Fundamental Homomorphism (基础同态定理)

基础同态定理

fundamental,

2. homomorp

Zhang Yanmei

ymzhang@bupt.edu.cn

College of Computer Science & Technology

Beijing University of Posts & Telecommunications

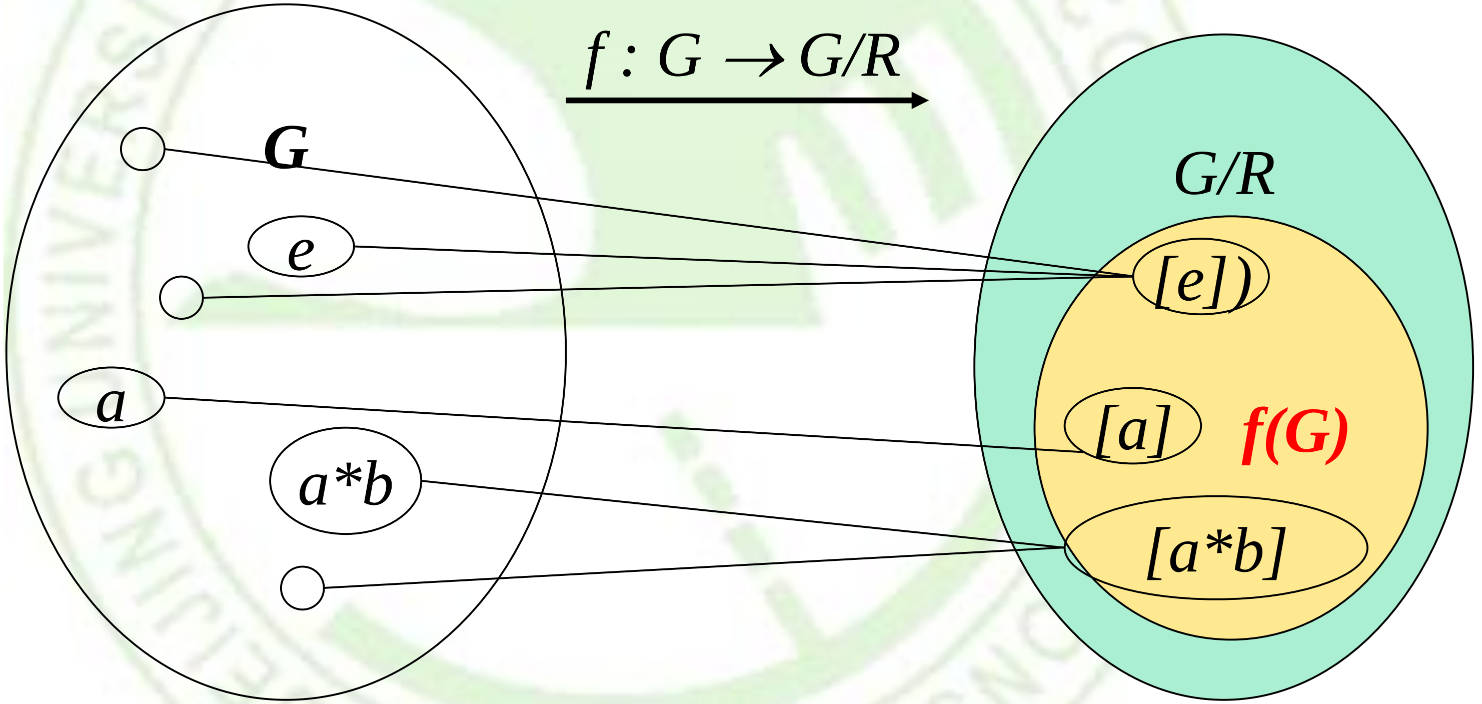
Theorem natural homomorphism(自然同态)

- Let
  同余
  - R be a congruence relation on a groupoid $(G, *)$,
  - $(G/R, \otimes)$ be the corresponding quotient groupoid.
- Then the function $f_R: G \to G/R$ defined by
  - $f_R(a) = [a]$
- is an onto homomorphism, called the *natural homomorphism.*

自然同态

Theorem - Proof

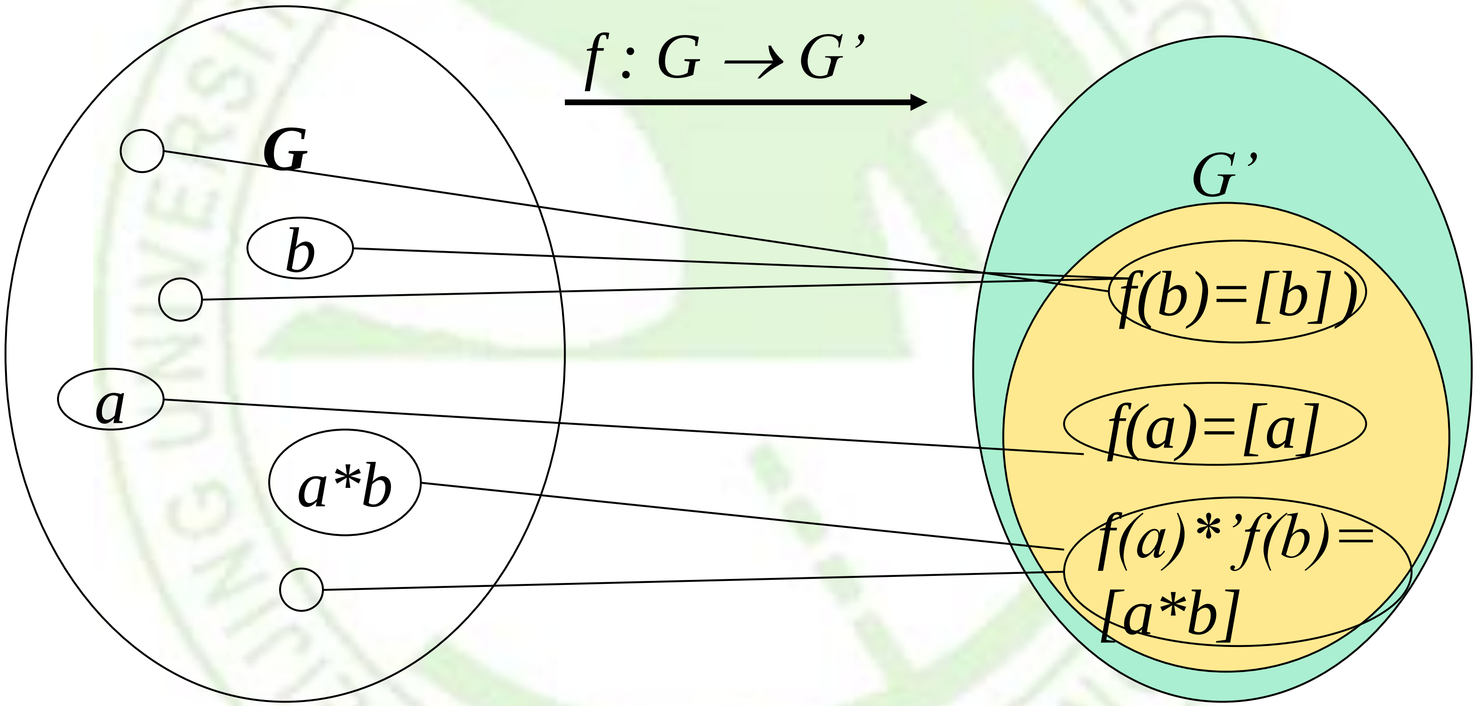
- If $[a] \in G/R$, then
  - $f_R(a) = [a]$,
  - so f_R is an onto function.
- if a and b are elements of G, then
  - $f_R(a*b) = [a*b] = [a]\otimes[b] = f_R(a)\otimes f_R(b)$
- so f_R is a homomorphism.



G is natual homomorphic to G/R

Fundamental Homomorphism Theorem

- Let
  - f: $G \rightarrow G'$ be a homomorphism of the groupoid (G, $*$) *onto* the groupoid (G', $*'$).
  - R be the relation on G defined by
    - $a\ R\ b$ *if and only if* $f(a) = f(b)$, for a and b in S.
- Then
  - R is a congruence relation.
  - (G', $*'$) and the quotient semigroup (G/R, $\otimes$) are isomorphic.



G is onto homomorphic to G’, R: aRb iff f(a)=f(b), then G’≅ G/R.

Proof(1)

- R is an equivalence relation
  - $a\ R\ a$ for every $a \in G$, since $f(a) = f(a)$.
  - if $a\ R\ b$, then $f(a) = f(b)$, so $b\ R\ a$.
  - if $a\ R\ b$ and $b\ R\ c$,
  - $f(a) = f(b)$ and $f(b) = f(c)$,
  - so $f(a) = f(c)$ and $a\ R\ c$.
  - Hence R is an equivalence relation.

Proof(2)

- R is a congruence relation.
  - Suppose that $a\ R\ a_1$ and $b\ R\ b_1$.
  - $f(a) = f(a_1)$ and $f(b) = f(b_1)$.
  - $f(a*b) = f(a)*'f(b) = f(a_1)*'f(b_1) = f(a_1*b_1)$, since f is a homomorphism,
  - Hence $(a*b)\ R\ (a_1*b_1)$.

Proof(3)

- Define a relation $\overline{f} = \{([a], f(a)) \mid [a] \in G/R\}$ from G/R to G', then
  - $\overline{f}$ is a function.
    - Suppose that $[a] = [a']$.
    - $a\ R\ a'$, so $f(a) = f(a')$, which implies that $\overline{f}$ is a function.
    - write $\overline{f}: G/R \to G'$, where $\overline{f}([a]) = f(a)$ for $[a] \in G/R$.

Proof(4)

- $\overline{f}$ is an homomorphism. 同态
  - $\overline{f}\ ([a]\otimes[b])$
  - $= \overline{f}\ ([a*b])$
  - $= f\,(a*b)$
  - $= f\,(a) *' f(b)$
  - $= \overline{f}\,([a]) *' \overline{f}\,([b])$.

- Q.E.D.

Proof(5)

- $\overline{f}$ is one to one.
  - Suppose that $\overline{f}([a]) = \overline{f}([a'])$.
  - $f(a) = f(a')$, so $a\ R\ a'$, which implies that $[a] = [a']$.
  - Hence $\overline{f}$ is one to one.
- $\overline{f}$ is onto.
  - Suppose that $b \in T$.
  - $f(a) = b$ for some element a in S, since f is onto,
  - $\overline{f}([a]) = f(a) = b$, so $\overline{f}$ is onto.

$$
\begin{tikzcd}
S \arrow[rr, "f"] \arrow[dr, "f_R"'] & & T \\
& S/R \arrow[ur, "\overline{f}"'] &
\end{tikzcd}
$$

Note

- Theorem 4(b) can be described by the diagram above
  - f_R is the natural homomorphism.
- It follows from the definitions of f_R and $\overline{f}$ that
  - $\overline{f} \otimes f_R = f$
- since
  - $(\overline{f} \otimes f_R)(a) = \overline{f}(f_R(a)) = \overline{f}([a]) = f(a)$.

Definition (Normal Subgroup)

- Let
  - H be a subgroup of a group G
  - $a \in G$
- The *left and right coset*(左陪集,右陪集) of H in G determined by a is the set
  - $aH = \{ah \mid h \in H\}$
  - $Ha = \{ha \mid h \in H\}$
- A subgroup H of G is *normal* (正规子群) if
  - $aH = Ha$, for all a in G

Warning

- If $Ha = aH$, it does not follow that, for $h \in H$ and $a \in G$, $ha = ah$.
- But $ha = ah'$, where h' is some element in H.

Note

- If H is a subgroup of G, we shall need in some applications to compute all the left cosets of H in G.
  - First, suppose that $a \in H$. Then $aH \subseteq H$, since H is a subgroup of G;
  - Moreover, if $h \in H$, then $h = ah'$, where $h' = a^{-1}h \in H$, so that $H \subseteq aH$.
  - Thus, if $a \in H$, then $aH = H$.

Example 3

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

- Let
  - G be the symmetric group S_3.
  - The subset $H = \{f_1, g_2\}$ is a subgroup of G.
- Compute all the distinct left cosets of H in G.

Solution: $H = \{f_1, g_2\}$

- Solution
  - If $a \in H$, then $aH = H$. Thus
  - $f_1 H = g_2 H = H$.
  - $f_2 H = \{f_2, g_1\}$
  - $f_3 H = \{f_3, g_3\}$
  - $g_1 H = \{g_1, f_2\} = f_2 H$
  - $g_3 H = \{g_3, f_3\} = f_3 H$
- The distinct left cosets of H in G are
  - H, $f_2 H$, and $f_3 H$.

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Theorem

- *If K is a finite subgroup of a group G, then every left coset of K in G has exactly as many elements as K.*

Proof(1)

- *Let K is a subgroup of group G.*
  - *aK be a left coset of K in G, where a* $\in$*G.*
  - *f: K* $\rightarrow$ *aK be defined by f(k)=ak, for k* $\in$*K.*
- *f is one-to-one*
- *f is onto*
- *Therefore, f is bijection, K and aK have the same number of elements.*

Proof(2): f is one-to-one

- *Let K is a subgroup of group G.*
  - *aK be a left coset of K in G, where $a \in G$.*
  - *$f: K \rightarrow aK$ be defined by $f(k)=ak$, for $k \in K$.*
- *f is one-to-one*
  - *Assume $f(k_1)=f(k_2)$, for $k_1,k_2 \in K$.*
  - *$ak_1=ak_2$*
  - *$k_1=k_2$, by left cancelation.*
  - *f is one-to-one*

Proof(3): f is onto

- *Let K is a subgroup of group G.*
  - *aK be a left coset of K in G, where a* $\in$*G.*
  - *f: K* $\rightarrow$ *aK be defined by f(k)=ak, for k*$\in$*K.*
- *f is onto*
  - *Let b be an arbitrary element in aK,*
  - *b=ak for some k*$\in$*K.*
  - *f(k)=ak=b*
  - *f is onto.*
- *Therefore, f is bijection, K and aK have the same number of elements.*

Lagrange's Group Theorem

- *The order of a subgroup divides the order of the group.*
- *Tips:*
  - The distinct left cosets of subgroup H in group S_3 are
    - $H=\{f_1, g_2\}$, $f_2H= \{f_2, g_1\}$, and $f_3H=\{f_3, g_3\}$.

Theorem (equivalence class vs coset)

- Let
  - R be a congruence relation on a group G
  - $H = [e]$, the equivalence class containing the identity.
- Then
  - H is a normal subgroup of G
  - $[a] = aH = Ha$, for each $a \in G$

Proof (1)

- Let a and b be any elements in G.
- Then $b \in \boldsymbol{[a]}$
  - *iff* $[b] = [a]$, for R is an equivalence relation.
  - *iff* $[e] = [a]^{-1}[a] = [a]^{-1}[b] = [a^{-1}b]$, for G/R is a group.
  - *iff* $H = [e] = [a^{-1}b]$.
  - *iff* $a^{-1}b \in H$ or $b \in \boldsymbol{aH}$.
- So $[a] = aH$ for every $a \in G$.

Proof (2)

- Similarly, $b \in [a]$
  - *iff* $H = [e] = [a][a]^{-1} = [b][a]^{-1} = [ba^{-1}]$.
  - *iff* $ba^{-1} \in H$ or $b \in Ha$.
- Thus $[a] = aH = Ha$, and H is normal.

Proof (3)

- *How to show H* is a subgroup of *G?*
  - $e \in H$,
  - *Proved* $H = [e] = [a^{-1}b]$, *iff* $b \in [a]$.
  - *any* $x \in [e]$, $x^{-1}e \in H$, *so* $x^{-1} \in H$.
  - *any* $x,y \in [e]$, *because* $x^{-1} \in H$, *so* $(x^{-1})^{-1}y \in H$, *thus* $xy \in H$.
  - *Hence, binary operation is closed in H.*

Notice:(equivalence class vs coset)

- The quotient group G/R consists of all the left cosets of $N = [e]$.
- The operation in G/R is given by
  - $(aN)(bN) = [a]\otimes[b] = [ab] = abN$
- and the function f_R: $G \to G/R$, defined by
  - $f_R(a) = aN$
- is a homomorphism from G onto G/R. For this reason, we will often write G/R as G/N.

Theorem 4

- Let
  - N be a normal subgroup of a group G
  - R be the following relation on G
    - $a\ R\ b$ *if and only if* $a^{-1}b \in N$.
- Then
  - (a) R is a congruence relation on G.
  - (b) N is the equivalence class $[e]$ relative to R, where e is the identity of G.

Proof (1)

- R is an equivalence relation
  - Let $a \in G$.
    - $a\ R\ a$, since $a^{-1}a = e \in N$,
    - R is reflexive.
  - Suppose that $a\ R\ b$
    - $a^{-1}b \in N$.
    - $(a^{-1}b)^{-1} = b^{-1}a \in \mathrm{N}$,
    - $b\ R\ a$.
    - R is symmetric.

Proof (2)

- R is an equivalence relation
  - Suppose that $a\ R\ b$ and $b\ R\ c$.
    - $a^{-1}b \in N$ and $b^{-1}c \in N$.
    - $(a^{-1}b)(b^{-1}c) = a^{-1}c \in N$,
    - $a\ R\ c$.
    - R is transitive.

Proof (3)

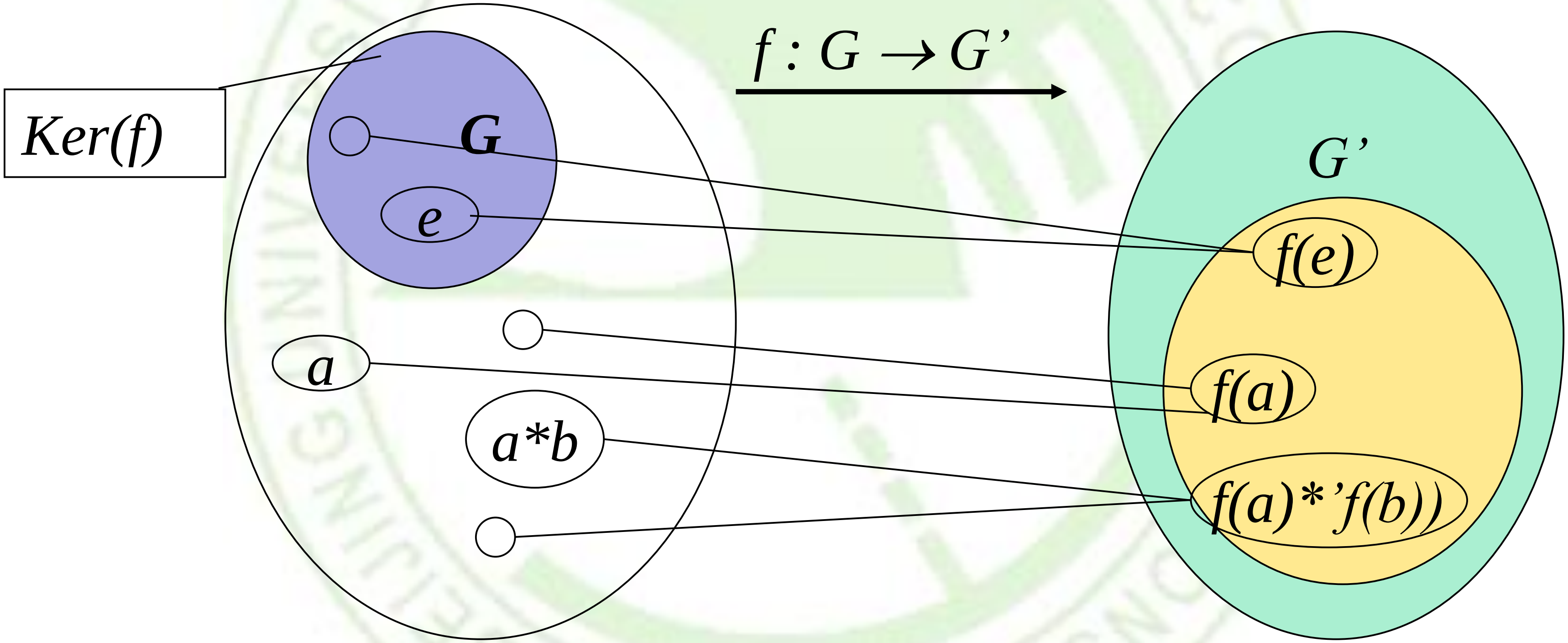
- R is a congruence relation on G.
  - Suppose that $a\ R\ b$ and $c\ R\ d$.
    - Then $a^{-1}b \in N$ and $c^{-1}d \in N$
  - Since N is normal, $Nd = dN$
  - since $a^{-1}b \in N$, then $a^{-1}bd = dn$ for some $n \in N$.
  - $(ac)^{-1}bd = (c^{-1}a^{-1})(bd) = \mathbf{c^{-1}(a^{-1}b)d = (c^{-1}d)\,n} \in N$
  - so $ac\ R\ bd$.
  - Hence R is a congruence relation on G.

Proof (4)

- Suppose that $x \in N$.
  - *for N is subgroup,* $x^{-1} \in N$, *so* $x^{-1}e \in N$,
  - *Thus* xRe, $x \in [e]$,
  - $N \subseteq [e]$.
- Conversely, if $x \in [e]$,
  - $x\ R\ e$
  - $x^{-1}e = x^{-1} \in N$
  - *for N is subgroup,* $x \in N$
  - $[e] \subseteq N$
- Hence $N = [e]$.

Corollary 2

- Let
  - f be a homomorphism from a group $(G, *)$ *onto* a group $(G', *')$
  - the *kernel(核)* of f, $ker(f)$, be defined by
    - $ker(f) = \{a \in G \mid f(a) = e'\}$.
- Then
  - ker(f) is a normal subgroup of G.
  - The quotient group $G/ker(f)$ is isomorphic to G'.



Group G is onto homomorphic to G', exist ker(f).

Example 6

- Consider the homomorphism f from $\mathbb{Z}$ onto $\mathbb{Z}_n$ defined by $f(m) = [r]$, where r is the remainder when m is divided by n. Find $ker(f)$.
- Solution
  - An integer m in $\mathbb{Z}$ belongs to $ker(f)$
  - if and only if $f(m) = [0]$
  - if and only if m is a multiple of n
  - Hence $ker(f) = n\mathbb{Z}$.

The conclusion is …

- Following are equivalent.
  - a onto homomorphism from G to G/R or G' ,
  - a congruence relation R on group G $(f(a)=f(b))$,
  - a normal subgroup N of G $(aN=Na)$,
  - a congruence relation R on G $([e]= N, [a]=aN)$,
  - the kernel of a homomorphism from G to G' $(\{a \mid f(a)=f(e)\})$.

交换群的子群都是正规子群

正规子群 $\Leftrightarrow$ $\forall a \in G$

$aH=Ha$

$aHa^{-1} \in H$

$aHa^{-1}=H$

阿贝尔群的子群
都是它的正规子群

Homework

- 4,18, 30 @353-354
- Ex1: Let G be a group, and let N and H be subgroups of G such that N is normal in G. Prove that
- (1)HN is a subgroup of G.
- (2)N is normal subgroup of HN.

Key ideas for review

- Binary operation
  - Commutative, Associative
- Semigroup, Monoid, Group
  - Subsemigroup, Submonoid, Subgroup
- Isomorphism, Homomorphism
  - Congruence relation R on semigroup $(S, *)$
  - Quotient semigroup S/R,
- Order of group, S_n , Z_n,置换群
- Left and right coset, Normal subgroup