Modern Algebra I

Sungchan Yi

Spring 2023

Part I

Groups and Subgroups

Introduction

Section 1. Introduction and Examples

수 체계의 확장.

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \longrightarrow \mathbb{C}$$

학부 현대대수학의 최종 목표는 다음 정리를 증명하는 것.

Theorem. n차 방정식의 일반해는 존재하지 않는다. $(n \geq 5)$

March 6th, 2023

추상적인 개념을 공부하는 이유는 구체적인 example 때문이다. Example이 곧 motivation이 되기 때문이다.[1]

- Complex numbers $\mathbb{C}$. $a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$ and $+, \times$ defined on them.
- The unit circle $U = \{a + bi : a^2 + b^2 = 1, a, b \in \mathbb{R}\} = \{e^{i\theta} : 0 \leq \theta < 2\pi\}$. U is not closed under addition, but closed under addition.

  Note that the above two representations are intrinsically the 'same' representations of the unit circle. We write

  $$(U, \cdot) \approx \big([0, 2\pi), +_{2\pi}\big)$$

  and say that these two are **isomorphic**.

[1] 이인석 교수님: 추상화는 구체적인 example이 없으면 의미 없다.

- **Roots of Unity**: $U_n = \{\xi \in \mathbb{C} : \xi^n = 1\}$. We can see that

  $$\xi_k = e^{\frac{2\pi k}{n} i}, \quad (k = 0, \ldots, n-1).$$

  When we multiply two elements for example, we do the following.

  $$\xi_1 \cdot \xi_2 = e^{\frac{2\pi}{n} i} \cdot e^{\frac{4\pi}{n} i} = e^{\frac{6\pi}{n} i} = \xi_3$$

  If we look closely, we see that we have transformed elements of $(U, \cdot)$ to $\big([0, 2\pi), +_{2\pi}\big)$. This can be done because the two sets are **isomorphic**!

Section 2. Binary Operations

March 8th, 2023

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

$$*: S \times S \to S$$

We write $a * b$ instead of $*(a, b)$.

Remark. If you consider the number systems like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, we already know operations defined on them. We are just naming them *binary operations.* The examples came first, and the definitions came afterwards. We can also see that the definitions are really useful, and it will serve as a tool for formalizing our theory.

Example. Examples of binary operations.

(1) Addition $+$ and multiplication $\cdot$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Subtraction $-$ is not a binary operation on $\mathbb{N}$. We extend $\mathbb{N}$ to $\mathbb{Z}$, so that $-$ is a binary operation on $\mathbb{Z}$.

(3) The set of functions $f : \mathbb{R} \to \mathbb{R}$, and $+, -, \times, \circ$ defined on it.

Definition. (Closure) For a set S and a binary operation $*$ on S, suppose that $H \subset S$. We restrict the domain of $*$ to $H \times H$. Then

$$* \mid_{H \times H} : H \times H \to S.$$

If the image of $* \mid_{H\times H} \subset H$, then we say that H **is closed under** $*$.

Remark. When we learn new definitions, it's very important to think about examples that we already know. Often books give trivial examples first, and then show some non-trivial examples, motivating us to study. Books are written in that way!

Definition. Let $(S, *)$ be given. We say that

(1) $*$ is **commutative** if $a * b = b * a$ for all $a, b \in S$.

(2) $*$ is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Example. Consider these binary operations on $\mathbb{Z}$.

(1) $a * b = a$, $*$ is not commutative but associative.

(2) $a * b = a + 2$, $*$ is not commutative nor associative.

Remark. To study these binary operations, we first start with finite sets where we can write tables with the results of the binary operation.

$$S = \{a\} \implies \begin{array}{c|c} * & a \\ \hline a & a \end{array}, \qquad S = \{a, b\} \implies \begin{array}{c|c|c} * & a & b \\ \hline a & & a * b \\ \hline b & b * a & \end{array}$$

Consider the relation between binary operation on a finite set S and tables. Binary operation is a function, so we have the existence and uniqueness of $a * b$. In terms of tables, we see that each cell in the table should have a value and it should be uniquely determined. So we conclude that *we can describe a binary operation with a table.*

March 13th, 2023

Section 3. Isomorphic Binary Structures

Consider $S = \{a, b, c\}, S' = \{1, 2, 3\}$ and binary operations $*, *'$, defined as the following.

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

$*'$	1	2	3
1	2	1	3
2	3	1	2
3	1	2	3

We see that if we rename a, b, c to $1, 2, 3$ respectively, we see that the tables are actually *equivalent*. How do we formalize the notion of equivalence of binary structures $(S, *), (S', *')$?

Definition. (Isomorphism) Let $(S, *)$ and $(S', *')$ be binary structures. If there exists a bijection $\varphi : S \to S'$ such that

$$\varphi(a * b) = \varphi(a) *' \varphi(b), \quad \forall a, b \in S,$$

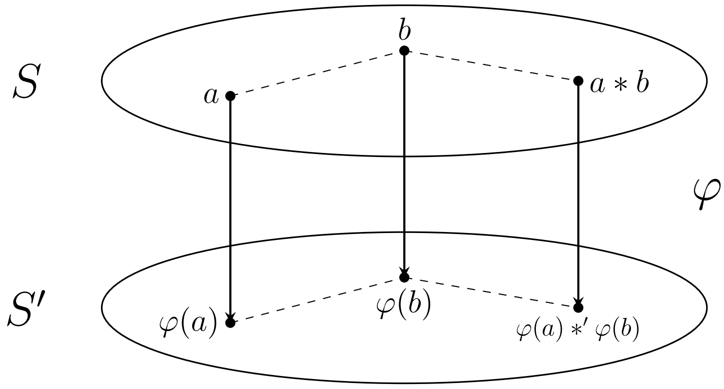
then φ is called an **isomorphism** between $(S, *)$ and $(S', *')$. We say that $(S, *)$ and $(S', *')$ are **isomorphic** to each other.

Definition. (Homomorphism) Let $(S, *)$ and $(S', *')$ be binary structures. A map $\varphi : S \to S'$ such that

$$\varphi(a * b) = \varphi(a) *' \varphi(b), \quad \forall a, b \in S$$

is called a **homomorphism** between $(S, *)$ and $(S', *')$.

Remark. Isomorphisms are *renaming functions* that preserve the structure of a set. Isomorphisms are homomorphisms that are bijective. Also, homomorphisms can be seen as a somewhat confusing(?) renaming functions, since they aren't bijective.



Example. Examples of isomorphisms.

(1) Let $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ with $\varphi(x) = e^x$ for $x \in \mathbb{R}$.

(2) Let $\varphi : (\mathbb{Z}, +) \to (2\mathbb{Z}, +)$ with $\varphi(n) = 2n$ for $n \in \mathbb{Z}$.

(3) Non-example: $(\mathbb{Z}, *) \not\simeq (\mathbb{R}, *)$ (different cardinality)

Remark. Structural properties: properties preserved by isomorphisms

(1) Number of elements (cardinality, for infinite sets)

(2) Commutativity, associativity

(3) The equation $a * x = b$, $\forall a, b \in S$ has a solution in S

We can disprove the existence of an isomorphism by showing that any of the structural properties do not hold.

Example. For $(\mathbb{Z}, \cdot)$ and $(\mathbb{Z}^+, \cdot)$ we want to show that these two are not isomoprhic. Consider the equation $x^2 = x$. In $\mathbb{Z}$, the solutions are $x = 0, 1$, but in $\mathbb{Z}^+$, the solution is unique, $x = 1$.

Proof. Suppose that $\mathbb{Z}$ and $\mathbb{Z}^+$ are isomorphic, and let φ be the isomorphism. Let $\varphi(0) = a$, $\varphi(1) = b$. Then $a \neq b$, since φ is a bijection. However,

$$a = \varphi(0 \cdot 0) = \varphi(0) \cdot \varphi(0) = a \cdot a, \quad b = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = b \cdot b$$

but in $\mathbb{Z}^+$ there is only one solution to $x^2 = x$. This is a contradiction, so φ is not an isomorphism.

Definition. (Identity) Let $(S, *)$ be a binary structure. If $e \in S$ satisfies

$$e * a = a * e = a, \quad \forall a \in S,$$

then e is called the **identity** element of S.

Theorem. Identities are unique, if it exists.

Proof. Let $e, e' \in S$ be identities of S. Then,

$$e = e * e' = e' * e = e'$$

so $e = e'$.

Theorem. If $\varphi : S \to S'$ is an isomorphism, φ maps the identity to the identity.

Proof. Let $e \in S$ be the identity of S. For any $t \in S'$, there exists $s \in S$ such that $\varphi(s) = t$. Then

$$t *' \varphi(e) = \varphi(s * e) = \varphi(s) = t, \quad \varphi(e) *' t = \varphi(e * s) = \varphi(s) = t,$$

so $\varphi(e)$ is the identity of S'.

March 15th, 2023

Section 4. Groups

Definition. (Inverse) Let $(S, *)$ be a binary structure with identity $e \in S$. If $x \in S$ satisfies

$$a * x = x * a = e \text{ for some } a \in S,$$

then x is an **inverse** of a, and we write $x = a^{-1}$.

Definition. (Group) Let $(G, *)$ be a binary structure, with the following properties.

(1) $*$ is associative.

(2) G has an identity element.

(3) For all $x \in G$, there exists an inverse of x in G.

Then $G = (G, *)$ is called a **group**.

$(\mathbb{N}, +)$ is not a group. The equation $n + x = m$, $(n, m \in \mathbb{N})$ does not have a solution if $n \leq m$. So we extend the number system to $\mathbb{Z}$ and consider $n + x = m$ for $n, m \in \mathbb{Z}$. This equation always has a solution, this is due to the fact that $(\mathbb{Z}, +)$ is a group! $+$ is associative, $\mathbb{Z}$ has an identity 0, and also has an inverse for any $n \in \mathbb{Z}$!

So if $(G, *)$ is a group, equations of the from $a * x = b$ for given $a, b \in G$ can be solved by multiplying a^{-1} on the left.

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

Note that all three properties of the group was used!

Example.

(1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are all groups.

(2) $(\mathbb{N}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ are not groups, since they don't have an inverse for 0.

(3) $(\mathbb{Q}^\times, \cdot), (\mathbb{R}^\times, \cdot), (\mathbb{C}^\times, \cdot)$ are groups.

(4) The roots of unity with multiplication form a group.

Definition. (Commutative) A group G is **commutative/abelian** if

$$a * b = b * a \text{ for all } a, b \in G.$$

Proposition. (Basic properties of groups) Let G be a group.

(1) G has a unique identity.

(2) For $a \in G$, its inverse a^{-1} is unique.

(3) Left and right cancellation laws hold.

Remark. $(G, *)$ is a group $\iff$ $*$ is associative, has left identity, has left inverse.

Proof. ($\Longleftarrow$) Let e be a left identity of G. For any $a \in G$, let a' be a left inverse of a. Then, $a' * a * e = e * e = e = a' * a = a' * e * a$. Let a'' be a left inverse of a', then multiplying a'' on the left gives

$$a'' * a' * a * e = a'' * a' * e * a \implies a * e = e * a = a,$$

so $a * e = a$, proving that e is also a right identity.[2]

Let a' be a left inverse of a, and let a'' be a left inverse of a'. Then $a''*a'*a*a' = e*a*a' = a*a'$, also $a'' * a' * a * a' = a'' * e * a' = a'' * a' = e$. Therefore $a * a' = e$, proving that a' is also a right inverse.[3]

Remark. For finite groups, the elements in a single row or column should be unique. For example, if some two elements $a * x$, $a * y$ in the same row (but different column) are the same, we can use the left cancellation law to show that $x = y$. This is a contradiction.

So, let $G = \{e, a\}$ be a group with identity e. Then its operation table is determined uniquely, as the following.

$*$	e	a
e	e	a
a	a	e

As for $G = \{e, a, b\}$, it is also unique.

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

[2] Alternatively, $ae = eae = (a''a')a(a'a) = a''ea'a = ea = a$.

[3] Alternatively, $aa' = (a''a')aa' = a''(a'a)a' = a''ea' = e$.

March 20th, 2023

Definition. (Equivalence Relation) A relation $\mathcal{R}$ on S is a **equivalence relation** if it satisfies the following.

(1) (Reflexive) $x\mathcal{R}x$. ($x \in S$)

(2) (Symmetric) If $x\mathcal{R}y$, then $y\mathcal{R}x$. ($x, y \in S$)

(3) (Transitive) If $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$. ($x, y, z \in S$)

Example.

(1) Relation '=' on $\mathbb{Q} = \left\{\frac{y}{x} : x \in \mathbb{Z}^\times, y \in \mathbb{Z}\right\}$. Defined as $\frac{y}{x} = \frac{y'}{x'} \iff xy' = yx'$. The second equality is equality in $\mathbb{Z}$. We are defining '=' in $\mathbb{Q}$ using '=' in $\mathbb{Z}$.

(2) Relation '>' on $\mathbb{Z}$ is not symmetric, so it is not an equivalence relation.

Theorem 0.22. Equivalence relation $\sim$ on a set S yields a partition of S.

Example. Let $S = \mathbb{Z}$, $x \sim y \iff x \equiv y \pmod 5$. Then

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} \sqcup \overline{2} \sqcup \overline{3} \sqcup \overline{4},$$

where $\overline{x} = \{y \in \mathbb{Z} : x \sim y\}$.

Section 5. Subgroups

Definition. (Subgroup) Let $(G, *)$ be a group, $H \subset G$. H is a **subgroup** of G if $(H, * |_{H \times H})$ is also a group. We write $H \leq G$.

Example.

(1) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.

(2) (Trivial Subgroup) $\{e\} \leq G$.

(3) (Improper Subgroup) $G \leq G$.

(4) $\{e\} \leq \mathbb{Z}_2 \leq \mathbb{Z}_4$.

(5) $V_4 \not\leq \mathbb{Z}_4$ (different subgroup lattices).

(6) $\mathbf{SL}_n(\mathbb{R}) \leq \mathbf{GL}_n(\mathbb{R})$.

The following is a method to check that H is a subgrouop of G.

Theorem. Let G be a group and $H \subseteq G$. Then $H \leq G$ if and only if

(1) H is closed under the binary operation $*$ on G.

(2) Identity $e \in H$.

(3) For all $x \in H$, there exists an inverse $x^{-1} \in H$.

How can we find non-trivial subgroups? We include an element and generate elements, since the binary operations are always closed!

Theorem. Let G be a group, and let $a \in G$. Then

$$\{a^n : n \in \mathbb{Z}\} \leq G.$$

Proof. Let $H = \{a^n : n \in \mathbb{Z}\}$. Then for $a^n, a^m \in H$ $(n, m \in \mathbb{Z})$, $a^n a^m = a^{n+m} \in H$ (closed), $e = a^0 \in H$ (has an identity), $(a^n)^{-1} = a^{-n} \in H$ (has an inverse). So $H \leq G$.

Remark. Let $H = \{a^n : n \in \mathbb{Z}\}$.

(1) H is the smallest subgroup of G containing a.

(2) Any subgroup of G containing a has H as a subgroup.

(3) H is commutative.

Definition. (Cyclic) Let G be a group and let $H = \{a^n : n \in \mathbb{Z}\} \leq G$ for $a \in G$.

(1) H is called the **cyclic subgroup** generated by a, and we write $H = \langle a \rangle$.

(2) If there exists $x \in G$ such that $G = \langle x \rangle$, then G is called a **cylic group**.

Example. $U_n = \{\xi \in \mathbb{C} : \xi^n = 1\} = \langle \xi \rangle$, is a cyclic group where $\xi = e^{\frac{2\pi i}{n}}$. If we visualize this on the complex plane, the element ξ generates the whole group, in a cycle, hence the name cyclic group.

March 22nd, 2023

Section 6. Cyclic Groups

Theorem. Every cyclic group is commutative.

Always consider $U_n \simeq (\mathbb{Z}_n, +_n)$ as an example, when dealing with cyclic groups.

Theorem. A subgroup of a cyclic group is also cyclic.

Proof. Let $G = \langle g \rangle$ be a cyclic group, and let $H \leq G$. Choose the smallest positive $r \in \mathbb{N}$ such that $g^r \in H$. We show that $H = \langle g^r \rangle$. It is clear that $\langle g^r \rangle \leq H$, since H is a subgroup.

Suppose that there exists $s \in \mathbb{Z}$ such that $g^s \in H$, but $g^s \notin \langle g^r \rangle$. Then there exists unique quotient and remainder $q \in \mathbb{Z}, t \in \{1, \cdots, r-1\}$ such that $s = rq + t$. Then $g^s, g^{rq} \in H$, so $g^s (g^{rq})^{-1} = g^t \in H$, contradicting the minimality of r. Thus $H \leq \langle g^r \rangle$ and $H = \langle g^r \rangle$.

Example. $(\mathbb{Z}, +) = \langle 1 \rangle$. So any subgroup of $(\mathbb{Z}, +)$ should be $\langle n \rangle = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Definition. Let $S \subset G$. Then $\langle S \rangle$ is the smallest subgroup of G generated by S.

If $H = \langle a, b \rangle \leq \mathbb{Z}$, we can rewrite $H = \langle g \rangle$ for some $g \in \mathbb{Z}$. We know that $g = \gcd(a, b)$.

Definition. (Greatest Common Divisor) Let $r, s \in \mathbb{N}$. The **greatest common divisor** of r, s is the generator d which generates $\langle r, s \rangle \leq \mathbb{Z}$. We write $d = \gcd(a, b)$ and if $\gcd(r, s) = 1$, we say that r, s are **relatively prime**.

Remark. $\gcd(r, s) = 1 \iff mr + ns = 1$ for some $m, n \in \mathbb{Z}$.

We want to classify all cyclic groups!

Theorem. (Classification of Cyclic Groups) Suppose that $G = \langle g \rangle$ is cyclic.

(1) $|G| = \infty \iff G \simeq \mathbb{Z}$.

(2) $|G| = n \iff G \simeq \mathbb{Z}_n$.

Proof.
(1) Consider the map $\varphi : G \to \mathbb{Z}$, defined as $\varphi(g) = 1$. We first check that φ is well-defined. This is clear, since $|G| = \infty$, so $n \neq m \in \mathbb{Z} \iff g^n \neq g^m$. Otherwise, $|G|$ would be finite. This also implies that φ is bijective. Also φ is a homomorphism, since $\varphi(g^n g^m) = n + m = \varphi(g^n) + \varphi(g^m)$. φ is an isomorphism and $G \simeq \mathbb{Z}$.

(2) Consider the map $\varphi_n : G \to \mathbb{Z}_n$, defined as $\varphi_n(g) = 1$. We can check that φ_n is a well-defined isomorphism.

Theorem. Let $G = \langle a \rangle$ be a cyclic group of order n.

(1) Let $b = a^s \in G$. Then $|\langle b \rangle| = \dfrac{n}{\gcd(n, s)}$.

(2) $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(n, s) = \gcd(n, t)$.

Proof. (1) We want to find the smallest positive integer m such that $b^m = e$. ($a^{ms} = e$, so $n \mid ms$) Take $d = \gcd(n, s)$, then $\gcd\left(\frac{n}{d}, \frac{s}{d}\right) = 1$. If $\frac{n}{d} \mid \frac{s}{d} \cdot m$, then $\frac{n}{d} \mid m$. Hence the smallest positive integer m is $\frac{n}{d}$.

(2) Directly follows from (1). May have to prove that $\langle a^s \rangle = \left\langle a^d \right\rangle$.

Corollary. If $G = \langle a \rangle$ with order n, other generators of G are the elements of the form a^r where $\gcd(r, n) = 1$.

Part II

Permutations, Cosets and Direct Products

March 27th, 2023

Section 8. Groups of Permutations

Definition. (Permutation) A **permutation** on a set A is a bijective function $\varphi : A \to A$.

Remark. Let S_A be the set of permutations on A. Then $f \circ g \in S_A$ for all $f, g \in S$, $\circ$ has associativity, and $id \in S_A$, $f^{-1} \in S_A$ for all $f \in S$. Therefore $(S, \circ)$ is a group.

We study the case when A is a finite set, i.e, $A = \{1, 2, \ldots, n\}$.

Definition. (Symmetric Group) Let $A = \{1, 2, \ldots, n\}$. Let S_n be the set of all permutations on A. Then $(S_n, \circ)$ is called the **symmetric group on n letters**.

Let B be a set with n elements. We denote S_B be the set of all permutations on B. With the composition operation $\circ$, we see that $S_B \simeq S_n$ as groups.

Example.

(1) $S_2 = \{e, \tau\}$ where $\tau = (1, 2)$.

(2) On S_3, there are 6 permutations.

$$S_3 = \{e, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$$

where μ_i swaps other two elements other than i, and $\rho_1 = (1, 2, 3), \rho_2 = (1, 3, 2)$.

(3) Also we can see that S_3 is the group of symmetries on an equilateral triangle. Each ρ_i represents a rotation, and each μ_i represents a reflection.

Remark. S_3 is not commutative. Check that $\rho_1 \circ \mu_1 = \mu_3$, but $\mu_1 \circ \rho_1 = \mu_2$. In fact, S_3 is the non-commutative group having the smallest order.

A natural question arises here: Can we get S_n from the symmetries of a regular n-gon?

Example. We try this for S_4, but this doesn't work. Symmetries of a square consists of 4 rotations and 4 reflections, which is a total of 8 elements, but $|S_4| = 4! = 24$.

Definition. (Dihedral Group D_n) The group of symmetric of a regular n-gon is called the **n-th dihedral group D_n**.

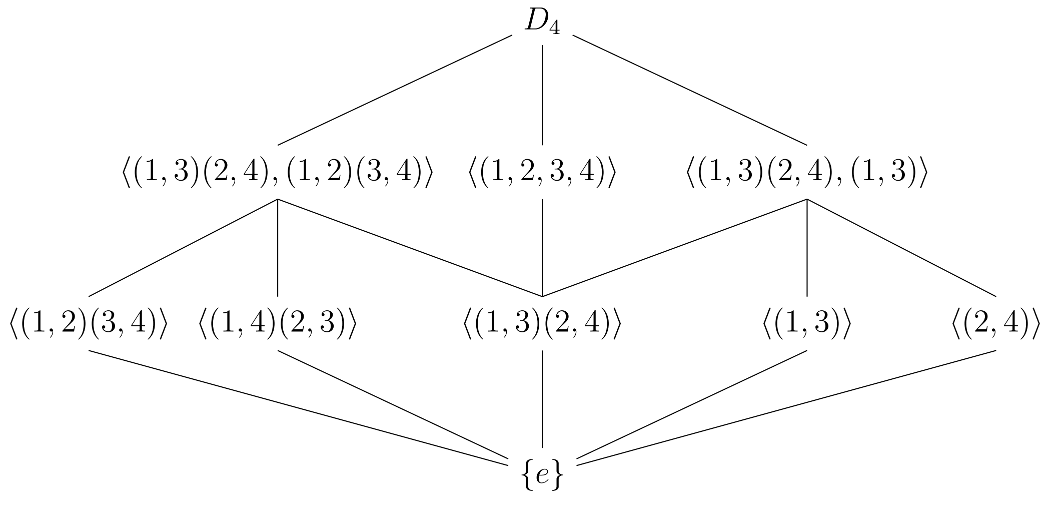
Remark.

(1) $D_3 \simeq S_3$, $D_4 < S_4$, D_4 is not commutative, so S_4 is not commutative.

(2) $|D_n| = 2n$.

(3) D_4 is generated by 2 elements. $D_4 = \langle \rho, \mu \rangle$, where ρ is a rotation by 90 degrees, and μ is some reflection.

(4) Subgroup lattice of D_4.


D_4
$\langle (1,3)(2,4), (1,2)(3,4) \rangle$
$\langle (1,2,3,4) \rangle$
$\langle (1,3)(2,4), (1,3) \rangle$
$\langle (1,2)(3,4) \rangle$
$\langle (1,4)(2,3) \rangle$
$\langle (1,3)(2,4) \rangle$
$\langle (1,3) \rangle$
$\langle (2,4) \rangle$
$\{e\}$

Lemma. For a group homomorphism $\varphi : G \to H$, $\operatorname{im}\varphi \leq H$. Additionally if φ is injective, $G \simeq \operatorname{im}\varphi \leq H$.

Proof. $\operatorname{im}\varphi$ is closed under the binary operation on H, since for any $a, b \in G$, $\varphi(a)\varphi(b) = \varphi(ab)$, and $ab \in G$, so $\varphi(a)\varphi(b) \in H$. $\varphi(e)$ is the identity, and $\varphi(a)^{-1} = \varphi(a^{-1})$. So $\operatorname{im}\varphi \leq H$. If φ is injective, restricting the range of φ to $\operatorname{im}\varphi$ gives an isomorphism, so $G \simeq \operatorname{im}\varphi$.

Why do we study symmetric groups? It is because of the following theorem. It states that all groups are isomorphic to some permutation group.

Theorem. (Cayley) Every group is isomorphic to some subgroup of S_n.

Proof. Consider $\varphi : G \to S_G$ such that $\varphi(g) = \lambda_g$, where $\lambda_g(x) = gx$ for $x \in G$. (left multiplication by g) We check that $\lambda_g \in S_G$, since groups have the cancellation law. Now check that φ is a monomorphism, then $G \simeq \operatorname{im} \varphi \leq S_G$.

Section 9. Orbits, Cycles and the Alternating Groups

Definition. Equivalence relation $\sim_\sigma$ on A with respect to $\sigma \in S_A$ is defined as

$$\text{For } a, b \in A,\ a \sim_\sigma b \iff \exists\, n \in \mathbb{Z} \text{ such that } a = \sigma^n(b).$$

Remark. Check that $\sim$ is indeed an equivalence relation.

Definition. Equivalence classes in A induced from the relation $\sim_\sigma$ are called the **orbits of** σ.

Example. Consider $\sigma = (1,3,6)(2,5,7,4)(8)$. Then $\{1,3,6\}, \{2,4,5,7\}, \{8\}$ are orbits.

If we represent orbits in circles, σ can be represented as 2 circles. $\tau = (1,2,3,4)$ would be represented as a circle, and $\tau' = (1,2,3)(4)$ would be represented as a circle.

Definition. (Cycles)

(1) A permutation $\sigma \in S_n$ is called a **cycle** if σ has at most 1 orbit with more than 1 element.

(2) The **length** of a cycle σ is the number of elements in its largest orbit.

τ is a cycle of length 4, τ' is a cycle of length 3, but σ is not a cycle.

Question. *For any $\sigma \in S_n$, can σ be represented as a composition of cycles?*

Theorem. Every permutation of a finite set is a product of disjoint cycles.

Proof. Take any $\sigma \in S_n$. Then the equivalence relation $\sim_\sigma$ induces a partition on $\{1, 2, \ldots, n\}$ as $\bigsqcup_{i=1}^{k} B_i$. Then $\sigma|_{B_i} \colon B_i \to B_i$ is a well-defined permutation. Now define

$$\mu_i(x) = \begin{cases} \sigma(x) & (x \in B_i), \\ x & (x \notin B_i). \end{cases}$$

Then μ_i is a cycle of B_i, and $\sigma = \mu_1 \circ \mu_2 \circ \cdots \circ \mu_k$.

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

Remark. $(1,2,3) = (1,3)(1,2)$, $(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_2)$.

Corollary. Any permutation is a product of transpositions, since disjoint cycles can be decomposed into a product of transpositions by the above remark.

Note that this representation is not unique. Since $\tau^2 = id$ for any transposition τ, we can always multiply two same transpositions at the end.

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

Proof.

(Step 1) Take $\sigma \in S_n$, $\tau \in S_n$ (transposition). Then for σ and $\tau\sigma$, their number of orbits differ by 1.

- Case 1. $\tau = (i, j)$ where i, j are not in the same orbit.
  Let $\sigma = (b, j, \dots)(a, i, \dots)(\dots)$. Then $\tau\sigma = (b, i, \dots, a, j, \dots)(\dots)$. So the number of orbits differ by 1.

- Case 2. $\tau = (i, j)$ where i, j are in the same orbit.
  Left as exercise.

(Step 2) Suppose we could write $\sigma = \tau_1\tau_2 \cdots \tau_t = \tau_1'\tau_2' \cdots \tau_s'$ where τ_i, τ_j' are transpositions. Then the number of orbits of σ, t and s have the same parity. This follows directly from Step 1.

So this definition is well-defined!

Definition. A permutation $\sigma \in S_n$ is called

(1) **even** if σ is a product of even number of transpositions.

(2) **odd** if σ is a product of odd number of transpositions.

Definition. (Alternating Group) We define the **alternating group** A_n as

$$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}.$$

Theorem.

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

Proof. Consider a map $\lambda_\tau : A_n \to S_n \setminus A_n$ defined as $\lambda_\tau(\sigma) = \tau \circ \sigma$ where τ is any transposition. Then λ_τ is a bijection.

April 3rd, 2023

Section 10. Cosets and the Theorem of Lagrange

Example. Motivation.

(1) $A_n \leq S_n$. We call $S_n \setminus A_n$ a coset of A_n.

(2) $3\mathbb{Z} \leq \mathbb{Z}$. We call $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ are cosets of $3\mathbb{Z}$.

We saw that A_n and $S_n \setminus A_n$ have the same number of elements. This was done by constructing a bijection between two sets. But we know that a bijection between $3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2$ exist. We guess that the number of elements would be the same.

So if G is a finite group and $H \leq G$, we conjecture that we can partition G by cosets of H, and each cosets have the same number of elements. So $|H| \mid |G|$.

Definition. Let G be a group, $H \leq G$. Define a relation $\sim_L$ on G as

$$a \sim_L b \iff a^{-1}b \in H.$$

Remark. We can also define $\sim_R$ on G as $a \sim_R b \iff ba^{-1} \in H$.

Theorem. $\sim_L$ is an equivalence relation.

Proof.

- $\forall a \in G$, $a^{-1}a = e \in H$. $a \sim_L a$.
- $\forall a, b \in G$, if $a^{-1}b \in H \implies (a^{-1}b)^{-1} = b^{-1}a \in H$. $b \sim_L a$.
- $\forall a, b, c \in G$, if $a^{-1}b, b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. $a \sim_L c$.

Definition. (Coset) Let G, H be groups and $H \leq G$. For $a \in G$, we define

(1) The **left coset** of H as $aH = \{ah : h \in H\}$.

(2) The **right coset** of H as $Ha = \{ha : h \in H\}$.

We see that $a \neq b$ does not imply $aH \neq bH$. If $a, b \in H$, then $aH = bH = H$. So when would we get the same coset?

Remark. $aH = bH \iff H = a^{-1}bH \iff a \sim_L b$.

Example.

(1) For a transposition $\tau \in S_n$, τA_n is a coset of A_n with odd permutations. So it is different from A_n. So for any odd permutation $\sigma \in S_n$, $\sigma A_n = \tau A_n$, and $\sigma \sim_L \tau$.

(2) $3\mathbb{Z} \leq \mathbb{Z}$. $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$ are cosets. Since $\mathbb{Z}$ is commutative, the left and right cosets are equal to each other.

Remark. If G is commutative and $H \leq G$, $aH = Ha$ for $a \in G$.

Check for non-commutative groups that left and rights cosets need not be equal!

Theorem. (Lagrange) Let G be a finite group with $H \leq G$. Then $|H| \mid |G|$.

Proof. If we construct a bijection between any two left cosets, $|H|$ would be $|G|$ divided by the number of left cosets. Which would imply $|H| \mid |G|$.

Recall that left cosets are defined as the equivalence classes with respect to the relation $\sim_L$. So G is a disjoint union of cosets, $G = \bigsqcup aH$. Therefore, $|G| = (\text{number of left cosets}) \cdot |H|$.

Lemma. $|aH| = |bH|$ for $a \in G$, $H \leq G$.

Proof. $\varphi : aH \to bH$ is a bijection. Check by yourself!

Corollary. The number of left cosets and the number of right cosets are equal.

Corollary. Every group of prime order is cyclic.

Proof. Let $|G| = p$, where p is prime. Take $a \in G$ which is not the identity. Then the cyclic subgroup $\langle a \rangle \leq G$ must have order 1 or p. But a must have order p because it is not the identity. So $|\langle a \rangle| = p$, which implies that $G = \langle a \rangle$.

This is a very important result related to the classification of finite (simple) groups. We have seen all groups of order 2, 3, 4. But for larger orders, we can't enumerate them all. With this result, we directly know that for groups with prime order p, the group is isomorphic to $\mathbb{Z}_p$.

This is also a direct result of Lagrange's theorem, since $\langle a \rangle \leq G$.

Theorem. The order of an element in a finite group divides the order of the group. In other words, $|\langle a \rangle| \mid |G|$, for $a \in G$.

Definition. (Index) Let G be a group, (not necessarily finite) and $H \leq G$. We define the **index**

of H in G as

$$(G : H) = \text{number of left cosets of } H = \text{number of right cosets of } H.$$

If $|G| < \infty$, $(G : H) = |G| \, / \, |H|$.

Theorem. For a group G, suppose that $K \leq H \leq G$. If $(G : H)$, $(H : K)$ are finite,

$$(G : K) = (G : H) \, (H : K) \, .$$

Proof. Write $G = \bigsqcup_{i=1}^{n} a_i H$, $H = \bigsqcup_{j=1}^{m} b_j K$, and show that $G = \bigsqcup_{i,j} a_i b_j K$. Check by yourself!

Section 11. Direct Products, Finitely Generated Abelian Groups

Definition. (Cartesian Product) For sets $S_1, \dots, S_n$, define

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n = \{(a_1, \dots, a_n) : a_i \in S_i\}.$$

What if S_i already have a group structure?

Definition. (Direct Product) Let $G_1, \dots, G_n$ be groups. Define a binary operation $\cdot$ as

$$(a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n).$$

Then the **direct product** $\prod_{i=1}^{n} G_i$ is a group with this binary operation.

Notation. We also write the direct sum as $\bigoplus_{i=1}^{n} G_i$ for additive groups.

Example. Compare the Klein 4-group V_4 with $\mathbb{Z}_2 \times \mathbb{Z}_2$. They have the exact same structure! $V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. From this example, we found out that order 4 group is either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now we know all groups of order up to 5. How about order 6? We know S_3 and $\mathbb{Z}_6$.

Example. Consider $\mathbb{Z}_2 \times \mathbb{Z}_3$. We can check that $(1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ has order 6, so $\langle (1, 1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Why was it that $\mathbb{Z}_4 \not\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, but $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$?

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

Proof.

($\Longleftarrow$) We need to find a generator of $\mathbb{Z}_m \times \mathbb{Z}_n$ with order mn. Take $a = (1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$. The order of this element should be divisible by m, n. So mn is the smallest positive integer, and $|\langle (1, 1) \rangle| = mn$.

($\Longrightarrow$) Suppose that $d = \gcd(a, b) > 1$. Then for all $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\frac{mn}{d}(a, b) = (0, 0)$. So (a, b) cannot generate the entire group (which has mn elements). Therefore $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic.