Chapter 1 Group theory

§1 Binary operation.

Definition. Let X be a set. A **(binary) operation** on X is a map $X \times X \to X$.

infix notation $a*b$, $a+b$, $a\cdot b$. not functional form $f(a,b)$

Definition. Let $*$ be a binary operation on X.

1. The operation $*$ is **associative** if $(a*b)*c = a*(b*c)$ for all $a, b, c \in X$.
2. The operation $*$ is **commutative** if $a*b = b*a$ for all $a, b \in X$.

Theorem 1.1 (Generalized associativity). *Let $*$ be an associative operation on a set X. Then for any $x_1, \ldots, x_n \in X$ all possible parenthesizations (加括号) of the expression $x_1 * x_2 * \cdots * x_n$ are equal.*

Pf: by induction of n.

Remark: because of this thm. we may omit some parenthesis when the b.o. is associative.

Definition. Let $*$ be a binary operation on a set X. An element $e \in X$ is an **identity element** or **neutral element** with respect to $*$ if $e*x = x*e = x$ for any $x \in X$.

may not exist for some b.o. (e.g. $a*b = a-b$).

Lemma 1.2. *Let $*$ be a binary operation on a set X. If an identity for $*$ exists, it is unique.*

Proof. If $e, e' \in X$ are identity elements then $e_L = e_L * e'_R = e'_R$. □

Definition. Let $*$ be a binary operation on a set X with identity element e. An element $y \in X$ is an **inverse** (with respect to $*$) of $x \in X$ if $y*x = x*y = e$. An element is **invertible** if it has an inverse.

Lemma 1.3. *Let $*$ be an associative operation on X with identity element e. If an inverse of $x \in X$ exists, it is unique.*

Proposition 1.4. *For an associative operation $*$ on X with identity element e*

1. *if $a \in X$ is invertible then a^{-1} is also invertible and $(a^{-1})^{-1} = a$*
2. *if $a, b \in X$ are invertible then $a*b$ is also invertible and $(a*b)^{-1} = b^{-1} * a^{-1}$.*

§2. Residue classes

Definition. Let $m \in \mathbb{N}$. Integers a and b are **congruent** modulo m if $a - b$ is divisible by m.
Notation: $a \equiv b \pmod{m}$, $a \equiv_m b$.

Proposition 2.1. *Let $m \in \mathbb{N}$.*

1. *$a \equiv a \pmod{m}$ for any $a \in \mathbb{Z}$*
2. *if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ for any $a, b \in \mathbb{Z}$*
3. *if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ for any $a, b, c \in \mathbb{Z}$*
4. *if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{m}$ for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}$*
5. *every integer is congruent modulo m exactly to one of $0, 1, \ldots, m-1$.*

} shows congrument modulo is a equivalent relation

quotient set $\mathbb{Z}/m\mathbb{Z}$ (contains m elements)

Definition. The elements of $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ are called the **residue classes** modulo m.

Remark. $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

(check it is correctly defined)

Introduce on $\mathbb{Z}/m\mathbb{Z}$ addition $+$ and multiplication $\cdot$. If $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, we define

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Check the operation is correctly defined.

i.e $\forall\, a \neq a'$, $b \neq b'$ and $\overline{a} = \overline{a'}$ $\overline{b} = \overline{b'}$ check: $\overline{a+b} = \overline{a'+b'}$ $\overline{ab} = \overline{a'b'}$

Proposition 2.2. *Let $m \in \mathbb{N}$.*

1. *Addition in $\mathbb{Z}/m\mathbb{Z}$ is commutative and associative*
2. *$\overline{0}$ is the identity element in $\mathbb{Z}/m\mathbb{Z}$ with respect to addition If $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ then $\overline{-a}$ is its additive inverse*

Proposition 2.3. *Let $m \in \mathbb{N}$.*

1. *Multiplication in $\mathbb{Z}/m\mathbb{Z}$ is commutative and associative*
2. *$\overline{1}$ is the identity element in $\mathbb{Z}/m\mathbb{Z}$ with respect to multiplication*
3. *$\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ is invertible with respect to multiplication iff $\gcd(a, m) = 1$. In particular if p is prime, all non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ are invertible with respect to multiplication*

$\mathbb{Z}/p\mathbb{Z}$ is a field

Pf: 3. If $a \in \mathbb{Z}$ and $\gcd(a, m) = 1$ then $ab + mn = 1$ for some $b, n \in \mathbb{Z}$ by Bézout's identity. Then $\overline{a}\overline{b} = \overline{ab} = \overline{1 - mn} = \overline{1}$. Conversely, if $\overline{a}\overline{b} = \overline{1}$ for some $b \in \mathbb{Z}$ then $\overline{ab} = \overline{1}$ whence $ab = 1 + mn$ for some $n \in \mathbb{Z}$. This implies $\gcd(a, m) = 1$.

$n, m \in \mathbb{Z}$, $d = \gcd(n, m)$ then $\exists\, a, b \in \mathbb{Z}$ $d = am + bn$.

§3. Permutation.

Definition. A **permutation** of n elements is a bijection from the set $\{1, \ldots, n\}$ to itself. The **identity permutation** is the identity map of this set. The **product** of two permutations is their composition.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \quad \text{or} \quad \big(\sigma(1)\sigma(2)\cdots\sigma(n)\big).$$

(two-line / one-line notation)

use "bijection" case to represent the bijection.

e.g. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$, $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$. $\Rightarrow$ $\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

Find inverse: interchange the 1st and 2nd line. rearrange the 1st line to 1 2 3 4 ··· (ascend order)

Definition. Let σ be a permutation of n elements, $1 < k \leq n$ and there are k distinct numbers $1 \leq m_1, \ldots, m_k \leq n$ such that

i) $\sigma(m_i) = m_{i+1}$ for $1 \leq i \leq k-1$
ii) $\sigma(m_k) = m_1$
iii) $\sigma(t) = t$ for $t \neq m_1, \ldots, m_k$

Such permutations is called a **cyclic permutation** or a **k-cycle**. The set $\{m_1, \ldots, m_k\}$ is the **support** of σ.

Two cycles are **disjoint** if their supports do not intersect.

Proposition 3.1 (Cycle decomposition). *1. Any non-identity permutation can be uniquely expressed as a product of disjoint cycles.*

2. Disjoint cycles commute.

Example. The below permutation is expressed as the product of a 2-cycle and a 3-cycle.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

2 cycle. support $\{1, 5\}$

3 cycle support $\{2, 4, 6\}$

§4. Group

Definition. A set G with binary operation $*$ is a **group** if:

I. $a*(b*c)=(a*b)*c$ for all $a,b,c\in G$ (**associativity**)

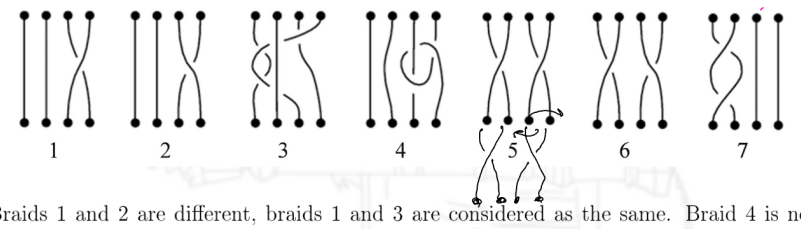
II. There exists $e\in G$ (an **identity element**) such that $a*e=e*a=a$ for any $a\in G$

III. For any $a\in G$ there is $a'\in G$ (an **inverse** of a) such that $a*a'=a'*a=e$

A group G is **commutative**, or **abelian** if $a*b=b*a$ for all $a,b\in G$. A group is **finite** if it has a finite number of elements. The **order** of a group is the number of its elements.

Examples.

1. If $k=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}/n\mathbb{Z}$ then k with respect to addition is an abelian group (the **additive group** of k).
2. If $k=\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{Z}/p\mathbb{Z}$ then $k^*=k\setminus\{0\}$ with respect to multiplication is an abelian group (the **multiplicative group** of k).
3. The set of all invertible matrices over $k=\mathbb{Q},\mathbb{R},\mathbb{C}$ with respect to multiplication $\mathrm{GL}_n(k)$ is a non-abelian group (the **general linear group**).
4. $T=\{z\in\mathbb{C}\mid |z|=1\}$ with respect to multiplication is an abelian group
5. The set of all permutations of n elements with respect to multiplication S_n is a non-abelian group (the **symmetric group**)
6. The set of all isometries of a fixed regular n-gon with respect to composition D_n is a non-abelian group (the **dihedral group**). It consists of n rotations and n reflections and thus $|D_n|=2n$.
7. The set of all braids one can make with n strands under concatenation is a non-abelian group. Its identity element is the untangled braid. If one starts with a set of straight strands whose ends are tied off, tangles it while leaving the ends tied, and then partitions it into two braids, one braid is the inverse of the other.



Braids 1 and 2 are different, braids 1 and 3 are considered as the same. Braid 4 is not considered a braid as the strands are required to move upside down. The concatenation of braids 5 and 6 yields braid 7.

Lemma 4.1 (Cancellation property). *Let G be a group with binary operation $*$. If $g*h=g*h'$ for some $g,h,h'\in G$ then $h=h'$.*

Proposition 4.2. *$G\times H$ with respect to the operation $\bullet$ is a group.*

operation $\bullet$ $\quad (g,h)\bullet(g',h')=(g*g',\ h\star h')$. $*$ is operation in G. $\star$ is operation in H.

Definition. $G\times H$ with above defined operation $\bullet$ is called the **direct product** of the groups G and H.

Definition. Let G be a finite group consisting of the elements e , $g_1,g_2,g_3,\cdots,g_n$. The **Cayley table** of G has g_ig_j at its (i,j)th position.

	e	g_2	g_3	$\cdots$	g_n
e	e	g_2	g_3	$\cdots$	g_n
g_2	g_2	g_2g_2	g_2g_3	$\cdots$	g_2g_n
g_3	g_3	g_3g_2	g_3g_3	$\cdots$	g_3g_n
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
g_n	g_n	g_ng_2	g_ng_3	$\cdots$	g_ng_n

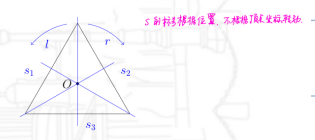
Proposition 4.3. *1. A group is commutative if and only if its Cayley table is symmetric.*

2. Each row and column of the Cayley table is a permutation of the elements of the group.

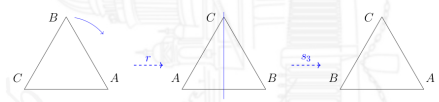
2. Let $S_3=\{(123),(213),(132),(321),(231),(312)\}$.

$\circ$	(123)	(213)	(132)	(321)	(231)	(312)
(123)	(123)	(213)	(132)	(321)	(231)	(312)
(213)	(213)	(123)	(231)	(312)	(132)	(321)
(132)	(132)	(312)	(123)	(231)	(321)	(213)
(321)	(321)	(231)	(312)	(123)	(213)	(132)
(231)	(231)	(321)	(213)	(132)	(312)	(123)
(312)	(312)	(132)	(321)	(213)	(123)	(231)

3. Consider a regular triangle with center O. Then $D_3=\{e,r,l,s_1,s_2,s_3\}$ where e is the identity map, r is the clockwise rotation about O by 120°, l is the counterclockwise rotation about O by 120°, and s_1,s_2,s_3 are the reflections across the lines connecting the midpoints of each side to the opposite vertices.



Example of calculation: $s_3r=s_1$.



	e	l	r	s_1	s_2	s_3
e	e	l	r	s_1	s_2	s_3
l	l	r	e	s_2	s_3	s_1
r	r	e	l	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r	l
s_2	s_2	s_1	s_3	l	e	r
s_3	s_3	s_2	s_1	r	l	e

§5. Subgroup.

Definition. Let G be group. A non-empty subset $H \subset G$ is a **subgroup** of G (notation: $H < G$) if

↳ 此处的"<"不是"真"的含义.

I. $hh' \in H$ for any $h, h' \in H$.

II. $h^{-1} \in H$ for any $h \in H$.

Lemma 5.1. *If $H < G$ then $e \in H$.*

Proof. If $h \in H$ then $h^{-1} \in H$ and $e = hh^{-1} \in H$. □

Remark. If H is a subgroup of G, then the H with respect to the restriction of the group operation from G is a group.

Examples.
1. In any group G, there are **trivial** subgroups $\{e\} < G$ and $G < G$.
2. For $m \in \mathbb{N}$, the set $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.
3. The set of complex nth roots of unity U_n is a subgroup of $T = \{z \in \mathbb{C} \mid |z| = 1\}$.
4. The set of positive real numbers $\mathbb{R}_{>0}$ is a subgroup of the multiplicative group of $\mathbb{R}$.
5. The set $T_n = \{z \in \mathbb{C} \mid z^n = 1\}$ is a subgroup of T.
6. The set of all matrices with determinant 1 over $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathrm{SL}_n(k)$ is a subgroup $\mathrm{GL}_n(k)$ (the **special linear group**).
7. The set of all permutations of n elements with a given fixed point is a subgroup of S_n.
8. The set of all the even permutations of n elements A_n is a subgroup of S_n (the **alternati group**).
9. The subset of all rotations in D_n is a subgroup.

e.g. (1) two trivial subgroup. $\{e\}$ and G. ($G < G$, $\{e\} < G$)

(2) The set of all matrices with determinant 1 over $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathrm{SL}_n(k)$ is a subgroup of $\mathrm{GL}_n(k)$ (the **special linear group**).

(3) 8. The set of all the even permutations of n elements A_n is a subgroup of S_n (the **alternating group**). even per × even per = even per

Theorem 5.2. *Any subgroup G of the additive group $\mathbb{Z}$ has the form $m\mathbb{Z}$ for some a non-negative $m \in \mathbb{Z}$.*

Lemma 5.3. *Let $\{H_i\}_{i \in I}$ be a family of subgroups of a group G and $H = \bigcap_{i \in I} H_i$. Then $H < G$.*

Definition. Let $X \subset G$ be a subset of a group G. The smallest subgroup of G containing X is called the **subgroup generated by** X, and is denoted by $\langle X \rangle$. Thus $\langle X \rangle$ is defined by the following conditions: $X \subset \langle X \rangle$ and if $H < G$, $X \subset H$, then $\langle X \rangle \subset H$. Clearly the subgroup generated by X is unique (if exists).

If $\langle X \rangle = G$, the group G is said to be **generated** by X, or X is a **generating set** of G or a set of **generators** of G.

Remark. For a finite set $X = \{x_1, \ldots, x_n\}$, we often write $\langle x_1, \ldots, x_n \rangle$ instead of $\langle \{x_1, \ldots, x_n\} \rangle$.

Proposition 5.5. *Let G be a group, $X \subset G$. The intersection of all subgroups of G, containing X is the subgroup generated by X.*

$\langle X \rangle = \bigcap_{i \in I} A_i$ A_i subgroup contain X → show the existence of $\langle X \rangle$ (intersection always exist).

Proof. By Lemma 5.3, the intersection of all subgroups of G containing X is a subgroup of G. Denote it by $\langle X \rangle$. The set X is contained in all the intersecting subgroups, thus it is contained in $\langle X \rangle$. ✓1 On the other hand, if a subgroup H contains X, then H is one of the intersecting subgroups and $\langle X \rangle \subset H$. ✓2 ✓1 subgroup ✓2 is smallest. □

Proposition 5.6. *Let G be a group, $X \subset G$. The subgroup generated by X is the set of all the products of elements of X and and their inverses:*

$$\langle X \rangle = \{y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n} \mid y_i \in X, \varepsilon_i = \pm 1 \text{ for all } i = 1, \ldots, n\}.$$

Proof. Denote the set of all the products of elements of X and their inverses by Y. First prove that $Y \subset \langle X \rangle$. Let $y = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n} \in Y$. If $H < G$ is an arbitrary subgroup containing X, then H also contains $y_1^{\varepsilon_1}, \ldots, y_n^{\varepsilon_n}$, and thus contains their product y. Therefore y belongs to the intersection of all such subgroups H, which is equal to $\langle X \rangle$ by Proposition ~~??~~ 5.5

Conversely, one can easily verify that Y is a subgroup of G. Since $X \subset Y$, the inverse inclusion $\langle X \rangle \subset Y$ follows. □

e.g. S_3 is not generated by any single element, but is generated by any set that contains a transposition (換) and a 3-cycle. For example, $S_3 = \langle (132), (231) \rangle$ since $(132)(231) = (321), (231)(132) = (213), (231)^{-1} = (312)$.

§6. Order of element

Definition. Let G be a group, $g \in G$ and $n \in \mathbb{Z}$. Define the nth **power** of g by

$$g^n = \begin{cases} \underbrace{gg\cdots g}_{n \text{ times}}, & \text{if } n > 0 \\ \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{-n \text{ times}}, & \text{if } n < 0 \\ e, & \text{if } n = 0 \end{cases}$$

Proposition 6.1. *For any $g \in G$ and $m, n \in \mathbb{Z}$*

1. $g^{n+m} = g^n g^m$
2. $(g^n)^m = g^{nm}$

Proof. Assume for example that $n > 0, m < 0, n + m > 0$. Then

$$g^{n+m} = \underbrace{gg\cdots g}_{n+m \text{ times}} = \underbrace{gg\cdots g}_{n-(-m) \text{ times}} = \underbrace{gg\cdots g}_{n \text{ times}}\underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{-m \text{ times}} = g^n g^m.$$

The other cases are treated similarly. □

Remark. When the group operation is given by addition, the identity element is denoted by 0, and the inverse of g is $-g$. In this case, the nth power of g is written as ng. This notation is called the **additive** notation, as opposed to the default **multiplicative** notation.

Definition. Let G be a group and $g \in G$. The **order** of g (denoted by $\operatorname{ord}_G g$ or simply $\operatorname{ord} g$) is the least $m \in \mathbb{N}$ such that $g^m = e$. If $g^m \neq e$ for any $m \in \mathbb{N}$, then g is said to be of **infinite order**.

Remark $\operatorname{ord} g = \operatorname{ord} g^{-1}$

Proposition 6.3. *Let $g \in G$ be an element of finite order n. If $m \in \mathbb{Z}$, then $g^m = e$ if and only if $n|m$.* → 整除

Proof. If $m = ns + r, 0 \leq r < n$ then $g^m = g^{ns+r} = (g^n)^s g^r = e^s g^r = g^r$. If $r = 0$, then $g^m = e$. If $r \neq 0$, then $g^r \neq e$ since $r < n, g^n = e$ and n is the least exponent satisfying this property. □

Proposition 6.4. *If G is a group and $g \in G$ then $|\langle g \rangle| = \operatorname{ord}(g)$.* → $\langle g \rangle$ 中的元素数目.

Proposition 6.5. *Let G be a group, $a, b \in G$ commute and $\langle a \rangle \cap \langle b \rangle = \{e\}$. If $\operatorname{ord} a = n, \operatorname{ord} b = m$, then $\operatorname{ord} ab = \operatorname{lcm}(n, m)$.*

✕ not correct

Proof. Let $N = \operatorname{lcm}(n, m)$. Then $n, m | N$, whence $a^N = b^N = e$ and $(ab)^N = a^N b^N = e$. If $(ab)^k = e$ for some $k > 0$ then $a^k = b^{-k}$ and $a^k = b^k = e$. Now Proposition 6.3 implies $n, m \mid k$ whence $k \geq N$. □

① $d = \gcd(n,m)$, $n = dn'$, $m = dm'$ $\Rightarrow \gcd(n',m') = 1$, $\operatorname{lcm}(m,n) = n'm'd$

② $\gcd(a,b) = 1$, $b \mid ac$ $\Rightarrow b \mid c$

③ $\gcd(a,b) = 1$, $a \mid c$, $b \mid c$ $\Rightarrow ab \mid c$

Corollary 6.6. *The order of a permutation represented as the product of disjoint cycles equals the least common multiple of the length of these cycles.*

§7 Coset and Normal subgroup.

陪集.

Definition. Let G be a group, $H < G$, and $g \in G$. The set

$$gH = \{gh \mid h \in H\}$$

is called a **left coset** of H. Similarly, the set

$$Hg = \{hg \mid h \in H\}$$

is a **right coset** of H.

The set of all left cosets of H is denoted by G/H.

Remarks. 1. $eH = He = H$.

2. If G is commutative, the left and right cosets coincide.

Definition. Let G be a group, $H < G$. Introduce the relations $\sim_H$ and ${}_H\sim$ on G : $g \sim_H g'$ if $g^{-1}g' \in H$ and $g {}_H\sim g'$ if $g'g^{-1} \in H$.

Remark. If G is commutative, the above relations coincide.

Proposition 7.1. *The relations $\sim_H$ and ${}_H\sim$ are equivalence relations; the equivalence class of $g \in G$ with respect to $\sim_H$ equals gH, and the equivalence class of $g \in G$ with respect to ${}_H\sim$ equals Hg.*

Pf: 1. check the equivalence.

2. Note that $y \in G$ belongs to the equivalence class of $g \in G$ if and only if $g \sim_H y$. This holds if and only if $g^{-1}y \in H$, that is $g^{-1}y = h$ for some $h \in H$. This, in turn, is equivalent to the fact that $y = gh$, i.e., $y \in gH$.

Corollary 7.2. *Let G be a group, $H < G$. The left (right) cosets of H form a partition of G.*

common cosets:

Examples. 1. $G = \mathbb{Z}, H = m\mathbb{Z}$, the left (= the right) cosets are $\{a + mn \mid m \in \mathbb{Z}\}, 0 \le a \le m-1$

2. $G = \mathbb{C}^*, H = T$, the left (= the right) cosets are $\{z \in \mathbb{C} \mid |z| = r\}, r > 0$ ($T = \{z \in \mathbb{C} \mid |z| = 1\}$)

3. $G = D_3, H = \{e, s_1\}$, the left cosets are $\{e, s_1\}, \{r, s_3\}, \{l, s_2\}$, the right cosets are $\{e, s_1\}, \{r, s_2\}, \{l, s_3\}$ non-commutative.

4. $G = D_3, H = \{e, r, l\}$, the left (= the right) cosets are $\{e, r, l\}, \{s_1, s_2, s_3\}$

$s_1H = eH = \{e, s_1\}$
$s_2H = rH = \{re, rs_1\} = \{r, s_3\}$
$s_3H = lH = \{le, ls_1\} = \{l, s_2\}$

Definition. Let G be a group. A subgroup $H < G$ is called **normal** (notation: $H \triangleleft G$), if $Hg = gH$ for any $g \in G$. 注意. g不是从H中取.

Lemma 7.3. *Let G be a group, $H < G$. The following conditions are equivalent:*

1. *H is normal;*
2. *$ghg^{-1} \in H$ for all $g \in G, h \in H$.* criterion: if the conjugate of all the element $\in H$, then $H \triangleleft G$.

Pf: "⇒" $gh = h'g$. for some $h' \in H$. $ghg^{-1} = h' \in H$. "⇐" prove $gH \subset Hg$ and $Hg \subset gH$.

Definition. Let G be a group, $g, h \in G$. The element ghg^{-1} is called a **conjugate** of h; or it is said that h and ghg^{-1} are **conjugate**.

example of normal subgroup:

Examples. 1. $\{e\} \triangleleft G, G \triangleleft G$.

2. Every subgroup of an abelian group is normal.

3. $\{e, r, l\}$ is a normal subgroup of D_3, $\{e, s_1\}$ is not a normal subgroup of D_3 .

4. $\mathrm{SL}_n(k) \triangleleft \mathrm{GL}_n(k)$. Indeed, if $h \in \mathrm{SL}_n(k)$ and $g \in \mathrm{GL}_n(k)$, then $\det(ghg^{-1}) = \det(g) \cdot \det(h) \cdot \det(g^{-1}) = \det(h) = 1$, so $ghg^{-1} \in \mathrm{SL}_n(k)$.

5. $A_n \triangleleft S_n$. Indeed, if $h \in A_n$ and $g \in S_n$, then $ghg^{-1} \in A_n$ as the product of an even permutation and two ~~odd~~ permutations with same parity

$GL_n(k)$ invertible. w.r.t. multiple
$SL_n(k)$. invertible. w.r.t. multiple. det = 1.

A_n all even per

§8 Lagrange's Theorem.

Definition. Let G be a group, $H < G$. The number of the left cosets of H is called the **index** of H and is denoted by $|G : H|$.

Lemma 8.1. *Let G be a group, $H < G$. Then there is a bijection between the set of the left cosets of H and the set of the right cosets of H. In particular, these numbers are equal if one of them is finite.*

Proof. Consider $\varphi\colon G \to G, \varphi(g) = g^{-1}$. Then $\varphi(gH) = Hg^{-1}$ since for any $h \in H$ one has $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1}$ and $h^{-1} \in H$, similarly for any $h \in H$ one has $hg^{-1} = (gh^{-1})^{-1} = \varphi(gh^{-1})$ and $h^{-1} \in H$. Since φ is a bijection, it induces bijection from the set of the left cosets to the set of the right cosets. □

Proposition 8.2. *Any subgroup of index 2 is normal.*

Theorem 8.3 (Lagrange's Theorem)**.** *If G is a finite group, $H < G$, then $|G| = |H| \cdot |G : H|$.* → 表示元素数目.

Proof. First prove that all the left cosets of H are equal-sized. Note that for each $g \in G$ the map $H \to gH$, $h \mapsto gh$, defines a bijection between H and gH. Indeed, if $gh = gh'$, then $h = h'$, and the subjectivity of this map follows from the definition of gH. Since H is one of the cosets, the number of element of any coset equals $|H|$. Thus, G is partitioned into $|G : H|$ cosets of size $|H|$ each which completes the proof. □

Corollary 8.4. *The order of a finite group G is divisible by the order of any of its element.* order of G = G 中元素个数.

Corollary 8.5. *Let G be a finite group. Then $g^{|G|} = e$ for any $g \in G$.*

Theorem 8.6 (Euler)**.** *Let $m \in \mathbb{N}, a \in \mathbb{Z}$, and $\gcd(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$, where $\varphi(m)$ is the Euler function defined as the number of integers k in the range $1 \le k \le n$ for which $\gcd(m, k) = 1$.*

Proof. Consider $G = \{\overline{b} \in \mathbb{Z}/m\mathbb{Z} \mid b \in \mathbb{Z}, \gcd(b, m) = 1\}$. It is a group under multiplication by Proposition 2.3 and $|G| = \varphi(m)$. Now $\overline{a} \in G$ and Corollary 8.5 implies $\overline{a}^{\varphi(m)} = \overline{1}$ which gives the required congruence. □

§9. Quotient group and commutator subgroup.

G - group. $H \triangleleft G$. a binary operation on G/H: $(gH)(g'H) = (gg')H$, $gH, g'H \in G/H$.

Theorem 9.1. *The above operation is well-defined and is a group operation on G/H.*

Proof. One has to verify that $(\widetilde{g}\widetilde{g}')H = (gg')H$ if $\widetilde{g} \in gH$ and $\widetilde{g}' \in g'H$. These conditions imply $\widetilde{g} = gh$, $\widetilde{g}' = g'h'$ for some $h, h' \in H$; then $\widetilde{g}\widetilde{g}' = (gh)(g'h') = g(hg')h'$. Since $H \triangleleft G$, $hg' = g'h''$ for some $h'' \in H$, one has $\widetilde{g}\widetilde{g}' = gg'h''h' \in gg'H$.

The identity element of G/H is the coset $eH = H$, since $(eH)(gH) = (eg)H = gH = (ge)H = (gH)(eH)$ for any $g \in G$. Further, for $g, g', g'' \in G$ one has $((gH)(g'H))(g''H) = (gg'H)(g''H) = (gg')g''H = g(g'g'')H = (gH)(g'g''H) = (gH)((g'H)(g''H))$. Finally, the coset $g^{-1}H$ is the inverse of gH since $(gH)(g^{-1}H) = gg^{-1}H = eH = g^{-1}gH = (g^{-1}H)(gH)$. □

Definition. The set of left cosets G/H together with above operation is called the **quotient group** of G by H. the order of quotient group = index

Definition. Let G be a group, $x, y \in G$. The element $[x, y] = xyx^{-1}y^{-1}$ is called the **commutator** of x, y. The subgroup $\langle\{[x, y] \mid x, y \in G\}\rangle$ is the **commutator subgroup** of G and is denoted by $K(G)$.

Theorem 9.2. *Let G be a group. Then*

1. *$K(G) \triangleleft G$ and $G/K(G)$ is commutative*
2. *If $H \triangleleft G$ and G/H is commutative, then $K(G) \subset H$.* commutator subgroup is the minimum subgroup.

Definition. Let G be a group. The set $Z(G) = \{a \in G \mid ab = ba \text{ for any } b \in G\}$ is called the **center** of G. "kind of measure" of commutivity of G.

Theorem 9.4. *The center of a group is a normal subgroup.*

Proof. The fact that $Z(G)$ is a subgroup is easily verified. For $a \in Z(G), b \in G$, one has $bab^{-1} = abb^{-1} = a \in Z(G)$, which implies its normality. □

quotient groups

Examples.

1. G/G is a one-element group.
2. $G/\{e\}$ can be identified with G. Indeed, each coset of $\{e\}$ is of the form $\{g\}, g \in G$ and hence can identified with g. Clearly, under this identification the operation on the quotient group corresponds to the group operation on G: $\{g\}\{g'\} = \{gg'\}$.
3. The construction of the residue classes modulo n and the definition of addition on them is a particular case of the quotient group G/H for $G = \mathbb{Z}, H = n\mathbb{Z}$.
4. $G = D_4, H = \{e, q\}$. Then G/H contains the following cosets: $H = \{e, q\}, rH = \{r, l\}, s_1H = \{s_1, s_2\}, t_1H = \{t_1, t_2\}$ and its Cayley table is

	H	rH	s_1H	t_1H
H	H	rH	s_1H	t_1H
rH	rH	H	t_1H	s_1H
s_1H	s_1H	t_1H	H	rH
t_1H	t_1H	s_1H	rH	H

Example of calculation: $(s_1H)(rH) = s_1rH = t_2H = t_1H$ since $s_1r = t_2$.

§10. Homomorphism.

一种"保运算的态射".

Definition. Let G, H be groups. A map $\varphi: G \to H$ is called a **homomorphism** if

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ for any } x, y \in G.$$

"inside" "same"

A homomorphism from G to G is called an **endomorphism** of G. The set of all homomorphisms from G to H is denoted by $\mathrm{Hom}(G, H)$ and the set of all endomorphisms of G is denoted by $\mathrm{End}(G)$.

Lemma 10.1. *If $\varphi \in \mathrm{Hom}(G, H)$ then $\varphi(e_G) = e_H$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$ for all $x \in G$.*

Proof. Note that $e_G e_G = e_G$. Therefore, $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ whence $e_H = \varphi(e_G)\varphi(e_G)^{-1} = \varphi(e_G)\varphi(e_G)\varphi(e_G)^{-1} = \varphi(e_G)$.

Now let $x \in G$. Then $e_H = \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$ and $e_H = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$ which gives $\varphi(x)^{-1} = \varphi(x^{-1})$. □

Examples for homomorphism.

Examples.

1. Let G, H be groups. The map from G to H, $g \mapsto e$, is a **trivial** homomorphism.
2. Let $G = \mathbb{R}, H = \mathbb{R}^*$. The exponent $\exp: \mathbb{R} \to \mathbb{R}^*, \exp(x) = e^x$, is a homomorphism since $e^{x+y} = e^x \cdot e^y$ for all $x, y \in \mathbb{R}$.
3. Let $G = \mathbb{C}, H = \mathbb{R}$. The module $|\ \ |: \mathbb{C} \to \mathbb{R}^*$ is a homomorphism, since $|xy| = |x||y|$ for all $x, y \in \mathbb{C}$.
4. Let $G = S_n, H = \{\pm 1\}$. The sign $\mathrm{sgn}: S_n \to \{\pm 1\}$ is a homomorphism by the statement that relates the parities of two permutations and the parity of their product.
5. Let $k = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}$ and $G = H = k$ and $a \in k$. The map $\varphi: k \to k$, $\varphi(x) = ax$ is a homomorphism.
6. Let $k = \mathbb{R}, \mathbb{Q}, \mathbb{C}$ and $G = \mathrm{GL}_n(k)$, $H = k^*$. The determinant $\det: \mathrm{GL}_n(k) \mapsto k^*$ is a homomorphism since $\det(AB) = \det A \cdot \det B$ for all $A, B \in \mathrm{GL}_n(k)$.
7. Let G be an arbitrary finite group of order n, $H = S_n$. The map $\Phi: G \to S_n$, $\Phi(g) = \sigma_g$ for $\sigma_g(h) = gh, h \in G$, is a homomorphism since $\Phi(gg')(h) = \sigma_{gg'}(h) = (gg')h$ and $(\Phi(g) \circ \Phi(g'))(h) = \Phi(g)(\Phi(g')(h)) = \sigma_g(\sigma_{g'}(h)) = g(g'h)$ for any $h \in G$.

Proposition 10.2. *Let G_1, G_2, G_3 be groups and $\varphi \in \mathrm{Hom}(G_1, G_2), \psi \in \mathrm{Hom}(G_2, G_3)$. Then $\psi \circ \varphi \in \mathrm{Hom}(G_1, G_3)$.*

Vector space　　Topological space　　Group.

linear map　　continuous map　　homomorphic map. ⇒ composition of ~ is still ~.

Definition. Let $\varphi \in \mathrm{Hom}(G, H)$. The **kernel** of φ is

$$\mathrm{Ker}(\varphi) = \{x \in G \mid \varphi(x) = e_H\}.$$

The **image** of φ is

$$\mathrm{Im}(\varphi) = \{y \in H \mid y = \varphi(x) \text{ for some } x \in G\}.$$

Proposition 10.3. *If $\varphi \in \mathrm{Hom}(G, H)$ then $\mathrm{Im}(\varphi) < H$, $\mathrm{Ker}(\varphi) \triangleleft G$.*

Proof. Let $h, h' \in \mathrm{Im}(\varphi)$. Then there exist $g, g' \in G$ such that $\varphi(g) = h, \varphi(g') = h'$. Then $\varphi(gg') = \varphi(g)\varphi(g') = hh'$, whence $hh' \in \mathrm{Im}(\varphi)$. Further, $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1} = h^{-1}$, whence $e_H \in \mathrm{Im}(\varphi)$ and $h^{-1} \in \mathrm{Im}(\varphi)$ whenever $h \in \mathrm{Im}(\varphi)$.

Now let $g, g' \in \mathrm{Ker}(\varphi)$. Then $\varphi(g) = \varphi(g') = e_H$. Now $\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$, so $gg' \in \mathrm{Ker}(\varphi)$. Also $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H$, whence $e_G \in \mathrm{Ker}(\varphi)$ and $g^{-1} \in \mathrm{Ker}(\varphi)$ for any $g \in \mathrm{Ker}(\varphi)$.

Finally, if $g \in \mathrm{Ker}(\varphi), x \in G$, then $\varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x^{-1}) = \varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \phi(e_G) = e_H$, whence $xgx^{-1} \in \mathrm{Ker}(\varphi)$. It shows that $\mathrm{Ker}(\varphi)$ is a normal subgroup of G. □

Lemma 10.4. *Let $\varphi \in \mathrm{Hom}(G, H)$. Then φ is injective if and if and only if $\mathrm{Ker}(\varphi) = \{e_G\}$.*

Similarly in vector space.

L is injective ⟺ $\ker L = \{0\}$

Proof. If φ is injective and $\varphi(g) = e_H$ then $g = e_G$ since $\varphi(e_G) = e_H$.

Conversely, if $\mathrm{Ker}(\varphi) = \{e_G\}$ and $g, g' \in G$ are such that $\varphi(g) = \varphi(g')$, then $\varphi(g^{-1}g') = \varphi(g^{-1})\varphi(g') = \varphi(g)^{-1}\varphi(g') = e_H$, so $g^{-1}g' \in \mathrm{Ker}(\varphi) = \{e_G\}$ and $g = g'$. □

$\langle X \rangle = G$

Proposition 10.5. *Let G, H be groups and $X \subset G$ be a generating set of G. If $\varphi, \psi \in \mathrm{Hom}(G, H)$ and $\varphi(x) = \psi(x)$ for any $x \in X$ then $\phi = \psi$.*

Proof. By Proposition 5.6, any $g \in G$ can be expressed as $g = y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}, y_i \in X, \varepsilon_i = \pm 1$. Then

$$\varphi(g) = \varphi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}) = \varphi(y_1)^{\varepsilon_1} \cdots \varphi(y_n)^{\varepsilon_n} = \psi(y_1)^{\varepsilon_1} \cdots \psi(y_n)^{\varepsilon_n} = \psi(y_1^{\varepsilon_1} \cdots y_n^{\varepsilon_n}) = \psi(g).$$

Use Prop. 10.5 to solve:

Problem 10.6. *Prove that if $\varphi \in \mathrm{End}(\mathbb{Z})$ then there is $a \in \mathbb{Z}$ such that $\varphi(x) = ax, x \in \mathbb{Z}$.*

the only type of endo in $\mathbb{Z}$.

Solution. Put $a = \varphi(1)$ and $\psi \in \mathrm{End}(\mathbb{Z}), \psi(x) = ax$. Since 1 generates $\mathbb{Z}$ and $\varphi(1) = \psi(1)$, Proposition 10.5 completes the proof. □

把$\varphi(1)$的值赋给 a.　ψ是代表

$\psi \in \mathrm{End}(\mathbb{Z})$. (see Example 5.)

applies Prop 10.5.

Problem 10.7. *Prove that there is only the trivial homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}$.*

Solution. If $\varphi \in \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z})$ then

$$0 = \varphi(\overline{0}) = \varphi(\underbrace{\overline{1} + \cdots + \overline{1}}_{m \text{ times}}) = \underbrace{\varphi(\overline{1}) + \cdots + \varphi(\overline{1})}_{m \text{ times}} = m\varphi(\overline{1})$$

由此 whence $\varphi(\overline{1}) = 0$. Since $\overline{1}$ generates $\mathbb{Z}/m\mathbb{Z}$, Proposition 10.5 completes the proof. □

Problem 10.8. *Prove that there is only one non-trivial homomorphisms from D_3 to $\mathbb{Z}/6\mathbb{Z}$.*

Solution. Let $\varphi \in \mathrm{Hom}(D_3, \mathbb{Z}/6\mathbb{Z})$. Since $r^2 s_1 = s_2 = s_3 r$, one has $2\varphi(r) + \varphi(s_1) = \varphi(r^2 s_1) = \varphi(s_3 r) = \varphi(s_1) + \varphi(r)$. It gives $\varphi(r) = \overline{0}$ and hence $\varphi(l) = \overline{0}$ and $\varphi(s_1) = \varphi(s_2) = \varphi(s_3)$. Further, $s_1^2 = e$ implies $2\varphi(s_1) = \overline{0}$ whence $\varphi(s_1) = \overline{0}$ or $\overline{3}$. Overall, we get only one non-trivial homomorphism $\varphi(s_1) = \varphi(s_2) = \varphi(s_3) = \overline{3}, \varphi(r) = \varphi(l) = 0$. □

$r = l^{-1}$　$\varphi(r^{-1}) = (\overline{0})^{-1}$

§ 11. Isomorphisms.

in vector space. isomorphism. → dim =

Definition. Let G, H be groups. A map $\varphi\colon G \to H$ is called an **isomorphism** if φ is a bijective homomorphism. Groups G, H are called **isomorphic** (notation: $G \cong H$) if there exists an isomorphism between them.

Remark. If the groups are finite, they are isomorphic if one can rearrange the elements of one of them so that their Cayley tables become identical.

Lemma 11.1. *Isomorphism is an equivalence relation on the set of all groups.*

Pf: check $G \cong G$, $G \cong H \Rightarrow H \cong G$, $G_1 \cong G_2$ and $G_2 \cong G_3 \Rightarrow G_1 \cong G_3$.

isomorphism preserve some properties.

Proposition 11.2. *A group isomorphic to a commutative group is commutative.*

Proof. Let $\varphi\colon G \to H$ be an isomorphism and G be commutative. Then $xy = \varphi(\varphi^{-1}(x)\varphi^{-1}(y))) = \varphi(\varphi^{-1}(y)\varphi^{-1}(x))) = yx$ for any $x, y \in H$. □

Proposition 11.3. *If $\varphi\colon G \to H$ is an isomorphism, then $\operatorname{ord}_G g = \operatorname{ord}_H \varphi(g)$ for any $g \in G$.*

Proof. Let $\operatorname{ord}_G g = n, \operatorname{ord}_H \varphi(g) = m$. Then $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$, whence $n \geq m$. On the other hand, $\varphi(g^m) = \varphi(g)^m = e_H = \varphi(e_G)$, whence $g^m = e_G$, and so $m \geq n$. □

★ Generally, isomorphic groups have identical group properties. Thus, in order to show that two groups are non-isomorphic it is enough to find a property that holds in one group and does not hold in another.

1) G_1 is commutative. G_2 not.

2) G_1 has element of order n. G_2 don't have.

Examples.
1. The identity map $\mathrm{id}_G\colon G \to G$ is an isomorphism.
2. Let $G = \{\pm 1\}$ be a group under multiplication, $H = \mathbb{Z}/2\mathbb{Z}$. The map $1 \mapsto \bar{0}, -1 \mapsto \bar{1}$ is an isomorphism.
3. Let $G = \mathbb{R}_{>0}$ be the group of positive real numbers under multiplication, $H = \mathbb{R}$. The logarithm $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ is an isomorphism. $\ln(x+y) = \ln x + \ln y$
4. $\mathbb{Z}/n\mathbb{Z} \cong T_n$. The map $\bar{\ell} \mapsto \cos(\ell/2\pi n) + i\sin(\ell/2\pi n)$ is an isomorphism. → T_n 是绕 n 次旋转反回原点
5. Let $G = D_3, H = S_3$. Any isometry of a regular triangle generates a permutation of its three vertices. The corresponding map from G to H is an isomorphism.

2) $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $G = \{\pm 1\}$.

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

×	1	−1
1	1	−1
−1	−1	1

4) $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	1	ξ	ξ^2
1	1	ξ	ξ^2
ξ	ξ	ξ^2	1
ξ^2	ξ^2	1	ξ

5) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$|D_6| = 6$ $|S_4| = 24$. ∴ isomorphism

Problem 11.4. *Prove that $\mathbb{Q} \ncong \mathbb{Q}_{>0}$ where $\mathbb{Q}_{>0}$ is the group of positive rational numbers under multiplication.*

一定有 $\varphi(0) = 1$.

Solution. Let φ be an isomorphism from $\mathbb{Q}$ to $\mathbb{Q}_{>0}$ and $\varphi(1) = q \in \mathbb{Q}, q \neq 1$. Then for any $n \in \mathbb{N}$ one has $q = \varphi(n \cdot 1/n) = \varphi(1/n)^n$. Thus for any $n \in \mathbb{N}$ the equation $x^n = q$ has a solution in $\mathbb{Q}$, which is false. → $q = 1$. contradicts. □

Theorem 11.5 (Fundamental theorem on homomorphisms). *Let G, H be groups, $\varphi \in \operatorname{Hom}(G, H)$. Then $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.*

Proof. Denote $J = \operatorname{Ker}(\varphi)$ which is a normal subgroup of G by Proposition 10.3 and define the map $\Phi\colon G/J \to \operatorname{Im}(\varphi), \Phi(gJ) = \varphi(g)$. The map is well-defined: if $gJ = g'J$, then $g = g'x$ for some $x \in J$ and $\varphi(g) = \varphi(g'x) = \varphi(g')\varphi(x) = \varphi(g')$.

Check that Φ is a homomorphism:

$$\Phi(gJ)\Phi(g'J) = \varphi(g')\varphi(g') = \varphi(gg') = \Phi((gg')J) = \Phi(gJ \cdot g'J), \quad g, g' \in G.$$

If $gJ \in \operatorname{Ker}\Phi$ then $e_H = \Phi(gJ) = \varphi(g)$ so $g \in J$ and $gJ = J$. Thus $\operatorname{Ker}\Phi$ is trivial and Φ is injective by Lemma 10.4. If $h \in \operatorname{Im}(\varphi)$ then $\varphi(g) = h$ for some $g \in G$ and $\Phi(gJ) = \varphi(g) = h$ which shows that Φ is surjective. □

Examples.
1. If $\det\colon \mathrm{GL}_n(\mathbb{R}) \mapsto \mathbb{R}^*$ then $\operatorname{Ker}(\det) = \mathrm{SL}_n(\mathbb{R}), \operatorname{Im}(\det) = \mathbb{R}^*$, which gives $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.
2. Let G, H be arbitrary groups, consider the projection $\mathrm{pr}_G\colon G \times H \to G$, $\mathrm{pr}_G((g,h)) = g$. Clearly it is a homomorphism and $\operatorname{Ker}(\mathrm{pr}_G) = \{e_G\} \times H, \operatorname{Im}(\mathrm{pr}_G) = G$, whence $G \times H/\{e_G\} \times H \cong G$.

order $|G \times H| = |H| \times |G|$

$|G/H| = |G| / |H|$

$G \times H / e \times H \cong G$.

$G/H \times H \not\cong G$

e.g. $G = \mathbb{Z}/4\mathbb{Z}$. $H = \{\bar{0}, \bar{2}\}$, $G/H = \{\{\bar{0}, \bar{2}\}, \{\bar{1}, \bar{3}\}\}$

ord $\{\bar{0}, \bar{2}\} \times \bar{0} = 1$. ord in G 1, 4, 2, 4.

	ord
$\{\bar{0}, \bar{2}\}$	1.
$\{\bar{1}, \bar{3}\}$	2

1, 2, 2, 2.

§12. Classifications of groups.

Definition. A group G is **cyclic** if it is generated by one element, i.e., there exists $g \in G$ such that $G = \langle g \rangle$.

Examples. 1. $\mathbb{Z}$ is cyclic $\langle \bar{1} \rangle$

2. $\mathbb{Z}/m\mathbb{Z}$ is cyclic $\langle \bar{1} \rangle$

3. $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. If (a, b) generates $\mathbb{Z} \times \mathbb{Z}$ then $(a + 1, b)$ can not be generated.

Theorem 12.1. *A finite cyclic group of order m is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. An infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Proof. Let G be a cyclic group generated by $g \in G$. Consider the homomorphism $\psi_g \colon \mathbb{Z} \to G, \psi_g(n) = g^n$. Its image equals $\langle g \rangle = G$. Theorem 11.5 implies $\mathbb{Z}/\operatorname{Ker}(\psi_g) \cong G$. By Theorem 5.2 the subgroup $\operatorname{Ker}(\psi_g)$ is either zero or has the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$, which gives the required statement. □

Proposition 12.2. *If G is a finite group of prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. By Corollary 8.4, the order of any element of G must be a divisor of p, and thus is equal to 1 or p. The only element of order 1 is e, therefore, there is $g \in G$ of order p. But $|\langle g \rangle| = \operatorname{ord}_G g = p$ by Proposition 6.4 and thus $\langle g \rangle = G$. Therefore G is a cyclic group generated by g and is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by Theorem 12.1. □

Proposition 12.3. *$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if and only if $(m, n) = 1$.*

Proof. Suppose $\gcd(m, n) = 1$. It suffices to show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic. We check that $(\bar{1}, \bar{1})$ is its generator. For any $a, b \in \mathbb{Z}$, it suffices to check that the system

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

is solvable which follows from the Chinese remainder theorem.

Now let $\gcd(m, n) = d > 1$. Then $\operatorname{lcm}(m, n) = N = mn/d < mn$, so $N(\bar{a}, \bar{b}) = (N\bar{a}, N\bar{b}) = (\bar{0}, \bar{0})$ for any $(\bar{a}, \bar{b}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. On the other hand, $N\bar{1} \neq \bar{0}$ in $\mathbb{Z}/mn\mathbb{Z}$, therefore $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/mn\mathbb{Z}$ are not isomorphic. □

Proposition 12.4. *1. A group of order 4 is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

2. A group of order 6 is isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3.

Proof. 1. Let $|G| = 4$. The order of any non-identity elements of G can be either 2 or 4 by Corollary 8.4. If there is an element of G of order 4, then G is a cyclic group and thus is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. If the orders of all non-identity elements of G are 2, then for any non-identity distinct $a, b \in G$ one has $G = \{e, a, b, ab\}$, whence $ba = ab$. Indeed, $ba \neq a$ since $b \neq e$, $ba \neq b$ since $a \neq e$ and $ba \neq e$ since $a \neq b$. Now the bijection from G to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ given by $e \mapsto (\bar{0}, \bar{0}), a \mapsto (\bar{1}, \bar{0}), b \mapsto (\bar{0}, \bar{1}), ab \mapsto (\bar{1}, \bar{1})$ is a homomorphism since the correspondent Cayley tables are identical.

2. Let $|G| = 6$. If G contains an element of order 6, then G is a cyclic group and thus is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Otherwise, the orders of the non-identity elements of G may be 2 or 3. All non-identity elements cannot be of order 2, because if $\operatorname{ord}_G a = \operatorname{ord}_G b = \operatorname{ord}_G ab = 2$, then $\langle a, b \rangle = \{e, a, b, ab\} < G$, which contradicts Lagrange's theorem. Also, all non-identity elements cannot be of order 3, since the inverse of an element of order 3 is a distinct element of order 3, so their number is even. Therefore there are $a, b \in G$ such that $\operatorname{ord}_G a = 2, \operatorname{ord}_G b = 3$.

Now we claim that $G = \{e, b, b^2, a, ab, ab^2\}$, since these elements are all distinct. For example, if $b = ab^2$, then $ab = e$, whence $b = a$, a contradiction. If $b^2 = a$ then $b = b^4 = a^2 = e$, a contradiction. The remaining cases are treated similarly. We now want to find ba in this list. It is clear that $ba \neq e, a, b, b^2$. If $ba = ab$, then $(ab)^2 = b^2, (ab)^3 = a, (ab)^4 = b, (ab)^5 = ab^2$, whence $\operatorname{ord}_G ab = 6$, a contradiction. Thus the only remaining possibility is $ba = ab^2$ and in this case $G \cong S_3$. Indeed, one can match a to an arbitrary transposition, b to one of two 3-cycles and the remaining elements to the correspondent products of these transposition and cycle. Then the correspondent Cayley tables of G and S_3 are identical. □

§13. Group action.

Definition. An **action** of a group G on a set M is given by a mapping $G \times M \to M, (g, m) \mapsto gm$, that satisfies the following properties:

I. $g_2(g_1 m) = (g_2 g_1)m$ for any $g_1, g_2 \in G, m \in M$

II. $em = m$ for any $m \in M$

Examples.
1. The **trivial** action of an arbitrary group G on a set M given by $gm = m$ for all $g \in G, m \in M$
2. Let $M = \mathrm{M}_{n,1}(\mathbb{R}), G = \mathrm{GL}_n(\mathbb{R})$. The multiplication $(A, v) \mapsto Av$, where $A \in \mathrm{GL}_n(\mathbb{R}), v \in \mathrm{M}_{n,1}(\mathbb{R})$, gives an action of G on M, since $B(Av) = (BA)v$ and $E_n v = v$.
3. Let M be the set of colorings of the vertices of a regular n-gon in s colors and $G = D_n$. Each symmetry permutes the vertices, mapping one coloring to another, which defines an action of G on M.
4. The group S_n acts on $\mathbb{R}[x_1, \dots, x_n]$ by $(\sigma \cdot f)(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.
5. Let G be a group, $M = G$. Multiplication $((g, m) \mapsto gm)$ gives an action of G on itself.
6. Let G be a group, $M = G$. Conjugation $((g, m) \mapsto gmg^{-1})$ defines an action of G on itself.

Definition. Let a group G act on M and $m \in M$. The **stabilizer subgroup** of m is defined as $G_m = \{g \in G : gm = m\}$ and the **orbit** of m is defined as $\operatorname{Orb} m = \{gm, g \in G\} \subset M$.

An action of G on M is **transitive**, if there is only one orbit, i.e., for any two elements $m_1, m_2 \in M$, there exists $g \in G$ such that $gm_1 = m_2$. An element $m \in M$ is a **fixed point** of $g \in G$ if $gm = m$.

Proposition 13.1. $G_m < G$

Proof. If $g_1, g_2 \in G_m$, then $(g_2 g_1)m = g_2(g_1 m) = g_2 m = m$, i.e. $g_2 g_1 \in G_m$. Moreover, $e \in G_m$ since $em = m$. If $gm = m$, then $g^{-1}m = g^{-1}(gm) = (g^{-1}g)m = em = m$, thus $g \in G_m$ implies $g^{-1} \in G_m$. □

Proposition 13.2. *Let G act on M. The relation $\sim$ on M, defined by $m_1 \sim m_2$ if $gm_1 = m_2$ for some $g \in G$, is an equivalence relation.*

Proof. If $gm_1 = m_2$ then $g^{-1}m_2 = m_1$ and $m_1 \sim m_2$ implies $m_2 \sim m_1$. If $gm_1 = m_2$ and $g'm_2 = m_3$, then $(g'g)m_1 = g'(gm_1) = g'm_2 = m_3$ and $m_1 \sim m_2, m_2 \sim m_3$ imply $m_2 \sim m_1$. Finally, $em = m$ and $m \sim m$ which completes the proof. □

Theorem 13.3 (Orbit-Stabilizer Theorem). *For a finite group G acting on a set M*

$$|\operatorname{Orb} m| \cdot |G_m| = |G|$$

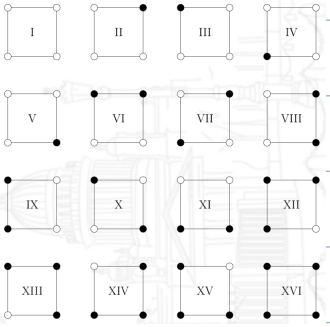
for any $m \in M$.

Proof. Denote $H = G_m$ and define the map $\Gamma : G/H \to \operatorname{Orb} m$ by $\Gamma(gH) = gm$. If $gH = g'H$, then $g' = ga$ for some $a \in H$, whence $g'm = (ga)m = g(am) = gm$, i.e. Γ is well-defined.

We will show that Γ is bijective. The surjectivity is obvious and if $\Gamma(gH) = \Gamma(g'H)$, then $m = (g^{-1}g')m$, whence $g^{-1}g' \in H$, thus $gH = g'H$.

By Lagrange's theorem, the index of H in G equals $|G|/|H|$, which yields the required identity. □

Example. Consider the action of D_4 on the colorings of the vertices of a square in 2 colors. It has the following orbits: {I}, {II,III,IV,V}, {VI,VIII,IX,XI}, {VII,X}, {XII,XIII,XIV,XV}, {XVI}. The stabilizer of II is $\{e, s_2\}$, the stabilizer of VI is $\{e, t_1\}$, the stabilizer of VII is $\{e, s_1, s_2, q\}$.



Lemma 13.4 (Burnside). *Let a group G act on a set M. The number of orbits equals*

$$N = \frac{1}{|G|}\sum_{g\in G}|M^g|,$$

where $M^g = \{m \in M : gm = m\}$.

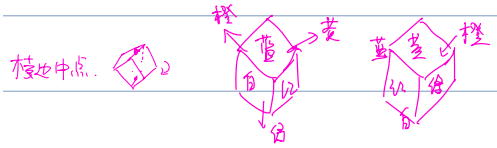
Proof. We count the number of elements of the set $W = \{(g, m) \in G \times M : gm = m\}$ in two different ways. On one hand, $|W| = \sum_{g\in G}|\{m \in M : gm = m\}| = \sum_{g\in G}|M^g|$. On the other hand, if $\Omega_1, \dots, \Omega_N$ are the orbits then

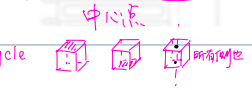
$$|W| = \sum_{m\in M}|\{g \in G : gm = m\}| = \sum_{m\in M}|G_m| = \sum_{m\in M}\frac{|G|}{|\operatorname{Orb} m|} = |G|\sum_{i=1}^{N}\sum_{m\in\Omega_i}\frac{1}{|\operatorname{Orb} m|}$$
$$= |G|\sum_{i=1}^{N}\sum_{m\in\Omega_i}\frac{1}{|\Omega_i|} = |G|\sum_{i=1}^{N}1 = |G|\cdot N.$$

□

Exercise 13.3. *Find the number of rotationally distinct colorings of the faces of a cube using three colors.*

Hint. The group of the rotational symmetries of a cube consists of the following 24 elements: the identity, the rotations through 120° and 240° about 4 axes connecting the opposite vertices of the cube, the rotations through 180° about 6 axes connecting the midpoints of the opposite edges, and the rotations through 90°, 180° and 270° about 3 axes connecting the centers of the opposite faces.





(3) 90°, 270° $|M^g| = 3^3$ → cycle, color.

180° $|M^g| = 3^4$ 一个 cycle 涂一种色.

Problem 13.5. *How many different necklaces can be formed with 6 black and white beads?*

Solution. Consider the set M of all possible colorings of a regular hexagon in two colors and the action of D_6 on it. Clearly, $|M| = 2^6 = 64$. It is easy to see that the number of different necklaces is equal to the number of orbits under this action which can be calculated using Burnside's lemma.

The group D_6 consists of 12 symmetries:

- the identity transformation
- two rotations by $\pi/3$
- two rotations by $2\pi/3$
- the central symmetry
- three reflections across the diagonals
- three reflections across the lines connecting the midpoints of the opposite edges.

For each symmetry g we count M^g, the number of colorings of the hexagon in two colors that remain unchanged under g. For example, if g is the rotation by $2\pi/3$, there are 4 such colorings: two monochromatic colorings and two colorings with alternating colors. As a result, one has

$$N = \frac{1}{12}(64 + 2\cdot 2 + 2\cdot 4 + 8 + 3\cdot 16 + 3\cdot 8) = 13.$$

□

Remark. Let D_n act on the set M of the colorings of the vertices of a regular n-gon in k colors. The size of M^g can be calculated as follows. A symmetry g defines a permutation $\sigma \in S_n$ of the vertices which can be expressed as the product of q disjoint cycles. Clearly, a coloring belongs to M^g iff all the vertices belonging to the same cycle are of the same color. It gives $|M^g| = k^q$.

§14 Application of group action.

Theorem 14.1 (Cauchy). *Let p be a prime. If $p||G|$, then G contains an element of order p.*

Proof. Put $M = \{(x_1, x_2, \ldots, x_p) \in G^p \mid x_1x_2\cdots x_p = e\}$. Every p-tuple from M is uniquely defined by its first $p-1$ entries, thus M consists of $|G|^{p-1}$ elements.

Note that if $x_1x_2\cdots x_p = e$, then $x_2\cdots x_px_1 = e$, which allows one to define an action of the cyclic group $\mathbb{Z}/p\mathbb{Z}$ on M:

$$\overline{n}\cdot(x_1, x_2, \ldots, x_p) = (x_{n+1}, \ldots, x_p, x_1, \ldots, x_n), \quad 0 \le n \le p-1.$$

By the Orbit-Stabilizer Theorem, the orbits in M contain 1 or p elements. An orbit consists of one element if and only if its only element is of the form $(x, x, \ldots, x)$ and $x^p = e$. Since $|M|$ is equal to the sum of the sizes of the orbits, the number of x such that $x^p = e$ is a multiple of p. The identity element is one of these elements, hence there are at least $p-1$ non-identity elements that are of order p, i.e. the set of such elements is nonempty. □

Theorem 14.2. *If $|G| = p^n$, then $Z(G)$ is non-trivial.*

Proof. Consider the action of the group G on itself by conjugation. It defines a partition of G into the disjoint orbits whose size is equal to 1 or $p^k, k \in \mathbb{N}$, by the Orbit-Stabilizer Theorem. Therefore the number of one-element orbits is divisible by p. An element has one-element orbit under conjugation if and only if is in $Z(G)$, and hence $p||Z(G)|$. Since $e \in Z(G)$, its size cannot be less than p. □

Corollary 14.3. *Any group of order p^2 is abelian.*

Proof. If $G \neq Z(G)$, pick up $g \notin Z(G)$. Let $H = \{h \in G \mid gh = hg\}$ which is a subgroup of G and $Z(G) \subset H, g \in H$. By Lagrange's Theorem, $|Z(G)|, |H|$ divide $|G| = p^2$ while $1 < |Z(G)| < |H|$ which is not possible. □

Proposition 14.4. *Let G be a finite group and p be the smallest prime divisor of $|G|$. Then any subgroup of H of index p is normal.*

Proof. Let $\Omega = G/H, |\Omega| = p$. Consider the action of H on Ω by left multiplication: $h \cdot gH = (hg)H$, $h \in H, g \in G$. It gives a partition of Ω into a disjoint union of orbits whose sizes by the Orbit-Stabilizer Theorem are divisors of $|H|$ and hence of $|G|$. Since p is the smallest prime divisor of $|G|$, the size of an orbit can be either 1 or p.

Obviously the orbit of $H \in \Omega$ consists of one element, hence the other orbits also consist of one element. Therefore $(hg)H = gH$ for all $h \in H, g \in G$, whence $hg = gh'$ for some $h' \in H$, which implies $H \triangleleft G$. □

Chapter 2 Rings and Fields.

§15. Introduction.

Definition. Let R be a set with two binary operations denoted by $+$ and $\cdot$ and call *addition* and *multiplication*, respectively. Assume the following properties are satisfied:

从公理角度与 vector space 类似.
除 7.8. (在数乘中. 乘法可交换无意义).

1. $a+(b+c)=(a+b)+c$ for any $a,b,c\in R$ (that is, $+$ is associative)
2. there exists $\mathbf{0}\in R$ such that $\mathbf{0}+a=a=a+\mathbf{0}$ for all $a\in R$ (that is, $\mathbf{0}$ is the identity element with respect to $+$; it is called **zero**);
3. for any $a\in R$, there exists $a'\in R$ such that $a+a'=\mathbf{0}=a'+a$ (that is, a has the inverse with respect to $+$; it is usually denoted by $-a$);
4. $a+b=b+a$ for any $a,b\in R$ (that is, $+$ is commutative);
5. $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(b+c)\cdot a=b\cdot a+c\cdot a$ for any $a,b,c\in R$ (*distributivity*).
6. $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for any $a,b,c\in R$ (that is $\cdot$ is associative);
7. there exists an element $\mathbf{1}\in R$ such that $\mathbf{1}\cdot a=a=a\cdot\mathbf{1}$ for any $a\in R$ (that is, $\mathbf{1}$ is the identity element with respect to $\cdot$; it is called a **unity**);
8. $a\cdot b=b\cdot a$ for any $a,b\in R$ (that is, $\cdot$ is commutative);

Then R with the above two operations is called an **associative commutative ring with unity** or simply a **ring**.

可能有 1 项未满足.
如 8 x. associative, non-commutative with unity.
7 x associative, commutative without unity.

Remark. Any ring is a commutative group with respect to addition

Examples.
1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with respect to standard addition and multiplication.
2. $\mathbb{Z}/m\mathbb{Z}$ with respect to addition and multiplication of residue classes.
3. $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$
4. $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$
5. If R is a ring, $R[t]$ is a ring (在未说明时 R. 可以是 ifi 可集)
6. The set of all subsets of a given set X with respect to $A+B=A\triangle B, A\cdot B=A\cap B$
7. If R is a ring, $\mathrm{M}_n(R)$ is a non-commutative ring with unity
8. $2\mathbb{Z}$ is a commutative ring without unity

Remark. If R is a ring, $R^*=R\setminus\{0\}$ is a group under multiplication

Lemma 15.1. *If R is a ring then*

1. $a\cdot\mathbf{0}=\mathbf{0}\cdot a=\mathbf{0}$ *for all* $a\in R$
2. $(-a)b=-(ab)$ *for any* $a,b\in R$

Proof. One has $a\cdot\mathbf{0}+a\cdot\mathbf{0}=a\cdot(\mathbf{0}+\mathbf{0})=a\cdot\mathbf{0}$. Canceling out $a\cdot\mathbf{0}$ gives the first result. The equality $(-a)b+ab=(-a+a)b=\mathbf{0}\cdot b=\mathbf{0}$ implies the second result. □

Definition. A **field** k is a ring such that for any $a\in k, a\neq\mathbf{0}$, there exists $a'\in k$ such that $a\cdot a'=a'\cdot a=\mathbf{1}$ (that is, a has the inverse with respect to $\cdot$; it is usually denoted by a^{-1}).

ring + inverse of $\cdot$ → field

The **characteristic** of a field is the order of $\mathbf{1}$ in its additive group, i.e., the smallest positive integer p such that $\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{p\text{ times}}=\mathbf{0}$. If the order is infinite then the characteristic is said to be 0. Notation: $\mathrm{char}(k)=p$.

Examples.
1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are field of zero characteristic
2. $\mathbb{Z}/p\mathbb{Z}$ for a prime p is a field of characteristic p
3. $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ is a field of zero characteristic

Definition. An **integral domain** R is a ring such that $ab\neq\mathbf{0}$ for any $a,b\in R, a,b\neq\mathbf{0}$.

Any field is an integral domain (inverse not true. $\mathbb{Z}$ - not field but integral domain.)

Examples

3. $R[t]$ is an integral domain if R is an integral domain
4. $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain if m is a composite number (非质数)

Proposition 15.2 (Cancellation is integral domains)**.** *Let R be an integral domain and $a,b,c\in R$. If $a\neq\mathbf{0}$ and $ab=ac$ then $b=c$.*

Proof. One has $a(b-c)=\mathbf{0}$ whence $b-c=\mathbf{0}$. □

Definition. Rings R_1, R_2 are **isomorphic** if there exists a bijection $\Phi\colon R_1 \to R_2$ such that $\Phi(a+b) = \Phi(a) + \Phi(b)$ and $\Phi(ab) = \Phi(a)\Phi(b)$ for all $a, b \in R_1$.

Example. Let V be an n-dimensional vector space over a field k. Then $\mathcal{L}(V)$ is isomorphic to $\mathrm{M}_n(k)$.

§16. Ideals. (↓ R is an integral domain)

Definition. A non-empty subset $I \subset R$ is an **ideal** of R if:

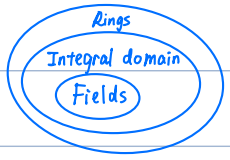
I. $a + a' \in I$ for all $a, a' \in I$

II. $ra \in I$ for all $a \in I, r \in R$

Examples. 1. $\{\mathbf{0}\}, R$ are ideals of R

2. $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$

3. $\{f \in R[x] \mid f(a) = 0\}$ is an ideal of $R[x]$, where $a \in R$ is fixed



Proposition 16.1. *Let I be an ideal of R. Then I is a subgroup of the additive group of R.*

Proof. If $a \in I$ then $\mathbf{0} = \mathbf{0} \cdot a \in I$ and $-a = (-1) \cdot a \in I$. □

Corollary 16.2. *Any ideal I of $\mathbb{Z}$ has the form $m\mathbb{Z}$ for some a non-negative $m \in \mathbb{Z}$.*

Proposition 16.3. *A ring k is a field iff $\{\mathbf{0}\}, k$ are its only ideals.*

Proof. Let I be an ideal of a field k and $a \in I, a \neq \mathbf{0}$. Then $b = (ba^{-1})a \in I$ for any $b \in k$ whence $I = k$.

If $a \in k, a \neq \mathbf{0}$, consider the ideal (a). If $\{\mathbf{0}\}, k$ are its only ideals of k then $(a) = k$. In particular $\mathbf{1} \in (a)$ whence $a \in k^*$ and k is a field. □

Proposition 16.4. *Let $a_1, \ldots, a_n \in R$. Then $I = \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}$ is an ideal of R.* (denote by $I = (a_1, \ldots a_n)$ in R.

Proof. If $a = r_1a_1 + \cdots + r_na_n, a' = r_1'a_1 + \cdots + r_n'a_n$ for some $r_1, r_1', \ldots, r_n, r_n' \in R$, then $a + b = (r_1 + r_1')a_1 + \cdots + (r_n + r_n')a_n \in I$. Similarly, if $a = r_1a_1 + \cdots + r_na_n$ for some $r_1, \ldots, r_n \in R$ and $r \in R$, then $ra = (rr_1)a_1 + \cdots + (rr_n)a_n \in I$. □

Definition. The ideal defined in Proposition 16.4 is called the ideal **generated** by $a_1, \ldots, a_n$ and is denoted by $(a_1, \ldots, a_n)$. An ideal **principal** if it is generated by a single element.

An element $a \in R$ is **divisible** by $b \in R, b \neq 0$ (or b **divides** a) (notation: $b \mid a$) if $a = bc$ for some $c \in R$. Elements $a, b \in R, a, b \neq \mathbf{0}$ are **associated** if a divides b and b divides a.

A **unit** is an element having a multiplicative inverse. The set of units of a ring R is denoted R^*. (R^* is a group under multiplication)

→ in $\mathbb{Z}$. a, b associative iff $|a| = |b|$
in field any two elements associative.

Proposition 16.5. *1. $b \mid a$ if and only if $(a) \subset (b)$*

2. a, b are associated if and only if $(a) = (b)$

3. a, b are associated if and only if $a = bu$ for some $u \in R^*$

Theorem 16.7. *Let k be a field. Any ideal of $k[t]$ is principal. In particular, $(f, g) = (\gcd(f, g))$.*

Proof. Let I be an ideal in $k[t]$. Denote by f its element of minimum degree. Then for any $g \in I$ one has $g = fh + f_1$ for some $h, f_1 \in k[t], \deg f_1 < \deg f$. Since $f, g \in I$, one can conclude that $f_1 \in I$ whence $f_1 = 0$. Thus $I \subset (f)$. The inverse inclusion is obvious.

Now let $f, g \in k[t]$. By Bezout's identity, there exist $h_1, h_2 \in k[t]$ such that $fh_1 + gh_2 = d$, where $d = \gcd(f, g)$. Then $rd = (rh_1)f + (rh_2)g \in (f, g)$ for any $r \in k[t]$ that is $(d) \subset (f, g)$. The inverse inclusion follows from the fact that $d \mid h_1f + h_2g$ for any $h_1, h_2 \in k[t]$. □

Example. Consider the ideal $I = (x, 2)$ in the ring $\mathbb{Z}[x]$. Assume $I = (f)$ for some $f \in \mathbb{Z}[x]$. Then $f \mid 2$ and $f \mid x$, whence $f = \pm 1$. But $1 \notin I$ since 1 cannot be expressed as $xg(x) + 2h(x)$ for any $g, h \in \mathbb{Z}[x]$. Therefore I is not a principal ideal.

(if k not a field, k is a ring only, I may be not principle).

§17. Quotient ring.

Let I be an ideal of R. Any ideal is a subgroup of the additive group of R, thus the quotient group R/I can be considered. $a \sim b$ if $a-b \in I$.

Proposition 17.1. *Multiplication $\overline{a} \cdot \overline{b} = \overline{ab}$ is a well-defined operation on R_+/I which together with addition determines the structure of a (commutative associative unitary) ring.*

Proof. Suppose $a' - a = s, b' - b = t$ for some $a, a', b, b' \in R$ and $s, t \in I$. Then $a'b' - ab = (a+s)(b+t) - ab = at + sb + st \in I$, which proves that multiplication is well-defined.

The commutativity of multiplication follows from the commutativity of the ring R and the definition of multiplication: $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

The other axioms of the ring are verified in a similar manner. □

Definition. The quotient group R/I with above defined multiplication is called the **quotient ring** of R by I.

Proposition 17.2. *Let k be a field, $f \in k[t]$ be an irreducible polynomial. Then $k[t]/(f)$ is a field.*

Proof. It suffices to prove that $\overline{g}$ is invertible for any $g \in k[t], g \notin (f)$. Since f is irreducible, either $f \mid g$ or $\gcd(f, g) = 1$. The former case is impossible since $g \notin (f)$, thus $\gcd(f, g) = 1$. Then Bezout's identity implies that there exist $h_1, h_2 \in k[t]$ such that $h_1 f + h_2 g = 1$. Thus $\overline{h_2} \cdot \overline{g} = \overline{h_2 g} = \overline{1}$ in $k[t]/(f)$ as required. □

Proposition 17.3. *$\mathbb{R}[t]/(t^2+1)$ is isomorphic to $\mathbb{C}$.*

Proof. Define the mapping $\Phi\colon \mathbb{R}[t]/(t^2+1) \to \mathbb{C}$ by $\Phi(\overline{g}) = g(i)$ ← 等价类 t=i 代入.

First, if $f \mid g_1 - g_2$, then $g_1(t) - g_2(t) = (t^2+1)h(t)$ for some $h \in \mathbb{R}[t]$, whence $g_1(i) - g_2(i) = 0$. It shows that Φ is well-defined.

Further,

$$\Phi(\overline{g}_1 + \overline{g}_2) = \Phi(\overline{g_1 + g_2}) = (g_1 + g_2)(i) = g_1(i) + g_2(i) = \Phi(\overline{g}_1) + \Phi(\overline{g}_2)$$

which implies that Φ preserves addition. A similar argument can be given for multiplication.

It remains to check that Φ is bijective. The surjectivity is evident. If $\Phi(\overline{g}_1) = \Phi(\overline{g}_2)$ then $h(i) = 0$ for $h = g_1 - g_2$. Then $h(-i) = \overline{h(i)} = \overline{h(i)} = 0$ and h is divisible both by $t - i$ and $t + i$ and thus by $(t-i)(t+i) = t^2 + 1$. Therefore $\overline{g}_1 = \overline{g}_2$. □

可以证明. $\mathbb{R}[t]/f$ is isomorphic to $\mathbb{C}$.

一定成立. 对任意的 $h(t)$ 的成立. 等价类

§18. Irreducible Polynomial over $\mathbb{Z}/p\mathbb{Z}$.

Definition. A **monic** polynomial is a polynomial in which the leading coefficient is equal to 1.

Proposition 18.1. *Let k be a field, $f \in k[t]$. Then f is divisible by a polynomial of degree 1 iff it has a root.*

Proof. If $\alpha \in k, f(\alpha) = 0$ then $(t - \alpha) | f(t)$ by the factor theorem. If $(at + b) | f(t)$ for $a, b \in k, a \neq 0$ then clearly $f(-ba^{-1}) = 0$. □

Proposition 18.2. *Let k be a field, $f \in k[t]$ and $\deg f = n$. If f is reducible, it is divisible by a monic polynomial $g \in k[t], \deg g \leq [n/2]$.*

依按序 check 时, 每一步只用考虑 irreducible 的 (在时再更高的步骤就已完成)这个 check).

Proof. Since f is reducible, $f = gh$ for some $g, h \in k[t], \deg g, \deg h < n$. Assume $\deg g \leq \deg h$. Then $\deg g + \deg h = n$ implies $\deg g \leq [n/2]$. Finally $f = (a^{-1}g)(ah)$ where a is the leading coefficient of g. Now $a^{-1}g$ is monic and $\deg a^{-1}g \deg g \leq [n/2]$. □

The above statement allows one to search the irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ of a given degree n using the list of the irreducible polynomials of degree $\leq [n/2]$.

Problem 18.3. *Prove that $f = t^5 + t^2 + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$ is irreducible.*

Solution. It suffices to verify that f is not divisible by any irreducible (monic) polynomial over $\mathbb{Z}/2\mathbb{Z}$ of degree 1 and 2. Since f has no roots, the first case is impossible. Next, we need a list of irreducible polynomials of degree 2 over $\mathbb{Z}/2\mathbb{Z}$. We write down all polynomials of degree 2 and cross out the reducible ones, i.e., those having a root:

- ~~t^2~~ 先 check deg = 1. - f has no roots.
- ~~$t^2 + \overline{1}$~~ 再 check deg = 2. 对于 deg 1 check 过. 所有的 reducible poly. 都不同款.
- ~~$t^2 + t$~~
- $t^2 + t + \overline{1}$

We see that there exists a unique irreducible polynomial over $\mathbb{Z}/2\mathbb{Z}$ of degree 2. Since it does not divide f, f is irreducible. □

Problem 18.4. *Prove that $f = t^6 + t^3 + \overline{1}$ over $\mathbb{Z}/2\mathbb{Z}$ is irreducible.*

Solution. Suppose

$$t^6 + t^3 + \overline{1} = (t^3 + a_2 t^2 + a_1 t + a_0)(t^3 + b_2 t^2 + b_1 t + b_0).$$

Since $a_0 b_0 = \overline{1}$, we must have $a_0 = b_0 = \overline{1}$. By looking at the coefficients at t^5 and t, one can see $a_2 = b_2$ and $a_1 = b_1$. Then the coefficient at t^3 is $a_0 + a_1 b_2 + a_2 b_1 + b_0 = \overline{0}$, which is false. Now suppose

$$t^6 + t^3 + \overline{1} = (t^4 + a_3 t^3 + a_2 t^2 + a_1 t + a_0)(t^2 + b_1 t + b_0).$$

Again $a_0 = b_0 = \overline{1}$ and $a_3 = b_1, a_1 = b_1$. The coefficient at t^3 is $a_1 + a_2 b_1 + a_3 b_0 = \overline{0}$, whence $a_2 = b_1 = \overline{1}$. Now the coefficient at t^2 is $a_0 + a_1 b_1 + a_2 b_0 = \overline{1}$, which is false. □

对 modulo 构成的 residual class.

$\bar{f}$ is irreducible $\Rightarrow$ f is irreducible

$\Leftarrow$

$\bar{f}$ is reducible $\not\Rightarrow$ f is reducible.

§19. Finite Fields.

Proposition 19.1. *If k is a finite field, then the characteristic of k is a prime number.*

Proof. If $\operatorname{char} k = ab, a, b > 1$, notice that $\mathbf{0} = \underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{ab \text{ times}} = (\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{a \text{ times}})(\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{b \text{ times}})$. The field is an integral domain, so one of the two multipliers is equal to $\mathbf{0}$, but $a, b < ab$, a contradiction. □

Proposition 19.2. *Let k be a field.*

1. *If $\operatorname{char} k = p$, then k contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*
2. *If k is finite, then $\operatorname{char} k = p$ and $|k| = p^n$.*

Proof. (1) Consider $L = \{\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n \text{ times}} \mid n \geq 0\} \subset k$. Since $-\mathbf{1} = \underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{p-1 \text{ times}}$, one can see that L is a subgroup of the additive group of k generated by $\mathbf{1}$. Proposition 6.4 implies that $|L| = p$.

Now show that L is a field. Since L is a group under addition, we need only to verify the properties related to multiplication. First, L is closed under multiplication:

$$(\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{m \text{ times}}) \cdot (\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n \text{ times}}) = \underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{mn \text{ times}}.$$

Obviously $\mathbf{1} \in L$, and it remains to prove the existence of the multiplicative inverse of any non-zero element of L. If $0 < r < p$, then $\gcd(r, p) = 1$, so $rx + py = 1$ for some $x, y \in \mathbb{Z}$. Obviously, x and y must be of different sign. If $x < 0$, then it can be replaced by $x + pa$, for any $a \in \mathbb{Z}$, since $r(x + pa) + p(y - ra) = 1$, thus one can assume x to be positive. It remains to note that then $(\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{r \text{ times}}) \cdot (\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{x \text{ times}}) = \mathbf{1}$.

Finally, it is easy to see that the map $(\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n \text{ times}}) \mapsto \overline{n}$ from L to $\mathbb{Z}/p\mathbb{Z}$ is a field isomorphism.

(2) Consider the sequence $\mathbf{1}, \mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}, \ldots$ in k. Since k is finite, one has $\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{n \text{ times}} = \underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{m \text{ times}}$ for some $m > n$. Then $\underbrace{\mathbf{1}+\cdots+\mathbf{1}}_{m-n \text{ times}} = 0$, that is, $\operatorname{char} k = p$ for some prime p. Hence k contains a subfield L consisting of p elements. Consider k as a vector space over L. Since k is finite, the the dimension of this vector space is finite, denote it by n. Let $a_1, \ldots, a_n \in k$ be its basis. Then each $a \in k$ can be uniquely expressed in the form $a = \alpha_1 a_1 + \cdots + \alpha_n a_n$, which gives a bijection between k and L^n. Since the latter set has p^n elements, k also has p^n elements. □

Proposition 19.3. *If $f \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible and $\deg f = n$, then $|\mathbb{Z}/p\mathbb{Z}[x]/(f)| = p^n$.*

Proof. It suffices to prove that $\mathbb{Z}/p\mathbb{Z}[x]/(f) = \{\overline{h} \in \mathbb{Z}/p\mathbb{Z}[x] \mid \deg h < n\}$ and all elements of this set are distinct. Clearly, $\overline{g} = \overline{h}$, where $g = fg_1 + h$ and $\deg h < \deg f = n$. If $\overline{h_1} = \overline{h_2}$ with $\deg h_1, \deg h_2 < n$, then $h_1 - h_2 = fh$ for some $h \in \mathbb{Z}/p\mathbb{Z}[x]$ and $\deg(h_1 - h_2) < n$. This is possible only if $h_1 - h_2 = 0$. □