MATH430 Modern Algebra

Albert Peng

April 27, 2023

Contents

1 Groups and Subgroups

1.1 Binary Operations

Definition. A **binary operation** $*$ on set S is a function $S \times S \to S$, or equivalently, $(a, b) \mapsto a * b$.

Example.

- $+$ is a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- Multiplication is a binary opperation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- Division is <u>not</u> a binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ since we cannot divide by 0.
- $S = \mathbb{R} - \{0\}$ with divison is a binary operation.

Let S be set of function $f : \mathbb{R} \to \mathbb{R}$, where binary operations satisfy

- $(f + g)(x) = f(x) + g(x)$
- $(f\, g)(x) = f(x)g(x)$
- $f \circ g(x) = f(g(x))$

Definition. A binary operation $*$ on S is called **commutative** if $a * b = b * a$, $\forall\, a, b \in S$

Definition. A binary operation $*$ on S is called **associative** if $(a*b)*c = a*(b*c)$, $\forall\, a, b, c \in S$

Thus, associativity also implies

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

Composition of functions is *associative* but not *commutative*. Note that they are not necessarily correlated.

Definition. Let $*$ be a binary operation on S. An element $e \in S$ is called an identity element of S if $e * a = a * e = a$, $\forall\, a \in S$.

Note: If there is an identity element then it is unique.

Proof. Let e, e' be identity elements. $e = e * e' = e'$. ∎

Example.

- $+$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ has 0 as the identity element
- $\cdot$ on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ has 1 as the identity element
- $+$ ono $\mathbb{Z}^{+}$ has no identity element.

1.2 Groups

Definition. A **group** is a set G with a binary operation $*$ such that

1. $*$ is associative
2. $\exists$ an identity element $e \in G$
3. Every element $a \in G$ has an inverse, where $\exists b \in G$ such that $a * b = b * a = e$.

Note that the inverse of a is unique.

Proof. if $b_1, b_2 \in G$ such that $b_1 * a = a * b_1 = e$ and $b_2 * a = a * b_2 = e$, then

$$b_1 * a * b_2 = \begin{cases} b_1 * (a * b_2) = b_1 * e = b_1 \\ (b_1 * a) * b_2 = e * b_2 = b_2 \end{cases} \implies b_1 = b_2$$

■

Denote the inverse of a as a^{-1}, so that $a * a^{-1} = a^{-1} * a = e$ and the group as $(G, *)$

Example.

- $(\mathbb{Z}, +)$ is a group with identity 0 and inverse of a is $-a$
- $(\mathbb{Z}, \cdot)$ is NOT a group, as inverse of 2 does not exist in $\mathbb{Z}$
- $(\mathbb{Q}, \cdot)$ is NOT a group, as inverse of 0 does not exist in $\mathbb{Q}$
- $(\mathbb{Q}\backslash\{0\}, \cdot)$ is a group with identity 1 and inverse of a is $1/a$
- $(M_n(\mathbb{R}), +)$ is a group with identity 0 matrix and inverse of A is $-A$
- $(M_n(\mathbb{R}), \cdot)$ is NOT a group since inverse of A DNE if $\det(A) = 0$
- $(GL_n(\mathbb{R}), \cdot)$ is a group with identity I_n and inverse of A is A^{-1}

Definition. If $(G, *)$ is a commutative group, then it is called an **abelian group**.

Example. Let $*$ be defined by $a * b = ab/2$, then $(\mathbb{Q}^+, *)$ is an abelian group.

1.3 Properties of Groups

Suppose $(G, *)$ is a group.

1. $(a * b)^{-1} = b^{-1} * a^{-1}$
2. $a * b = e \implies b = a^{-1}$
3. Cancellation Law: $a * b = a * c \implies b = c$. $b * a = c * a \implies b = c$
4. $a * x = b$ has unique solution, where $x = a^{-1} * b$
5. $\left(a^{-1}\right)^{-1} = a$

For $n \geq 1, a \in G$, we denote

- $a^n := \underbrace{a * a * ... * a}_{n \text{ times}}$
- $a^0 := e$

- $a^{-n} := \underbrace{a^{-1} * a^{-1} * ... * a^{-1}}_{n\text{times}} = (a^n)^{-1}$
- $a^{n+m} = a^n * a^m$

Example. The group of integers modulo of n is $\mathbb{Z}_n := \{[0], [1], ..., [n-1]\}$. then, $(\mathbb{Z}_n, +)$ is a group with

- identity $= [0]$
- inverse of $[i] = [n-i]$
- $[i] + ([j] + [k]) = ([i] + [j]) + [k]$

Example. $\{1, i, -1, -i\}$ is a group under multiplication.

- identity $= 1$
- every element has an inverse
- multiplication on $\mathbb{C}$ is associative by definition

Notice that $G_1 = \{1, i, -1, -1\}$ and $G_2 = \mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ form a **group isomorphism**, where $f : G_1 \to G_2$, with $f(1) = [0], f(i) = [1], f(-1) = [2], f(-i) = [3]$, and f is one-to-one and onto with respect to group operations.

Definition. Two groups $(G_1, *_1), (G_2, *_2))$ are **isomorphic** if there is a one-to-one and onto map $f : G_1 \to G_2$ such that

$$f(a) *_2 f(b) = f(a *_1 b) \, \forall a, b \in G_1$$

such a function is called **isomorphism**. This is denoted as $(G_1, *_1) \simeq (G_2, *_2)$.

Definition. The **order** of a group, $|G|$ is number of elements of G.

For groups of order 2, $G = \{e, a\}$, there is only ONE way to fill the table.

$*$	e	a
e	e	a
a	a	e

Rows and columns related to e are obvious. In particular, $a * a \neq a$ because cancellation law would imply $a = e$, which cannot be the case.

For groups of order 3, $G = \{e, a, b, c\}$, up to isomorphism, there is only one group.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

For groups of order 4: fact - up to isomorphism, there are two groups.

1.4 Finite Non-abelian Groups

1.4.1 Permutations

Definition. A **permutation** of A is a one-to-one and onto function $\sigma : A \to A$.

Example. Given $A = \{1,2,3,4\}$, we can have $\tau : 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 3$, or equivalently,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

In particular, the number of permutations of a set with n elements $= n!$.

The set of permutations of A with composition of function is a group, denoted by S_A, where

- τ, σ one-to-one and onto $\implies \sigma \circ \tau$ one-to-one and onto
- identity element is the identity map
- $\sigma \in S_A \implies \sigma^{-1} \in S_A$, where

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Here if $A = \{1,2,...,n\}$, let S_n (**Symmetric Groups**) be the permutation of S, $|S_n| = n!$.

$$\begin{aligned} &n = 1\, |S_1 = 1|, S_1 = e \\ &n = 2\, |S_2 = 2| \implies S_2 \text{ abelian} \\ &n = 3\, |S_3| = 6 \implies \text{ not abelian}, \tau \circ \sigma \neq \sigma \circ \tau \end{aligned}$$

S_n not abelian for $n \geq 3$.

Another way of showing elements of S_n

$$n = 6 \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \iff \sigma = \underbrace{(1\ 4\ 6)}_{3-\text{cycle}}\ \underbrace{(2\ 3)}_{2-cycle}(5) = (1\ 4\ 6)(2\ 3) = (3\ 2)(4\ 6\ 1)$$

1.4.2 Dihedral Groups

Let D_n be a group of symmetris of a regular n-gon, where D_n is the set of permutations $\sigma \in S_n$ such that i, j adjacent $\iff \sigma(i), \sigma(j)$ adjacent.

- $D_3 = S_3$
- $D_4 : \sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 4 \notin D_4$, and $\sigma = (1\ 3), (2\ 4), (1\ 2)(3\ 4) \in D_4$

Fact: $|D_n| = 2n$

Suppose $\tau = (1\ 3), \sigma = (1\ 2\ 3\ 4)$ D_n is a group under composition of functions, where $\tau, \sigma \in D_n$

$$\tau(\sigma(i)), \tau(\sigma(j)) \text{ adjacent} \iff \sigma(i), \sigma(j) \text{ adjacent} \iff i, j \text{ adjacent}$$

Now, if ρ is rotation by $2\pi/n$ and τ is reflection with respect to x-axis,

$$D_n = \{e, \rho, \rho^2, ..., \rho^{n-1}, \tau, \tau \circ \rho, ..., \tau \circ \rho^{n-1}\}$$

By convention, if G is an abrbitrary group, we can write ab instead of $a * b$.

1.5 More on Isomorphism Groups

Definition. An operation f is **injective**, or **one-to-one** on a set S if $\forall s_1, s_2 \in S, f(s_1) = f(s_2) \implies s_1 = s_2$.

Definition. An operation f is **surjective**, or **onto** on for $f : X \longrightarrow Y$ if $im(f) = Y$. In other words, $\forall y \in Y, \exists x \in X$ such that $f(x) = y$.

Let there be groups $(G_1, *_1), (G_2, *_2)$. Then isomorphhism $\phi(G_1 \to G_2)$ is one-to-one, onto, and

$$\phi(a *_1 b) = \phi(a) *_2 \phi(b), \exists a, b \in G_1$$

We can say that $G_1 \simeq G_2$, they are isomorphic.

Example. $(M_2(\mathbb{R}), +)$ is isomorphic to $(\mathbb{R}^4, +)$, where

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = (a \ b \ c \ d)$$

Facts:

1. If $\phi : G_1 \to G_2$ is an isomorphism, then $\phi^{-1} : G_2 \to G_1$ is also an isomorphism, where $\phi^{-1}(x *_2 y) = \phi^{-1}(x) *_1 \phi^{-1}(y), \exists x, y, \in G_2$.
2. Isomorphism relationship is an equivalence relation on the set of all groups
   (a) $G \simeq G$. identity map is an isomorphism
   (b) $G_1 \simeq G_2 \implies G_2 \simeq G_1$
   (c) $G_1 \simeq G_2$ and $G_2 \simeq G_3 \implies G_1 \simeq G_3$

Proof. (1) Let $a = \phi^{-1}(x), b = \phi^{-1}(y)$, so $\phi(a) = x, \phi(b) = y$. $x *_2 y = \phi(a) *_2 \phi(b) = \phi(a *_1 b)$

(3) $\phi : G_1 \to G_2, \psi : G_1 \to G_2$

$$\begin{aligned} \psi \circ \phi(a *_1 b) &= \psi(\phi(a *_1 b)) \\ &= \psi(\phi(a) *_2 \phi(b))) \\ &= \psi(\phi(a)) *_3 \psi(\phi(b)) \\ &= \psi \circ \phi(a) *_3 \psi \circ \phi(b) \end{aligned}$$

■

Example.

- $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$ not isomorphic
- *Exercise:* Are $(\mathbb{R} - \{0\}, \cdot)$ and $(\mathbb{C} - \{0\}, \cdot)$ isomorphic?

Proof. If $\phi : \mathbb{R} - \{0\} \to \mathbb{C} - \{0\}$ is an isomorphism, $\underbrace{\phi(a * 1)}_{=\phi(a)} = \phi(a)\phi(1) \implies \phi(1) = 1$. There $\exists a \in \mathbb{R} - \{0\}$ such that $\phi(a) = i$. So $\phi(a^4) = 1 \implies a^4 = 1 \implies a = \pm 1$. Then, $\phi(-1) = i, 1 = \phi(1) = \phi(-1)^2 = i^2 = -1$, so there is a contradiction and it is not isomorphic. ■

1.6 Subgroups

Definition. For group G with non-empty subset $H \subseteq G$ is called a **subgroup** such that

- $e \in H$
- $\forall a \in H, a^{-1} \in H$
- $\forall a, b \in H, ab \in H$

We can also denote this subgroup with $H \leq G$.

Definition. If G is a subgroup, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups are **proper subgroups**. The subgroup $\{e\}$ is the **trivial subgroup** of G. All other subgroups are non-trivial.

Example.

- G and $\{e\}$ are subgroups of G.
- $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
- $(\mathbb{R}^+, +)$ not subgroup of $(\mathbb{R}, +)$
- Subgroups of $\mathbb{Z}_4 : \{[0]\}, \mathbb{Z}_4, \{[0], [2]\}$
- Subgroups of $\mathbb{Z}_5 : \{[0]\}, \mathbb{Z}_5$
- D_n is a subgroup of S_n

Proposition. A non-empty subset H of G is a subgroup if and only if $\forall a, b \in H, \underbrace{ab^{-1}}_{(*)} \in H$.

Proof. If H is a subgroup and $a, b \in H$, then $b^{-1} \in H$, so $ab^{-1} \in H$.

Conversely, if $ab^{-1} \in H$ is satisfied, then since $H \neq \phi$, there exists $a \in H$ and we can set $b = a$ so $aa^{-1} \in H$, so $e \in H$.

If $a \in H$, since $e, a \in H$, by (*), $ea^{-1} \in h \implies a^{-1} \in H$.

If $a, b \in H$, then by ii $b^{-1} \in H$, so $a, b^{-1} \in H$, so $(*)$ gives $a(b^{-1})^{-1} \in H$, so $ab \in H$ ■

1.7 Cyclic Subgroups

For group G with $a \in G$, $H = \{a^n \mid n \in \mathbb{Z}\} \subset G$. H is a subgroup:

- $e \in H$
- $a^n \in H, a^{-n} \in H$
- $a^n, a^m \in H, a^n a^m = a^{n+m} \in H$

We denote $H =< a >$ where it is the subgroup generated by a, and $< a >$ is a **cyclic** subgroup of G.

Note: $< a >$ is a subset of every subgroup of G which contains a.

Example. $\mathbb{Z}_8 = \{[0], [1], [2], ..., [7]\}$.

$$< [2] >=< [0], [2], [4], [6], [8] >$$

$$< [3] >=< [0],[3],[6],[1],[4],[7],[2],[5] >= \mathbb{Z}_8$$
$$< [4] >=< [0],[4] >$$

Example. $G = (\mathbb{Z}, +)$. $< 5 >= \{..., -10, -5, 0, 5, 10, ...\}$

Definition. $a \in G$, the **order** of $a := |< a >|$. If $< a >$ is infinite, we say a has **infinite order**.

Fact:

- If order of a is finite, then order of a = smallest $n \in \mathbb{Z}$ such that $a^n = e$.
- If order of a is infinite, then $a^{n_1} \neq a^{n_2}$ if $n_1 \neq n_2$

Proof. Suppose n is the smallest positive integer such that $a^n = e$, $< a >= \{e, a, ..., a^{n-1}\}$ all distinct elements. Clearly, if $0 \leq i < j \leq n-1$ and $a^i = a^j$, then $e = a^{j-i}$, which is not possible. $\forall m \in \mathbb{Z}$, we have $m = nq + r, 0 \leq r \leq n-1$, so

$$a^m = a^{nq+r} = a^r \in \{e, a, ..., a^{n-1}\}$$

(ii). Since $< a >$ is infinite, there is no $n > 0$ such that $a^n = e$. Now, if $a^i = a^j$, then $a^{j-i} = e, j - i > 0$ is a contradiction. ∎

Example.

- Order of 5 in $(\mathbb{Z}, +)$ infinite
- Order of [5] in $(\mathbb{Z}_6, +)$ is 6
- Order of [5] in $(\mathbb{Z}_{10}, +)$ is 2

G is **cyclic** if $G =< a >$ $\exists a \in G$.

Fact: Every cyclic group is abelian

Proof. If $G =< a >$ and $g_1, g_2 \in G$, then $g_1 = a^{n_1}, g_2 = a^{n_2}$ with $n_1, n_2 \in Z$

$$\begin{cases} g_1 g_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} \\ g_2 g_1 = a^{n_2} a^{n_1} = a^{n_1+n_2} \end{cases} \implies g_2 g_1 = g_1 g_2$$

∎

Example.

- $(\mathbb{Z}, +)$ is cyclic $\mathbb{Z} =< 1 >$.
- $(\mathbb{Z}_n, +)$ is cyclic $\mathbb{Z}_n =< [1] >$
- $S_n, n \geq 3$ is not cyclic and not even abelian.
- $D_n, n \geq 3$ is not cyclic and not even abelian.

Theorem. Suppose G is cyclic.

- If $|G| = \infty$, then $G \simeq (\mathbb{Z}, +)$.
- If $|G| = n$, then $G \simeq (\mathbb{Z}_n, +)$.

Proof. If k is the smallest positive integer such that $a^k = e$, then $G = \{e, a, ..., a^{k-1}\}$ If $|G| = \infty$, then there is no positive k such that $a^k = e$, so $a^{n_1} = a^{n_2}$ implies $n_1 = n_2$. Thus define $\phi : \mathbb{Z} \to G, n \mapsto n^{a^n}$. Clearly ϕ onto, one-to-one, and $\phi(n_1 + n_2) = a^{n_1+n_2} = a^{n_1}a^{n_2} = \phi(n_1)\phi(n_2)$. So ϕ is an isomorphism.

Otherwise if $|G| = n$, then n is the smallest positive integer such that $a^n = e$. Then we can define $\phi : \mathbb{Z}_n \to G, [i] \mapsto a^i, 0 \leq i \leq n-1$. ϕ onto, one-to-one. If $i + j = qn + r$, $0 \leq r \leq n - r$, then $\phi([i] + [j]) = \phi([r]) = a^r$ and $\phi([i])\phi([j]) = a^i a^j = a^{i+j} = a^{qn+r} = a^r$, so ϕ is an isomorphism. ■

Example. Let $H =< (1,2)(3,4,5) >\leq S_5$. For what n is $H \simeq \mathbb{Z}_n$?

$$\sigma^2 = (3,5,4), \sigma^3 = (1,2)(3,4,5)(3,5,4) = (1,2), \sigma^4 = (3,4,5), \sigma^5 = (1,2)(3,5,4), \sigma^6 = e$$

Thus, $H =< \sigma >= \{e, \sigma, ..., \sigma^5\} \simeq (\mathbb{Z}_6, +)$.

Proposition. Every subgroup of a cyclic group is cyclic.

Proof. Let G be cyclic $G =< a >$ and $H \leq G$. If $H = \{e\}$, we are done.

Let k be the smallest positive integer such that $a^k \in H$. Then, to claim $H =< a^k >$, then first for $\subseteq$:

$$a^k \in H \implies < a^k >\subseteq H$$

For $H \subseteq< a^k >$, suppose $a^m \in H$. Divide m by k with $m = kq + r, 0 \leq r \leq k - 1$. Then,

$$a^m = a^{kq+r} = a^{kq}a^r = h \in H \implies a^r = (a^k)^{-q}h \in H$$

Our choice of k implies $r = 0$, so $m = kq$, $a^m = a^{kq} \in< a^k >$ ■

Corollary. All subgroups of $(\mathbb{Z}, +)$ are of the form $< n >, n \in \mathbb{Z}^+$

If $n, m \in \mathbb{Z}$, consider $\{rm + sn \,|\, r, s \in \mathbb{Z}\} \leq (\mathbb{Z}, +)$. By the corollary, there is d such that $\{rm + sn \,|\, r, s \in \mathbb{Z} =< d >\}$ for some positive integer $d \in \mathbb{Z}$.

Definition. The **greatest common divisor** of m and n, $d = gcd(m,n)$ where if $m = p_1^{a_1} \cdots p_t^{a_t}, n = p_1^{b_1} \cdots p_t^{b_t}$. Then $gcd(m,n) = p_1^{\min(a_1,b_1)} \cdots p_t^{(\min(a_t,b_t))}$.

Example. Since $gcd(8, 28) = 4$ with $(-3)8 + (1)24 = 4, \{8r + 28s \,|\, r, s \in \mathbb{Z}\} = \{..., -4, 0, 4, 8, ...\} =< 4 >$

Definition. If $gcd(m,n) = 1$, we say m and n are **relatively prime** or **coprime**. Now if $d = gcd(n,m)$, then $n = n_1 d, m = m_1 d$, $m, n \in Z$ with $gcd(n_1, m_1) = 1$.

Corollary. m, n are relatively prime $\iff \exists r, s \in \mathbb{Z}$ such that $rn + sm = 1$.

Example. Let $G =< a >, |G| = n, G = \{e, a, ..., a^{n-1}\}$. Let $H \leq G, H =< a^m >$. What is $|H|$?

We let $b = a^m, H =< a^m >$. Let $|H| =$ smallest positive k such that $b^k = e$. We want $(a^m)^k = e = a^{mk}$. Thus, $n \,|\, mk$ (n divides mk).

Let $d = gcd(n,m)$ so that $n = n_1 d, m = m_1 d$ with $gcd(m_1, n_1) = 1$. Then $n_1 d \,|\, m_1 dk \implies n_1 \,|\, m_1 k \implies n_1 | k$. So smallest $k = n_1 = \frac{n}{d} = \frac{n}{gcd(n,m)}$, so $|H| = \frac{n}{gcd(n,m)}$.

In particular, $< a^m >= G$ iff $\frac{n}{gcd(m,n)} = n \implies gcd(m,n) = 1$

Example. $G = 6, G = \{e, a, ..., a^5\}$. $| < a^{>} | = 3, | < a^5 > | = 6$

Definition. The **generators** of G is $\{a \in G$ such that $G =< a >\}$

If $|G| = n$ and $G =< a >$, then a^m generates $G \iff \gcd(m, n) = 1$. More generally, for any $a^m \in G, | < a^m > | = \frac{n}{gcd(m,n)}$

Corollary. If G is cyclic of finite order and $H \leq G$, then $|H| \leq |G|$.

Example. Find all generators of $(\mathbb{Z}_q, +)$. $\{[1], [2], [4], [5], [7], [8]\}$

Example. $G = (\mathbb{Z}_{18}, +)$. Find a subgroup of order 6. Let $H \leq G, H =< [m] >$, $|H| = 18/gcd(m, 18) = 6$. Thus, we can have $m = 3, 15$.

Fact: If G is cyclic of order n, $G =< a >$, then $< a^{m_1} >=< a^{m_2} > \iff gcd(m_1, n) = gcd(m_2, n)$

Corollary. If G is cyclic of order n, for any $d|n$, there is eactly one subgroup of order d in G.

Proof. If $H =< a^m >, H = n/gcd(m, n) = d \implies gcd(m, n) = \frac{n}{d}$. For example if $m = \frac{n}{d}$, then $gcd(m, n) = gcd(\frac{n}{d}, n) = \frac{n}{d}$. $| < a^{\frac{n}{d}} > | = d$. Uniqueness follows from the above fact. ∎

Example. Klein 4 Group

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

$< a >= \{e, a\}, < b >= \{e, b\}, < c >= \{e, c\}$.

1.8 Generators

Let $H \leq G$ and $a, b \in G$. Then $< a, b >$ is the subgroup generated by a, b which is the set of all combinations of a, b.

Example. $ab^{-1}a^2b^3 \in< a, b >, (ab^{-1}a^2b^3)^{-1} = (b^{-3}a^{-2}ba^{-1}) \in< a, b >, e = a^0 \in< a, b >$

In general, $\{a_i, i \in I\} \subset G$. This is the subgroup of G generated by $a_i, i \in I$.

Fact: If $H_j, j \in J$ are subgroups of G, then $\cap_{j\in J} H_j$ is a subgroup of G.

- $e \in H_j$ for all j, so $e \in \cap_{j\in J} H_j$.
- If $a, b \in \cap_{j\in J} H_j$ then $a, b \in H_j \; \forall j$, so $ab^{-1} \in H_j$ for all j. So $ab^{-1} \in \cap_{j\in J} H_j$

We can also consider $< a_i, i \in I >=$ the intersection of all subgroups of G which contain $a_i, i \in I$.

Proof. $\subseteq :< a_i, i \in I >\subseteq$ any subgroup of G which contain all the a_i.

$\supseteq :< a_i, i \in I >$ is a subgroup of G and contains all the a_i. ∎

Definition. If G is generated by a finite number of elements, $G =< a_1, ..., G_k >$, then G is called **finitely generated**.

Example. $(\mathbb{Q}, +)$ is not finitely generated. Let $\frac{a_1}{b_1}, ..., \frac{a_n}{b_n} \in \mathbb{Q}$, then

$$H =< \frac{a_1}{b_1}, ..., \frac{a_n}{b_n} >= \{t_1 \frac{a_1}{b_1} + ... + t_n \frac{a_n}{b_n}; t_1, ..., t_n \in \mathbb{Z}\}$$

Let p be a prime number such that $p > b_1, ..., b_n$. Then $\frac{1}{p} \notin H$. If $\frac{1}{p} = \frac{t_1 a_1}{b_1} + ... + \frac{t a_n}{b_n} = \frac{A}{b_1, ...b_n, A \in \mathbb{Z}}$. so $pA = b_1 ... b_n$ but p not divisible $b_1 ... b_m n$.

1.9 Dihedral Group Revisited

Diheral group D_n with $n \geq 3$, with $|D_n| = 2n$. We can have $\rho = (1, 2, ..., n)$ which is a counter-clockwise rotation by $\frac{2\pi}{n}$. μ is a reflection with respect to x-axis, such that $\mu^2 = e$. Then,

$$D_n = \{e, \rho, \rho^2, ..., \rho^{n-1}, \mu, \mu\rho, ..., \mu\rho^{n-1}\}$$

Note that by definition and using inversees, $\mu\rho^i = \rho^{n-i}\mu \forall 1 \leq i \leq n$.

We can also describe this as $D_n =< \rho, \mu >$.

2 Structure of Groups

2.1 Permutation Groups

Definition. $\phi : G \to G'$ is called a **homomorphism** if $\forall a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Example.

- $G \xrightarrow{\phi} G'$, $\phi(a) = e'$ is a homomorphism.
- $Z_n \xrightarrow{\phi} D_n, [i] \mapsto \rho^i$ is a homomorphism. This is one-to-one but not onto.
- $GL_2(\mathbb{R}) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{R}, ad - c \neq 0\}$ group under matrix multiplication.
  $GL_2(\mathbb{R}) \to (\mathbb{R} - \{0\}, \cdot)$.

Proposition. If $\phi : G \to G'$ is a homomorphism, then

1. $\phi(e) = e'$
2. $\phi(a^{-1}) = \phi(a)^{-1}\ \forall a \in G$
3. If $H \leq G$, then $\phi(H) \leq G'$ where $\phi(H) = \{\phi(a) | a \in G\}$.
4. If $K \leq H'$, then $\phi^{-1}(K) \leq G$ where $\phi^{-1}(k) = \{a \in G | \phi(a) \in K\}$

Proof. (1). $\underbrace{\phi(ee)}_{\phi(e)} = \phi(e)\phi(e)$ so $e' = \phi(e)$.

(2). $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$, and $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e) = e'$, so $\phi(a^{-1})$ is inverse of $\phi(a)$.

(3). $H \leq G$ so $e \in H$, so $\phi(e) \in \phi(H) \implies e' \in \phi(H)$.

If $x, y \in \phi(H)$, then there are $a, b \in H$ such that $\phi(a) = x$ and $\phi(b) = y$. So, $xy^{-1} = \phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(H)$.

(4). Exercise ∎

Theorem. **[Cayley's Theorem]**

Let S_A be a group of permutations of set A. Then $\forall$ group G, $\exists$ set A and a one-to-one homomorphism $\phi : G \to S_A$. So, G is isomorphic to $\phi(G)$, and $\phi(G) \leq S_A$.

Example.

- $G = D_n$, $D_n \leq S_n$.
- $G = \mathbb{Z}_n$, then $\mathbb{Z}_n \to S_n$
- $G = GL_2(\mathbb{R})$. If $A \in GL_2(\mathbb{R})$ then $\mathbb{R}^2 \xrightarrow[f_A]{} \mathbb{R}^2$, $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto A \begin{bmatrix} x \\ y \end{bmatrix}$ is one-to-one and ontto so f_A is a permutation of $\mathbb{R}^2$. In addition, $f_{AB} = f_A \circ f_B$, so $GL_2(\mathbb{R}) \xrightarrow{\phi} S_{\mathbb{R}^2}$, $A \mapsto f_A$ iss a group homomorphism. ϕ is one-to-one: If $f_A = f_B$, then $A \begin{bmatrix} x \\ y \end{bmatrix} = B \begin{bmatrix} x \\ y \end{bmatrix}\ \forall x, y \in R$. Then $A = b$

Proof. If $g \in G$, then the function $\lambda_g : G \to G$ has $\lambda_g(x) = gx$.

λ_g one-to-one: If $\lambda_g(x) = \lambda_g(y)$, then $gx = gy$, so $x = y$.
λ_g onto: $\forall y \in g, \lambda_g(g^{-1}y) = gg^{-1}y = y$.

So, $\lambda_g \in S_G$Note that λ_g is <u>not</u> a group homomorphism, as $gxy \neq gxgy$

So, we have the map $\phi : G \to S_G, g \mapsto \lambda_g$.

Now, we want to show that ϕ is one-to-one homomorphism:

ϕ is a homomorphism:

$$\underbrace{\phi(g_1 g_2)}_{\lambda_{g_1,g_2}(x)} = \phi(g_1) \circ \phi(g_2) \implies \lambda_{g_1,g_2}(x) = g_1 g_2(x) = \lambda_{g_1}(g_2 x) = \lambda_{g_1} \circ \lambda_{g_2}(x)$$

ϕ is one-to-one: If $\phi(g_1) = \phi(g_2)$, then $\lambda_{g_1} = \lambda_{g_2}$, so $\forall x \in G$, $\lambda_{g_1}(x) = \lambda_{g_2}(x)$, so $g_1 x = g_2 x \implies g_1 = g_2$ ■

Definition. Let $\phi : G \to G'$ be a homomorphism. The **kernel** of ϕ is

$$ker(\phi) := \{a \in G; \phi(a) = e'\} = \phi^{-1}(\{e'\})$$

Note that since $\{e'\} \leq G', ker(\phi) \leq G$.

Example. $\phi : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto$ [remainder of n/a]. $\ker(\phi) = n\mathbb{Z}$

Proposition. ϕ one-to-one $\iff \ker(\phi) = \{e\}$

Proof. $\implies$: Clear

$\impliedby$: If $\phi(a) = \phi(b)$, then $\phi(a) = \phi(b)^{-1} = e'$. So $\phi(a)\phi(b^{-1}) = e' \implies \phi(ab^{-1}) = e'$, so $ab^{-1} = e \implies a = b$ ■

2.1.1 Odd and even permutation

Definition. A 2-cycle is called a **transposition**

In general, if $(a_1, a_2, ..., a_{m-1}, a_m) \in S_n$, then $(a_1, a_2, ..., a_m) = (a_1, a_m)(a_1, a_{m-1})...(a_1, a_2)$.

Every $\sigma \in S_n$ is a product of transpositions that is not unique

Example. $\sigma = (1, 2, 4)(3, 6) = (1, 4)(1, 2)(3, 6)$

Theorem. If $\sigma \in S_n$, then σ cannot be written both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Let $\sigma = (a_1, b_1) \ldots (a_k, b_k)$. σ is an odd/even permutation if k is odd/even.

In general, $\forall n$, the number of odd permutations and even permutations is the same.

$$A_n := \text{set of even permutations} \subset S_n, \;\; B_n := \text{set of odd permutations} \subset S_n$$

Proof. Let σ be any 2-cycle. Define $\lambda_\tau : A_n \to B_n, \sigma \mapsto \tau_\sigma$.

λ_τ is onto and one-to-one:
Onto: If $\rho \in B_n$, then $\tau\rho \in A_n$ and $\lambda_\tau(\tau\rho) = \underbrace{\tau\tau}_{e}\rho = \rho$

One-to-one: $\tau\sigma_1 = \tau\sigma_2 \implies \sigma_1 = \sigma_2$. Thus, $|A_n| = |B_n|$ ■

Proposition. A_n is a subgroup of order $\frac{n!}{2}$ in S_n.

Proof.
- $e \in A_n$
- $\sigma_1, \sigma_2 \in A_n$ ten $\sigma_1\sigma_2 \in A_n$
- If $\sigma \in A_n, \sigma = (a_1, b_1) \dots (a_k, b_k), \sigma^{-1} = (a_k, b_) \dots (a_1, b_1) \in A_n$

■

A_n is the **alternating group** on n elements.

If $\sigma \in S_n$, we can define

$$sign(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ even} \\ -1, & \text{if } \sigma \text{ odd} \end{cases}$$

$\{1, -1\}$ is a group under multiplication.

Here, $sgn : S_n \to \{1, -1\}$ is a homomorphism with $sign(\sigma_1\sigma_2) = sign(\sigma_1)sign(\sigma_2)$.

Thus, $\ker(sgn) = A_n$

2.2 Finitely Generated Abelian Groups

Direct product of groups Let G_1, G_2 be two groups. The cartesian product of G_1, G_2 is $G_1 \times G_2 = \{(a_1, a_2); a_1 \in G_1, a_2 \in G_2\}$

Group operation on $G_1 \times G_2$ is defined as $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$. Identity $= (e_1, e_2)$. Inverse of $(a_1, a_2) = (a_1^{-1}, a_2^{-1})$.

This ia a group, called the **direct product** of G_1, G_2.

Example. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\underbrace{([0],[0])}_{a}, \underbrace{([0],[1])}_{b}, \underbrace{([1],[0])}_{c}, \underbrace{([1],[1])}_{d}\}$. Here, $a^2 = b^2 = c^2 = e$. So $Z_2 \times Z_2$ not isomorphic to $\mathbb{Z}_4$.

Example. $\mathbb{Z}_2 \times \mathbb{Z}_3 :< ([1],[1]) >= \{(0,0),(1,1),(0,2),(1,0),(0,1),(1,2)\}$. Thus $Z_2 \times Z_3$ is cyclic so $Z_2 \times Z_3 \simeq Z_6$.

Proposition. $Z_m \times \mathbb{Z}_n$ is cyclic (therefore isomorphic to $\mathbb{Z}_{mn}$) if and only if $gcd(m,n) = 1$.

Proof. $\Longleftarrow$ If $gcd(m,n) = 1$, then $\mathbb{Z}_m \times Z_n =< ([1],[1]) >$.

If order of $([1],[1])$ is k,then $([k],[k]) = ([0],[0])$, so $m \mid n$ and $n \mid k$. Since $gcd(m,n) = 1$, we get $nm \mid k$ so $k \geq mn \implies$ order of $([1],[1]) = mn$, so $([1],[1])$ generates the group.

"$\Longrightarrow$": If $gcd(m,n) = d > 1$, then if $([a],[b]) \in \mathbb{Z}_n \times \mathbb{Z}_m$,

$$\frac{nm}{d}([a],[b]) = ([\frac{anm}{d}, \frac{bnm}{d}]) = ([0],[0])$$

and $\frac{nm}{d} < nm$, so G is not generated by only $([a],[b])$ so G is not cyclic. ■

More generally, for $G_1, ..., G_k$, the direct product is

$$G_1 \times \ldots \times G_k = \{(a_1, ..., a_k) | a_i \in G_i, 1 \leq i \leq k\}$$

with natural rules of operations, identity, and inverses. Then, $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k} \simeq \mathbb{Z}_{n_1 \ldots n_k}$ if $gcd(n_i, n_j) = 1 \forall i \neq j$.

Proposition.

- $G_1 \times G_2 \simeq G_2 \times G_2$. $\phi : G_1 \times G_2 \to G_2 \times G_1, (a, b) \mapsto (b, a)$ is an isomorphism.
- If $H_1 \leq G_1$ and $H_2 \leq G_2$, then $H_1 \times H_2 \leq G_1 \times G_2$.

Example. $\mathbb{Z}_2 \times \mathbb{Z}_2$. $H = \{([0], [0]), ([1], [1])\} \leq \mathbb{Z}_2 \times \mathbb{Z}_2$ is not of the form $H_1 \times H_2$

Proposition. $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ is cyclic if and only if $\gcd(n_i, n_j) = 1$,$i \neq j$

2.3 More on Finitely Generated Abelian Groups

Theorem. Every finitely generated abelian group is isomorphic to

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}} \times \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{m \text{ times}}$$

where p_i are prime numbers, $n_i \geq 1$ where p_i not necessarily distinct.

Example. Find, up to isomorphism, all abelian groups of order 72.

Notice that abelian groups of order 8 are $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Abelian grous of order 9 up to isomorphism are $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$. Thus, there are $3 \times 2 = 6$ groups.

Corollary. if G is abelian of order n and $m \mid n$ then G has a subgroup of order m. Then G has a subgroup of order m.

<u>Remark:</u> You can show that A_4 has no subgroup of order 6.

Proof. If $G =< a >$ is cyclic with $|G| = n$, $m \mid n$,

$$| < a^{\frac{n}{m}} > | = \frac{n}{gcd(\frac{n}{m}, n)} = \frac{n}{\frac{n}{m}} = m$$

If G is arbitrary by the theorem but abelian, $G = \mathbb{Z}_{p_1^{n_1}} \times \ldots \times \mathbb{Z}_{p_k}^{n_k}$, then $m = p_1^{m_1} \ldots p_k^{m_k}$.

Since $\mathbb{Z}_{p_i^{n_i}}$ cyclic, and since $p_i^{m_i} \mid p_i^{n_i}$, $\mathbb{Z}_{p_i^{n_i}}$ has a subgroup H_i of order $P_i^{m_i}$. Then $H_1 \times \ldots \times H_k \leq G$ and has order $P_1^{m_1} \times \ldots \times P_k^{m_k} = m$. ∎

2.4 Cosets

Let $H \leq G$. We say $a \sim b$ if and only if $a^{-1}b \in H$

- Reflexive: $a^{-1}a = e \in H$
- Symmetric: $a^{-1}b \in H \implies (a^{-1}b)^{-1} = b^{-1}a \in H$
- Transitive: $a^{-1}b, b^{-1}c \in H \implies ac^{-1} \in H$

So, we get a partition of G as the disjoint union of equivalence class.

Definition. Let $a \in G$. The equivalence class containing a is aH, the **left coset** of H is:

$$\{x \in G | a \sim x\} = \{x \in G | a^{-1}x = h \in H\} = \{x \in G \mid x = ah, h \in H\} = aH$$

Example. $G = S_3 = \{e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\} = \{e, \tau_1, \tau_2, \tau_3, \sigma, \sigma^2\}$ Here, $H = \{e, \sigma, \sigma^2\} \leq S_3$. Then, the left cosets of H are

- $eH = \sigma H = H = \sigma^2 H = \{\sigma^2, e, \sigma\} = H$
- $\tau_1 H = \{\tau_1, \tau_1\sigma, \tau_1\sigma^2\} = \{\tau_1, \tau_2, \tau_3\} = \tau_2 H = \tau_3 H$

Proposition.

- $aH = bH \iff a \sim b$
- $a \in aH$
- $aH = H \iff a \in H$
- aH is a subgroup of $G \iff aH = H$

Proof. If $aH \leq G, e \in aH$. So $e = ah \implies a^{-1} \in H \implies a \in H$, so $a \in H \implies ah = H$ ■

Example. Let $G = (\mathbb{Z}, +)$. $H =< 5 >= \{5n | n \in \mathbb{Z}\}$. All the left cosets of H can be given by

- $0 + H = \{5n | n \in \mathbb{Z}\} = 5 + H$
- $1 + H = \{5n + 1 | n \in \mathbb{Z}\} = 6 + H$
- $2 + H = \{5n + 2 | n \in \mathbb{Z}\} = 7 + H$
- $3 + H = \{5n + 3 | n \in \mathbb{Z}\} = 8 + H$
- $4 + H = \{5n + 4 | n \in \mathbb{Z}\} = 9 + H$

Example. Let $G = (\mathbb{R}, +)$, $H = (\mathbb{Z}, +) \leq G$. The left coset can be given by $r + \mathbb{Z}, r \in \mathbb{R}$. In this case, there are infinitely many distinct left cosets where $0 < x < y < 1$, $x + \mathbb{Z} \neq y + \mathbb{Z}$.

Theorem.

1. If $H \leq G, |H| = m$, then every left coset of H has m elements.
2. **[Lagrange's Theorem]** If $H \leq G$ and $|G| = n$, then $|H| \bigm| |G|$

Proof. (1) Let aH be a left coset, then $\phi : H \to aH, h \mapsto ah$ clearly shows ϕ is one-to-one and onto. $ah_1 = ah_2 \implies h_1 = h_2$. Thus, $|H| = |aH|$.

(2) Let $H = m$ and suppose H has r distinct left cosets $a_1H, ..., a_rH$. Then, $|a_iH| = |H| = m$ and $G = \cup_{i=1}^r a_iH$. So, $\underbrace{G}_{n} = \sum_{i=1}^n |a_iH| = rm$, so $m \bigm| n$. ■

Corollary. If $|G| = n$ and $a \in G$, then order of a divides n

Proof. Let $m = ord(n)$ and $H =< a > -\{e, a, ..., a^{m-1}\}.Som = |H| \bigm| |G| = n$ ■

Corollary. If $|G| = p$ where p is a prime number, then G is cyclic.

Proof. Pick $e \neq a \in G$, then $1 \neq ord(a) \bigm| p$, so $ord(a) = p, | < a > | = p \implies < a >= G$. ■

Definition. If $H \leq G$, the number of distinct left cosets of H in G is denoted by $(G : H)$, the **index** of H in G.

If G is a finite group $(G : H) = \frac{|G|}{|H|}$.

2.4.1 Right Cosets

We can have similar definitions with right cosets. For $H \leq G$,

$$a \sim' b \iff ba^{-1} \in H$$

Equivalence class containing $a = \{x \in G \mid a \sim' x\} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h \forall h \in H\} = \{x \in G \mid x = ha \forall h \in H\} = Ha$

Proposition.

- $Ha = H \iff a \in H$
- $Ha = Hb \iff ab^{-1} \in H$
- $Ha = Hb, Ha \cap Hb = \emptyset \forall a, b \in G$
- $Ha \leq G \iff a \in H$
- If $|H| < \infty$, then $|Ha| = |H|$.

Example. $S_3 = \{e, \tau_1, \tau_2, \tau_3, \sigma, \sigma^2\}$. $H \leq S_3$, $H = \{e, \tau_1\}$

All right cosets can be given by

- $He = \{e, \tau_1\}$
- $H\tau_1 = \{\tau_1, e\}$
- $H\tau_2 = \{\tau_2, \sigma^2\}$
- $H\tau_3 = \{\tau_3, \sigma\}$
- $H\sigma = \{\tau_3, \sigma\}$
- $H\sigma^2 = \{\sigma^2, \tau_2\}$

Example. $G = S_3, H = \{e, \sigma, \sigma^2\} \leq S_3$.

Left Cosets:

- $eH = \sigma H = \sigma^2 H = H$
- $\tau_1 H = \tau_2 H = \tau_3 H = \{\tau_1, \tau_2, \tau_3\}$

Right Cosets:

- $He = H\sigma_1 = H\sigma^2 = H$
- $H\tau_1 = H\tau_2 = H\tau_3 = \{\tau_1, \tau_2, \tau_3\}$.

In this specific case, every left coset is a right coset.

Example. $H = 5\mathbb{Z} \leq \mathbb{Z}$. Left cosets of H are given by $5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$. The right cosets are $5\mathbb{Z}, 5\mathbb{Z} + 1, 5\mathbb{Z} + 2, 5\mathbb{Z} + 3, 5\mathbb{Z} + 4$.

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

$$aH = Ha \, \forall a \in G$$

3 Homomorphisms and Factor Groups

3.1 Factor Group

Definition. A subgroup H of G is called a **normal** subgroup if $aH = Ha$ for every $a \in G$, denoted as $H \trianglelefteq G$.

Example.

- $\{e, \sigma, \sigma^2\} \trianglelefteq S_3$
- $\{e, \tau_1\} \ntrianglelefteq S_3$
- $A_n \trianglelefteq S_n$
- Every subgroup of an abelian group is normal.
- If G is finite and $H \leq G$ is of index 2, then H is normal.

Proof. For aH if $a \in H, aH = Ha = H$. Otherwise if $a \notin H$, then $aH \cap H = \emptyset$, $|aH| = |H| = \frac{|G|}{2}$. Also, $Ha \cap H = \emptyset, |Ha| = |H| = \frac{|G|}{2}$, so $Ha = \{b \in G | b \notin H\} = Ha$ ∎

Proposition. If $\phi : G \to G'$ is a homomorphism, then $\ker(\phi) \trianglelefteq G$.

Proof. Prove that for $a \in G, a\ker(\phi) = \ker(\phi)a$, where $\ker(\phi) = \{b \in G | \phi(b) = e'\}$

$\subseteq$: If $b \in \ker(\phi)$, then $\phi(aba^{-1}) = \phi(a)\underbrace{\phi(b)}_{e'}\phi(a^{-1}) = e'$.

So, $aba^{-1} \in \ker(\phi)$, let $b' = aba^{-1} \in \ker(\phi)$, then $ab = b'a \in \ker(\phi)a$. The $\supseteq$ direction is similar ∎

Example. $\phi : S_n \to \{1, -1\}, \phi(\sigma) = sgn(\sigma), \ker(\phi) = A_n$.

Proposition. H is normal $\iff aHa^{-1} = H$ for all $a \in G$.

Proof. $\Longleftarrow$: If $a \in$,we show $aH = Ha$.

$aH \subseteq Ha$: If $h \in H$, then $ah^{-1}a \in H$, so $aha^{-1} = h'$ for some $h' \in H$. So, $ah = h'a \implies ah \in Ha$

$Ha \subseteq aH$: If $h \in H$, then $a^{-1}Ha = H$ by assumption so $a^{-1}ha = h^{-1} \in h$

$\implies$: Exercise ∎

Proposition. H is normal in $G \iff aHa^{-1} \subset H$ for every $a \in G$. (This is an alternative to the proposition above)

Proof. $\implies$: clear

$\Longleftarrow$ We show $H \subset aHa^{-1}$ for every $a \in G$. We have $a^{-1}H(a^{-1})^{-1} \subset H$, so $a^{-1}Ha \subseteq H$. So for any $h \in H, a^{-1}ha = h' \in H$. So $h = ah'a^{-1} \implies h \in aHa^{-1}$. ∎

Remark: $aHa^{-1} \leq G$ for any $a \in G$.

- $e = aea^{-1} \in aHa^{-1}$

- If $aha^{-1} \in aHa^{-1}$, then $(aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$.
- If $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1}$, then $(ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}$.

For $5\mathbb{Z} \leq \mathbb{Z}$, with left cosets $a = \{5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4\}$. Here, the group operation on A is $(a+5\mathbb{Z}) * (b+5\mathbb{Z}) = (a+b)+5\mathbb{Z}$. But can we always do this:

$H \leq G$. Let A be set of left cosets of H in G, such that $(aH)(bH) = abH$? Is this a group operation?

- Associativity: $(aHbH)cH = abHcH = (ab)cH = a(bc)H = (aH)(bcH) = aH(bHcH)$. This works.
- Identity: $(eH)(aH) = eaH = aH$
- Inverse: $(a^{-1}H)(aH) = (aH)(a^{-1}H) = eH$

However, this is <u>not</u> a group operation because this may not be well defined.

From previous sections, we had left cosets of $H = \{e, \tau_1\} \leq S_3$:

- $eH = \tau_1 H = H = \{e, \tau_1\}$
- $\tau_2 H = \sigma H = \{\tau_2, \sigma\}$
- $\tau_3 H = \sigma^2 H = \{\tau_3, \sigma^2\}$.

Here, $(\tau_2 H)(\tau_2 H) = \tau_2^2 H = eH = H$ but $(\sigma H)(\sigma H) = \sigma^2 H \neq H$, while $\tau_2 H = \sigma H$

Definition. An operation if **well-defined** if $aH = a'H$ and $bH = b'H \implies abH = a'b'H$

<u>Fact:</u> If $H \leq G$, then the operation

$$(aH)(bH) = (ab)H$$

is well defined (and therefore is a group operation on the set of left cosets of H) if and only if $H \trianglelefteq G$.

Proof. First, suppose $H \trianglelefteq G$. If $aH = a'H$ and $bH = b'H$, then $a^{-1}a', b^{-1}b' \in H$. We want to show that $abH = a'b'H$ (or therefore, $b^{-1}a^{-1}a'b' \in H$.)

Let $h_1 = a^{-1}a', h_2 = b^{-1}b'$. Then $b^{-1}a^{-1}a'b' = b^{-1}h_1b' = b^{-1}h_1bh_2 = (b^{-1}h_1b)h_2 \in H$, so $abH = a'b'H$.

Next, suppose the operation is well-defined. To show $H \trianglelefteq G$, we show $aha^{-1} \in H$ for every $a \in G, h \in H$.:

We have $hH = eH, a^{-1}H = a^{-1}H$. So,

$$(hH)(a^{-1}H) = (eH)(a^{-1}H) \implies (ha^{-1})H = a^{-1}H \implies \left(a^{-1}\right)^{-1} ha^{-1} \in H \implies ah^{-1}a \in H$$

∎

Definition. If $H \trianglelefteq G$, operation $(aH)(bH) = abH$ on the set of left cosets is a group operation, denoted as G/H, the **factor group of** G **by** H.

Example. $5\mathbb{Z} \trianglelefteq \mathbb{Z}$ then $\mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}_5$

Proposition.

1. If $N \trianglelefteq G$, then there is a natural onto homomorphism $\phi : G \to G/N, \phi(a) = aN$, where

$$\ker \phi = \{a \in G | \phi(a) = N\} = \{a \in G | aN = N\} = N$$

Corollary. Converse of Lagrange's Theorem is not true. For example, A_4 has no subgroup of order 6.

Proof. If H is a subgroup of order 5 in A_4, then $(A_4 : H) = 2$. So H is normal. If we look at the factor grouo A_4/H, $|A_4/H| = 2 \implies \forall \sigma \in A_4, (\sigma H)(\sigma H) = eH \in A_4/H$. Hence $\sigma^2 H = H$, so $\sigma^2 \in H \; \forall \sigma \in A_4$. However, in A_4, $|H| \geq 8$ so this is not possible. ■

Proposition. If $\phi : G \to G'$ is a homomorphism, then

$$G/\ker \phi \simeq im(\phi)$$

$(\ker(\phi) \trianglelefteq G, im(\phi) = \phi(G) \leq G')$

Proof. Define $\psi : G/\ker(\phi) \to im(\phi)$ by $\psi(a \ker(\phi)) = \phi(a)$. This is well-defined because if $a \ker \phi = b \ker \phi$, then $a^{-1}b \in \ker(\phi) \implies \phi(a^{-1}b) = e' \implies \phi(a)^{-1}\phi(b) = e'$, so $\phi(b) = \phi(a)$.

ψ is clearly a homomorphism: $\psi(a \ker(\phi) b \ker(\phi)) = \psi(ab \ker(\phi)) = \phi(ab) = \phi(a)\phi(b) = \psi(a \ker(\phi))\psi(b \ker(\phi))$.

Then, ψ onto: For any $\phi(a), \psi(aN) = \phi(a)$. Meanwhile ψ one-to-one: If $\psi(a \ker \phi) = \psi(b \ker \phi)$, then $\phi(a) = \phi(b) \implies \phi(a^{-1}b) = e'$, so $a^{-1}b \in \ker \phi \implies a \ker \phi = b \ker \phi$. ■

Example. If $\phi : G \longrightarrow G'$ is a homomorphism which is not trivial (not every $g \in G$ is sent to e') with $|G'| = 15, |G| = 18$, what is $|\ker \phi|$?

Known: $18 = |G|/|\ker(\phi)| = |im(\phi)|$

Example. Factor groups:

- $G/G \simeq \{e\}$
- $G/\{e\} \simeq G$
- $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n . \phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n \implies \mathbb{Z}/\ker \phi \simeq im(\phi) \implies \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.
- $\mathbb{Z} \times \mathbb{Z}/ < (1,1) >$

For group G with $N \trianglelefteq G$, the group structure of G/N is $aNbN = abN$. The order is $|G/N| = (G : N)$, the index of N with G.

Example. $\mathbb{Z}_{12}/\langle[4]\rangle$ has $\left|\mathbb{Z}_{12}/\langle[4]\rangle\right| = \frac{12}{3} = 4$. Here, the order is not 2 so $\mathbb{Z}_{12}/N$ is not $\mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_{12}/N \sim \mathbb{Z}_4$.

Proposition. If G is cyclic and $N \trianglelefteq G$, then G/N is cyclic.

Proof. If $G = \langle a \rangle$, then show that G/N is generated by aN. If bN is given, then $b = a^m$ for some m, so $bN = a^m N = (aN)^m$. ■

Example. $\mathbb{Z} \times \mathbb{Z}/\langle(1,1)\rangle \simeq \mathbb{Z}$. Then, $(a_1, b_1) \sim (a_2, b_2) \iff a_1 - a_2 = b_1 - b_2$.

To show this, define $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $\phi(a,b) = a - b$. Then, since

- ϕ is homomorphism
- ϕ onto: If $n \in \mathbb{Z}$, then $\phi(n, 0) = n$.
- $\ker \phi = \{(a, b) | a - b = 0\} = \langle (1, 1) \rangle$

Together, this implies that $\mathbb{Z} \times \mathbb{Z} / \langle (1, 1) \rangle \simeq \mathbb{Z}$, where $\ker \phi = \langle (1, 1) \rangle, im(\phi) = \mathbb{Z}$.

Example. $\mathbb{Z} \times \mathbb{Z} / \langle (2, 1) \rangle \simeq \mathbb{Z}$.

Notice that $G = \{\frac{a}{2} | a \in \mathbb{Z}\} \leq \mathbb{Q}$. Then we can define $\psi : G \to \mathbb{Z}, g \mapsto 2g$ as a homomorphism that is clearly one-to-one and onto. Thus, ψ is clearly an isomorphism.

Then, define $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $\phi((a, b)) = a - 2b$. Then,

- ϕ homomorphism
- ϕ onto: If $n \in \mathbb{Z}, \phi((n, 0)) = n$.
- $\ker \phi = \{(a, b) | a - 2b = 0\} = \langle (2, 1) \rangle$

Together, this implies $\mathbb{Z} \times \mathbb{Z} / \langle (2, 1) \rangle \simeq \mathbb{Z}$.

Example. $\mathbb{Z} \times \mathbb{Z} / \langle (2, 2) \rangle \simeq \mathbb{Z} \times \mathbb{Z}_2$.

Define $\phi((a, b)) = (a - b, 0)$ if a even and $(a - b, 1)$ is a is odd. Then,

- ϕ homomorphism
- ϕ onto: If $(n, 0) \in \mathbb{Z} \times \mathbb{Z}_2$, then $\phi(2n, n) = (n, 0)$. If $(n, 1) \in \mathbb{Z} \times \mathbb{Z}_2$, then $\phi(2n+1, n+1) = (n, 1)$.
- $\ker \phi = \{(a, b) | a - b = 0, a \text{ even}\} = \langle (2, 2) \rangle$.

3.2 Simple Group

Definition. A group G is **simple** if G has no proper, non-trivial normal group.

Example. Any finite group of order is simple.

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

3.2.1 Center of Groups

Definition. We define for a group G its center as

$$Z(G) := \{z \in G \mid zg = gz \, \forall g \in G\}$$

Proposition. $Z(G)$ is a normal subgroup of G.

Proof. First, Show $Z(G)$ is a subgroup:

- $eg = ge \forall g \in G \implies e \in Z(G)$
- $z_1, z_2 \in Z(G) \implies z_1 z_2 g = z_1 g z_2 = g z_1 z_2$, so $z_1 z_2 \in Z(G)$.
- If $z \in Z(G), zg^{-1} = g^{-1} z \forall g$, so $(zg^{-1}) = (g^{-1}z)^{-1} \implies gz^{-1} = z^{-1} g \implies z^{-1} \in Z(g)$

Then, to show $Z(G) \trianglelefteq G$: If $g \in G, z \in Z(G)$, then $gzg^{-1} = gg^{-1}z = z \in Z(G)$. ■

Proposition. Group G is abelian $\iff Z(G) = G$.

Example. $Z(GL_n(\mathbb{R})) = \{rI_n \mid r \in \mathbb{R}\}$

3.2.2 Commutator of Groups

Definition. Let G be a group with $a, b \in G$. Then the **commutator** of a, b is defined as

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

Properties:

- $[a, b] = e \iff ab = ba$
- $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$

Definition. The **commutator subgroup** G' is the subgroup generated by all commutators

$$G' = \langle [a, b] \mid a, b \in G \rangle = \{[a_1, b_1], ..., [a_n, b_n]\}$$

Proposition. $G' \trianglelefteq G$

Proof. To show $g[a, b]g^{-1} \in G$,

$$g[ab]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}] \in G'$$

Proposition. G/G' abelian

Proof. The is to prove $aG'bG' = bG'aG'$.

$$b^{-1}a^{-1}ba = [b^{-1}, a^{-1}] \in G' \implies (ab)^{-1}(ba) \in G' \implies abG' = baG'$$

■

Proposition. If $N \trianglelefteq G$ and G/N abelian, $G' \leq N$.

Exercise: Let $G = S_3$. What is G'?.

We know A_3 has index 2 in S_3, so $A_3 \trianglelefteq S_3$, and S_3/A_3 has two elements so $S_3/A_3 \simeq \mathbb{Z}_2$, so it is abelian, so $G' \leq A_3$.

Check other side, then we get $G' = A_3$

3.3 Groups Acting on Sets

Definition. Let G be a group acting on sets. Then a set X is a G**-set** or G **acts on** X if there is a function

$$G \times X \longrightarrow X, \qquad (g, x) \mapsto g \cdot x$$

such that

- $e \cdot x = x \, \forall x \in X$
- $g_2 \cdot (g_1 \cdot x) = (g_2 g_1) \cdot x \, \forall x \in X, g_1, g_2 \in G$.

Proposition. If X is a G-set, then the function $\sigma_g : X \to X$, $\sigma_g(X) = g \cdot x$ is one-to-one and onto. Thus, σ_g is permutation of X, where $\sigma_g \in S_x$.

Proof. 1-to-1: If $g \cdot x = g \cdot y$, then $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \implies e \cdot x = e \cdot y \implies x = y$.

Onto: If $y \in X$, then let $x = g^{-1} \cdot y \in X$. Then, $g \cdot x = g \cdot (g^{-1} \cdot y) = e \cdot y = y$. ■

Proposition. The function $\phi : G \to S_X, \phi(g) = \sigma_g$ is a group homomorphism.

Proof. If $g_1, g_2 \in G, \phi(g_1 g_2)(x) = \sigma_{g_1, g_2}(x) = (g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

Also, $(\phi(g_1) \cdot \phi(g_2))(x) = \phi(g_1)(\phi(g_2) \cdot x) = g_1 \cdot (g_2 \cdot x)$. They are equal and form a homomorphism. ■

Example.

- Let $G = GL_n(\mathbb{R}), X = \mathbb{R}^n$. If $A \in GL_n(\mathbb{R}), v \in \mathbb{R}^n$ then we can define group action $A \cdot v = Av$ so that $I \cdot v = v \, \forall v$, $(AB)v = A(Bv)$.
- Trivial action: For some groups G, X, $g \cdot x = x, \forall g \in G, x \in X$
- S_n acting on $\{1, ..., n\}$ is a group action.
- Group G acting on itself by multiplication is a group action: $X = G, g \cdot x := gx$. Then, $e \cdot x = ex = x$ and $(g_1 g_2)x = g_1(g_2 x)$.
- Group G acting on itself by conjugation is a group action: $X = G, g \cdot x := gxg^{-1}$. Then, $e \cdot x = exe^{-1} = x$. Meanwhile, $(g_1 g_2) \cdot x = g_1 g_1 x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1}$ and $g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1}$. Thus they are equal.

Definition. Let G act on X then for any $x \in X$, we define the **isotropy group** as

$$G_x := \{g \in G \,\big|\, gx = x\}$$

Proposition. If X is a G-set, then $\forall x \in X, G_x \leq G$.

Proof.
- $e \in G_x : ex = x$
- If $g_1, g_2 \in G_x$, then $g_1 x = x, g_2 x = x \implies (g_1 g_2)x = g_1(g_2 x) = g_1 x = x \implies g_1 g_2 \in G$.
- If $g \in G_x$, then $gx = x$. Then $g^{-1} g x = g^{-1} x \implies g^{-1} x = x \implies g^{-1} \in G_x$.

■

Definition. [**Orbit**] If G acts on X and $x \in X$, then **orbit** of X is

$$Gx := \{gx \,\big|\, g \in G\} \subset X$$

Proposition. If x and y are in the same orbit, we write $x \sim y$. In fact, this is an equivalence relationship, where $y = gx \exists g \in G$

- $x \sim x : x = ex$
- $x \sim y \implies y \sim x : y = gx \implies g^{-1} y = g^{-1} g x = x$, so $y \sim x$
- Transitive: If $y = gx, z = g' y$, then $z = g' g x = (g' g)x \implies z \sim x$.

Theorem. If G acts on X and $x \in X$, then

$$|Gx| = (G : G_x)$$

where Gx is the orbit of x and $(G : G_x)$ is the number of left cosets of G_x.

Proof. Define ϕ : cosets of G_x in $G \longrightarrow G_x$, where $\phi(aG_x) = a \cdot x$, $a \in G$.

- ϕ well-defined: $aG_x = bG_x \implies a^{-1}b \in G_x \implies a^{-1}bx = x \implies ax = bx$.
- ϕ is 1-to-1: $bx = ax \implies a^{-1}bx = x \implies ab^{-1} \in G_x \implies bG_x = aG_x$.
- ϕ onto: $\phi(aG_x) = ax$

Thus, $(G : G_x) = |Gx|$ ■

Definition. For group G acting on X, define $X_G := \{x \in X \mid g \cdot x = x \forall g \in G\} \subseteq X$. Note that $x \in X_G$ iff the orbit of x has only one element.

Theorem. If G is a group with $|G| = p^n$ for prime p and X is a G-set, then

$$|X| \equiv |X_G| \mod p$$

Proof. Let $Gx_1, ..., Gx_r$ be all distinct orbits with more than one element. then,

$$|X| = |X_G| + \sum_{i=1}^{r} |Gx_i| = |X_G| + \sum_{i=1}^{r} (G : G_{x_i})$$

Recall that $|Gx_i| > 1$ and G is finite, so $(G : G_{x_i}) = \frac{|G|}{|G_{x_i}|} = \frac{p^n}{|G_{x_i}|} > 1 \implies |G_{x_i}|$ is a multiple of p.

Then, $p \mid (G : G_{x_i}) \forall 1 \leq i \leq r \implies p \mid \sum_{i=1}^{r} (G : G_{x_i}) \implies |X| \equiv |X_G| \mod p$ ■

Example. Suppose D_4 is acting on $\{1, 2, 3, 4\}$. $|D_4| = 8$ and $p = 2$. This means that $|X|, |X_G|$ must be both odd or both even.

Example. If $\mathbb{Z}_{11}$ is acting nontrivially on X and X and $|X| = 20$, what is $|X_G|$?
Since action is non-trivial, $|X_G| \neq 20$ so it has to be the case that $|X_G| = 9$.

Theorem. **[Cauchy's Theorem]** If $p \mid |G|$, then G has a subgroup of order p, equivalently G has an element of order p.

Proof. Let $X = \{(g_1, .., g_p) \mid g_1, ..., g_p \in G, g_1 ... g_p = e\}$. Then $|X| = ||G| \times \ldots \times |G| = |G|^{p-1} \implies p \mid |x|$.

Then, let $G = \mathbb{Z}_p$ act on X by shifting so that $i \cdot (g_1, ..., g_p) = (g_{i+1}, ..., g_i)$. To verify that this is a group action, $0 \cdot (g_1, ..., g_p) = (g_1, ..., g_p)$ and $(i + j) \cdot (g_1, ..., g_p) = i \cdot (j \cdot (g_1, ..., g_p))$.

Since $|G| = |\mathbb{Z}_p| = p$, we get $|X| \equiv |X_G| \mod p$, where

$$X_G = \{(g_1, ..., g_p) \in X \mid i \cdot (g_1, ..., g_p) = (g_1, ..., g_p), 0 \leq i \leq p - 1\} = \{(a, ..., a) \mid a^p = e\}$$

Since $p \mid |X|$, we have $p \mid |X_G| \implies |X_G| \geq p$, so $\exists (a, ..., a) \in X_G, a^p = e, a \neq e$. ■

Remark:

1. If G is abelian and $m \mid |G|$, then G has a subgroup of order m.
2. $|A_4| = 12$, but A_4 has no subgroup of order 6.
3. If $p = 2$, then any group with even number of elements has an element of order 2, and $a^2 = e \implies a = a^{-1}$

Corollary. If $|G| = p^n$ with p prime, then $Z(G) \neq \{e\}$.

Proof. Let $X = G$ and let G act on X by conjugation: $g \cdot x = gxg^{-1}$.

$$X_G = \{x \in X \mid g \cdot x = x \forall g\} = \{x \in G \mid gxg^{-1} = x \forall g \in G\} = \{x \in G \mid gx = xg\} = Z(G)$$

Then by theorem,

$$\begin{cases} |X| \equiv |X_G| \mod p \\ p \mid |X| \end{cases} \implies \begin{cases} p \mid |X_G| \\ e \in X_G, \text{ so } 1 \leq |X_G| \end{cases} \implies |X_G| \geq p, \text{ so } Z(G) \neq \{e\}$$

■

Corollary. If $|G| = p^2$, then G is abelian. So, $G \simeq \mathbb{Z}_{p^2}$, or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. From previous corollary, it is clear that $|Z(G)| > 1$. Since $Z(G) \leq G, |Z(G)| \mid p^2 \implies |Z(G)| = p$ or $|Z(G) = p^2|$ ■

4 Rings and Fields

4.1 Rings and Fields

Definition. A **ring** is a set R with 2 binary operations $+$(addition) and $\cdot$(multiplication), denoted as $(R, +, \cdot)$ such that

- $(R, +)$ is an abelian group, with identity 0.
- $\cdot$ is associative
- Distributivity holds: $(a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$

Example.

- $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ are rings.
- $(M_n(\mathbb{R}), +, \cdot)$ is a ring.
- $(2\mathbb{Z}, +, \cdot)$ is a ring.
- $(\mathbb{Z}_n, +, \cdot)$ is a ring with $\cdot$ operation being $[a] \cdot [b] = [\text{remainder of } ab]$.

Properties of Rings.

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(ab)$
3. $(-a)(-b) = ab$

Proof. (1). $0 \cdot a = (0 + 0) \cdot a \implies 0 = 0\dot{a}$.

(2). $(-a) \cdot b + a \cdot b = (a - a) \cdot b = 0 \implies (-a) \cdot b = -(a \cdot b)$

(3). $(-a)(-b) = -(-ab) = ab$ ■

Definition. Let $(R, +, \cdot)$ be a ring. Then

- R is a **commutative ring** if $ab = ba \forall a, b$
- R is a **ring with unity** if it has a multiplicative identity, where $a1 = 1a = a\, \forall a$
- R is a **division ring** if R has unity and every non-zero a has a multiplicative inverse, where $a \neq 0 \in R \implies \exists b \in R$ such that $ab = ba = 1$
- R is a **Field** if it is a commutative division ring.

Example.

- *Commutative Ring:* $(\mathbb{Q}, +, \cdot)$ is commutative but $(M_n(\mathbb{R}), +, \cdot)$ is not.
- *Ring with Unity:* $(M_n(\mathbb{R}), +, \cdot)$ has unity but $(\mathbb{Z}_2, +, \cdot)$ has no unity.
- *Division Ring:* $(\mathbb{Q}, +, \cdot)$ is a division ring but $(\mathbb{Z}, +\cdot)$ is not.
- *Field:* $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ are fields.

Definition. A element a in ring R is a **unit** if it has a multiplicative inverse, $\exists b \in R$ such that $ab = ba = 1$.

<u>Remark</u>: A unity is *unique* if it exists.

Example. $R = \{a + bi + cj + dk \mid i, j, k, 1 \text{ follow quarternion group}\}$ is a division ring but not a field.

Definition. If R is a ring and $a, b \in R$ are non-zero but $ab = 0$, then a, b are called **zero-divisor**.

Proposition. A unit in R is never a zero-divisor.

Example. $\mathbb{Z}_n$ is a ring. Then for $\mathbb{Z}_6$, $[2], [3], [4]$ are zero-divisors. $[1], [5]$ are units.

Proposition. More generally in Z_n, with $1 \leq m \leq n - 1$,

$$[m] \text{ is a unit } \iff gcd(m, n) = 1$$

$$[m] \text{ is a zero-divisor } \iff gcd(m, n) > 1$$

Proof. (1). " $\Longleftarrow$: " If $gcd(m, n) = 1$, then $1 = am + bn$ for $a, b \in \mathbb{Z}$. If r is the remainder of a by n, $a = sn + r$, then $1 = snm + rm + bn = rm + (sn + b)n$, so $[r][m] = [1]$ in $\mathbb{Z}_n$. Thus, m is a unit.

" $\implies$ ": If $[m]$ is a unit, then $[r][m] = 1$ for some $r \in \mathbb{Z}_n$. So, $rm = 1 + nq \iff 1 = rm - nq$ for some $q \in \mathbb{Z}$. Thus, $[m]$ is a unit.

(2).$\Longleftarrow$: If $gcd(m, n) > 1$, then $m = m_1 d, n = n_1 d$, where $m_1, n_1 \in \mathbb{Z}$. So, $mn_1 = m_1 d n_1 = m_1 n \implies [m][n_1] = 0 \implies m$ is a zero-divisor.

$\implies$: If $[m]$ is a zero-divisor, then $[m]$ is not a unit. From previous result, $gcd(m, n) \neq 1 \implies gcd(m, n) > 1$. ■

Corollary. If p prime, $\mathbb{Z}_p$ is a field.

Definition. A ring R is an **integral domain** if R is commutative with unity and no zero-divisors.

Remark: In an integral domain, multiplicative canellation law holds.

Example. $(\mathbb{Z}, +, \cdot)$ is an integral domain. $(\mathbb{Z}_n, +, \cdot)$ is an integral domain $\iff$ n is prime.

Definition. If R, R' are rings, then $\rho : R \to R'$ is a **ring homomorphism** if

- $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\phi(b)$

If ϕ is also one-to-one and onto, then ϕ is a **ring isomorphism**

Example. $\phi : (\mathbb{Z}, +, \cdot) \to (2\mathbb{Z}, +, \cdot).\phi(a) = 2a$. Here, $\phi(ab) \neq \phi(a)\phi(b) \implies \phi$ is not a ring homomorphism.

Example. $\phi : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$, $\phi(a) = [\text{remainder of } a \text{ by } n]$. Then, ϕ is a ring homomorphism.

Fact: If R is a ring with unity, then the unit elements in R form a group under multiplication.

Example. In $\mathbb{Z}_5$ under multiplication, the unit elements are $\{[1], [2], [3], [4]\}$. In particular, $\{[2], [4]\}$ are generators and it is thus isomorphic to $\mathbb{Z}_4$.

Fact: For any prime p, $\mathbb{Z}_p - \{[0]\}$ is a group under multiplication, denoted as $\mathbb{Z}_p^{\times}$.

Useful Number theory equivalances

- $a \equiv b \mod n \iff n \mid a - b$
- $a \equiv b \mod n \iff a^r \equiv b^r \mod n$
- $a \equiv b \mod n \iff ca \equiv cb \mod n \, \forall c$

Theorem. **[Fermat's Little Theorem].** If $a \in \mathbb{Z}$ and p prime such that $gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \mod p$$

Proof. $|\mathbb{Z}_p^\times| = p - 1$. So $\forall [m] \in \mathbb{Z}_p^\times, [m]^{p-1} = [1]$. So, remainder of m^{p-1} by p is 1, which is saying $m^{p-1} \equiv 1 \mod p$.

Now, if $a \in \mathbb{Z}, \gcd(a, p) = 1$, and m is remainder of a by p. Then $1 \leq m \leq p - 1$, so $a \equiv m \mod p \implies a^{p-1} \equiv m^{p-1} \equiv 1 \mod p$ ■

Corollary. If p is prime and $a \in \mathbb{Z}$, then

$$a^p \equiv a \mod p$$

Proof. If $p \mid a$, then $p \mid a^p \implies a^p \equiv a \equiv 0 \mod p$.
Otherwise if $p \nmid a$, then $gcd(p, a) = 1$. $a^{p-1} \equiv 1 \mod p \implies a^p \equiv a \mod p$. ■

Example. Find remainder of 40^{100} by 19.

Note that $40 \equiv 2 \mod 19$. $40^{90} \equiv 40^{18} \equiv 1 \mod 19 \implies 40^{100} \equiv 40^{10} \equiv 2^{10} \equiv 32^2 \equiv 13^2 \equiv (-6)^2 \equiv 17 \mod 19$

Example. Prove $15 \mid n^{33} - n \, \forall n \in \mathbb{Z}$.

General idea: Show $3 \mid n^{33} - n$ and $5 \mid n^{33} - n$ separately.

$3 \mid n^{33} - n$: If $3 \mid n$, then this is obvious. If $3 \nmid n$, then $n^2 \equiv 1 \mod 3 \implies (n^2)^{16} \equiv 1 \mod 3 \implies n^{33} \equiv n \mod 3$.

$5 \mid n^{33} - n$: If $5 \mid n$, then this is obvious. If $5 \nmid n$, then $n^4 \equiv 1 \mod 5 \implies n^{32} \equiv 1 \mod 5 \implies n^{33} \equiv n \mod 5$.

Definition. If $n \geq 2 \in \mathbb{Z}$, then **Euler's ϕ function** is $\phi(n) =$ the number of *units* in $\mathbb{Z}_n$.

Fact: The units of $\mathbb{Z}_n$ form a group under multiplication: $|\mathbb{Z}_n^\times| = \phi(n)$

Theorem. For any $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, it is the case that

$$a^{\phi(n)} \equiv 1 \mod n$$

Example. For $\mathbb{Z}_6$, [1] and [5] are units $\implies \phi(6) = 2$. So, if $gcd(a, 6) = 1$, then $a^2 \equiv \mod 6$.

Example. Find remainder of 151^8 by 8.

$\phi(8) = 4$. If $\gcd(a, 8) = 1$, then $a^4 \equiv 1 \mod 8$. $\gcd(151, 8) = 1 \implies$ remainder is 1.

Theorem. The equation $ax \equiv b \mod n$ has solution if and only if $\gcd(a, n) \mid b$. Then, there are $d := \gcd(a, n)$ solutions in $\mathbb{Z}_n$.

Proof. <u>Case 1</u>: $\gcd(a,n)=1$. Then for $ax \equiv b \mod n$, let $a = nq+r, b = np+s$.

Thus, $\gcd(a,n)=1 \iff \gcd(r,n)=1 \implies [r]$ is a unit $\implies [r]$ has an inverse.

Then $[r][x]=[s]$ in $\mathbb{Z}_n \implies [x] = [r]^{-1}[s]$ in $\mathbb{Z}_n$, a unique solution.

<u>Case 2</u>: $\gcd(a,n)=d$. Then if $ax \equiv b \mod n$ has solution, then $ax-b=nk$ for some $k \in \mathbb{Z}$, so $b = ax-nk \implies d \,\big|\, b$.

Conversely, suppose $d \,\big|\, b$, We have $a=a_1d, n=n_1d, b=b_1d$ and $\gcd(a_1,n_1)=1$. Then

$$ax \equiv b \mod n \iff n \,\big|\, ax-b \iff n_1d \,\big|\, d(ax-b) \iff n_1 \,\big|\, a_1x-b_1 \iff a_1x \equiv b_1 \mod n_1$$

Since $\gcd(a_1,n_1)=1$, the equation has a unique solution in $\mathbb{Z}_{n_1}$ so there are d solutions in $\mathbb{Z}_n$. ∎

Example. Solve $12x \equiv 25 \mod 7$

$\iff 5x \equiv 4 \mod 7 \implies [5][x]=[4] \implies [x]=[3][4], x=[5]$.

Example. Solve $4x \equiv 32 \mod 20$.

$\gcd(6,20)=2 \implies 2$ solutions. $6x \mod 32 \mod 10 \iff 3x \equiv 16 \mod 5 \iff 3x \equiv 6 \mod 10$. Thus $[3]^{-1}=[7] \implies [x]=[7][6]=[2]$ in $\mathbb{Z}_{10}$. In $\mathbb{Z}_{20}$, the solutions are $\{[2],[12]\}$

5 Constructing Rings and Fields

Definition. Recall that a ring D is an **integral domain** if it

- has a unity
- is commutative
- has no zero divisors

Then, we can construct a *field* F containing D, where let $S = \{(a,b) \mid a,b \in D, b \neq 0\}$. Then we say $(a,b) \sim (c,d)$ if $ad = bc$.

If the *equivalence* class of (a,b) is $[(a,b)]$, let F be a set of equivalence classes. Then F is a ring with

- $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$
- $[(a,b)][(c,d)] = [(ac,bd)]$

if they are well-defined.

Checking whether this is *well-defined*: If $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then $(ad+bc, cd) \sim (a'd' + b'c', b'd')$

- Identity: $[(0,1)]$
- Inverse: $-[(a,b)] = [(-a,b)]$
- Unity: $[(1,1)]$
- Let $\phi : D \to F, \phi(a) = [(a,1)]$. ϕ is a ring homomorphism and is one-to-one, $[(a,1)] = [(b,1)] \iff a = b$

<u>Remark:</u> If D is a field, then $F = D$. In other words, ϕ onto. If $[(a,b)] \in F, \phi(ab^{-1}) = [(a,b)]$, since $[(ab^{-1},1)] = [(a,b)]$

Example. If R_1, R_2 are rings, $R_1 \times R_2 = \{(a,b) \mid a \in R_1, b \in R_2\}$. Then

$$\begin{cases} (a,b) + (a',b') = (a+a', b+b') \\ (a,b)(a',b') = (aa', bb') \end{cases} \quad \implies R_1, R_2 \text{ a ring}$$

$\mathbb{Z} \times \mathbb{Z}$ has zero divisors: $(1,0)(0,1) = (0,0)$

[Add Everything from Notes]

5.1 Polynomial Rings

Definition. Let R be a ring. A **polynomial** $f(x)$ with coefficients in R is of the form $a_0 + a_1 x + ... + a_n x^n$ where x indeterminant, $a_1, ..., a_n$ coefficients, a_0 is the constant term.

- If n is the largest integer such that $a_n \neq 0$, $f(x)$ has **degree** n.
- If $f(x)$ is the zero polynomial ($a_0 = ... = a_n = 0$), the degree is *not well-defined.*
- If $deg(f(x)) = 0$ or $f(x) = 0$, we say $f(x)$ is **constant**
- If R has a **unity**, we write x^k

Let the set of all polynomials with coefficients in R be $R[x]$. Set

$$f(x) = a_0 + a_1x + ... + a_nx^n, \qquad g(x) = b_0 + b_1x + ... + b_mx^m, \qquad n \geq m$$

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + ... + a_nx^n$$

$$f(x)g(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + ... + a_nb_mx^{n+m}, \qquad \text{coefficient of } x^k = \sum_{i=1}^{k} a_ib_{k-i}$$

<u>Fact:</u> $R[x]$ is a ring.

- Identity is the zero-polynomial
- If R commutative, then $R[x]$ commutative
- If R has unity 1, then $R[x]$ has unity

Example. Find all polynomials of degree 2 in $\mathbb{Z}_2[x]$: $\{x^2, x^2 + x, x^2 + 1, x^2 + x + 1\}$

Let F be a field, $F[x]$. If $a \in F$, then

$$f(x) = a_nx^n + ... + a_1x + a_0 \in F$$

Then the function $F[x] \xrightarrow{\phi_a} F, f(x) \mapsto f(a)$, and

$$\phi_a(f(x)g(x)) = f(a)g(a) \qquad \phi_a(f(x) + g(x)) = \phi_a(f(x)) + \phi_a(g(x)) = f(a) + g(a)$$

Example. Let $F = \mathbb{Z}_5, f(x) = x^5 - x, g(x) = x^5 + 1$. $f(x)$ has 5 zeros, $\{0, 1, 2, 3, 4\}$ and $g(x)$ has 1 zero $\{4\}$.

5.2 Unique Factorization of Polynomials

Example. Let $F = \mathbb{Z}_5$. Divide $3x^4 + 2x^3 + x + 2$ by $x^2 + 4$: $3x^4 + 2x^3 + x + 2 = (x^2 + 4)(3x^2 + 2x + 3) + 3x$

Division Algorithm. Let F be a field, and $f(x), g(x) \in F[x]$ such that $g(x) \neq 0$. Then there are unique polynomials $q(x), r(x)$ such that

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

Proof. Let $f(x) = a_nx^n + ... + a_1x + a_0, g(x) = b_mx^m + ... + b_1x + b_0$, and $S = \{f(x) - g(x)h(x) \mid h \in F[x]\}$

If the polynomial is in S_r then we are then, and $f(x) = g(x)h(x)$. Otherwise, let $r(x)$ be the polynomial with smallest degree in S, where $c_tx^t + ... + c_1x + c_0$, so $f(x) = g(x)h(x) + r(x)$ for some $h(x)$.

Then, to show $t < m$ or $\deg(r(x))$ <$\deg(g(x))$, I suppose otherwise that $t \geq m$. Then $f(x) - g(x)(h(x) + \frac{c_t}{b_m}x^{t-m}) \in S$.

$$f(x) - g(x)\left(h(x) - \frac{c_t}{b_m}x^{t-m}\right) = r(x) - \frac{c_t}{b_m}g(x)x^{t-m}$$

Here, $\frac{c_t}{b_m}g(x)x^{t-m} = c_tx^t +$ lower terms ■

Corollary. $a \in F$ is a zero of $f(x) \iff f(x) = (x-a)g(x)$ for some $g(x) \in F[x]$

Proof. $\Longleftarrow$. Plug in a. $f(a) = 0$.

$\implies$: By division algorithm, $f(x) = (x-a)q(x) + r(x)$, where $r(x) = 0$ or $degr(x) < 1$, so $r(x) = c$ is a constant. Evaluate at a: $f(a) = (a-a)g(a) + c \implies c = 0$ ■

Corollary. Every non-zero polynomial of degree n has at most n zeros in F.

Proof. Prove by induction on n. If $n = 0$, $f(x) = c, c \neq 0$, so there is no zero.

For $n-1 \implies n$, if $f(x)$ has no zeros, then we are done.

Otherwise, let a be a zero of $f(x)$, so $f(x) = (x-a)g(x)$, deg $g(x) = n-1$. If b is a zero of $g(x)$, then $0 = f(b) = (b-a)g(b)$. Since F is a field $b - a = 0$ or $g(b) = 0$. But, $g(x)$ has at most $n-1$ zeros, so $f(x)$ has at most n zeros. ■

Definition. A non-constant polynomial $f(x) \in F[x]$ is called **reducible** if it could be written as $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x], deg(g(x)), deg(h(x)) < deg(f(x))$.

$f(x)$ is **irreducible** if it is not reducible.

Example. $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible, but it is reducible in $\mathbb{R}[x]$.

Proposition. Let $f(x) \in F[x]$.

- If $deg(f(x)) = 1$, then $f(x)$ is irreducible.
- If $deg(f(x)) = 2$, then $f(x)$ is reducible $\iff f(x)$ has zero in F.
- If $deg(f(x)) = 3$, then $f(x)$ is reducible $\iff f(x)$ has zero in F.

Proof. For degree 2 $\Longleftarrow$: Clear: If $a \in F$ has a zero, $f(x) = (x-a)g(x)$.

$\implies$: If $f(x)$ reducible, then $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$,$deg(g(x)) = deg(h(x)) = 1$. Write $g(x) = b_0x + b_1, b_0 \neq 0$. Then, $-\frac{b_1}{b_0}$ is a zero of g and therefore also a zero of f.

Note: Key to this proposition is that any linear equation has a zero solution, but everything beyond is a mystery. ■

Example. $f(x) = (x^2+2)^2 \in \mathbb{R}[x]$ reducible but has no zeros.

Example. $x^2 - 2, x^3 - 2$ reducible in $\mathbb{Q}[x]$ but has no solutions in $\mathbb{Q}$.

Proposition. If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ is reducible in $\mathbb{Q}[x] \iff f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Z}[x], deg(g(x)), deg(h(x)) < deg(f(x))$.

Proof. See book.

Corollary. If $f(x) = x^n + ... + a_1x + a_0 \in \mathbb{Z}[x]$. Then every rational zero of $f(x)$ is an integer which divides a_0.

Proof. If $\frac{p}{q}$ is a zero of $f(x)$, then $gcd(p,q)=1$

$$f\left(\frac{p}{q}\right)=\frac{p^n}{q^n}+a_{n-1}\frac{p^{n-1}}{q^{n-1}}+...+a_1\frac{p}{q}+a_0=\frac{p^n+a_{n-1}p^{n-1}q+...+a_1pq^{n-1}+a_0q^n}{q^n}=0$$

■

Notice that q divides the numerator, so since q divides $a_{n-1}p^{n-1}q+...+a_1pq^{n-1}+a_0q^n$, it must be that $q \mid p^n$. Since they are relatively prime, $q=\pm1$ so $\frac{p}{q}=c\in\mathbb{Z}$. Also, using similar logic, p divides $a_0q^n=\pm a_0$, so $p \mid a_0$.

Example. Is $x^5+8x+2\in\mathbb{Q}[x]$ irreducible? For $f(x)=x^5+8x+2$, the possible zeros are $\pm1,\pm2$. None of the above is a zero $f(x)$, so $f(x)$ irreducible in $\mathbb{Q}[x]$.

[Eisenstein Criterion]. If $f(x)=a_nx^n+...+a_1x+a_0\in\mathbb{Z}[x]$ and if there is a prime p such that p divides $a_0,...,a_{n-1}$ AND p does not divide a_n, then $f(x)$ irreducible in $\mathbb{Q}[x]$.

Example. $f(x)=x^4+8x+2$. Let $p=2$. By eisenstein, $f(x)$ is irreducible.

Proof. Suppose $f(x)=g(x)h(x)$, and let $deg(g(x)),deg(h(x))<deg(f(x))$. Let

$$g(x)=b_mx^m+...+b_1x+b_0 \qquad h(x)=c_lx^l+...+c_1x+c_0, \qquad m+l=n$$

Then, $a_0=b_0c_0, a_n=b_mc_l$. If $p \mid a_0=b_0c_0$ and p^2 does not divide a_0, then p divides exactly one of b_0,c_0.

WLOG, assume $p \mid b_0$ and does not divide c_0. But if $p\nmid a_n$, then $p\nmid b_m$. Let i be the smallest integer such that $p\nmid b_i$, so $p \mid b_0,...,b_{i-1}$, $i\le m<n$. Now, $a_i=b_ic_0+b_{i-1}c_1+...+b_1c_{i-1}c_i$, so $p \mid b_ic_0$ but $p\nmid b_i,c_0$ which is a contradiction. So $p\nmid a_n$. ■

Definition. **Polynomial factorization**: If F is a field and $f(x)\in F[x]$, then we factor $f(x)$ as $f(x)=f_1(x)\dots f_l(x)\in F[x]$ and irreducible. This factorization is unique up to reordering and nonzero constants.

5.3 Ideals

If $(R,+,\cdot)$ is a ring and $S\subset R$ is a non-empty subset, then S is a **subring** if

- S closed under multiplication
- $(S,+)\le(R,+)$

Example. $(\mathbb{Z},+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$

Example. $A=\{f(x)\in\mathbb{R}[x] \mid f(0)=0\}$

When is R/S a ring with $(a+S)+(b+S)=(a+b)+S$ and $(a+S)(b+S)=ab\in S$ well-defined?

Definition. A subset $I\subseteq R$ is an **ideal** if

- $(I,+)\le(R,+)$
- If $r\in R$ and $a\in I$, then $ra,ar\in I$.

Fact: Every *ideal* is a subring (Ideal is a stronger condition)

Example. $\mathbb{Z}$ is not an ideal of $\mathbb{R} : 2 \in \mathbb{Z}, \sqrt{3} \in \mathbb{R}, 2\sqrt{3} \notin \mathbb{Z}$

Theorem. If I is an ideal in R, then multiplication is well-defined on R/I, so R/I is a ring.

Proof. Suppose $a + I = a' + I$ and $b + I = b' + I$, then $a - a', b - b' \in I$. $ab - a'b' = a(b - b') + b'(a - a') \in I \implies ab - a'b' \in I \implies ab + I = a'b' + I$ ■

Example. What are ideals of $\mathbb{Z}$? If I is an ideal, then it is a subgroup, so it is of the form $I = n\mathbb{Z}$. Every such subgroup is an ideal.

Example. What are ideals of $\mathbb{R}$? 0 is always an ideal. R is also an ideal.

Proof. If $a \neq 0$ and $a \in I$, then $\forall r \in \mathbb{R}, \frac{r}{a} \cdot a \in I$, so $r \in I$. ■

Example. What are the ideals of $\mathbb{R}[x]$?

Proof. If $I \subseteq \mathbb{R}[x]$ is an ideal and $I \neq \{0\}$, let $f(x) \in I$ be polynomial of smallest degree.

If $g(x) \in I$, divide $g(x)$ by $f(x)$, where $g(x) = f(x)g(x) + r(x)$, $r(x) = 0$ or $deg(r(x)) = deg(f(x))$.

Since $g(x), f(x)g(x) \in I$, $r(x) = g(x) - f(x)g(x) \in I$. So by the choice of $f(x), r(x) = 0 \implies g(x) = g(x)f(x)$. $I = \{f(x)g(x) \mid g(x) \in \mathbb{R}[x]\}$. ■

<u>Remark:</u> The same argument holds for all $F[x]$.

Definition. If R is a commutative ring and $a \in R$, then $I = \{ar \mid r \in R\}$ is an ideal of R. In particular, I is the **principle ideal** generated by a, denoted as $I = (a)$.

Example. In $\mathbb{Z}[x], I = \{f(x) \mid f(0) \text{ even}\}$ is an ideal. $2, x \in I$, so I is not a principle ideal.

Proposition. If $\phi : R \to S$ is a ring homomorphism, then $ker\phi := \{a \in R \mid \phi(a) = 0\}$ is an ideal of R.

Proof. We already know that $(ker(\phi), +) \leq (R, +)$. Now if $r \in R, a \in ker\phi$, then $\phi(ra) = \phi(r)\phi(a) = 0$ and $\phi(ar) = \phi(a)\phi(r) = 0 \implies ar, ra \in ker\phi$. ■

Corollary. If R is a field, then $\ker \phi = \{0\}$ or $ker\phi = R$. So ϕ is 1-to-1 or ϕ is the 0.

Definition. An ideal $I \subseteq R$ is a **maximal ideal** if $I \neq R$ and there is no proper ideal J s.t. $I \nsubseteq J$. In other words, if $I \subseteq J \subseteq R$, then $J = R$ or $J = I$.

Example. [Maximial Ideas of $\mathbb{Z}$] Let $I = n\mathbb{Z}$ and $n, m > 0$. $n\mathbb{Z} \subseteq m\mathbb{Z} \iff n \in m\mathbb{Z} \iff m \mid n$. So, $n\mathbb{Z} = m\mathbb{Z}$ for $n, m \geq 1 \iff n \mid m$ and $m \mid n \iff m = n$. So $n\mathbb{Z}$ is a maximal ideal $\iff n$ is prime.

Proposition. Suppose F is a field and $f(x) \in F[x]$. Then I is a maximal ideal $\iff f(x)$ is irreducible.

Proof. $\implies$. Suppose $f(x) = g(x)h(x)$, $0 < \deg g(x), h(x) < \deg f(x)$. Let $I = (f(x)) = \{f(x)q(x) \mid q(x) \in F[x]\}$. We claim that $I = (f(x)) \subsetneqq (g(x))$ since every polynomial in I has degree $\geq \deg f(x)$, so $g(x) \notin I$. Also $(g(x)) \neq F[x]$, since $1 \notin (g(x))$.

$\impliedby$. Prove by contrapositive. If $I \subsetneqq J \neq F[x]$, then $J = (g(x))$. So $f(x) \in (g(x)) \implies f(x) = g(x)h(x)$ for some $h(x)$.

- If $\deg g(x) = 0$, then $g(x) = c \in F \implies \frac{1}{c} \cdot c \in J \implies 1 \in J \implies h(x) = 1 \in J \implies J = F[x]$.
- If $\deg h(x) = 0$, then $h(x) = c \neq 0 \in F$, so $g(x) = \frac{1}{c} f(x) \in (f(x)) \implies (g(x)) \subseteq (f(x)) \implies J = I$.

So $0 < \deg g(x), h(x) < \deg f(x)$, so $f(x)$ reducible. ■

Example. If F is a field, what are maximal ideals of $F[x]$?.

$I = (x^2 + 1) \subset \mathbb{R}[x]$ is a maximal ideal.