Theorem 1.4.5. Let $G = \langle a\rangle$ with $|a| = n, k \in \mathbb{Z}^+$ and $d = \gcd(n, k)$. Then,

1. $\langle a^k\rangle = \langle a^d\rangle$ and
2. $\left|a^k\right| = \dfrac{n}{d}$

Corollary 1.4.1. Let $G = \langle a\rangle$ with $|a| = n$ and $m \in \mathbb{Z}^+$. Then a^m is a generator of G if and only if $\gcd(n, m) = 1$

Corollary 1.4.2. Let $G = \langle a\rangle$ with $|a| = n$. Then for every positive divisor d of n, $\exists! H \leqslant G$ with $|H| = d$.

Remark 1.4.5. The distinct subgroups of $G = \langle a \rangle$ where $|a| = n$ are those subgroups $\langle a^d \rangle$ where d is a positive divisor of n.

Exercise 1.4.3. Sketch the subgroup lattice of $\mathbb{Z}_{18}$. Find all generators of each distinct subgroups.

Solution. Recall from Remark 14 that the distinct subgroups is generated by $\langle a^d \rangle$ where d is a positive divisor of n. Note that the positive divisors of 18 are 1, 2, 3, 6, 9, 18. Then, we have the following
Subgroup of order 18: (We'll use Corollary 2)

$$\mathbb{Z}_{18} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle$$

Subgorup of order 9: (From Corollary 2, $\gcd(9, k) = 1$)

$$\left\langle \frac{18}{9} \cdot 1 \right\rangle = \langle 2 \rangle = \langle 4 \rangle = \langle 8 \rangle = \langle 10 \rangle = \langle 14 \rangle = \langle 16 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$$

Subgroup of order 6: ($\gcd(6, k) = 1$)

$$\left\langle \frac{18}{6} \cdot 1 \right\rangle = \langle 3 \rangle = \langle 15 \rangle = \{0, 3, 6, 9, 12, 15\}$$

Subgroup of order 3: ($\gcd(3, k) = 1$)

$$\left\langle \frac{18}{3} \cdot 1 \right\rangle = \langle 6 \rangle = \langle 12 \rangle = \{0, 6, 12\}$$

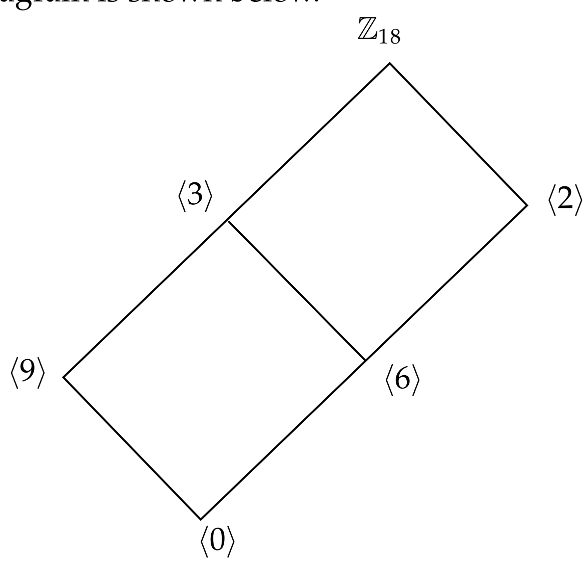
Subgorup of order 2: ($\gcd(2, k) = 1$)

$$\left\langle \frac{18}{2} \cdot 1 \right\rangle = \langle 9 \rangle$$

Subgroup of order 1:

$$\langle 0 \rangle = \{0\}$$

The lattice diagram is shown below.



Exercise 1.4.4. If a is an element of a group where $\left|a^4\right| = 12$, what are the possibilities for $|a|$?

Solution. Since $\left|a^4\right| = 12$, then we have $\left(a^4\right)^{12} = a^{48} = e$. Thus, we have $|a| \mid 48$. So $48 = |a| \cdot k, \exists k \in \mathbb{Z}^+$. Since $\langle a^4 \rangle \leqslant \langle a \rangle$, $\left|\langle a^4 \rangle\right| \mid \langle a \rangle = |a|$, so $12 \mid |a|$ Therefore, $|a| = 12 \cdot m, \exists m \in \mathbb{Z}^+$. This gives us $48 = |a| \cdot k = 12 \cdot mk \Rightarrow mk = 4$ So the values of m could be $1, 2, 4$. Therefore, we have $|a| = 12, 24, 48$.

Case 1: If $|a| = 12$, then $\left|a^4\right| = \dfrac{12}{\gcd(12,4)} = \dfrac{12}{4} = 3$

Case 2: If $|a| = 24$, then $\left|a^4\right| = \dfrac{24}{\gcd(24,4)} = \dfrac{24}{4} = 6$

Case 3: If $|a| = 48$, then $\left|a^4\right| = \dfrac{48}{\gcd(48,4)} = \dfrac{48}{4} = 12$

The first two cases are contradictions. Therefore the order of $|a|$ is 48.

Exercise 1.4.5. Let $G = \langle a \rangle$, with $|a| = 72$. Find

(a) $\left|a^{188}\right|$, and

(b) all generators of the subgroup of G of order 12

Solution.

(a) Note that $a^{188} = a^{2\cdot 72+44} = \left(a^{72}\right)^2 \cdot a^{44} = a^{44}$

$$\left|a^{188}\right| = \left|a^{44}\right| = \frac{72}{\gcd(72,44)} = \frac{72}{4} = 18$$

(b) We need to find m such that $\gcd(m,12) = 1$ since $12 = \left|a^{\frac{72}{12}}\right| = \left|\left(a^6\right)^m\right|$ where $\gcd(m,12) = 1$. Therefore, $m = 1, 5, 7, 11$. Thus, the generators of a subgroup of order 12 are $a^6, a^{30}, a^{42}, a^{66}$.

Exercise 1.4.6. Suppose a, b are elements of a finite group. Prove:

- If $|a| = \left|a^2\right|$, then $|a|$ is odd
- $|a| = \left|b^{-1}ab\right|$

Solution.

- Note that $\dfrac{|a|}{\gcd(|a|,2)} = \left|a^2\right| = |a|$ (group is finite). Therefore, $\gcd(|a|,2) = 1$. This implies that $|a|$ is odd.
- Note that $\left|b^{-1}ab\right| < \infty$. Suppose $|a| = m$ and $\left|b^{-1}ab\right| = n$ where $m, n \in \mathbb{Z}^+$. This implies that

$$\begin{aligned} e = \left(b^{-1}ab\right)^n &= \left(b^{-1}ab\right)\left(b^{-1}ab\right)\ldots\left(b^{-1}ab\right) \\ &= b^{-1}a^n b \end{aligned}$$

Note that $e = b \cdot e \cdot b^{-1}$. Thus, we can use this to generate

$$e = b \cdot e \cdot b^{-1} = b\big(b^{-1}a^n b\big)b^{-1} = a^n$$

Therefore, $m \mid n$.

Now, $e = a^m \Rightarrow e = b^{-1}eb = b^{-1}(a^m)b = \big(b^{-1}ab\big)^m$. This implies that $n \mid m$ where $m, n \in \mathbb{Z}^+$.

Since $m \mid n$ and $n \mid m$, we get $m = n$.

Exercise 1.4.7. Prove that if a group G has no proper nontrivial subgroups, then G is a cyclic group.

Proof. Let $g \in G$ with $g \neq e$. Then $\langle g \rangle \leqslant G$ and $\langle g \rangle \neq \{e\}$. Since G has no proper nontrivial subgroup, $\langle g \rangle = G$. Hence, G is cyclic. ■

Exercise 1.4.8. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the torsion subgroup of G.

Proof. Let $T = \{a \in G \mid a^n = e \exists n \in \mathbb{Z}^+\}$. We will show that $T \leqslant G$ using 3-step subgroup test.

- We know that $e^n = e, \forall n \in \mathbb{Z}^+ \Rightarrow e \in T$.
- Let $a, b \in T$. Then $a^{n_1} e \exists n_1 \in \mathbb{Z}^+$ and $b^{n_2} = e \exists n_2 \in \mathbb{Z}^+$. We have,

  $$(ab)^{n_1 n_2} = a^{n_1 n_2} b^{n_1 n_2} = (a^{n_1})^{n_2} \cdot (b^{n_2})^{n_1} = e^{n_2} \cdot e^{n_1} = e \text{ and } n_1 n_2 \in \mathbb{Z}^+$$

- Let $a \in T$. Then $a^n = e \exists n \in \mathbb{Z}^+$. Therefore, $\big(a^{-1}\big)^n = (a^n)^{-1} = e^{-1} = e$

1.5 Friday, October 7: Cosets and Theorem of Lagrange

1.5.1 Cosets

Theorem 1.5.1. Let G be a group and suppose $H \leqslant G$. Let the relation $\sim_L$ be defined on G by $a \sim_L b \Leftrightarrow a^{-1}b \in H$ and let the relation $\sim_R$ be defined on G by $a \sim_R b \Leftrightarrow ab^{-1} \in H$. Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Definition 1.5.1. Let G be a gorup and suppose $H \leqslant G$. The subset

$$Ha = \{ha \mid h \in H\}$$

of G is the **right coset of** H **containing** a whit the set

$$aH = \{ah \mid h \in H\}$$

of G is the **left coset of** H **containing** a. In aH or Ha, a is called a **coset representative**. Any element of aH or Ha can be made a representative of the coset.

Exercise 1.5.1. Let $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ (**quaternion group**) with identity element 1 and noncummitative multiplication given by

$$(-1)^2 = 1, i^2 = j^2 = k^2 = -1$$

$$ij = -ji - k, jk = -kj = i, ki = -ik = j$$

$$-x = (-1)x = x(-1) \forall x \in Q_8$$

- Find the center of this group
- Let $H = \{1, j, -1, -j\}$. Find the left and right cosets of subgroup H in Q_8

Solution.
- Note that we are looking for values in Q_8 that commutes with every element. Thus, $z(Q_8) = \{z \in Q_8 \mid xz = zx \, \forall x \in Q_8\} = \{1, -1\}$.
- The left cosets of subgroup H in Q_8 are

$$H = (1)H = jH = (-1)H = (-j)H$$

and

$$kH = \{k, -i, -k, i\} = (-i)H = (-k)H = iH$$

So we have $H \cup kH = Q_8$.
- The right cosets are

$$H = H(1) = Hj = H(-1) = H(-j)$$

and

$$Hi = \{i, -k, -i, k\} = H(-k) = H(-i) = Hk$$

So we have, $H \cup Hi = Q_8$.

Exercise 1.5.2. Consider $\langle U(\mathbb{Z}_{16}), \cdot_{16} \rangle$. Find the left cosets of the subgroups $\langle 7 \rangle$ and $\langle 11 \rangle$ in $U(\mathbb{Z}_{16})$

Solution. Note that $U(Z_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\}$.

- For $\langle 7 \rangle$, we have

$$\begin{aligned} \langle 7 \rangle &= \{1, 7\} = 1\langle 7 \rangle = 7\langle 7 \rangle \\ 3\langle 7 \rangle &= \{3, 5\} = 5\langle 7 \rangle \\ 9\langle 7 \rangle &= \{9, 15\} = 15\langle 7 \rangle \\ 11\langle 7 \rangle &= \{11, 13\} = 13\langle 7 \rangle \end{aligned}$$

  So we have 4 left cosets of $\langle 7 \rangle$. Note that the right cosets are the same since the group is abelian.
- For $\langle 11 \rangle$

$$\begin{aligned} \langle 11 \rangle &= \{1, 11, 9, 3\} \\ 5\langle 11 \rangle &= \{5, 7, 13, 15\} \end{aligned}$$

  So we have 2 left cosets of $\langle 11 \rangle$.

Remark 1.5.1. Let G be a group and $H \leqslant G$.

1. If $e \in G$ is the identity, $eH = H = He$
2. For any $a \in G$, $a \in aH$
3. Let $a, b \in G$

   a. $aH = bH \Leftrightarrow a^{-1}b \in H$
   b. $Ha = Hb \Leftrightarrow ab^{-1} \in H$
4. Let $a \in G$

   (a) $aH = H \Leftrightarrow a \in H$
   (b) $Ha = H \Leftrightarrow a \in H$
5. If G is abelian, then $aH = Ha$. The converse is not necessarily true. That is, there exist subgroups H for which $aH = Ha$, for all $a \in G$, even if G is not abelian.

1.5.2 Theorem of Lagrange

Theorem 1.5.2. Let G be a group and suppose $H \leqslant G$. Then for any $a \in G, |H| = |aH| = |Ha|$.

Theorem 1.5.3. (Lagrange) Let G be a finite group and suppose $H \leqslant G$. Then $|H|$ divides $|G|$.

Corollary 1.5.1. Let G be a finite group with $|G| = n$. Then, for any $a \in G$, $|a|$ divides n and $a^n = e$.

Exercise 1.5.3. Consider the dihedral group D_{10} where $a^{10} = b^2 = (ab)^2 = e$. Find the order of the element $ba^6b^{-1}a^{22}b^6$

Solution. Note that $|D_{10}| = 2 \cdot 10 = 20$ and $D_{10} = \langle a \rangle \cup \left\{a^k b \mid k = 0, 1, \ldots, 9\right\}$. Moreover, $ba^k = a^{10-k}b, k \in \mathbb{Z}^+$. Note that

$$ba^6b^{-1}a^{22}b^6 = a^4bba^2 = a^4a^2 = a^6$$

Therefore, $\left|ba^6b^{-1}a^{22}b^6\right| = \left|a^6\right| = \dfrac{10}{\gcd(10,6)} = \dfrac{10}{2} = 5$

Corollary 1.5.2. Every group of prime order is cyclic.

Definition 1.5.2. The number of distinct left cosets of H in G is called the **index of** H **in** G and is denoted by $[G : H]$.

Remark 1.5.2. A subgroup with index 1 is the whole group.

Corollary 1.5.3. If G is a finite group and $K \leqslant H \leqslant G$, then $[G : K] = [G : H] \cdot [H : K]$

Theorem 1.5.4. Let $H \leqslant G$. Then the number of left cosets of H is equal to the number of right cosets of H in G.

Exercise 1.5.4. If H and K are subgroups of G and $g \in G$, show that $g(H \cap K) = gH \cap gK$

Proof.
$(\subseteq)$ Let $gx \in g(H \cap K)$.

$$\begin{aligned}
&\Rightarrow x \in H \cap K \\
&\Rightarrow x \in H \wedge x \in K \\
&\Rightarrow gx \in gH \wedge gx \in gK \\
&\Rightarrow gx \in gH \cap gK
\end{aligned}$$

$(\supseteq)$ Let $gy \in gH \cap gK$.

$$\begin{aligned}
&\Rightarrow gy \in gH \wedge gy \in gK \\
&\Rightarrow y \in H \wedge y \in K \\
&\Rightarrow y \in H \cap K \\
&\Rightarrow gy \in g(G \cap K)
\end{aligned}$$

Exercise 1.5.5. Suppose G is a finite group with $|G| = n$ and $\gcd(k, n) = 1$. If $g \in G$ and $g^k = e$, show that $g = e$.

Proof. Note that $|g| \mid n = |G|$. Since $g^k = e$, $|g| \mid k$. This means that $|g|$ is a common divisor of $n \wedge k$. Therefore, $|g| = 1$ since $\gcd(k, n) = 1$. Therefore $g = e$. ■

Exercise 1.5.6. Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 40$ and $|G| = 600$, what are the possible orders of H?

Solution. By the theorem of Lagrange, we have $|K| \mid |H|$ and $|H| \mid |G|$. This implies that $40 \mid |H|$ and $|H| \mid 600$. Thus, there exists $k_1, k_2 \in \mathbb{Z}^+$ such that $|H| = 40k_1$ and $600 = |H|k_2$. Therefore, $600 = |H|k_2 = 40k_1k_2 \Rightarrow k_1k_2 = 15$.

Case 1: If $k_1 = 1$ and $k_2 = 15$, $|H| = 40k_1 = 40 \cdot 1 = 40 = |K|$. This is not possible since K is a proper subgroup of H.

Case 2: If $k_1 = 15$ and $k_2 = 1$, $|H| = 40k_1 = 40 \cdot 15 = 400 = |G|$. This is not possible since $H < G$.

Case 3: If $k_1 = 5$ and $k_2 = 3$, $|H| = 40k_1 = 40 \cdot 3 = 120$.

Case 4: If $k_1 = 3$ and $k_2 = 5$, $|H| = 40k_1 = 40 \cdot 5 = 200$.

Therefore, $|H| = 120$ or 200.

Exercise 1.5.7. Determine up to isomorphism all groups of order four.

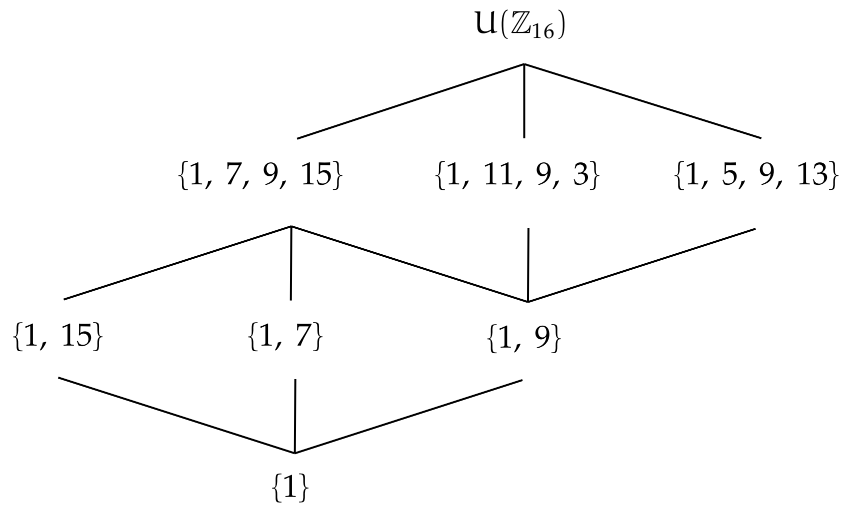
Solution. Let G be a group with $|G| = 4$.

Case 1: G is cyclic: $G = \langle a \rangle = \{e, a, a^2, a^3\} \cong \mathbb{Z}_4, \exists a \in G$.

Case 2: G is not cyclic. Therefore G has no elements of order 4. Thus, $\forall x \in G, x \neq e, |x| \mid |G| = 4$, but $|x| \neq 4$. So we only have $|x| = 2$. Remember that this is isomorphic to V_4 (Klein-4). Up to isomorphism, there are only two groups of order 4.

Exercise 1.5.8. Sketch the lattice diagram of $U(\mathbb{Z}_{16})$

Solution. Since $|U(\mathbb{Z}_{16})| = 8$. If $H \leqslant U(\mathbb{Z}_{16})$, then $|H| = 1, 2, 4$, or 8 by Lagrange theorem. We will see the subgroups generated by each element. Note that $\langle 1 \rangle = \{1\}$, $\langle 7 \rangle = \{1, 7\}$, $\langle 11 \rangle = \{1, 11, 9, 3\} = \langle 3 \rangle \cong \mathbb{Z}_4$, $\langle 5 \rangle = \{1, 5, 9, 13\} = \langle 13 \rangle \cong \mathbb{Z}_4$, $\langle 15 \rangle = \{1, 15\}$, $\langle 9 \rangle = \{1, 9\}$. The lattice diagram is shown below,



1.6 Friday, October 14: Group of Permutations, Orbits, Cycles and the Alternating Groups

1.6.1 Group of Permutations

Definition 1.6.1. Let A be a nonempty set. A **permutation** of the set A is a bijection from A to A.

Remark 1.6.1.

1. Let $|A| = n$. There are $n!$ permutations of the set A.
2. If σ and τ arre permutations of A, then $\sigma \circ \tau$ is also a permutation of A.
3. It is known that composition of functions is associative.
4. The identity map $i : A \to A$ such that $i(x) = x, \forall x \in A$ is a permutation.
5. If σ is a permutation of A, then σ^{-1} is also a perrmutation of A.

Theorem 1.6.1. Let A be a nonempty set. Then the set S_A of all permutations of A is a group under composition.

Remark 1.6.2.

1. Consider the group $\langle S_A, \circ \rangle$ and let $\sigma, \tau \in S_A$. We will use notation $\sigma\tau$ for $\sigma \circ \tau$.
2. The action of $\sigma\tau$ on A is read in right-to-left order, that is, first

apply τ and then σ. Therefore, we have $(\sigma\tau)(a) = (\sigma(\tau(a)))$.
3. If sets A and B have the same cardinality, then $S_A \cong S_B$.

Exercise 1.6.1. Show that if sets A and B have the same cardinality, then $S_A \cong S_B$.

Proof. Since $|A| = |B|$, there should exist a function from A to B where the function is bijective. In other words, $\exists f : A \to B$.

$$\begin{aligned} \phi : S_A &\to S_B \\ \sigma &\mapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

Note that $f \circ \sigma \circ f^{-1} : B \to B$ and f, f^{-1}, σ are bijective maps. It is known that composition of bijective maps gives a bijective map. so $f \circ \sigma \circ f^{-1} \in S_B$.
We will show that the function is one-to-one. Let $\sigma_1, \sigma_2 \in S_A$ and suppose $\phi(\sigma_1) = \phi(\sigma_2)$. We have

$$\begin{aligned} f \circ \sigma_1 \circ f^{-1} &= f \circ \sigma_2 \circ f^{-1} \\ f^{-1}\left(f \circ \sigma_1 \circ f^{-1}\right) \circ f &= f^{-1}\left(f \circ \sigma_2 \circ f^{-1}\right) \circ f \\ \left(f^{-1} \circ f\right) \circ \sigma_1 \circ \left(f^{-1} \circ f\right) &= \left(f^{-1} \circ f\right) \circ \sigma_2 \circ \left(f^{-1} \circ f\right) \\ id_A \circ \sigma \circ id_A &= id_A \circ \sigma_2 \circ id_A \\ \sigma_1 &= \sigma_2 \end{aligned}$$

We show that the function is onto. Let $\sigma' \in S_B$. Then $f^{-1} \circ \sigma' \circ f \in S_A$. Observe that

$$\begin{aligned} \phi(f^{-1} \circ \sigma' \circ f) &= f \circ \left(f^{-1} \circ \sigma' \circ f\right) \circ f^{-1} \\ &= \left(f \circ f^{-1}\right) \circ \sigma' \circ \left(f \circ f^{-1}\right) \\ &= id_B \circ \sigma' \circ id_B \\ &= \sigma' \end{aligned}$$

To show the homomorphism property, we let $\sigma_1, \sigma_2 \in S_A$.

$$\begin{aligned} \phi(\sigma_1 \circ \sigma_2) &= f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1} \\ &= f \circ (\sigma_1 \circ id_A \circ \sigma_2) \circ f^{-1} \\ &= f \circ \left(\sigma_1 \circ \left(f^{-1} \circ f\right) \circ \sigma_2\right) \circ f \\ &= \left(f \circ \sigma_1 \circ f^{-1}\right) \circ \left(f \circ \sigma_2 \circ f^{-1}\right) \\ &= \phi(\sigma_1) \circ \phi(\sigma_2) \end{aligned}$$

Therefore $S_A \cong S_B$. ■

Definition 1.6.2. Let $A = \{1, 2, \ldots, n\}$. The group of all permutations of A is called the **symmetric group of n letters and is denoted by S_n**.

Exercise 1.6.2. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 6 & 3 & 4 & 2 & 1 & 7 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 1 & 7 & 6 & 5 & 9 & 3 & 4 \end{pmatrix} \in S_9$. Find $\alpha\beta$.

Solution.

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 9 & 5 & 2 & 4 & 3 & 7 & 8 & 6 \end{pmatrix} \text{ and } \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 3 & 5 & 1 & 7 & 2 & 8 & 9 \end{pmatrix}$$

Definition 1.6.3. Let A be a nonempty set. A **permutation group of** A is a set of permutations of A that forms a group under composition. A permutation group of A is a subgroup of S_A.

Theorem 1.6.2. (Cayley's Theorem) Every group is isomorphic to a group of permutations.

Exercise 1.6.3. Let $n \in \mathbb{Z}^+$ and $G \leqslant S_n$. If $i \in \{1, 2, \ldots, n\}$, the **stabilizer in G is**

$$\text{stab}_G(i) = \{a \in G \mid a(i) = i\}$$

Show that $\text{stab}_G(i) \leqslant G$

Proof. We will use the 2-step subgroup test.

- By definition of subgroup, the identity map id $\in G \leqslant S_n$ fixes i. In other words, id $(i) = i\, \forall i$. Therefore, id $\in$ stab_G
- Let $\alpha\beta \in$ $\text{stab}_G(i)$. Note that $\beta(i) = i$ and β is bijective, so $\beta^{-1}(i) = i$. We have

$$\left(\alpha\beta^{-1}\right)(i) = \alpha\left(\beta^{-1}(i)\right) = \alpha(i) = i$$

  Therefore, $\alpha\beta^{-1} \in$ $\text{stab}_G(i)$.

Thus, $\text{stab}_G(i) \leqslant G$. ■

Theorem 1.6.3. Let $\sigma \in S_n$. Then the relation $\sim$ on $A = \{1, 2, \ldots, n\}$ defined by $x \sim y$ if and only if $y = \sigma^k(x)$ for some $k \in \mathbb{Z}$ is an equivalence relation on A.

1.6.2 Orbits

Definition 1.6.4. Let $\sigma \in S_n, A = \{1, 2, \dots, n\}$ and $a \in A$. The **orbit of** σ **containing** a **is** $\{\sigma^k(a) \mid k \in \mathbb{Z}\}$.

Definition 1.6.5. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit.

Remark 1.6.3. If $\sigma \in S_n$ is a cyckle, consider the largest orbit $\{a, \sigma(a), \sigma^2(a), \dots, \sigma^{k-1}(a)\}$. We write the permutation σ as

$$(a\ \sigma(a)\ \sigma^2(a)\ \dots \sigma^{k-1}(a)) \text{ or } (a, \sigma(a), \sigma^2(a), \dots, \sigma^{k-1}(a))$$

where $\sigma^k(a) = a$ (a cycle of length k or k-cycle).

Remark 1.6.4. Strictly speaking, cycle notation is ambiguous since for example, $(3\,6\,1)$ might denote a permutation in S_6, in S_7, or in any $S_n, n \geqslant 6$. In context, however, this won't cause any problem because it will always be made clear which S_n is under discussion.

1.6.3 Cycles and Alternating Groups

Definition 1.6.6. (Disjoint Cycles) Two cycles are said to be **disjoint** if they have no number in common, that is, if $\sigma = (a_1\, a_2 \dots a_k), \tau = (b_1\, b_2 \dots b_1) \in S_n$ we have $a_i \neq b_j$ for all i and j.

Theorem 1.6.4. The product of disjoint cycles commute.

Remark 1.6.5. Every permutation $\sigma \in S_n$ can be written as a cycle or as a product of disjoint cycles.

Theorem 1.6.5. Let $\sigma \in S_n$ be written as a product of disjoint cycles. Then the order of σ is the least common multiple of the lengths of its cycles.

Exercise 1.6.4. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 9 & 8 & 6 & 3 & 4 & 2 & 1 & 7 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 1 & 7 & 6 & 5 & 9 & 3 & 4 \end{pmatrix} \in S_9$. Write α and β in cycle notation. Find $\beta\alpha\beta^{-1}$ and $|\beta\alpha\beta^{-1}|$.

Solution. We have $\alpha = (1538)(297)(46)$ and $\beta = (183)(479)(56)$. Note that $\beta^{-1} = (381)(974)(56)$. Therefore

$$\beta\alpha\beta^{-1} = (1386)(249)(57)$$

and

$$\left|\beta\alpha\beta^{-1}\right| = \text{LCM}(4,3,2) = 12$$

Remark 1.6.6. If σ is an m-cycle, then $|\sigma| = m$

Definition 1.6.7. A cycle of length 2 is called a transposition.

Remark 1.6.7.

1. A transposition leaves all elements but two fixed, and maps each of these onto the other.
2. Let $n \geqslant 2$. Every permutation in S_n is a product of transpositions. This implies that any rearrangement of n objects can be achieved by successively interchanging of them.
3. If $\tau_1, \tau_2, \ldots, \tau_m$ are transpositions, then
$$(\tau_1\tau_2 \cdots \tau_n)^{-1} =$$
4. If $\sigma \in S_n$ and $n \geqslant 2$, then
$$\sigma = \tau_1\tau_2 \cdot \tau_m$$

Theorem 1.6.6. No permutation in S_n can be expressed as a product of an even number of transpositions and as a product of an odd number of transpositions.

Definition 1.6.8. A permutation of finite set is **even (odd)** if it is a product of even (odd) number of transpositions.

Exercise 1.6.5. Let $b = (123)(145)$. Write b^{49} in cycle form. Is b^{49} an even permutation?

Solution. Note that $b = (123)(145) = (14523)$. This implies that $|b| = 5$. Then,

$$(b^5)^9 \cdot b^4 = b^4 = b^{-1} = (32541)$$

$b^{49} = b^{-1}$ is an odd length. Therefore, b^{49} is an even permutation. That is, $b^{-1} = (32)(25)(54)(41)$ that has even number of transpositions.

Exercise 1.6.6. If α and β are distinct transpositions, what are the possibilities for $|\alpha\beta|$?

Solution.

Case 1: If $\alpha = (ab), \beta = (cd), a, b, c, d$ are distinct and $\alpha\beta = (ab)(cd)$. So $|\alpha\beta| = \text{lcm}(2, 2) = 2$

Case 2: If $\alpha = (ab), \beta = (bc), a, b, c$ are distinct and $\alpha\beta = (ab)(bc) = (bca)$. So $|\alpha\beta| = 3$.

Exercise 1.6.7. Give a cyclic subgroup of A_8 order 4 and a noncyclic subgroup of A_8 of order 4.

Solution. Let $\alpha = (1234)(78) = (12)(23)(34)(78) \in A_8$. Note that $\langle\alpha\rangle = \{(1), (1234)(78), (13)(24), (4321)(87)\}$.

Next we need to find non-cyclic. So this is isomorphic to Klein-4. This is given by $\{(1), (12)(34), (56)(78), (12)(34)(56)(78)\}$.

Exercise 1.6.8. Find three permutations σ in S_9 such that $\sigma^3 = (157)(283)(469)$.

Solution. Note that $\left|\sigma^3\right| = \text{lcm}(3, 3, 3) = 3$. This implies that $\left(\sigma^3\right)^3 = \sigma^9 = (1)$. From a theorem in the last discussion, we have $|\sigma| \mid 9 \Rightarrow |\sigma| = 1, 3, 9$. Since $\sigma^3 \neq (1), |\sigma| \neq 1, 3$, we have $|\sigma| = 9$. We have

$$\sigma = (124586739)$$
$$\sigma = (142568793)$$
$$\sigma = (139524786)$$

Remark 1.6.8.
1. (1) (identity permutation) is even (we define it to be even for $n = 1$)
2. A cycle of odd length is even and a cycle of even length is odd

Theorem 1.6.7. Let $n \geqslant 2$. Then the number of even permutations in S_n is the same as the number of odd permutations in S_n.

Definition 1.6.9. The set A_n of all even permutations in S_n is called the **alternating group of n letters**. Also, $|A_n| = \dfrac{n!}{2}$

Theorem 1.6.8. $A_n \leqslant S_n$

1.7 Friday, October 21: Direct Product, Subgroups Generated by a Subset, and Finitely Generated Abelian Groups

1.7.1 Direct Product

Definition 1.7.1. Let $\langle G_1, \cdot \rangle$ and $\langle G_2, \cdot \rangle$ be groups. The (external) direct product of G_1 and G_2 is the group $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ with binary operation $*$ defined by

$$(a_1, a_2) * (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot' b_2)$$

for every $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$

Remark 1.7.1.

1. e_G identity element of group G, $e_{G_1 \times G_2} = q(e_{G_1}, e_{G_2}), \forall (g_1, g_2) \in G_1 \times G_2, (g_1, g_2)^{-1} = \left({g_1}^{-1}, \{g_2\}^{-1} \right)$
2. In general, if $G_1, G_2, \ldots, G_n$ are groups, then $\Pi_{i=1}^{n} G_i$ is a group with binary operation $*$ defined by

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots a_n b_n)$$

   for every $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \Pi_{i=1}^{n} G_i$. Moreover, if $G_1, G_2, \ldots, G_n$ are abelian groups, then $\Pi_{i=1}^{n} G_i$ is also abelian
3. If $|G_i| < \infty$, for each $i \in \{1, 2, \ldots, n\}$, then $|\Pi_{i=1}^{n} G_i| = \Pi_{i=1}^{n} |G_i| < \infty$

Recall 1. (Least Common Multiple) Let a, b be nonzero integers and m be a positive integer. Then m is the least common multiple of a and b if m satisfies the following:

1. $a \mid m$ and $b \mid m$, that is m is a multiple of both a and b;
2. $\forall c \in \mathbb{Z}$, if $a \mid c$ and $b \mid c$, then $m \mid c$.

Theorem 1.7.1. Let G_1, G_2 be finite groups. If $(a, b) \in G_1 \times G_2$, then $|(a, b)| = \text{lcm}(|a|, |b|)$

Remark 1.7.2. In general, if $G_1, G_2, \ldots, G_n$ are finite groups and $(g_1, g_2, \ldots, g_n) \in \Pi_{i=1}^{n} G_i$, then $|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$

Example 1. How many elements of order 10 are in $\mathbb{Z}_{25} \times \mathbb{Z}_{100}$?

Solution. Let $(a, b) \in \mathbb{Z}_{25} \times \mathbb{Z}_{100}$ such that $|(a, b)| = \text{lcm}(|a|, |b|) = 10$. Note that the elements of the order of $\mathbb{Z}_{25}$ is $\{1, 5, 25\}$ and the order of elements of $\mathbb{Z}_{100}$ is $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$.

Case 1: $|a| = 1$ and $|b| = 10$
So we have $a = 0$ and $b \in \{10, 30, 70, 90\}$. Therefore, there are 4 elements of $\mathbb{Z}_{25} \times \mathbb{Z}_{100}$ with order 10.

Case 2: $|a| = 5$ and $|b| = 2$
So we have $a \in \{5, 10, 15, 20\}$ and $b = 50$. Therefore, there are 4 elements of $\mathbb{Z}_{25} \times \mathbb{Z}_{100}$ with order 10 for this case.

Case 3: $|a| = 5$ and $|b| = 10$
So we have $a \in \{5, 10, 15, 20\}$ and $b \in \{10, 30, 70, 90\}$. Therefore, there are 16 elements of $\mathbb{Z}_{25} \times \mathbb{Z}_{100}$ with order 10 for this case.

Hence, there are 24 elements of $\mathbb{Z}_{25} \times \mathbb{Z}_{100}$ with order 10.

Exercise 1.7.1. Find $|(9, -i, (62547)(3612))|$ where $(9, -i, (62547)(3612)) \in {\mathbb{Z}_{13}}^* \times U_4 \times S_8$

Solution. For $|9|$, note that $\langle 2 \rangle = \mathbb{Z}_{13}^*$ and $\langle 3 \rangle = \{1, 3, 9\} \Rightarrow |\langle 3 \rangle| = 3$. Thus
$$|9| = \left|3^2\right| = \frac{3}{\gcd(3, 2)} = 3$$
For $-i$, note that $\langle -i \rangle = \{-i, -1, i, 1\}$. So $|-i| = 4$.
For $(62547)(3612)$, this is equal to $(15476)(23)$. Therefore, $|(15476)(23)| = \text{lcm}(5, 2) = 10$.
Therefore,
$$\begin{aligned} |(9, -i, (62547)(3612))| &= \text{lcm}(|9|, |-i|, |(62547)(3612)|) \\ &= \text{lcm}(3, 4, 10) \\ &= 60 \end{aligned}$$

Remark 1.7.3.

1. Let G_1, G_2 be groups. Then $G_1 \times G_2 \cong G_2 \times G_1$
2. Suppose that $\prod_{i=1}^{n} G_i$ is the direct product of groups G_i,
   (a) Observe that direct products $\prod_{i=1}^{n} H_i$ where $H_i \leqslant G_i$, are subgroups of $\prod_{i=1}^{n} G_i$
   (b) The subsets
   $$\overline{G_i} = \{(e_1, \ldots, e_{i-1}, g_i, e_{i+}, \ldots, e_n) \mid g_i \in G_i\}$$
   where $e_i \in G_i$ is the identity element of G_i, are subgroups of $\prod_{i=1}^{n} G_i$. Moreover, it can be shown that $\overline{G_i} \cong G_i$

Recall 2. If $a, b \in \mathbb{Z}^+$, then $\text{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$

Theorem 1.7.2. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$

Corollary 1.7.1. $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} \cong \mathbb{Z}_{m_1 m_2 \cdots m_k}$ if and only if $\gcd(m_i, m_j) = 1$ for $i \neq j$.

1.7.2 Subgroups Generated by a Subset

Recall 3. Let G be a group

1. Suppose $a \in G$. Then $\langle a \rangle$ is the smallest subgroup of G that contains a
2. Let $\{H_i\}_{i \in I}$ be a family of subgroups of G. Then $\bigcap\limits_{i \in I} H_i$ is also a subgroup of G.

Remark 1.7.4. Let G be a group and let $S = \{a_i \in G \mid i \in I\}$, where I is some index set.

1. Then the smallest subgroup of G containing all of the $a_i's$ is the subgroup of $\langle S \rangle$ of G generated by S. In particular, $\langle \{a\} \rangle = \langle a \rangle$, for $a \in G$
2. If $\langle S \rangle = G$, we say that S generates G or G is generated by S. We call S a generating set for G and the elements of S are said to be generators of G. If S is finite, then G is said to be finitely generated.
3. Observe that the subgroup $\langle S \rangle$ is the set of all possible products, in every order, of elements of S and their inverses. That is

$$\langle S \rangle = \left\{ {a_{i_1}}^{m_1}, {a_{i_2}}^{m_2} \cdots {a_{i_n}}^{m_n} \mid n = 1, 2, \ldots, a_{ij} \in S, m_j \in \mathbb{Z} \right\}$$

where a_{ij}s are not necessarily distinct. In particular, $\langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$

Remark 1.7.5. If $G_1, G_2, \ldots, G_n$ are cyclic groups, then $\Pi_{i=1}^n G_i$ is finitely generated with generating set

$$\{(a_1, e_2, \ldots, e_n), (e_1, a_2, e_3, \ldots, e_n), \ldots, (e_1, e_2, e_3, \ldots, e_{n-1}, a_n)\}$$

where $e_i \in G_i$ is the identity element of G_i and $G_i = \langle a_i \rangle$

1.7.3 Finitely Generated Abelian Groups

Theorem 1.7.3. (Fundamental Theorem of Finitely Generated Abelian Group (FTFGAG) (Kronecker, 1858)) Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{p_n}^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

where p_i are primes, not necessarily distinct, and $r_i \in \mathbb{Z}^+$. The direct product is unique except for possible rearrangement of factors. The number of factors $\mathbb{Z}$ (Betti number of G or (free) rank of G) is unique

Remark 1.7.6.

1. If G in Theorem 1.7.3 is finite, then its rank is equal to 0
2. To identify all abelian groups of order n up to isomorphism, determine the prime factorization of n

Exercise 1.7.2. Enumerate all abelian groups of given order of 1350, up to isomorphism

Solution. Note that $1350 = 2^1 \cdot 3^3 \cdot 5^2$. Thus we have 6 possible combinations listed below:

$$\begin{aligned} 1350 &= 2^1 \cdot 3^3 \cdot 5^2 \\ &= 2^1 \cdot 3^3 \cdot 5^1 \cdot 5^1 \\ &= 2^1 \cdot 3^2 \cdot 3^1 \cdot 5^2 \\ &= 2^1 \cdot 3^2 \cdot 3^1 \cdot 5^1 \cdot 5^1 \\ &= 2^1 \cdot 3^1 \cdot 3^1 \cdot 3^1 \cdot 5^2 \\ &= 2^1 \cdot 3^1 \cdot 3^1 \cdot 3^1 \cdot 5^1 \cdot 5^1 \end{aligned}$$

Therefore, the possible combinations are

$$\begin{aligned} &\mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_{25} \\ &\mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ &\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\ &\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ &\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \\ &\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \end{aligned}$$

Remark 1.7.7. Let G be a finite group abelian group. If m divides $|G|$, then $\exists H \leqslant G$ such that $|H| = m$

Exercise 1.7.3. Find a subgroup of $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$ of order 150

Solution. Note that $150 = 2^1 \cdot 2^0 \cdot 3^1 \cdot 5^2$. Thus, we have a subgroup H_2 that is defined by

$$\begin{aligned} H_2 &= \langle 2^{3-1} \rangle \times \langle 2^{1-0} \rangle \times \langle 3^{1-1} \rangle \times \langle 5^{2-2} \rangle \\ &= \langle 4 \rangle \times \langle 0 \rangle \times \langle 1 \rangle \times \langle 1 \rangle \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \end{aligned}$$

2 Second Half Semester

2.1 Friday, November 4: Normal Subgroups and Factor Groups

2.1.1 Normal Subgroups

Definition 2.1.1. Let G be a group. A subgroup N of G is said to be **normal** (or **invariant**) subgroup of G, denoted by $N \trianglelefteq G$, if $gN = Ng, \forall g \in G$.

Remark 2.1.1.

1. The condition $gN = Ng$ in the definition does not mean that $gn = ng, \forall n \in N$, rather, $\forall n \in N$, $gn = n'g$, for some $n' \in N$.
2. if $[G : H] = 2$, then $H \trianglelefteq G$.

Definition 2.1.2. Let G be a group, $H \leqslant G$, and $g \in G, h \in H$.
1. The element ghg^{-1} is called the **conjugate of** h **by** g.
2. The set gHg^{-1} is called the **conjugate of** H **by g**

Remark 2.1.2. It can be shown that $gHg^{-1} \leqslant G$ and $H \cong gHg^{-1}$

Theorem 2.1.1. Let G be a group and $N \leqslant G$. The following are equivalent:
1. $gN = Ng, \forall g \in G$
2. $gNg^{-1} = N, \forall g \in G$
3. $gNg^{-1} \subseteq N, \forall g \in G$

Exercise 2.1.1. Let $H, K \trianglelefteq G$. Show that $H \cap K \trianglelefteq G$.

Solution. Let G be a group and H, K are normal subgroups of G. Then $H \leqslant G$ and $K \leqslant G$. Hence $H \cap K \leqslant G$. Let $n \in H \cap K, g \in G$. So,

$$\begin{aligned}
&\Rightarrow n \in H \wedge n \in K \\
&gng^{-1} \in H \wedge gng^{-1} \in K \\
&gng^{-1} \in H \cap K
\end{aligned}$$

Therefore, $H \wedge K \subseteq G$. ∎

Exercise 2.1.2. Is $\langle(134)\rangle$ a normal subgroup of A_4?

Solution. Note that A_4 is the set of all even permutations in S_4 and

$$\begin{aligned}
A_4 = \{&(1), (12)(34),(13)(24), (14)(23), (123)(132), \\
&(124), (142), (134), (143), (234), (243)\}
\end{aligned}$$

We see that $\langle(134)\rangle = \{(1), (134), (143)\} \leqslant A_4$. Hence,

$$\begin{aligned}
(12)(34)\langle(134)\rangle &= \{(12)(34), (142), (132)\} \\
&\neq \{(12)(34), (123), (124)\} \\
&= \langle(134)\rangle(12)(34)\rangle
\end{aligned}$$

So $\langle(134)\rangle$ is not a subgroup of A_4. ∎

Exercise 2.1.3. Let $K, N \leqslant G$. If $N \trianglelefteq G$, show that $K \cap N \trianglelefteq K$

Proof. Since N and K are subgroups of G, $K \cap N \leqslant G$. In particular, since $K \cap N \subseteq K$, and K is also a group, $K \cap N \leqslant K$. Let $g \in K$ and $x \in K \cap N$. Then $x \in K$ and $x \in N$. We have $gxg^{-1} \in N(N \trianglelefteq G)$. Note that $gxg^{-1} \in K$. Therefore, $gxg^{-1} \in K \cap N$, so $K \cap N \trianglelefteq K$. ∎

Exercise 2.1.4. Let $H, K \trianglelefteq G$. Define the set $HK = \{hk \mid h \in H, k \in K\}$. Show that $HK \trianglelefteq G$.

Proof. We show first that $HK \leqslant G$ using 2-step subgroup test. Since $H, K \leqslant G, \forall h \in H, \forall k \in K, hk \in G$, so $HK \subseteq G$. Since $H, K \leqslant G, e_G = e_G \cdot e_G = e_H \cdot e_K \in HK \neq \varnothing$.

Let $h_1k_1, h_2k_2 \in HK$. Then

$$\begin{aligned}
(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\
&= h_1k'h_2^{-1} \quad (\text{where } k_1k_2^{-1} = k' \exists k' \in K) \\
&= h_1h_2^{-1}k'' \quad (K \trianglelefteq G, \exists k'' \in K, h_2^{-1} \in H \leqslant G)
\end{aligned}$$

Hence, $HK \leqslant G$. To show the normal subgroup, let $g \in G, hk \in HK (h \in H, k \in K)$. Then

$$g(hk)g^{-1} = (gh)e_G(kg^{-1}) = (gh)(g^{-1}g)(kg^{-1}) = (ghg^{-1})(gkg^{-1})$$

Therefore, $HK \trianglelefteq G$. ■

Theorem 2.1.2. Let G be a group and $N \trianglelefteq G$. Denote the set of all left cosets $\{gN \mid g \in G\}$ by G/N (read as G modulo N) and define $*$ on G/N by

$$(g_1N) * (g_2N) = (g_1g_2)N,$$

$\forall g_1N, g_2N \in G/N$. Then $\langle G/N, * \rangle$ is a group

Note: You need first to establish normal subgroup before proving factor group.

Definition 2.1.3. (Factor Group) Let G be a group and $N \trianglelefteq G$. The group G/N is called the **quotient group** or **factor group of** G **modulo** N.

Theorem 2.1.3. Let G be a group and $H \leqslant G$.

1. If G is abelian, then so is G/H.
2. If G is cyclic, then so is G/H.

Exercise 2.1.5. It was shown that $\{1, -1\}$ is a normal subgroup of Q_8. To which known group is $Q_8/\{1, -1\}$ isomorphic to?

Solution. Note that $|Q_8/\{1,-1\}| = \dfrac{8}{2} = 4$. Let $N = \{1, -1\}$. Moreover, $Q_8/\{1,-1\} = \{N, iN, jN, kN\}$ since $iN = \{i, -i\}, jN = \{j, -j\}, kN = \{k, -k\}$. So

$\cdot$	N	iN	jN	kN
N	N	iN	jN	kN
iN	iN	N	kN	jN
jN	jN	kN	N	iN
kN	kN	jN	iN	N

So $Q_8/\{1,-1\} \cong V_4$. ■

Exercise 2.1.6. Let H be a normal subgroup of G and K a subgroup of G that contains H.

(a) Verify: $H \trianglelefteq K$.

(b) Show that K is a normal in G if and only if K/H is normal in G/H.

Solution.

(a) Verify that $H \trianglelefteq K$.
Let $h \in H, k \in K$. Show that $khk^{-1} \in H$. Note that $k^{-1} \in K \leqslant G$. Since $H \trianglelefteq G$, $khk^{-1} \in H$.

(b) Show that K is normal in G iff K/H is normal in G/H.
($\Rightarrow$) Suppose $K \trianglelefteq G$. Show that $K/H \leqslant G/H$. $K/H = \{kH \mid k \in K\}$.

- Observe that since $K \trianglelefteq G, K/H \subseteq G/H$. Moreover, $e_k H = H \in K/H \wedge H \in G/H$ (H is identity element of G/H).
- Let $k_1H, k_2H \in K/H$, where $k_1, k_2 \in K \trianglelefteq G$.

$$(k_1H) * (k_2H)^{-1} = k_1H * k_2^{-1}H = (k_1k_2^{-1})H \in K/H$$

Therefore, $K/H \leqslant G/H$.
Let $gH \in G/H, kH \in K/H$, where $g \in G, k \in K$.

$$\begin{aligned}(gH) * (kH) * (gH)^{-1} &= (gH) * (kH) * (g^{-1}H) \\ &= gkg^{-1}H \in K/H\end{aligned}$$

($\Leftarrow$) Suppose $K/H \trianglelefteq G/H$. Show $K \trianglelefteq G$. Note that $K \leqslant G$. Let $k \in K, g \in G$. Show that $gkg^{-1} \in K$.

$$(gkg^{-1})H = (gH) * (kH) * (gH)^{-1} \in K/H \trianglelefteq G/H$$

Therefore, $gkg^{-1} \in K$, so $K \trianglelefteq G$. ∎

2.2 Friday, November 11: Homomorphism of Groups

Definition 2.2.1. (Homomorphism) A **homomorphism** ϕ from a group $\langle G, \cdot \rangle$ to a group $\langle G', \cdot' \rangle$ is a function $\phi : G \to G'$ that peserves the group operations, that is $\forall a, b \in G$,

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

If $G = G'$, then the homomorphism ϕ is an **endomorphism**. A homomorphism ϕ is called an **epimorphism** if ϕ is onto and a **monomorphism** if ϕ is one-to-one. If ϕ is an epimorphism, G' is called a **homomorphic image of** G. A bijective homomorphism is an **isomorphism**.

Theorem 2.2.1. (Properties of Homomorphism) Let $\phi : G \to G'$ be a homomorphism of groups.

1. $\phi(e) = e'$ where e is the identity element in G and e' is the iden-

tity element in G'

2. $(\phi(g))^{-1} = \phi(g^{-1}), \forall g \in G$
3. If $H \leqslant G$, then $\phi(H) \leqslant G'$. If $H' \leqslant G'$, then $\phi^{-1}(H) \leqslant G$
4. Let $H \leqslant G$. If H is abelian, then $\phi(H)$ is abelian. If H is cyclic, then $\phi(H)$ is cyclic
5. If $H \trianglelefteq G$, then $\phi(H) \trianglelefteq \phi(G)$. If $H' \trianglelefteq G'$, then $\phi^{-1}(H') \trianglelefteq G$
6. If $g \in G$ such that $|g| = n < \infty$ then $|\phi(g)| \mid n$

Definition 2.2.2. (Kernel) Let $\phi : G \to G'$ be a homomorphism of groups and e' is the identiy element of G'. Then **kernel** of ϕ, denoted by $\text{Ker}\phi$ is the set

$$\text{Ker}\phi = \{g \in G \mid \phi(g) = e'\} = \phi^{-1}(\{e'\})$$

Remark 2.2.1. Let $\phi : G \to G'$ be a homomorphism of groups

1. $\text{Ker}\phi \trianglelefteq G$
2. $\forall a, b \in G, \phi(a) = \phi(b) \Leftrightarrow a\text{Ker}\phi = b\text{Ker}\phi$
3. Let $g \in G, g' \in G'$. If $\phi(g) = g'$, then

$$\phi^{-1}(\{g'\}) = \{x \in G \mid \phi(x) = g'\} = g\text{Ker}\phi$$

4. If $|\text{Ker}\phi| = n < \infty$, then ϕ is an $n-\text{to}-1$ mapping from G onto $\phi(G)$.

Exercise 2.2.1. Let $\alpha : G \to G'$ and $\beta : G' \to G''$ be group homomorphisms. Show that the composition $\beta \circ \alpha : G \to G''$ is also a homomorphism.

Proof. Let $\alpha : G \to G'$ and $\beta : G' \to G''$ be group homomorphisms and let $x_1, x_2 \in G$. We have,

$$\begin{aligned}(\beta \circ \alpha)(x_1 \cdot x_2) &= \beta(\alpha(x_1 \cdot x_2)) \\ &= \beta(\alpha(x_1) \cdot' \alpha(x_2)) \\ &= \beta(\alpha(x_1)) \cdot'' \beta(\alpha(x_2)) \\ &= (\beta \circ \alpha)(x_1) \cdot'' (\beta \circ \alpha)(x_2)\end{aligned}$$

Therefore, the composition $\beta \circ \alpha : G \to G''$ is a homomorphism. ■

Exercise 2.2.2. Let $\phi : G \to G'$ be a homomorphism of groups. Show that if $H' \leqslant G'$, then $\phi^{-1}(H') \leqslant G$ $\quad (\phi^{-1}(H') = \{g \in G \mid \phi(g) \in H'\})$

Proof.

- Let e be the identity element of G and e' be the identity element of G'. Since ϕ is a homomorphism,

$$\phi(e) = e' \in H \leqslant G', e \in G$$

Hence, $e \in \phi^{-1}(H') \neq \varnothing$.

- Let $g_1, g_2 \in \phi^{-1}(H')$. Therefore, $\phi(g_1), \phi(g_2) \in H'$. We need to show that $g_1 g_2^{-1} \in \phi^{-1}(H')$. Then

$$\begin{aligned}\phi(g_1 \cdot g_2^{-1}) &= \phi(g_1) \cdot' \phi(g_2^{-1}) \\ &= \phi(g_1) \cdot' (\phi(g_2))^{-1} \in H' \leqslant G'\end{aligned}$$

Therefore $g_1 \cdot g_2^{-1} \in \phi^{-1}(H')$. ■

Exercise 2.2.3. Let $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ be a group homomorphism such that $\phi(7) = 6$. Compute $\phi(1)$, $\text{Ker}\phi$, and $\phi(\mathbb{Z}_{50})$.

Solution.

- Note that

$$6 = \phi(7) = \phi(1 +_{50} 1 +_{50} 1 +_{50} \ldots +_{50} 1) = \phi(1) +_{15} \phi(1) +_{15} \ldots +_{15} \phi(1)$$

Then, $7\phi(1) = 6 \Rightarrow \phi(1) = 3$.

- Note that the Kernel is given by $\text{Ker}\phi = \{g \in \mathbb{Z}_{50} \mid \phi(g) = 0\}$. Let $g \in \text{Ker}\phi$. Moreover, note that $5\phi(1) = 0$. Therefore,

$$\text{Ker}\phi = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\} = \langle 5 \rangle$$

- We have

$$\begin{aligned}\phi(\mathbb{Z}_{50}) &= \{\phi(g) \mid g \in \mathbb{Z}_{50}\} \\ &= \{0, 3, 6, 9, 12\} \\ &= \langle 3 \rangle \cong \mathbb{Z}_5\end{aligned}$$

Exercise 2.2.4. Show that the group G is abelian if and only if the function $\alpha : G \to G$ such that $\alpha(g) = g^{-1}$ where $g \in G$ is a homomorphism.

Proof.

($\Rightarrow$) Suppose G is abelian. Let $g_1, g_2 \in G$

$$\begin{aligned}\alpha(g_1 g_2) &= (g_1 g_2)^{-1} \\ &= g_2^{-1} g_1^{-1} \\ &= g_1^{-1} g_2^{-1} \\ &= \alpha(g_1)\alpha(g_2)\end{aligned}$$

Therefore, α is a homomorphism.

($\Leftarrow$) Suppose α is a homomorphism. Let $a, b \in G$. We need to show that $ab = ba$.

$$\begin{aligned} ab = \left[(ab)^{-1}\right]^{-1} &= [\alpha(ab)]^{-1} \\ &= \alpha((ab)^{-1}) \\ &= \alpha(b^{-1})\alpha(a^{-1}) \\ &= (\alpha(b))^{-1}(\alpha(a))^{-1} \\ &= \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} \\ &= ba \end{aligned}$$

Since G is a group with commutative opperation, G is an abelian group. ■

Theorem 2.2.2. Let $\phi : G \to G'$ be a homomorphism and e is the identity element of G. Then ϕ is one-to-one if and only if $\text{Ker}\phi = \{e\}$

Theorem 2.2.3. Let G be a group and $N \trianglelefteq G$. Then $\delta : G \to G/N$ given by $\delta(g) = gN, \forall g \in G$, is a group epimorphism with $\text{Ker}\delta = N$. The mapping δ is called the **canonical** or **natural homomorphism**

Theorem 2.2.4. Let $\phi : G \to G'$ be a homomorphism of groups with $\text{Ker}\phi = N$, and δ is the canonical homomorphism from $G \to G/N$. Then there exists a unique homomorphism $\mu : G/N \to G'$ such that $\phi = \mu \circ \delta$

Theorem 2.2.5. (First Isomorphism Theorem) Let $\phi : G \to G'$ be a homomorphism of groups. Then $G/\text{Ker}\phi \cong \phi(G)$.

Exercise 2.2.5. Let $G = \langle a \rangle$ with $|a| = 20$ and consider the group homomorphism $f : G \to G$ such that $f(g) = g^4$, for every $g \in G$

(a) Find the elements of Kerf and $f(G)$

(b) Using FIT, to what known group is $G/\text{Ker}f$ and $f(G)$ both isomorphic to?

(c) Give the elements of $G/\text{Ker}f$ and write its group table

Solution. Note that $g = a^k$, $\exists k \in \mathbb{Z}$ since $G = \langle a \rangle$

(a) We have

$$\begin{aligned} \text{Ker}f &= \{g \in G \mid f(g) = e\} \\ &= \left\{g \in G \mid g^4 = e\right\} \\ &= \left\{a^k \in G \mid a^{4k} = \left(a^k\right)^4 = e, \exists k \in \mathbb{Z}\right\} \end{aligned}$$

$$= \left\{e, a^5, a^{10}, a^{15}\right\} = \langle a^5 \rangle \cong \mathbb{Z}_4$$

(b) We have

$$\begin{aligned} f(G) = \{f(g) \mid g \in G\} &= \left\{g^4 \mid g \in G\right\} \\ &= \left\{(a^k)^4 \mid k \in \mathbb{Z}\right\} \\ &= \left\{(a^4)^k \mid k \in \mathbb{Z}\right\} \\ &= \left\{e, a^4, a^8, a^{12}, a^{16}\right\} \end{aligned}$$

(c) By FIT, $G/\mathrm{Ker} f \cong f(G) \cong \mathbb{Z}_5$

$\cdot$	$\mathrm{Ker} f$	$a\mathrm{Ker} f$	$a^2\mathrm{Ker} f$	$a^3\mathrm{Ker} f$	$a^4\mathrm{Ker} f$
$\mathrm{Ker} f$	$\mathrm{Ker} f$	$a\mathrm{Ker} f$	$a^2\mathrm{Ker} f$	$a^3\mathrm{Ker} f$	$a^4\mathrm{Ker} f$
$a\mathrm{Ker} f$	$a\mathrm{Ker} f$	$a^2\mathrm{Ker} f$	$a^3\mathrm{Ker} f$	$a^4\mathrm{Ker} f$	$\mathrm{Ker} f$
$a^2\mathrm{Ker} f$	$a^2\mathrm{Ker} f$	$a^3\mathrm{Ker} f$	$a^4\mathrm{Ker} f$	$\mathrm{Ker} f$	$a\mathrm{Ker} f$
$a^3\mathrm{Ker} f$	$a^3\mathrm{Ker} f$	$a^4\mathrm{Ker} f$	$\mathrm{Ker} f$	$a\mathrm{Ker} f$	$a^2\mathrm{Ker} f$
$a^4\mathrm{Ker} f$	$a^4\mathrm{Ker} f$	$\mathrm{Ker} f$	$a\mathrm{Ker} f$	$a^2\mathrm{Ker} f$	$a^3\mathrm{Ker} f$

2.3 Friday, November 18: Rings: Definition and Basic Properties

Definition 2.3.1. (Ring) A **ring** $\langle R, +, \cdot \rangle$ is a nonempty set R together with two binary operations addition $(+)$ and multiplication $(\cdot)$, such that the following axioms are satisfied

(R1) $\langle R, + \rangle$ is an abelian group

(R2) Multiplication is associative

(R3) For all $a, b, c \in R$, the **left distributive law**, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law**, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold

Remark 2.3.1. Let $\langle R, +, \cdot \rangle$ be a ring.

1. If the binary operation $+$ and $\cdot$ are clear from context, we simply denote the ring $\langle R, +, \cdot \rangle$ by R
2. We denote by 0_R the additive identity (zero element) of R. The additive inverse of $a \in R$ is $-a$
3. We write $a - b$ for $a + (-b)$
4. Multiplication in R is usually by juxtaposition, that is, we write ab for $a \cdot b$. Multiplication is assumed to be performed before addition in the absence of parenthesis

Theorem 2.3.1. Let R be a ring with additive identity 0_R, and $a, b, c \in R$. Then

1. $a \cdot 0_R = 0_R = 0_R \cdot a$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$ and $(a - b) \cdot c = a \cdot c - b \cdot c$

Definition 2.3.2. Let R be a ring

1. If multiplication in R is commutative, then R is said to be a **commutative ring**
2. If R contains an element 1_R such that $\forall a \in R, 1_R \cdot a = a = 1_R \cdot a$, then we call 1_R the **multiplicative identity** or **unity** of R. If R has a multiplicative identity, then R is said to be a **ring with unity**
3. If R is a ring with unity 1_R, an element $a \in R$ is called a **unit** if it has a **multiplicative inverse**, that is, $\exists b \in R$ such that $a \cdot b = 1_R = b \cdot a$. We denote the element b by a^{-1}

Theorem 2.3.2. The units of a ring R with unity, denoted by $U(R)$, form a group under multiplication

Definition 2.3.3. (Direct Product) Let $R_1, R_2, \ldots, R_n$ be rings and

$$R = \prod_{i=1}^{n} R_i = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R, 1 \leqslant i \leqslant n\},$$

addition $+$ and multiplication $\cdot$

$$\begin{aligned}(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) &= (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)\\ (r_1, r_2, \ldots, r_n) \cdot (s_1, s_2, \ldots, s_n) &= (r_1 \cdot s_1, r_2 \cdot s_2, \ldots, r_n \cdot s_n)\end{aligned}$$

$(r_1, r_2, \ldots, r_n), (s_1, s_2, \ldots, s_n) \in \prod_{i=1}^{n} R_i$. Then $\langle R, +, \cdot \rangle$ is a ring called **direct product of** $R_1, R_2, \ldots, R_n$. Observe that R is commutative or has unity if and only if each of $R_i, 1 \leqslant i \leqslant n$ is commutative or has unity

Remark 2.3.2. Let R be a ring with additive identity 0_R.

1. Let $a, b, c \in R$. If $a \neq 0_R$ and $ab = ac$, then it does not imply that $b = c$
2. If R is a ring with unity 1_R, then for each $a \in R, (-1_R) \cdot a = -a = 1_R(-a)$
3. Suppose R is a ring with unity. Then the unity is unique. Moreover, if $a \in R$ is a unit, then a^{-1} is also unique
4. If $R \neq \{0_R\}$ and R is a ring with unity 1_R, then $1_R \neq 0_R$

Exercise 2.3.1. Determine whether the indicated operations on the set give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, determine whether the ring is commutative and whether it has a unity.

1. $R = \left\{a + b\sqrt[3]{3} \mid a, b \in \mathbb{Q}\right\}$ under the usual addition and multiplication
2. $\mathbb{Z}^+$ under the usual addition and multiplication
3. $2\mathbb{Z} \times \mathbb{Z}$ under the addition and multiplication by components
4. $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ under addition and multiplication by components

Solution.

1. Let $a_1 + b_1\sqrt[3]{3}, a_2 + b_2\sqrt[3]{3} \in R$ where $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. We have
$$\begin{aligned}\left(a_1 + b_1\sqrt[3]{3}\right)\left(a_2 + b_2\sqrt[3]{3}\right) &= a_1a_2 + a_1b_2\sqrt[3]{3} + b_1a_2\sqrt[3]{3} + b_1b_2\sqrt[3]{3^2} \\ &= a_1a_2 + \left(a_1b_2 + b_1a_2 + b_1b_2\sqrt[3]{3}\right)\sqrt[3]{3}\end{aligned}$$
Note that $a_1a_2 \in \mathbb{Q}$ but $a_1b_2 + b_1a_2 + b_1b_2\sqrt[3]{3} \notin \mathbb{Q}$ where $b_1 \neq b_2 \neq 0$. Therefore, R is not a ring.
2. $\langle \mathbb{Z}^+, + \rangle$ is not an abelian group since it does not have the additive identity. That is, $0 \notin \mathbb{Z}^+$. Therefore, $\langle \mathbb{Z}^+, + \rangle$ is not a ring.
3. Note that $\langle 2\mathbb{Z}, +, \cdot \rangle$ is a commutative ring and $\langle \mathbb{Z}, +, \cdot \rangle$ is a commutative ring with unity. Therefore, $\langle 2\mathbb{Z} \times \mathbb{Z}, +, \cdot \rangle$ is a commutative ring.
4. Note that $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$ are commutative ring with unity. Therefore, $\langle \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}, +, \cdot \rangle$ is also a commutative ring with unity. The unity is given by $1_{\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z}} = (1, 1, 1) \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$.

Definition 2.3.4. (Subring) Let $S \neq \varnothing$ be a subset of a ring R. Then S is said to be a **subring** of R if S is also a ring under the same binary operations in R $(S \leqslant R)$

Theorem 2.3.3. (Subring Test) Let R be a ring and $\varnothing \neq S \subseteq R$. If $\forall a, b \in S, a - b \in S$ and $ab \in S$, then S is a subring of R

Exercise 2.3.2. Show that $S = \left\{ \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\} \leqslant M_{2\times2}(\mathbb{R})$

Proof. Note that $S \subseteq M_{2\times2}(\mathbb{R})$ and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S \neq \varnothing$ where $a = b = 0 \in \mathbb{R}$.

Let $\begin{bmatrix} 0 & 0 \\ a_1 & b_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ a_2 & b_2 \end{bmatrix} \in S, a_1, a_2, b_1, b_2 \in \mathbb{R}$. Then we have,

$$\begin{bmatrix} 0 & 0 \\ a_1 & b_1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ a_2 & b_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a_1 - a_2 & b_1 - b_2 \end{bmatrix} \in S \quad (\text{where } a_1 - a_2, b_1 - b_2 \in R)$$
$$\begin{bmatrix} 0 & 0 \\ a_1 & b_1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ a_2 & b_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ b_1 a_2 & b_1 b_2 \end{bmatrix} \in S \quad (\text{where } b_1 a_2, b_1 b_2 \in R)$$

Exercise 2.3.3. Prove: Let R be a ring and $S_1, S_2 \leqslant R$. Then $S_1 \cap S_2 \leqslant R$

Proof. Since $S_1, S_2 \leqslant R, S_1 \cap S_2 \subseteq R$. Note that $0_R \in S_1$ and $0_R \in S_2$. Therefore, $0_R \in S_1 \cap S_2 \neq \varnothing$.

Let $a, b \in S_1 \cap S_2$. Then $a, b \in S_1$ and $a, b \in S_2$. We have,

$$a - b \in S_1 \leqslant R \wedge a - b \in S_2 \leqslant R$$
$$ab \in S_1 \leqslant R \wedge ab \in S_2 \leqslant R$$

Therefore, $a - b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$. Hence, $S_1 \cap S_2 \leqslant R$. ■

Exercise 2.3.4. Prove: Let R be a ring. The **center** of R is the set $S = \{a \in R \mid ax = xa, \forall x \in R\} \leqslant R$

Proof. Note that $\forall x \in R, 0_R \cdot x = 0_R = x \cdot 0_R$. So $0_R \in S \neq \varnothing$. Moreover, $S \subseteq R$.

Let $a_1, a_2 \in S, x \in R$. Then,

$$(a_1 - a_2)x = a_1 x - a_2 x = x a_1 - x a_2 = x(a_1 - a_2)$$

Hence, $a_1 - a_2 \in S$. Moreover,

$$(a_1 a_2)x = a_1(a_2 x) = a_1(x a_2) = (a_1 x)a_2 = (x a_1)a_2 = x(a_1 a_2)$$

Hence, $a_1 a_2 \in S$. Therefore, the set $S = \{a \in R \mid ax = xa, \forall x \in R\} \leqslant R$. ■

2.4 Friday, November 25: Fields and Integral Domains

2.4.1 Fields

Definition 2.4.1. (Fields) Let R be a ring with unity $1_R \neq 0_R$. If every nonzero element of R is a unit, then R is called a **division ring** or a **skew field**. If R is a commutative division ring, then R is said to be a **field**. A noncommutative division ring is called a **strictly skew field**.

Remark 2.4.1. The ring R is a division ring if and only if $R^* = R \setminus \{0_R\}$ is a group under multiplication. The ring R is a field if and only if $R^* = R \setminus \{0_R\}$ is an abelian group under multiplication.

Exercise 2.4.1. Let $2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10. Prove that R is a field

Solution. By the Cayley tables, we have

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\cdot_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

Note that $\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$ is a commutative ring with unity, so $+_n$ and $\cdot_n$ are well-defined, associative, commutative, and satisfies distributive laws. Note that $2\mathbb{Z}_{10} \subseteq \mathbb{Z}_{10}$.

Caylet table shows that $2\mathbb{Z}_{10}$ is closed under $+_{10}$ and $\cdot_{10}$. So $+_{10}$ and $\cdot_{10}$ are binary operations on $2\mathbb{Z}_{10}$. The additive identity under addition is given by $0_{2\mathbb{Z}_{10}} = 0$ and for each element, $-0 = 0, -2 = 8, -4 = 6, -6 = 4, -8 = 2$. Thus, the additive inverses are also in $2\mathbb{Z}_{10}$. Therefore, $\langle 2\mathbb{Z}_{10}, +_{10}, \cdot_{10} \rangle$ is a commutative ring.

Note that the identity element under multiplication is $1_{2\mathbb{Z}_{10}} = 6$. And for each element, $2^{-1} = 8, 4^{-1} = 4, 6^{-1} = 6, 8^{-1} = 2$. Since $\langle 2\mathbb{Z}_{10}, +_{10}, \cdot_{10} \rangle$ is a commutative ring with unity and all nonzero elements are units, $\langle 2\mathbb{Z}_{10}, +_{10}, \cdot_{10} \rangle$ is a field. ■

Remark 2.4.2. The quaternions $\mathbb{H}$ of Sir Williman Rowan Hamilton, (1805 - 1865) are the standard example of a strictly skew field or non-commutative division ring.

Definition 2.4.2. A nonzero element a in a ring R is a **divisor of zero** or **zero divisor** if there exists a nonzero element b in R such that $ab = 0_R$ or $ba = 0_R$.

Theorem 2.4.1. The cancellation laws for multilication hold in a ring R if and only if R has no zero divisors.

Remark 2.4.3. Suppose R be a ring without zero divisors. Let $a, b \in R$ with $a \neq 0_R$.

1. Then $ax = b$, has at most one solution in R.
2. If R is a ring with unity and a is a unit, then $ax = b$ has a unique solution $x = a^{-1}b$. In the case that R is a commutative, in particular if R is a field, it is customary to write $a^{-1}b = ba^{-1}$ by $\frac{b}{a}$. This quotient notation must **not be used if** R **is not commutative**, for then we do not know whether $\frac{b}{a}$ denotes $a^{-1}b$ or ba^{-1}.

2.4.2 Integral Domain

Definition 2.4.3. (Integral Domain) A commutative ring with unity D with $1_D \neq 0_D$ is said to be an **integral domain** if it has no zero divisors.

Remark 2.4.4. In an integral domain D, $\forall a, b \in D$, if $ab = 0_D$, then $a = 0_D$ or $b = 0_D$.

Theorem 2.4.2. Every field is an integral domain.

Theorem 2.4.3. Every finite integral domain is a field.

Definition 2.4.4. A subring S of a field R is said to be a **subfield** of R if S is also a field under the same binary operations in R. A subring S of an integral domain R is said to be a **subdomain** of R if S is also an integral domain under the same binary operations in R.

Theorem 2.4.4. (Subfield Test) Let F be a field and $K \subseteq F$ with at least two elements. If $\forall a, b\,(b \neq 0_F) \in K$, $a - b \in K$ and $ab^{-1} \in K$, then K is a subfield of F.

Exercise 2.4.2. Consider the set $2\mathbb{Z}$ under the usual addition. Define a multilication $*$ by $a * b = (ab)/2$, for all $a, b \in 2\mathbb{Z}$.
1. Show that $2\mathbb{Z}$ with the defined operations is a commutative ring with unity
2. Is $\langle 2\mathbb{Z}, +, * \rangle$ an integral domain? Justify your answer
3. Is $\langle 2\mathbb{Z}, +, * \rangle$ a field? Justify your answer

Solution.
1. Note that $\langle m\mathbb{Z}, + \rangle$ is an abelian group, $m \in \mathbb{Z}$. We will show that $2\mathbb{Z}$ is closed under $*$. Let $2k_1, 2k_2 \in 2\mathbb{Z}$ where $k_1, k_2 \in \mathbb{Z}$. Then
$$(2k_1) * (2k_2) = \frac{(2k_1)(2k_2)}{2} = 2(k_1k_2) \in 2\mathbb{Z} \quad (\text{where } k_1k_2 \in \mathbb{Z})$$
Next,we will show that $*$ is well-defined on $2\mathbb{Z}$. Let $a, b, c, d \in 2\mathbb{Z}$ where $a = b$ and $c = d$. Then, we have
$$a * c = \frac{ac}{2} = \frac{bd}{2} = b * d$$
Therefore, $*$ is a binary operation on $2\mathbb{Z}$. We prove its associativity, $\forall a, b, c \in 2\mathbb{Z}$,
$$(a*b)*c = \frac{ab}{2}*c = \frac{\frac{ab}{2}c}{2} = \frac{(ab)c}{2 \cdot 2} = \frac{a(bc)}{2} = \frac{a\frac{bc}{2}}{2} = \frac{a(b*c)}{2} = a*(b*c)$$
We verify its RDL and LDL, $\forall a, b, c \in 2\mathbb{Z}$,
$$(a+b)*c = \frac{(a+b)c}{2} = \frac{ac+bc}{2} = \frac{ac}{2} + \frac{bc}{2} = (a*c) + (b*c)$$
and
$$a*(b+c) = \frac{a(b+c)}{2} = \frac{ab+ac}{2} = \frac{ab}{2} + \frac{ac}{2} = (a*b) + (a*c)$$
So, LDL and RDL holds. Lastly, let $a \in 2\mathbb{Z}$. Then,
$$2 * a = a * 2 = \frac{a \cdot 2}{2} = a$$
So we take, $1_{2\mathbb{Z}} = 2 \in 2\mathbb{Z}$. Therefore, $\langle 2\mathbb{Z}, +, * \rangle$ is a commutative ring with unity.
2. Let $a, b \in 2\mathbb{Z}$ and suppose $a * b = 0_{2\mathbb{Z}}$. Then
$$\frac{ab}{2} = a * b = 0_{2\mathbb{Z}} = 0$$
So $ab = 0$. This implies that $a = 0$ or $b = 0$. Therefore, $\langle 2\mathbb{Z}, +, * \rangle$ is an integral domain.
3. Let $a = 4 \in 2\mathbb{Z}^*$, then
$$1 * 4 = 4 * 1 = \frac{4 \cdot 1}{2} = 2 = 1_{2\mathbb{Z}}$$
but $1 \notin 2\mathbb{Z}^*$. Therefore, $\langle 2\mathbb{Z}^*, * \rangle$ is not an abelian group. So it is not a field.

Definition 2.4.5. (Characteristic) Let R be a ring. If there is a positive integer n such that $n \cdot a = 0_R$, for every $a \in R$, where $n \cdot a = a + a + \cdots + a$ (n addends), then the smallest such n is called the **characteristic** of R. If no such positive integer exists, we say that R has **characteristic 0**. Notation: $\operatorname{char} R = n$.

Theorem 2.4.5. Let R be a ring with unity 1_R. If 1_R has finite order n, then $\operatorname{char} R = n$. If $n \cdot 1_R \neq 0_R$ for all $n \in \mathbb{Z}^+$ (1_R has infinite order), then R has characteristic 0.

Theorem 2.4.6. The characteristic of an integral domain is either zero or a prime integer.

Exercise 2.4.3. Compute the characteristic of the following rings.

a. $X = \varnothing$, $\langle \mathscr{P}(X), \triangle, \cap \rangle$

b. $\mathbb{Z}_5 \times 5\mathbb{Z}$

Solution.

1. Note that $0_{\mathscr{P}(X)} = \varnothing$. Then, $\forall A \in \mathscr{P}(X)$,

$$2A = A \triangle A = (A \cup A)/(A \cap A) = A/A = \varnothing$$

Therefore, $\operatorname{char} \mathscr{P}(X) = 2$.

2. Note that $0_{\mathbb{Z}_5 \times 5\mathbb{Z}} = (0, 0)$. Also, $\operatorname{char} \mathbb{Z}_5 = 5$ but $\operatorname{char} 5\mathbb{Z} = 0$. Therefore, $\operatorname{char}(\mathbb{Z}_5 \times 5\mathbb{Z}) = 0$.

Exercise 2.4.4. A ring element a is called an **idempotent** if $a^2 = a$. In a commutative ring of characteristic 2, prove that the idempotents form a subring.

Proof. Let R be a commutative ring, $S = \{a \in R \mid a^2 = a\}$, and $\operatorname{char} R = 2$. Then, $\forall a \in S, a^2 = a \cdot a$ and $\forall x \in R, 2x = x + x = 0_R \Rightarrow x = -x$. Note that

$$0_R^2 = 0_R \cdot 0_R \Rightarrow 0_R \in S \neq \varnothing$$

Let $a, b \in S$. Then

$$\begin{aligned}
(a-b)^2 = (a-b)(a-b) &= a^2 + a(-b) + (-b)a + (-b)(-b) \\
&= a^2 - ab - ba + b^2 \\
&= a^2 - ab - ab + b^2 \\
&= a^2 + 2(-ab) + b^2 \\
&= a^2 + b^2 \\
&= a + b
\end{aligned}$$

$$\begin{aligned} &= a + (-b) \\ &= a - b \end{aligned}$$

Therefore, $a - b \in S$. Moreover,

$$(ab)^2 = a^2b^2 = ab$$

So, $ab \in S$. Therefore, $S \leqslant R$. ■

2.5 Friday, December 9: Ideals, Factor Rings and Ring Homomorphisms

2.5.1 Ideals

Definition 2.5.1. (Ideals) Let R be a ring and I be a subring of R.

1. I is called a **left ideal** of R if $\forall a \in I$ and $\forall r \in R, ra \in I$
2. I is called a **right ideal** of R if $\forall a \in I$ and $\forall r \in R, ar \in I$
3. I is called a **(two-sided) ideal** of R if I is both a left and right ideal of R

Theorem 2.5.1. (Ideal Test) A nonempty subset I of a ring R is an ideal of R if

1. $\forall a, b \in I, a - b \in I$
2. $\forall a \in I$ and $\forall r \in R, ra \in I$ and $ar \in I$

Definition 2.5.2. (Principal Ideal) Let R be a commutative ring with unity and $a \in R$. The ideal $I = \{ar \mid r \in R\}$ of R, denoted by $\langle a \rangle$ is called the **principal ideal generated by** a. An ideal I of R is a **principal ideal** if $I = \langle a \rangle$, for some $a \in R$.

Definition 2.5.3. (Proper Ideal) If R is a ring then $\{0_R\}$ (**trivial ideal**) and R (**improper ideal**) are ideals. An ideal $I \neq R$ of R is referred to as a proper ideal.

Exercise 2.5.1. Consider the ring $M_{2\times 2}(\mathbb{Z})$. Verify whether the following subset are ideal of $M_{2\times 2}(\mathbb{Z})$:

(a) $I = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{Z} \right\}$

(b) $J = M_{2\times 2}(2\mathbb{Z})$

Solution.

(a) Note that $I \subseteq M_{2\times 2}(\mathbb{Z})$ and $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$ where $a = 0 \in \mathbb{Z}$. So $I \neq \varnothing$. Let $\begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} \in I$. Then,

$$\begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & a-b \end{bmatrix} \in I$$

where $a - b \in \mathbb{Z}$.

Let $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}), \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} \in I$. Then, we have

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 0 & ya \\ 0 & wa \end{bmatrix} \notin I \text{ when } ay \neq 0$$

and

$$\begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ az & aw \end{bmatrix} \notin I \text{ when } az \neq 0$$

Therefore, I is not an ideal of $M_{2\times 2}(\mathbb{Z})$.

(b) Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$J. Let $\begin{bmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{bmatrix}, \begin{bmatrix} 2m_1 & 2m_2 \\ 2m_3 & 2m_4 \end{bmatrix} \in M_{2\times 2}(2\mathbb{Z})$. Then, we have

$$\begin{bmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{bmatrix} - \begin{bmatrix} 2m_1 & 2m_2 \\ 2m_3 & 2m_4 \end{bmatrix} = \begin{bmatrix} 2(k_1 - m_1) & 2(k_2 - m_2) \\ 2(k_3 - m_3) & 2(k_4 - m_4) \end{bmatrix} \in M_{2\times 2}(2\mathbb{Z})$$

where $k_i - m_i \in \mathbb{Z} \forall i = 1, 2, 3, 4$.

Let $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}), \begin{bmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{bmatrix} \in M_{2\times 2}(2\mathbb{Z})$. Then, we have

$$\begin{aligned}\begin{bmatrix} x & y \\ z & w \end{bmatrix}\begin{bmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{bmatrix} &= \begin{bmatrix} x2k_1 + y2k_3 & x2k_2 + y2k_4 \\ z2k_1 + w2k_3 & z2k_2 + w2k_4 \end{bmatrix} \\ &= \begin{bmatrix} 2(xk_1 + yk_3) & 2(xk_2 + yk_4) \\ 2(zk_1 + wk_3) & 2(zk_2 + wk_4) \end{bmatrix} \in M_{2\times 2}(2\mathbb{Z})\end{aligned}$$

where $(xk_1 + yk_3), (xk_2 + yk_4), (zk_1 + wk_3), (zk_2 + wk_4) \in \mathbb{Z}$. Moreover,

$$\begin{bmatrix} 2k_1 & 2k_2 \\ 2k_3 & 2k_4 \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 2k_1x + 2k_2z & 2k_1y + 2k_2w \\ 2k_3x + 2k_4z & 2k_3y + 2k_4w \end{bmatrix}$$

$$= \begin{bmatrix} 2(k_1x + k_2z) & 2(k_1y + k_2w) \\ 2(k_3x + k_4z) & 2(k_3y + k_4w) \end{bmatrix} \in M_{2\times 2}(2\mathbb{Z})$$

where $(k_1x + k_2z), (k_1y + k_2w), (k_3x + k_4z), (k_3y + k_4w) \in \mathbb{Z}$. Therefore, $M_{2\times 2}(2\mathbb{Z})$ is an ideal of $M_{2\times 2}(\mathbb{Z})$.

Exercise 2.5.2. Give an example to show that if I_1 and I_2 are ideals of a ring R, then $I_1 \cup I_2$ may not be an ideal.

Solution. Note that $2\mathbb{Z}$ and $5\mathbb{Z}$ are ideals of $\mathbb{Z}$. Consider the elements $2 \in 2\mathbb{Z}$ and $5 \in 5\mathbb{Z}$. Note that $2-5 = -3$ but $-3 \notin 2\mathbb{Z} \cup 5\mathbb{Z}$. Therefore, it is not an ideal.

2.5.2 Factor Rings

Theorem 2.5.2. Let R be a ring and I an ideal of R. Then the collection of additive cosets R/I of I is a ring with binary operations

$$\begin{cases} (a+I) + (b+I) & = (a+b) + I \\ (a+I)(b+I) & = ab + I \end{cases}$$

for every $a + I, b + I \in R/I$.

Remark 2.5.1.

1. We call the ring R/I described in Theorem 2.5.2 the **factor ring** or **quotient ring** of R modulo I.
2. $a + I = b + I$ iff $a \in b + I$ iff $b \in a + I$ iff $b - a \in I$ iff $a - b \in I$
3. Let I be an ideal of a ring R
   (a) If R is a commutative ring, then so is R/I
   (b) If R has unity, then R/I also has unity

Exercise 2.5.3. Let I be an ideal of a ring R

(a) Prove that the associative law for multiplication and the distribute laws hold in R/I
(b) Prove that if R is a commutative ring, then so is R/I
(c) Prove that if R has a unity, then R/I also has unity

Solution.

1. Let $a + I, b + 1, c + I \in R/I$ where $a, b, c \in R$. Then,

$$\begin{aligned}(a+I)[(b+I)(c+I)] &= (a+I)(bc+I) \\ &= abc + I \\ &= (ab+I)(c+I)\end{aligned}$$

$$= [(a+I)(b+I)]\,(c+I)$$

and for LDL and RDL,

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)(b+c+I)\\ &= a(b+c)+I\\ &= ab+ac+I\\ &= ab+I+ac+I\\ &= (a+I)(b+I)+(a+I)(c+I)\end{aligned}$$

and

$$\begin{aligned}[(a+I)+(b+I)]\,(c+I) &= (a+b+I)(c+I)\\ &= (a+b)c+I\\ &= ac+bc+I\\ &= ac+I+bc+I\\ &= (a+I)(c+I)+(b+I)(c+I)\end{aligned}$$

2. Suppose R is a commutative ring. Let $a+I, b+I \in R/I$. Then,

$$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$$

Therefore, R/I is also a commutative ring.
3. Suppose $1_R \in R$. Let $a+I \in R/I$. Then,

$$(a+I)(1_R+I) = a\cdot 1_R + I = a+I = 1_R\cdot a + I = (1_R+I)(a+I)$$

Therefore, $1_R + I$ is the identity element under multiplication.
By Cayley tables,

$+$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$6\mathbb{Z}$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$2+6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$	$6\mathbb{Z}$
$4+6\mathbb{Z}$	$4+6\mathbb{Z}$	$6\mathbb{Z}$	$2+6\mathbb{Z}$

$\cdot$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$
$6\mathbb{Z}$	$6\mathbb{Z}$	$6\mathbb{Z}$	$6\mathbb{Z}$
$2+6\mathbb{Z}$	$6\mathbb{Z}$	$4+6\mathbb{Z}$	$2+6\mathbb{Z}$
$4+6\mathbb{Z}$	$6\mathbb{Z}$	$2+6\mathbb{Z}$	$4+6\mathbb{Z}$

Since $2\mathbb{Z}$ is a commutative ring, $2\mathbb{Z}/6\mathbb{Z}$ is also a commutative ring. Moreover, the Cayley tables shows that $1_{2\mathbb{Z}/6\mathbb{Z}} = 4+6\mathbb{Z}$ and $(2+6\mathbb{Z})^{-1} = 2+6\mathbb{Z}$ and $(4+6\mathbb{Z})^{-1} = 4+6\mathbb{Z}$. Therefore, $2\mathbb{Z}/6\mathbb{Z}$ is a field. ■

Exercise 2.5.4. Show that $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$ and $2\mathbb{Z}/6\mathbb{Z}$ is a field.

Proof. Note that $6\mathbb{Z} \subseteq 2\mathbb{Z}$ and $0 = 6 \cdot 0 \in 6\mathbb{Z} \neq \varnothing$. Let $6m, 6k \in 6\mathbb{Z}$ $(m, k \in \mathbb{Z})$. Then,

$$6a - 6b = 6(a - b) \in 6\mathbb{Z} \text{ where } a - b \in \mathbb{Z}$$

Let $2n \in 2\mathbb{Z}$, $6m \in 6\mathbb{Z}$ $(n, m \in \mathbb{Z})$. Then,

$$2n \cdot 6m = 6m \cdot 2n = 6(2mn) \in 6\mathbb{Z}$$

where $2mn \in \mathbb{Z}$. Therefore, $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$. We need to show that $2\mathbb{Z}/6\mathbb{Z}$ is a field.

Since $6\mathbb{Z}$ is an ideal of $2\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$ is a ring with the following addition and multiplication tables.

2.5.3 Ring Homomorphisms

Definition 2.5.4. A **ring homomorphism** of a ring $\langle R, +, \cdot \rangle$ into a ring $\langle R', +', \cdot' \rangle$ is a function $f : R \to R'$ such that $\forall a, b \in R$,

$$f(a + b) = f(a) +' f(b)$$

and

$$f(a \cdot b) = f(a) \cdot' f(b)$$

Remark 2.5.2. Let $f : R \to R'$ be a ring homomorphism

1. If f is onto, then f is called a **ring epimorphism**
2. If f is one-to-one, then f is called a **ring monomorphism**
3. If f is bijective, then f is called a **ring isomorphism**. If $R = R'$, we also call f a **ring automorphism**

Definition 2.5.5. (Isomorphic Rings) Two rings R and R' are said to be **isomorphic** written $R \cong R'$ if there exists a (ring) isomorphism of a ring R with a ring R'.

Remark 2.5.3.

1. Isomorphism between rings define an equivalence relation on any collection of rings.
2. If $f : R \to R'$ is a ring homomorphism, then $f : \langle R, + \rangle \to \langle R', +' \rangle$ is a group homomorphism. Hence, all results from group homomorphism still hold:
   (a) $f(0_R) = 0_{R'}$
   (b) If $a \in R$, then $f(-a) = -f(a)$
   (c) For any $m \in \mathbb{Z}$, $f(ma) = mf(a)$

Exercise 2.5.5. Show that $f : \mathbb{C} \to M_{2\times 2}(\mathbb{R})$ given by

$$f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

for $a, b \in \mathbb{R}$ is a ring homomorphism

Proof. Let $a+bi, c+di \in \mathbb{C}$. Then,

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

and

$$\begin{aligned} f((a+bi)(c+di)) &= f((ac-bd)+(ad+bc)i) \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= f(a+bi)f(c+di) \end{aligned}$$

Therefore f is a ring homomorphism. ■

Exercise 2.5.6. Determine all ring homomorphisms from $\mathbb{Z}_4 \to \mathbb{Z}_{12}$

Proof. Suppose $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{12}$ is a ring homomorphism. Then, we have

$$\begin{aligned} \phi : \mathbb{Z}_4 &\to \mathbb{Z}_{12} \\ g &\mapsto g\phi(1) \end{aligned}$$

For the group homomorphisms, note that $|\phi(1)| = |1| = 4 \Rightarrow$

$|\phi(1)| = 1, 2, 4$ and $|\phi(1)| \mid |\mathbb{Z}_{12}| = 12 \Rightarrow |\phi(1)| = 1, 2, 3, 4, 6, 12$. So, $|\phi(1)| = 1, 2, 4$. Therefore, $\phi(1) = 0, 6, 3, 9$.

For the ring homomorphism, to preserve multiplication, note that $1 \cdot 1 = 1 \in \mathbb{Z}_4$, so

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

Note that $0^2 = 0, 6^2 = 0 \neq 6, 3^2 = 9 \neq 3, 9^2 = 9$. Hence $\phi(1) = 0, 9$. ■

Theorem 2.5.3. Let $f : R \to R'$ be a ring homomorphism

1. If S is a subring of R, then $f(S) = \{f(a) \mid a \in S\}$ is a subring of R'
2. If S' is a subring of R', then $f^{-1}(S') = \{a \in R \mid f(a) \in S'\}$ is a subring of R
3. If R is a commutative ring, then $f(R)$ is also a commutative ring
4. Let R be a ring with unity 1_R and $R' \neq \{0_{R'}\}$
   (a) Then $f(R)$ has unity $f(1_R)$
   (b) If $a \in R$ is a unit, then $f(a)$ is a unit in $f(R)$ with $(f(a))^{-1} = f(a^{-1})$
   (c) If $a \in R$ and $n \in \mathbb{Z}^+$, then $f(a^n) = (f(a))^n$

Definition 2.5.6. Let $f : R \to R'$ be a ring homomorphism. The **Kernel** of f is the set

$$\text{Ker} f = \{x \in R \mid f(x) = 0_{R'}\} = f^{-1}(\{0_{R'}\})$$

Remark 2.5.4. Let $f : R \to R'$ be a ring homomorphism.

1. Then f is an isomorphism if and only if f is onto and $\text{Ker} f = \{0_R\}$
2. If $g \in R, g' \in R'$ and $f(g) = g'$, then

$$f^{-1}(\{g'\}) = \{x \in R \mid f(x) = g'\} = g + \text{Ker} f$$

3. If I is an ideal of R, then $f(I)$ is an ideal of $f(R)$
4. If I' is an ideal of R', then $f^{-1}(I')$ is an ideal of R

Theorem 2.5.4. Let $f : R \to R'$ be a ring homomorphism. Then $\text{Ker} f$ is an ideal of R

Theorem 2.5.5. Let I be an ideal in a ring R. Then the map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a ring epimorphism with $\text{Ker}\pi = I$.

Remark 2.5.5. The mapping π is called the **natural homomorphism** from $R \to R/I$

Theorem 2.5.6. (First Isomorphism Theorem for Rings) Let $f : R \to R'$ be a ring homomorphism. Then $R/\mathrm{Ker} f \cong f(R)$

2.6 Friday, December 16: Prime and Maximal Ideals, and The Field of Quotients of an Integral Domain

Theorem 2.6.1. If R is a ring with unity, and I is an ideal of R containing a unit, then $I = R$

Corollary 2.6.1. A field contains no proper nontrivial ideals

Definition 2.6.1. (Maximal Ideal) An ideal $M \neq R$ of a ring R is said to be **maximal** if there is no proper ideal I in R with $M \subsetneq I$. That is, whenever J is an ideal of R such that $M \subseteq J \subseteq R$, then $J = M$ or $J = R$

Remark 2.6.1. The only ideal that properly contains a maximal ideal is the entire ring

Theorem 2.6.2. Let R be a commutative ring with unity and $I \neq R$ an ideal of R. Then R/I is a field if and only if I is a maximal ideal of R.

Corollary 2.6.2. A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

Definition 2.6.2. Let R be a commutative ring. An ideal $P \neq R$ of R is said to be **prime** if $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$.

Theorem 2.6.3. Let R be a commutative ring with unity and $I \neq R$ an ideal of R. Then R/I is an integral domain if and only if I is a prime ideal of R.

Corollary 2.6.3. Every maximal ideal of a commutative ring with unity is a prime ideal.

Remark 2.6.2.

1. The converse of Corollary 2.6.3 is not true, that is, a prime ideal of a commutative ring with unity need not be maximal.
2. In Corollary 2.6.3, ring R must have unity.

Theorem 2.6.4. Let D be an integral domain. Then there exists a field F that contains a subring isomorphic to D.

Remark 2.6.3.

1. We call F in Theorem 2.6.4 the **field of quotients** of D.
2. Let $\bar{D} = \{[a, 1] \mid a \in D\}$. Then F is a field which D is embedded. Note that

$$[a, 1] \odot [b, 1]^{-1} = [a, 1] \odot [1, b] = [a, b]$$

   We may therefore say that every element $[a, b] \in F$ is the product of $[a, 1] \in \bar{D}$ and the inverse of $[b, 1] \in \bar{D}$. This product is called quotient of $[a, 1]$ and $[b, 1]$ and is denoted by $\dfrac{[a, 1]}{[b, 1]}$. This explains why we choose to call F the field of quotients.
3. Thus, we can now say that any integral domain D can be enlarged (or embedded in) to a field F such that every element of F can be expressed as a quotient of two elements of D.

Theorem 2.6.5. Let F be a field of quotients of an integral domain D. If L is a field containing D, then L contains a subfield K such that $D \subseteq K \subseteq L$ with K isomorphic to F.

Theorem 2.6.6. Let R be a ring with unity 1_R. The mapping $\phi : \mathbb{Z} \to R$ given by $\phi(n) = n \cdot 1_R$ is a ring homomorphism.

Corollary 2.6.4. Let R be a ring with unity.

1. If R is of characteristic $n > 1$, then R contains a subring isomorphic to $\mathbb{Z}_n$.
2. If R is of characteristic 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 2.6.5. Let F be a field and p be prime.

1. If F is of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$.
2. If F is of characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$.

Definition 2.6.3. (Prime Field) A field F is called a **prime field** if it has no proper subfields.