Algebraic Structure (代数结构)
Chapter 1: Group Fundamentals

Shengli Liu (刘胜利)

liu-sl@cs.sjtu.edu.cn
Lab of Cryptography and Information Security
密码与信息安全实验室
计算机科学与工程系
上海交通大学

Cosets, Normal Subgroups and Homomorphisms

Definition 1.1 (coset 陪集)

Let H be a subgroup of G. If $g \in G$:

- The right coset of H generated by g is

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

- The left coset of H generated by g is

$$gH = \{gh : h \in H\}.$$

Example 1.2

$(\mathbb{Z}, +)$是一个整数加群。令

$$n\mathbb{Z} = \{dn \mid d \in \mathbb{Z}\} = \{\cdots, -3n, -2n, -n, 0, n, 2n, 3n, \cdots\}$$

则$(n\mathbb{Z}, +)$是一个子群，且有n个陪集。

Cosets, Normal Subgroups and Homomorphisms

Definition 1.1 (coset 陪集)

Let H be a subgroup of G. If $g \in G$:

- The right coset of H generated by g is

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

- The left coset of H generated by g is

$$gH = \{gh : h \in H\}.$$

Example 1.2

$(\mathbb{Z}, +)$是一个整数加群。令

$$n\mathbb{Z} = \{dn \mid d \in \mathbb{Z}\} = \{\cdots, -3n, -2n, -n, 0, n, 2n, 3n, \cdots\}$$

则$(n\mathbb{Z}, +)$是一个子群，且有n个陪集。

Lemma 1.3

Let H be a finite subgroup of G. Then $|gH| = |H|$ for any $g \in G$.

Proof.

Let $f : H \mapsto gH$ and $f(h) = gh$. Then f is onto and

$$h_1 = h_2 \Leftrightarrow gh_1 = gh_2.$$

So f is a one-to-one correspondence. Therefore

$$|gH| = |H|$$

. □

Specifically, $hH = H$ for all $h \in H$.

Lemma 1.3

Let H be a finite subgroup of G. Then $|gH| = |H|$ for any $g \in G$.

Proof.

Let $f : H \mapsto gH$ and $f(h) = gh$. Then f is onto and

$$h_1 = h_2 \Leftrightarrow gh_1 = gh_2.$$

So f is a one-to-one correspondence. Therefore

$$|gH| = |H|$$

. □

Specifically, $hH = H$ for all $h \in H$.

Lemma 1.4

Let $H \leq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \leq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Lemma 1.4

Let $H \preceq G$. Then the left cosets of H in G have the following properties:

1. $g \in gH$ *for all* $g \in G$.
2. *if* $a, b \in G$, *and if* $b = ah$ *for some* $h \in H$, *then* $aH = bH$.
3. *if* $a, b \in G$, *and if* $aH \cap bH$ *is non-empty then* $aH = bH$.

Proof.

1. $g = g \cdot 1$ and $1 \in H$, then $g \in gH$.
2. $bh' = a(hh')$ and $ah' = b(h^{-1}h')$ for all $h' \in H$. So $bH \subseteq aH$ and $aH \subseteq bH$, hence $aH = bH$.
3. Let $c \in aH \cap bH$. Then $c = ah'$ for some $h' \in H$, and $c = bh''$ for some $h'' \in H$. It follows from (2) that $cH = aH$ and $cH = bH$. Therefor $aH = bH$.

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

Fact 1.5

There are as many right cosets as left cosets.

Proof. Bijection: $f(aH) := Ha^{-1}$.

Definition 1.6 (index)

If H is a subgroup of group G, then the number of such cosets is referred to as the index of H in G, denoted by $[G : H]$.

Theorem 1.7 (Lagrange's Theorem)

If $H \leq G$, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H| \mid |G|$, and $\frac{|G|}{|H|} = [G : H]$.

Proof. There are $[G : H]$ cosets, each with $|H|$ members.

Fact 1.5

There are as many right cosets as left cosets.

Proof. Bijection: $f(aH) := Ha^{-1}$.

Definition 1.6 (index)

If H is a subgroup of group G, then the number of such cosets is referred to as the index of H in G, denoted by $[G : H]$.

Theorem 1.7 (Lagrange's Theorem)

If $H \leq G$, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H| \mid |G|$, and $\frac{|G|}{|H|} = [G : H]$.

Proof. There are $[G : H]$ cosets, each with $|H|$ members.

Fact 1.5

There are as many right cosets as left cosets.

Proof. Bijection: $f(aH) := Ha^{-1}$.

Definition 1.6 (index)

If H is a subgroup of group G, then the number of such cosets is referred to as the index of H in G, denoted by $[G : H]$.

Theorem 1.7 (Lagrange's Theorem)

If $H \leq G$, then $|G| = |H|[G : H]$. In particular, if G is finite then $|H| \mid |G|$, and $\frac{|G|}{|H|} = [G : H]$.

Proof. There are $[G : H]$ cosets, each with $|H|$ members.

Corollary 1.8

Let G be a finite group.

1. *If $a \in G$ then $|\langle a \rangle| \mid |G|$; in particular, $a^{|G|} = 1$.*
2. *If G has prime order, then G is cyclic.*

rough proof.

1. If $|a| = n$, then $H = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic subgroup of G with $|H| = n$. By Lagrange's theorem, $n \mid |G|$.
2. If $|G|$ is prime then we may take $a \neq 1$, and consequently $n = |G|$. Thus $|H| = |G|$, so $H = G$.

□

Corollary 1.8

Let G be a finite group.

1. *If $a \in G$ then $|\langle a \rangle| \mid |G|$; in particular, $a^{|G|} = 1$.*
2. *If G has prime order, then G is cyclic.*

rough proof.

1. If $|a| = n$, then $H = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic subgroup of G with $|H| = n$. By Lagrange's theorem, $n \mid |G|$.
2. If $|G|$ is prime then we may take $a \neq 1$, and consequently $n = |G|$. Thus $|H| = |G|$, so $H = G$.

□

Corollary 1.8

Let G be a finite group.

1. *If $a \in G$ then $|\langle a \rangle| \mid |G|$; in particular, $a^{|G|} = 1$.*
2. *If G has prime order, then G is cyclic.*

rough proof.

1. If $|a| = n$, then $H = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic subgroup of G with $|H| = n$. By Lagrange's theorem, $n \mid |G|$.
2. If $|G|$ is prime then we may take $a \neq 1$, and consequently $n = |G|$. Thus $|H| = |G|$, so $H = G$.

□

Corollary 1.8

Let G be a finite group.

1. *If $a \in G$ then $|\langle a \rangle| \mid |G|$; in particular, $a^{|G|} = 1$.*
2. *If G has prime order, then G is cyclic.*

rough proof.

1. If $|a| = n$, then $H = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic subgroup of G with $|H| = n$. By Lagrange's theorem, $n \mid |G|$.
2. If $|G|$ is prime then we may take $a \neq 1$, and consequently $n = |G|$. Thus $|H| = |G|$, so $H = G$.

□

Theorem 1.9 (Euler's Theorem)

If a and n are relatively prime positive integers, with $n \geq 2$, then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof.

The group $(\mathbb{Z}_n^*, \cdot)$ has order $\phi(n)$, So we have

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

□

Corollary 1.10 (Fermat's Little Theorem)

If p is a prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.

Theorem 1.9 (Euler's Theorem)

If a and n are relatively prime positive integers, with $n \geq 2$, then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof.

The group $(\mathbb{Z}_n^*, \cdot)$ has order $\phi(n)$, So we have

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

□

Corollary 1.10 (Fermat's Little Theorem)

If p is a prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.

Theorem 1.9 (Euler's Theorem)

If a and n are relatively prime positive integers, with $n \geq 2$, then $a^{\phi(n)} \equiv 1 \bmod n$.

Proof.

The group $(\mathbb{Z}_n^*, \cdot)$ has order $\phi(n)$, So we have

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

□

Corollary 1.10 (Fermat's Little Theorem)

If p is a prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$.

RSA算法

Example 1.11

密钥生成： 选择p, q素数，计算$N = pq$。计算$\phi(N) = (p-1)(q-1)$。选择e使得$\gcd(e, \phi(N)) = 1$，计算$d \equiv e^{-1} \mod \phi(N)$。公钥：$pk = (N, e)$，私钥：$sk = d$。

加密： 明文$M \in \mathbb{Z}_N$，利用公钥$pk = (N, e)$对明文M加密，得到密文$C \equiv M^e \mod N$；

解密： 密文$C \in \mathbb{Z}_N$，利用私钥$sk = d$对密文C解密，得到明文$M \equiv C^d \mod N$。

RSA算法

Example 1.11

密钥生成： 选择p, q素数，计算$N = pq$。计算$\phi(N) = (p-1)(q-1)$。选择e使得$\gcd(e, \phi(N)) = 1$，计算$d \equiv e^{-1} \mod \phi(N)$。公钥：$pk = (N, e)$，私钥：$sk = d$。

加密： 明文$M \in \mathbb{Z}_N$，利用公钥$pk = (N, e)$对明文M加密，得到密文$C \equiv M^e \mod N$；

解密： 密文$C \in \mathbb{Z}_N$，利用私钥$sk = d$对密文C解密，得到明文$M \equiv C^d \mod N$。

RSA算法

Example 1.11

密钥生成： 选择p, q素数，计算$N = pq$。计算$\phi(N) = (p-1)(q-1)$。选择e使得$\gcd(e, \phi(N)) = 1$，计算$d \equiv e^{-1} \mod \phi(N)$。公钥：$pk = (N, e)$，私钥：$sk = d$。

加密： 明文$M \in \mathbb{Z}_N$，利用公钥$pk = (N, e)$对明文M加密，得到密文$C \equiv M^e \mod N$；

解密： 密文$C \in \mathbb{Z}_N$，利用私钥$sk = d$对密文C解密，得到明文$M \equiv C^d \mod N$。

Theorem 1.12 (The Index is Multiplicative)

If $K \preceq H \preceq G$ *then* $[G : K] = [G : H][H : K]$.

Proof.

$[G : H] = \frac{|G|}{|H|}$ and $[H : K] = \frac{|H|}{|K|}$.
If G is finite, then

$$[G : H][H : K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K].$$

Otherwise, we need a bijection $f : G/H \to (G/K)/(K/N)$.

□

Theorem 1.12 (The Index is Multiplicative)

If $K \preceq H \preceq G$ *then* $[G : K] = [G : H][H : K]$.

Proof.

$[G : H] = \frac{|G|}{|H|}$ and $[H : K] = \frac{|H|}{|K|}$.
If G is finite, then

$$[G : H][H : K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G : K].$$

Otherwise, we need a bijection $f : G/H \to (G/K)/(K/N)$.

□

Definition 1.13

If $H \preceq G$ and $K \preceq G$, then define HK to be

$$HK = \{hk : h \in H, k \in K\}.$$

HK不一定是群。如果G是可交换群，那么HK一定是群！

Theorem 1.14

If $H \preceq G$ and $K \preceq G$, then $HK \preceq G$ iff $HK = KH$. In this case, HK is the subgroup generated by $H \cup K$.

Definition 1.13

If $H \preceq G$ and $K \preceq G$, then define HK to be

$$HK = \{hk : h \in H, k \in K\}.$$

HK不一定是群。如果G是可交换群，那么HK一定是群！

Theorem 1.14

If $H \preceq G$ and $K \preceq G$, then $HK \preceq G$ iff $HK = KH$. In this case, HK is the subgroup generated by $H \cup K$.

Definition 1.13

If $H \preceq G$ and $K \preceq G$, then define HK to be

$$HK = \{hk : h \in H, k \in K\}.$$

HK不一定是群。如果G是可交换群，那么HK一定是群！

Theorem 1.14

If $H \preceq G$ and $K \preceq G$, then $HK \preceq G$ iff $HK = KH$. In this case, HK is the subgroup generated by $H \cup K$.

Proof.

- $\Rightarrow$ If $HK \preceq G$, denote $(HK)^{-1}$ by the collection of all inverses of elements of HK, then $HK = (HK)^{-1}$. So $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.
- $\Leftarrow$ Because $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$. so the inverse of an element in HK also belongs to HK. The product of two elements in HK belongs to HK, because $(HK)(HK) = HKHK = HHKK = HK$.
- Since any subgroup containing H and K must contain HK. so HK is generated by $H \cup K$.

$\square$

Lemma 1.15

If $H \preceq G$, then $(aH)(bH) = abH$ for all $a, b \in G$ iff $cHc^{-1} = H$ for all $c \in G$. (Equivalently, $cH = Hc$ for all $c \in G$).

Proof.

- $\Rightarrow$ $cHc^{-1} \subseteq cHc^{-1}H$ since $1 \in H$, and $(cH)(c^{-1}H) = cc^{-1}H = H$. Thus $cHc^{-1} \subseteq H$, which implies that $H \subseteq c^{-1}Hc$. Since this holds for all $c \in G$, we have $H \subseteq cHc^{-1}$, then $cHc^{-1} = H$.
- $\Leftarrow$

$$(aH)(bH) = a(Hb)H = abHH = abH.$$

□

Lemma 1.15

If $H \preceq G$, then $(aH)(bH) = abH$ for all $a, b \in G$ iff $cHc^{-1} = H$ for all $c \in G$. (Equivalently, $cH = Hc$ for all $c \in G$).

Proof.

- $\Rightarrow$ $cHc^{-1} \subseteq cHc^{-1}H$ since $1 \in H$, and $(cH)(c^{-1}H) = cc^{-1}H = H$. Thus $cHc^{-1} \subseteq H$, which implies that $H \subseteq c^{-1}Hc$. Since this holds for all $c \in G$, we have $H \subseteq cHc^{-1}$, then $cHc^{-1} = H$.
- $\Leftarrow$

$$(aH)(bH) = a(Hb)H = abHH = abH.$$

□

normal subgroups

Definition 1.16 (normal subgroup)

Let $H \preceq G$. H is a normal group of G if any of following holds:

1. $cHc^{-1} \subseteq H$ for all $c \in G$.
2. $cHc^{-1} = H$ for all $c \in G$.
3. $cH = Hc$ for all $c \in G$.
4. Every left coset of H in G is also a right coset.
5. Every right coset of H in G is also a left coset.

Note

$H \trianglelefteq G$ indicates that H is a normal subgroup of G;
if H is a proper normal subgroup, we write $H \triangleleft G$.

normal subgroups

Definition 1.16 (normal subgroup)

Let $H \preceq G$. H is a normal group of G if any of following holds:

1. $cHc^{-1} \subseteq H$ for all $c \in G$.
2. $cHc^{-1} = H$ for all $c \in G$.
3. $cH = Hc$ for all $c \in G$.
4. Every left coset of H in G is also a right coset.
5. Every right coset of H in G is also a left coset.

Note

$H \trianglelefteq G$ indicates that H is a normal subgroup of G;
if H is a proper normal subgroup, we write $H \triangleleft G$.

Quotient groups

Definition 1.17 (quotient subgroup)

If $N \trianglelefteq G$, the quotient group G/N is defined to be the group of cosets of N in G under the operation of multiplication.

$$G/N = \{gN : g \in G\}$$

The multiplication is defined : $(aN)(bN) = (ab)N$.
The identity is N.

Example 1.18

- Let $GL(n, \mathbb{R})$ be the set of all nonsingular n by n matrices with real coefficients.
- Let $SL(n, \mathbb{R})$ be the subgroup formed by matrices whose determinant is 1.
- Then $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$

Quotient groups

Definition 1.17 (quotient subgroup)

If $N \trianglelefteq G$, the quotient group G/N is defined to be the group of cosets of N in G under the operation of multiplication.

$$G/N = \{gN : g \in G\}$$

The multiplication is defined : $(aN)(bN) = (ab)N$.
The identity is N.

Example 1.18

- Let $GL(n, \mathbb{R})$ be the set of all nonsingular n by n matrices with real coefficients.
- Let $SL(n, \mathbb{R})$ be the subgroup formed by matrices whose determinant is 1.
- Then $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$

Quotient groups

Definition 1.17 (quotient subgroup)

If $N \trianglelefteq G$, the quotient group G/N is defined to be the group of cosets of N in G under the operation of multiplication.

$$G/N = \{gN : g \in G\}$$

The multiplication is defined : $(aN)(bN) = (ab)N$.
The identity is N.

Example 1.18

- Let $GL(n, \mathbb{R})$ be the set of all nonsingular n by n matrices with real coefficients.
- Let $SL(n, \mathbb{R})$ be the subgroup formed by matrices whose determinant is 1.
- Then $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$

Quotient groups

Definition 1.17 (quotient subgroup)

If $N \trianglelefteq G$, the quotient group G/N is defined to be the group of cosets of N in G under the operation of multiplication.

$$G/N = \{gN : g \in G\}$$

The multiplication is defined : $(aN)(bN) = (ab)N$.
The identity is N.

Example 1.18

- Let $GL(n, \mathbb{R})$ be the set of all nonsingular n by n matrices with real coefficients.
- Let $SL(n, \mathbb{R})$ be the subgroup formed by matrices whose determinant is 1.
- Then $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$

Homomorphism

Definition 1.19 (Homomorphism)

If $f : G \mapsto G'$, where G and G' are groups, then f is said to be a homomorphism if for all $a, b \in G$, we have

$$f(ab) = f(a)f(b).$$

Lemma 1.20

If f is a homomorphism from G to G', then

- $f(1_G) = 1_{G'}$.
- *Let $a \in G$, then $f(a^{-1}) = f(a)^{-1}$.*

Homomorphism

Definition 1.19 (Homomorphism)

If $f : G \mapsto G'$, where G and G' are groups, then f is said to be a homomorphism if for all $a, b \in G$, we have

$$f(ab) = f(a)f(b).$$

Lemma 1.20

If f is a homomorphism from G to G', then

- $f(1_G) = 1_{G'}$.
- *Let $a \in G$, then $f(a^{-1}) = f(a)^{-1}$.*

Homomorphism

Definition 1.19 (Homomorphism)

If $f : G \mapsto G'$, where G and G' are groups, then f is said to be a homomorphism if for all $a, b \in G$, we have

$$f(ab) = f(a)f(b).$$

Lemma 1.20

If f is a homomorphism from G to G', then

- $f(1_G) = 1_{G'}$.
- *Let $a \in G$, then $f(a^{-1}) = f(a)^{-1}$.*

同态

Definition 1.21 (kernel)

If $f : G \mapsto G'$ is a homomorphism , the kernel of f is

$$\ker f = \{a \in G : f(a) = 1_{G'}\};$$

Fact 1.22

If f is a homomorphism from G to G', then

- $\ker f \trianglelefteq G$. *For $\forall a \in G$ and $b \in \ker f$,*

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)(1)f(a)^{-1} = 1.$$

Fact 1.23

If $N \trianglelefteq G$, define $\pi : G \to G/N$, then

- *π is a homomorphism with N the kernel.*

Definition 1.21 (kernel)

If $f : G \mapsto G'$ is a homomorphism , the kernel of f is

$$\ker f = \{a \in G : f(a) = 1_{G'}\};$$

Fact 1.22

If f is a homomorphism from G to G', then

- $\ker f \trianglelefteq G$. *For* $\forall a \in G$ *and* $b \in \ker f$,

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)(1)f(a)^{-1} = 1.$$

Fact 1.23

If $N \trianglelefteq G$, define $\pi : G \to G/N$, then

- *π is a homomorphism with N the kernel.*

Definition 1.21 (kernel)

If $f : G \mapsto G'$ is a homomorphism , the kernel of f is

$$\ker f = \{a \in G : f(a) = 1_{G'}\};$$

Fact 1.22

If f is a homomorphism from G to G', then

- $\ker f \trianglelefteq G$. *For $\forall a \in G$ and $b \in \ker f$,*

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)(1)f(a)^{-1} = 1.$$

Fact 1.23

If $N \trianglelefteq G$, define $\pi : G \to G/N$, then

- *π is a homomorphism with N the kernel.*

Definition 1.24 (natural homomorphism)

If $N \trianglelefteq G$. Define the map $\pi : G \mapsto G/N$ by $\pi(a) = aN$; π is called the natural homomorphism. And

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b).$$

$\ker f = \{a : aN = N, a \in G\} = N.$

Lemma 1.25

A homomorphism f is injective iff its kernel $K = \{1\}$.

Proof.

- $\Rightarrow$: $\forall a \in K$, we have $f(a) = f(1) = 1$, then $a = 1$.
- $\Leftarrow$: If $K = \{1\}$ and $f(a) = f(b)$, then

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = f(a)[f(a)]^{-1} = 1.$$

So $ab^{-1} \in K$. Thus $ab^{-1} = 1$, i.e. $a = b$.

□

Lemma 1.25

A homomorphism f is injective iff its kernel $K = \{1\}$.

Proof.

- $\Rightarrow$: $\forall a \in K$, we have $f(a) = f(1) = 1$, then $a = 1$.
- $\Leftarrow$: If $K = \{1\}$ and $f(a) = f(b)$, then

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = f(a)[f(a)]^{-1} = 1.$$

So $ab^{-1} \in K$. Thus $ab^{-1} = 1$, i.e. $a = b$.

□

Lemma 1.25

A homomorphism f is injective iff its kernel $K = \{1\}$.

Proof.

- $\Rightarrow$: $\forall a \in K$, we have $f(a) = f(1) = 1$, then $a = 1$.
- $\Leftarrow$: If $K = \{1\}$ and $f(a) = f(b)$, then

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = f(a)[f(a)]^{-1} = 1.$$

So $ab^{-1} \in K$. Thus $ab^{-1} = 1$, i.e. $a = b$.

□

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.
$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.
$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

Standard Terminology

- 单同态monomorphism = injective homomorphism
- 满同态epimorphism = surjective homomorphism
- 同构isomorphism = bijective homomorphism
- 自同态endomorphism = homomorphism of a group to itself
- 自同构automorphism = isomorphism of a group with itself

Example 1.26

1. $\phi : \mathbb{Z} \to \mathbb{R}^*$, and $\phi(n) = (-1)^n$.
2. $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ and $\phi(f(x)) = f'(x)$.
3. G is a cyclic group of order n with generator g.

$\phi : G \to G$ and $\phi(g^i) = g^{id}$ where $\gcd(d, n) = 1$.

单同态

满同态

同构

darkmoon scan retouch by fish 200

darkmoon scan retouch by fish 20

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \leq G$, then $f(M) \leq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \leq G'$, then $f^{-1}(K) \leq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \leq G$, then $f(M) \leq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \leq G'$, then $f^{-1}(K) \leq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \preceq G$, then $f(M) \preceq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \preceq G'$, then $f^{-1}(K) \preceq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \preceq G$, then $f(M) \preceq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \preceq G'$, then $f^{-1}(K) \preceq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \preceq G$, then $f(M) \preceq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \preceq G'$, then $f^{-1}(K) \preceq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \preceq G$, then $f(M) \preceq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \preceq G'$, then $f^{-1}(K) \preceq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

Lemma 1.27

Let $f : G \mapsto G'$ be a homomorphism.

1. *If $M \preceq G$, then $f(M) \preceq G'$. If f is an epimorphism and M is normal, then $f(M)$ is also normal. (If f is onto and $M \trianglelefteq G$, then $f(M) \trianglelefteq f(G)$.)*
2. *If $K \preceq G'$, then $f^{-1}(K) \preceq G$. If K is normal, so is $f^{-1}(K)$. (If $K \trianglelefteq G'$, then $f^{-1}(K) \trianglelefteq G$)*

Proof.

1. If $f(a), f(b) \in f(M)$, then $f(a)f(b)^{-1} = f(ab^{-1}) \in f(M)$.

   If M is normal and $c \in G$, then $f(c)f(M)f(c)^{-1} = f(cMc^{-1}) = f(M)$, so if f is surjective, then $f(M)$ is normal.

   问题：为什么一定要求f是满同态？ Otherwise $f(M) \trianglelefteq f(G)$.
2. If $a, b \in f^{-1}(K)$, then $f(ab^{-1}) = f(a)f(b)^{-1} \in K$, so $ab^{-1} \in f^{-1}(K)$. If for all $c \in G$ and $a \in f^{-1}(K)$, then $f(cac^{-1}) = f(c)f(a)f(c)^{-1}$, if K is normal, then $cac^{-1} \in f^{-1}(K)$, proving $f^{-1}(K)$ normal.

□

The Isomorphism Theorems

Suppose $N \trianglelefteq G$. f is a homomorphism from G to G', and π is a natural homomorphism from G to G/N, as the following picture:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & G' \\ G/N \arrow[ur, dashed, "\overline{f}"'] & \end{tikzcd}$$

We want to find a homomorphism $\overline{f} : G/N \to G'$ and $\overline{f}(aN) = f(a)$. That is

$$\overline{f} \circ \pi = f.$$

The Isomorphism Theorems

Theorem 1.28 (Factor Theorem)

Any homomorphism f whose kernel K contains N can be factored through G/N. In other words, there is a unique homomorphism $\overline{f} : G/N \to G'$ such that $\overline{f} \circ \pi = f$. Furthermore,

1. *$\overline{f}$ is an epimorphism iff f is an epimorphism.*
2. *$\overline{f}$ is a monomorphism iff $K = N$.*
3. *$\overline{f}$ is an isomorphism iff f is an empimorphism and $K = N$.*

Proof.

首先证明同态$\overline{f}$的存在性。构造性证明：
现规定：$\overline{f}(aN) = f(a)$，为证明$\overline{f}$是同态，需证明如下两步：

- 先证明$\overline{f} : G/N \to G'$是一个映射。
  即要证$\overline{f}(aN) \neq \overline{f}(bN) \Rightarrow aN \neq bN$，等价于$aN = bN \Rightarrow \overline{f}(aN) = \overline{f}(bN)$。
  若$aN = bN$，则$a^{-1}b \in N \subseteq K$，所以$f(a^{-1}b) = 1$，即$f(a) = f(b)$，
  即$\overline{f}(aN) = \overline{f}(bN)$。
- 再证明$\overline{f}$保持运算。

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

所以$\overline{f}$是同态，且由其定义知其是惟一的。 □

Proof.

首先证明同态$\overline{f}$的存在性。构造性证明：
现规定：$\overline{f}(aN) = f(a)$，为证明$\overline{f}$是同态，需证明如下两步：

- 先证明$\overline{f} : G/N \to G'$是一个映射。
  即要证$\overline{f}(aN) \neq \overline{f}(bN) \Rightarrow aN \neq bN$，等价于$aN = bN \Rightarrow \overline{f}(aN) = \overline{f}(bN)$。
  若$aN = bN$，则$a^{-1}b \in N \subseteq K$，所以$f(a^{-1}b) = 1$，即$f(a) = f(b)$，
  即$\overline{f}(aN) = \overline{f}(bN)$。
- 再证明$\overline{f}$保持运算。

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

所以$\overline{f}$是同态，且由其定义知其是惟一的。 □

Proof.

首先证明同态$\overline{f}$的存在性。构造性证明：
现规定：$\overline{f}(aN) = f(a)$，为证明$\overline{f}$是同态，需证明如下两步：

- 先证明$\overline{f} : G/N \to G'$是一个映射。
  即要证$\overline{f}(aN) \neq \overline{f}(bN) \Rightarrow aN \neq bN$，等价于$aN = bN \Rightarrow \overline{f}(aN) = \overline{f}(bN)$。
  若$aN = bN$，则$a^{-1}b \in N \subseteq K$，所以$f(a^{-1}b) = 1$，即$f(a) = f(b)$，
  即$\overline{f}(aN) = \overline{f}(bN)$。
- 再证明$\overline{f}$保持运算。

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

所以$\overline{f}$是同态，且由其定义知其是惟一的。

□

Proof.

首先证明同态$\overline{f}$的存在性。构造性证明：
现规定：$\overline{f}(aN) = f(a)$，为证明$\overline{f}$是同态，需证明如下两步：

- 先证明$\overline{f} : G/N \to G'$是一个映射。
  即要证$\overline{f}(aN) \neq \overline{f}(bN) \Rightarrow aN \neq bN$，等价于$aN = bN \Rightarrow \overline{f}(aN) = \overline{f}(bN)$。
  若$aN = bN$，则$a^{-1}b \in N \subseteq K$，所以$f(a^{-1}b) = 1$，即$f(a) = f(b)$，
  即$\overline{f}(aN) = \overline{f}(bN)$。
- 再证明$\overline{f}$保持运算。

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

所以$\overline{f}$是同态，且由其定义知其是惟一的。

□

Proof.

首先证明同态$\overline{f}$的存在性。构造性证明：
现规定：$\overline{f}(aN) = f(a)$，为证明$\overline{f}$是同态，需证明如下两步：

- 先证明$\overline{f} : G/N \to G'$是一个映射。
  即要证$\overline{f}(aN) \neq \overline{f}(bN) \Rightarrow aN \neq bN$，等价于$aN = bN \Rightarrow \overline{f}(aN) = \overline{f}(bN)$。
  若$aN = bN$，则$a^{-1}b \in N \subseteq K$，所以$f(a^{-1}b) = 1$，即$f(a) = f(b)$，
  即$\overline{f}(aN) = \overline{f}(bN)$。
- 再证明$\overline{f}$保持运算。

$$\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN).$$

所以$\overline{f}$是同态，且由其定义知其是惟一的。

□

1. $\overline{f}$ is an epimorphism iff f is an epimorphism.

   Because $\overline{f}$ has the same image as f, proving (1).

2. $\overline{f}$ is a monomorphism iff $K = N$.

   The kernel of $\overline{f} = \{aN : f(a) = 1\} = \{aN : a \in K\} = K/N$. Because $\overline{f}$ is a monomorphism iff K/N consists only of the identity element N (lemma 1.25), proving (2).

3. $\overline{f}$ is an isomorphism iff f is an epimorphism and $K = N$.

   (3) follows immediately from (1) and (2).

1. $\overline{f}$ is an epimorphism iff f is an epimorphism.

   Because $\overline{f}$ has the same image as f, proving (1).

2. $\overline{f}$ is a monomorphism iff $K = N$.

   The kernel of $\overline{f} = \{aN : f(a) = 1\} = \{aN : a \in K\} = K/N$. Because $\overline{f}$ is a monomorphism iff K/N consists only of the identity element N (lemma 1.25), proving (2).

3. $\overline{f}$ is an isomorphism iff f is an epimorphism and $K = N$.

   (3) follows immediately from (1) and (2).

1. $\overline{f}$ is an epimorphism iff f is an epimorphism.

   Because $\overline{f}$ has the same image as f, proving (1).

2. $\overline{f}$ is a monomorphism iff $K = N$.

   The kernel of $\overline{f} = \{aN : f(a) = 1\} = \{aN : a \in K\} = K/N$. Because $\overline{f}$ is a monomorphism iff K/N consists only of the identity element N (lemma 1.25), proving (2).

3. $\overline{f}$ is an isomorphism iff f is an epimorphism and $K = N$.

   (3) follows immediately from (1) and (2).

The Isomorphism Theorems: The first isomorphism theorem

Theorem 1.29 (First Isomorphism Theorem)

If $f : G \to G'$ is a homomorphism with kernel K, then the image of f is isomorphism to G/K.

Proof. Apply the factor theorem with $N = K$, and note that f must be an epimorphism of G onto its image.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, and therefore by lemma 1.14, $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Lemma 1.30

Let $H, N \preceq G$, with $N \trianglelefteq G$. Then

1. $HN = NH$, *and therefore by lemma 1.14,* $HN \preceq G$.
2. $N \trianglelefteq HN$.
3. $H \cap N \trianglelefteq H$.

Proof.

1. We have $hN = Nh$ for every $h \in G$, thus $HN \subseteq NH$ and $NH \subseteq HN$ and $HN = NH$.
2. Since $N \trianglelefteq G$, it must be normal in the subgroup HN.
3. 令$W = H \cap N$，则W是一个子群。对于任意$h \in H$，由于$W \subseteq N$而N是正规子群，有$hWh^{-1} \subseteq hNh^{-1} = N$。由于$W \subseteq H$，所以对于任意$h \in H$，有$hWh^{-1} \subseteq H$。所以有$hWh^{-1} \subseteq H \cap N = W$。$H \cap N$ is the kernel of natural homomorphism $\pi : G \to G/N$, restricted to H.

The Isomorphism Theorems

Theorem 1.31 (Second Isomorphism Theorem)

If H and N are subgroups of G, with $N \trianglelefteq G$, then

$$H/(H \cap N) \cong HN/N.$$

Proof.

Let $\pi : h \mapsto hN \ \ (H \to HN/N)$, since $\pi(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = \pi(h_1)\pi(h_2)$, so π is obviously a epimorphism. And

$$\begin{aligned} \ker \pi &= \{h : h \in H \wedge \pi(h) = N\} \\ &= H \cap N. \end{aligned}$$

Following first isomorphism theorem, finish the proof. □

The Isomorphism Theorems

Theorem 1.31 (Second Isomorphism Theorem)

If H and N are subgroups of G, with $N \trianglelefteq G$, then

$$H/(H \cap N) \cong HN/N.$$

Proof.

Let $\pi : h \mapsto hN \ \ (H \to HN/N)$, since $\pi(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = \pi(h_1)\pi(h_2)$, so π is obviously a epimorphism. And

$$\begin{aligned} \ker \pi &= \{h : h \in H \wedge \pi(h) = N\} \\ &= H \cap N. \end{aligned}$$

Following first isomorphism theorem, finish the proof. □

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。

现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。

现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。
现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。
现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。
现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。
现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

Theorem 1.32 (Third Isomorphism Theorem)

Let $H, N \trianglelefteq G$ and $N \subseteq H$. Then

$$G/H \cong (G/N)/(H/N).$$

思路：只需找到一个从G/N到G/H的满同态，并证明其内核是H/N，就可以用第一同构定理证明。
现定义$f : G/N \to G/H$为$f(aN) = aH$。

- 首先证明f是一个函数：如果$aN = bN$，那么$a^{-1}b \in N \subseteq H$，故$aH = bH$。
- 由于$a \in G$的任意性，知f是一个满射；
- 由于$f(aNbN) = f(abN) = abH = aHbH$，保持运算，故$f$是一个同态，且是一个满同态；

The Isomorphism Theorems

- f的内核：
  $\{aN, a \in G, f(aN) = aH = H\} = \{aN, a \in H\} = H/N$。
- 由第一同构定理，结论得证。

Let $\pi : gN \mapsto gH \ \ (G/N \to G/H)$. Moreover π is surjective, and $\ker \pi = H/N$. But $\pi(G/H) \cong (G/N)/(\ker \pi)$. Therefore $G/H \cong (G/N)/(H/N)$.

The Isomorphism Theorems

- f的内核：
  $\{aN, a \in G, f(aN) = aH = H\} = \{aN, a \in H\} = H/N$。
- 由第一同构定理，结论得证。

Let $\pi : gN \mapsto gH \ \ (G/N \to G/H)$. Moreover π is surjective, and $\ker \pi = H/N$. But $\pi(G/H) \cong (G/N)/(\ker \pi)$. Therefore $G/H \cong (G/N)/(H/N)$.

The Isomorphism Theorems

- f的内核：
  $\{aN, a \in G, f(aN) = aH = H\} = \{aN, a \in H\} = H/N$。
- 由第一同构定理，结论得证。

Let $\pi : gN \mapsto gH \ \ (G/N \to G/H)$. Moreover π is surjective, and $\ker \pi = H/N$. But $\pi(G/H) \cong (G/N)/(\ker \pi)$. Therefore $G/H \cong (G/N)/(H/N)$.

群与商群间的一一对应

设$N \trianglelefteq G$，则G中所有包含正规子群N的子群与商群G/N的子群有一一对应关系。令$N \leq H \leq G$，则$H/N \leq G/N$。

- 令$\psi(H) = H/N$定义一个从集合$\{H \mid N \leq H \leq G\}$到$\{Q \mid Q \leq G/N\}$的映射。
- 先证ψ是一个单射。如果$H_1/N = H_2/N$，那么对于任意$h_1 \in H_1$，定存在一个$h_2 \in H_2$，使得$h_1N = h_2N$。故$h_1^{-1}h_2 \in N \subseteq H_2$，所以$h_1 \in H_2$。故$H_1 \subseteq H_2$。同理可证$H_2 \subseteq H_1$。所以$H_1 = H_2$。
- 令$Q \subseteq G/N$，且$\pi : G \to G/N$是一个自然同态，则

$$\pi^{-1}(Q) = \{a \in G : aN \in Q\}$$

是一个包含N的G的一个子群。而且$\psi(\pi^{-1}(Q)) = \{aN : aN \in Q\} = Q$，因此$\psi$是一个满射。

群与商群间的一一对应

设$N \trianglelefteq G$，则G中所有包含正规子群N的子群与商群G/N的子群有一一对应关系。令$N \leq H \leq G$，则$H/N \leq G/N$。

- 令$\psi(H) = H/N$定义一个从集合$\{H \mid N \leq H \leq G\}$到$\{Q \mid Q \leq G/N\}$的映射。
- 先证ψ是一个单射。如果$H_1/N = H_2/N$，那么对于任意$h_1 \in H_1$，定存在一个$h_2 \in H_2$，使得$h_1N = h_2N$。故$h_1^{-1}h_2 \in N \subseteq H_2$，所以$h_1 \in H_2$。故$H_1 \subseteq H_2$。同理可证$H_2 \subseteq H_1$。所以$H_1 = H_2$。
- 令$Q \subseteq G/N$，且$\pi : G \to G/N$是一个自然同态，则

$$\pi^{-1}(Q) = \{a \in G : aN \in Q\}$$

是一个包含N的G的一个子群。而且$\psi(\pi^{-1}(Q)) = \{aN : aN \in Q\} = Q$，因此$\psi$是一个满射。

群与商群间的一一对应

设$N \trianglelefteq G$，则G中所有包含正规子群N的子群与商群G/N的子群有一一对应关系。令$N \leq H \leq G$，则$H/N \leq G/N$。

- 令$\psi(H) = H/N$定义一个从集合$\{H \mid N \leq H \leq G\}$到$\{Q \mid Q \leq G/N\}$的映射。
- 先证ψ是一个单射。如果$H_1/N = H_2/N$，那么对于任意$h_1 \in H_1$，定存在一个$h_2 \in H_2$，使得$h_1N = h_2N$。故$h_1^{-1}h_2 \in N \subseteq H_2$，所以$h_1 \in H_2$。故$H_1 \subseteq H_2$。同理可证$H_2 \subseteq H_1$。所以$H_1 = H_2$。
- 令$Q \subseteq G/N$，且$\pi : G \to G/N$是一个自然同态，则

$$\pi^{-1}(Q) = \{a \in G : aN \in Q\}$$

是一个包含N的G的一个子群。而且$\psi(\pi^{-1}(Q)) = \{aN : aN \in Q\} = Q$，因此$\psi$是一个满射。

群与商群间的一一对应

设$N \trianglelefteq G$，则G中所有包含正规子群N的子群与商群G/N的子群有一一对应关系。令$N \leq H \leq G$，则$H/N \leq G/N$。

- 令$\psi(H) = H/N$定义一个从集合$\{H \mid N \leq H \leq G\}$到$\{Q \mid Q \leq G/N\}$的映射。
- 先证ψ是一个单射。如果$H_1/N = H_2/N$，那么对于任意$h_1 \in H_1$，定存在一个$h_2 \in H_2$，使得$h_1N = h_2N$。故$h_1^{-1}h_2 \in N \subseteq H_2$，所以$h_1 \in H_2$。故$H_1 \subseteq H_2$。同理可证$H_2 \subseteq H_1$。所以$H_1 = H_2$。
- 令$Q \subseteq G/N$，且$\pi : G \to G/N$是一个自然同态，则

$$\pi^{-1}(Q) = \{a \in G : aN \in Q\}$$

是一个包含N的G的一个子群。而且$\psi(\pi^{-1}(Q)) = \{aN : aN \in Q\} = Q$，因此$\psi$是一个满射。

群与商群间的一一对应定理

If $N \trianglelefteq G$, then the map $\psi : H \to H/N$ sets up a one-to-one correspondence between subgroups of G containing N and subgroups of G/N. The inverse of ψ is the map $\tau : Q \to \pi^{-1}(Q)$, where π is the canonical epimorphism of G onto G/N. Furthermore,

(i) $H_1 \leq H_2$ iff $H_1/N \leq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

(iii) H_1 is a normal subgroup of H_2 iff H_1/N is a normal subgroup of H_2/N, and in this case,

$$H_2/H_1 \cong (H_2/N)/(H_1/N).$$

群与商群间的一一对应定理

If $N \trianglelefteq G$, then the map $\psi : H \to H/N$ sets up a one-to-one correspondence between subgroups of G containing N and subgroups of G/N. The inverse of ψ is the map $\tau : Q \to \pi^{-1}(Q)$, where π is the canonical epimorphism of G onto G/N. Furthermore,

(i) $H_1 \leq H_2$ iff $H_1/N \leq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

(iii) H_1 is a normal subgroup of H_2 iff H_1/N is a normal subgroup of H_2/N, and in this case,

$$H_2/H_1 \cong (H_2/N)/(H_1/N).$$

群与商群间的一一对应定理

If $N \trianglelefteq G$, then the map $\psi : H \to H/N$ sets up a one-to-one correspondence between subgroups of G containing N and subgroups of G/N. The inverse of ψ is the map $\tau : Q \to \pi^{-1}(Q)$, where π is the canonical epimorphism of G onto G/N. Furthermore,

(i) $H_1 \leq H_2$ iff $H_1/N \leq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

(iii) H_1 is a normal subgroup of H_2 iff H_1/N is a normal subgroup of H_2/N, and in this case,

$$H_2/H_1 \cong (H_2/N)/(H_1/N).$$

群与商群间的一一对应定理

If $N \trianglelefteq G$, then the map $\psi : H \to H/N$ sets up a one-to-one correspondence between subgroups of G containing N and subgroups of G/N. The inverse of ψ is the map $\tau : Q \to \pi^{-1}(Q)$, where π is the canonical epimorphism of G onto G/N. Furthermore,

(i) $H_1 \leq H_2$ iff $H_1/N \leq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

(iii) H_1 is a normal subgroup of H_2 iff H_1/N is a normal subgroup of H_2/N, and in this case,

$$H_2/H_1 \cong (H_2/N)/(H_1/N).$$

群与商群间的一一对应定理

(i) $H_1 \preceq H_2$ iff $H_1/N \preceq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

Proof.

- If $H_1 \preceq H_2$, then it is obvious $H_1/N \preceq H_2/N$.
- Converse follows with the fact that ψ is injective.
- 考虑H_1相对于H_2的陪集。陪集个数共有$[H_2 : H_1]$个。Let η map the left coset aH_1, $a \in H_2$, to the left coset $(aN)(H_1/N)$. The η is a well-defined and injective map of

$$\begin{aligned} aH_1 = bH_1 \quad & iff \quad a^{-1}b \in H_1; && (1)\\ & iff \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N; && (2)\\ & iff \quad (aN)(H_1/N) = (bN)(H_1/N); && (3) \end{aligned}$$

群与商群间的一一对应定理

(i) $H_1 \preceq H_2$ iff $H_1/N \preceq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

Proof.

- If $H_1 \preceq H_2$, then it is obvious $H_1/N \preceq H_2/N$.
- Converse follows with the fact that ψ is injective.
- 考虑H_1相对于H_2的陪集。陪集个数共有$[H_2 : H_1]$个。Let η map the left coset aH_1, $a \in H_2$, to the left coset $(aN)(H_1/N)$. The η is a well-defined and injective map of

$$\begin{aligned} aH_1 = bH_1 \quad & iff \quad a^{-1}b \in H_1; && (1)\\ & iff \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N; && (2)\\ & iff \quad (aN)(H_1/N) = (bN)(H_1/N); && (3) \end{aligned}$$

群与商群间的一一对应定理

(i) $H_1 \preceq H_2$ iff $H_1/N \preceq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

Proof.

- If $H_1 \preceq H_2$, then it is obvious $H_1/N \preceq H_2/N$.
- Converse follows with the fact that ψ is injective.
- 考虑H_1相对于H_2的陪集。陪集个数共有$[H_2 : H_1]$个。Let η map the left coset aH_1, $a \in H_2$, to the left coset $(aN)(H_1/N)$. The η is a well-defined and injective map of

$$\begin{aligned} aH_1 = bH_1 \quad & iff \quad a^{-1}b \in H_1; && (1)\\ & iff \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N; && (2)\\ & iff \quad (aN)(H_1/N) = (bN)(H_1/N); && (3) \end{aligned}$$

群与商群间的一一对应定理

(i) $H_1 \preceq H_2$ iff $H_1/N \preceq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

Proof.

- If $H_1 \preceq H_2$, then it is obvious $H_1/N \preceq H_2/N$.
- Converse follows with the fact that ψ is injective.
- 考虑H_1相对于H_2的陪集。陪集个数共有$[H_2 : H_1]$个。Let η map the left coset aH_1, $a \in H_2$, to the left coset $(aN)(H_1/N)$. The η is a well-defined and injective map of

$$\begin{aligned} aH_1 = bH_1 \quad & iff \quad a^{-1}b \in H_1; && (1)\\ & iff \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N; && (2)\\ & iff \quad (aN)(H_1/N) = (bN)(H_1/N); && (3) \end{aligned}$$

群与商群间的一一对应定理

(i) $H_1 \preceq H_2$ iff $H_1/N \preceq H_2/N$, and in this case,

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

Proof.

- If $H_1 \preceq H_2$, then it is obvious $H_1/N \preceq H_2/N$.
- Converse follows with the fact that ψ is injective.
- 考虑H_1相对于H_2的陪集。陪集个数共有$[H_2 : H_1]$个。Let η map the left coset aH_1, $a \in H_2$, to the left coset $(aN)(H_1/N)$. The η is a well-defined and injective map of

$$\begin{aligned} aH_1 = bH_1 \quad & iff \quad a^{-1}b \in H_1; && (1)\\ & iff \quad (aN)^{-1}(bN) = a^{-1}bN \in H_1/N; && (2)\\ & iff \quad (aN)(H_1/N) = (bN)(H_1/N); && (3) \end{aligned}$$

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

群与商群间的一一对应定理

(ii) H is a normal subgroup of G iff H/N is a normal subgroup of G/N, more generally,

Proof.

- Let $H \trianglelefteq G$. Then for any $a \in G$, we have

$$(aN)H/N(aN)^{-1} = (aHa^{-1})/N = H/N.$$

  Hence $H/N \trianglelefteq G/N$.
- $H/N \trianglelefteq G/N$. Consider the homomorphism $f : a \to (aN)(H/N)$.
- $Ker(f) = \{a, (aN)(H/N) = H/N, a \in G\} = \{a, aN \in H/N, a \in G\} = \{a \in H\} = H$.
- $Ker(f) = H \trianglelefteq G$.
- The third isomorphism gives (iii).

□

有限交换群

Lemma 2.1

在阶为n 的循环群$< a > (a^n = e)$中，对任意正整数$m|n$,都有子群H, H的阶是m.

Proof: 设$n = mt$, 考察$< b >$,其中$b = a^t$.易见

$$b^m = (a^t)^m = a^t m = a^n = e.$$

而对任意正整数$s < m$, 有$ts < n$, 故$b^s = (a^t)^s = a^{ts} \neq e$,即得$b$的阶为$m$, 随之$< b >$的阶为$m$. □

Lemma 2.2

设G是有限交换群，其阶$n = pm$，其中p为素数，则在G中存在阶为p的元素。

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 假设在小于m时结论成立。任取$e \neq a \in G$, 记$H =< a >$.
  - 若$p \mid |H|$，由H为有限循环群知H中存在，从而G中存在阶为p的元素。
  - 若$p \nmid |H|$, 记$\overline{G} = G/H$为G的商群。则$|\overline{G}| = |G|/|H| = pm'$, 其中$1 \leq m' < m$.由归纳假设知存在$b \in G$使得$bH$在$\overline{G}$ 中的阶为p. 于是$b \notin H$但$b^p \in H$. 设a的阶为s, 则$p \nmid |H| = s$且$(b^s)^p = (b^p)^s = e$.另一方面$b^s \neq e$, 这是因为若$b^s = e$,则由p, s互素，故有整数q, r 使得$qp + rs = 1$, 这时$b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$, 与前面$b \notin H$ 矛盾。故b^s的阶为p.

Lemma 2.2

设G是有限交换群，其阶$n = pm$，其中p为素数，则在G中存在阶为p的元素。

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 假设在小于m时结论成立。任取$e \neq a \in G$, 记$H =< a >$.
  - 若$p \mid |H|$，由H为有限循环群知H中存在，从而G中存在阶为p的元素。
  - 若$p \nmid |H|$, 记$\overline{G} = G/H$为G的商群。则$|\overline{G}| = |G|/|H| = pm'$, 其中$1 \leq m' < m$.由归纳假设知存在$b \in G$使得$bH$在$\overline{G}$ 中的阶为p. 于是$b \notin H$但$b^p \in H$. 设a的阶为s, 则$p \nmid |H| = s$且$(b^s)^p = (b^p)^s = e$.另一方面$b^s \neq e$, 这是因为若$b^s = e$,则由p, s互素，故有整数q, r 使得$qp + rs = 1$, 这时$b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$, 与前面$b \notin H$ 矛盾。故b^s的阶为p.

Lemma 2.2

设G是有限交换群，其阶$n = pm$，其中p为素数，则在G中存在阶为p的元素。

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 假设在小于m时结论成立。任取$e \neq a \in G$, 记$H =< a >$.
  - 若$p \mid |H|$，由H为有限循环群知H中存在，从而G中存在阶为p的元素。
  - 若$p \nmid |H|$, 记$\overline{G} = G/H$为G的商群。则$|\overline{G}| = |G|/|H| = pm'$, 其中$1 \leq m' < m$.由归纳假设知存在$b \in G$使得$bH$在$\overline{G}$ 中的阶为p. 于是$b \notin H$但$b^p \in H$. 设a的阶为s, 则$p \nmid |H| = s$且$(b^s)^p = (b^p)^s = e$.另一方面$b^s \neq e$, 这是因为若$b^s = e$,则由p, s互素，故有整数q, r 使得$qp + rs = 1$, 这时$b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$, 与前面$b \notin H$ 矛盾。故b^s的阶为p.

Lemma 2.2

设G是有限交换群，其阶$n = pm$，其中p为素数，则在G中存在阶为p的元素。

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 假设在小于m时结论成立。任取$e \neq a \in G$, 记$H =< a >$.
  - 若$p \mid |H|$，由H为有限循环群知H中存在，从而G中存在阶为p的元素。
  - 若$p \nmid |H|$, 记$\overline{G} = G/H$为G的商群。则$|\overline{G}| = |G|/|H| = pm'$, 其中$1 \leq m' < m$.由归纳假设知存在$b \in G$使得$bH$在$\overline{G}$ 中的阶为p. 于是$b \notin H$但$b^p \in H$. 设a的阶为s, 则$p \nmid |H| = s$且$(b^s)^p = (b^p)^s = e$.另一方面$b^s \neq e$, 这是因为若$b^s = e$,则由p, s互素，故有整数q, r 使得$qp + rs = 1$, 这时$b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$, 与前面$b \notin H$ 矛盾。故b^s的阶为p.

Lemma 2.2

设G是有限交换群，其阶$n = pm$，其中p为素数，则在G中存在阶为p的元素。

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 假设在小于m时结论成立。任取$e \neq a \in G$, 记$H =< a >$.
  - 若$p \mid |H|$，由H为有限循环群知H中存在，从而G中存在阶为p的元素。
  - 若$p \nmid |H|$, 记$\overline{G} = G/H$为G的商群。则$|\overline{G}| = |G|/|H| = pm'$, 其中$1 \leq m' < m$.由归纳假设知存在$b \in G$使得$bH$在$\overline{G}$ 中的阶为p. 于是$b \notin H$但$b^p \in H$. 设a的阶为s, 则$p \nmid |H| = s$且$(b^s)^p = (b^p)^s = e$.另一方面$b^s \neq e$, 这是因为若$b^s = e$,则由p, s互素，故有整数q, r 使得$qp + rs = 1$, 这时$b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$, 与前面$b \notin H$ 矛盾。故b^s的阶为p.

Theorem 2.3

设G是有限交换群，其阶$|G| = n$. 则对任意$m|n$, 存在G的子群H使得$|H| = m$.

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 设$m > 1$. 设p为素数且$p|m$. 由上面引理知G中存在阶为p的元素，记为a. 考虑商群$\overline{G} = G/ < a >$. 由$\frac{m}{p}|\frac{n}{p}$和归纳假设知$\overline{G}$中存在子群$\overline{H}$使得$|\overline{H}| = \frac{m}{p}$.
- 记H为$\overline{H}$在G到$\overline{G}$的自然满同态之下的完全原象。那么H是G的子群，且G到$\overline{G}$的自然满同态在H上的限制导出H到$\overline{H}$的满射，是群的满同态且核也为$< a >$. 故$|H| = | < a > | \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即$H$为所求的子群。

Theorem 2.3

设G是有限交换群，其阶$|G| = n$. 则对任意$m|n$, 存在G的子群H使得$|H| = m$.

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 设$m > 1$. 设p为素数且$p|m$. 由上面引理知G中存在阶为p的元素，记为a. 考虑商群$\overline{G} = G/ < a >$. 由$\frac{m}{p}|\frac{n}{p}$和归纳假设知$\overline{G}$中存在子群$\overline{H}$使得$|\overline{H}| = \frac{m}{p}$.
- 记H为$\overline{H}$在G到$\overline{G}$的自然满同态之下的完全原象。那么H是G的子群，且G到$\overline{G}$的自然满同态在H上的限制导出H到$\overline{H}$的满射，是群的满同态且核也为$< a >$. 故$|H| = | < a > | \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即$H$为所求的子群。

Theorem 2.3

设G是有限交换群，其阶$|G| = n$. 则对任意$m|n$, 存在G的子群H使得$|H| = m$.

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 设$m > 1$. 设p为素数且$p|m$. 由上面引理知G中存在阶为p的元素，记为a. 考虑商群$\overline{G} = G/ < a >$. 由$\frac{m}{p}|\frac{n}{p}$和归纳假设知$\overline{G}$中存在子群$\overline{H}$使得$|\overline{H}| = \frac{m}{p}$.
- 记H为$\overline{H}$在G到$\overline{G}$的自然满同态之下的完全原象。那么H是G的子群，且G到$\overline{G}$的自然满同态在H上的限制导出H到$\overline{H}$的满射，是群的满同态且核也为$< a >$. 故$|H| = | < a > | \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即$H$为所求的子群。

Theorem 2.3

设G是有限交换群，其阶$|G| = n$. 则对任意$m|n$, 存在G的子群H使得$|H| = m$.

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 设$m > 1$. 设p为素数且$p|m$. 由上面引理知G中存在阶为p的元素，记为a. 考虑商群$\overline{G} = G/ < a >$. 由$\frac{m}{p}|\frac{n}{p}$和归纳假设知$\overline{G}$中存在子群$\overline{H}$使得$|\overline{H}| = \frac{m}{p}$.
- 记H为$\overline{H}$在G到$\overline{G}$的自然满同态之下的完全原象。那么H是G的子群，且G到$\overline{G}$的自然满同态在H上的限制导出H到$\overline{H}$的满射，是群的满同态且核也为$< a >$. 故$|H| = | < a > | \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即$H$为所求的子群。

Theorem 2.3

设G是有限交换群，其阶$|G| = n$. 则对任意$m|n$, 存在G的子群H使得$|H| = m$.

Proof: 对m作归纳:

- $m = 1$时,结论显然成立。
- 设$m > 1$. 设p为素数且$p|m$. 由上面引理知G中存在阶为p的元素，记为a. 考虑商群$\overline{G} = G/ < a >$. 由$\frac{m}{p}|\frac{n}{p}$和归纳假设知$\overline{G}$中存在子群$\overline{H}$使得$|\overline{H}| = \frac{m}{p}$.
- 记H为$\overline{H}$在G到$\overline{G}$的自然满同态之下的完全原象。那么H是G的子群，且G到$\overline{G}$的自然满同态在H上的限制导出H到$\overline{H}$的满射，是群的满同态且核也为$< a >$. 故$|H| = | < a > | \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即$H$为所求的子群。

串珠染色问题

手链上珠子共6颗，现将每颗珠子进行染一种色，共有n种颜色，请问：可以得到多少种不同染色方案的手链？

如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？

二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$\tau_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5\ 6)$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 3\ 5)(2\ 4\ 6)$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\ 3)(2\ 5)(3\ 6)$$

$$\tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 3)(2\ 6\ 4)$$

串珠染色问题

手链上珠子共6颗，现将每颗珠子进行染一种色，共有n种颜色，请问：可以得到多少种不同染色方案的手链？
如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？
二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$\tau_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5\ 6)$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 3\ 5)(2\ 4\ 6)$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\ 3)(2\ 5)(3\ 6)$$

$$\tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 3)(2\ 6\ 4)$$

串珠染色问题

手链上珠子共6颗，现将每颗珠子进行染一种色，共有n种颜色，请问：可以得到多少种不同染色方案的手链？
如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？
二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$\tau_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)(2)(3)(4)(5)(6)$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5\ 6)$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 3\ 5)(2\ 4\ 6)$$

$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\ 3)(2\ 5)(3\ 6)$$

$$\tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\ 5\ 3)(2\ 6\ 4)$$

$$
\begin{aligned}
\tau_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\ 6\ 5\ 4\ 3\ 2) \\
r \circ \tau_0 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 6)(2\ 5)(3\ 4) \\
r \circ \tau_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{pmatrix} = (1\ 5)(2\ 4)(3)(6) \\
r \circ \tau_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} = (1\ 4)(2\ 3)(5\ 6) \\
r \circ \tau_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix} = (1\ 3)(2)(4\ 6)(5) \\
r \circ \tau_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 6)(4\ 5) \\
r \circ \tau_5 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix} = (1)(2\ 6)(3\ 5)(4)
\end{aligned}
$$

群在集合上的作用

Definition 3.1

The group G acts on the set X if for each $g \in G$, there is a mapping $x \to g \bullet x$ of X into itself, such that for every $g, h \in G$ and $x \in X$,

$$h \bullet (g \bullet x) = (hg) \bullet x,$$

and for every $x \in X$,

$$1 \bullet x = x.$$

- A group action induces a homomorphism from G to S_X.
- 或者说：If Φ is a homomorphism of G to S_X, then there is a corresponding action, defined by $g \bullet x = \Phi(g)(x)$, $x \in X$.
- The Kernel of Φ is the set of all $g \in G$ such that $g \bullet x = x$ for all x, i.e., the set of g's that fix everything in X.

群在集合上的作用

Definition 3.1

The group G acts on the set X if for each $g \in G$, there is a mapping $x \to g \bullet x$ of X into itself, such that for every $g, h \in G$ and $x \in X$,

$$h \bullet (g \bullet x) = (hg) \bullet x,$$

and for every $x \in X$,

$$1 \bullet x = x.$$

- A group action induces a homomorphism from G to S_X.
- 或者说：If Φ is a homomorphism of G to S_X, then there is a corresponding action, defined by $g \bullet x = \Phi(g)(x)$, $x \in X$.
- The Kernel of Φ is the set of all $g \in G$ such that $g \bullet x = x$ for all x, i.e., the set of g's that fix everything in X.

群在集合上的作用

Definition 3.1

The group G acts on the set X if for each $g \in G$, there is a mapping $x \to g \bullet x$ of X into itself, such that for every $g, h \in G$ and $x \in X$,

$$h \bullet (g \bullet x) = (hg) \bullet x,$$

and for every $x \in X$,

$$1 \bullet x = x.$$

- A group action induces a homomorphism from G to S_X.
- 或者说：If Φ is a homomorphism of G to S_X, then there is a corresponding action, defined by $g \bullet x = \Phi(g)(x)$, $x \in X$.
- The Kernel of Φ is the set of all $g \in G$ such that $g \bullet x = x$ for all x, i.e., the set of g's that fix everything in X.

群在集合上的作用

Definition 3.1

The group G acts on the set X if for each $g \in G$, there is a mapping $x \to g \bullet x$ of X into itself, such that for every $g, h \in G$ and $x \in X$,

$$h \bullet (g \bullet x) = (hg) \bullet x,$$

and for every $x \in X$,

$$1 \bullet x = x.$$

- A group action induces a homomorphism from G to S_X.
- 或者说：If Φ is a homomorphism of G to S_X, then there is a corresponding action, defined by $g \bullet x = \Phi(g)(x)$, $x \in X$.
- The Kernel of Φ is the set of all $g \in G$ such that $g \bullet x = x$ for all x, i.e., the set of g's that fix everything in X.

群在集合上的作用示例

The regular action: Every group acts on itself by multiplication on the left, $x \to gx$. In this case, the homomorphism Φ is injective, and we say that the action is faithful.

The trivial action: We take $gx = x$ for all $g \in G$, $x \in X$. This action is highly unfaithful..

Conjugation on elements: For $g, x \in G$, we define $g \bullet x = gxg^{-1}$. The Kernel is

$$\{g : gxg^{-1} = x, x \in X\},$$

that is

$$\{g : gx = xg, x \in X\}.$$

群在集合上的作用示例

The regular action: Every group acts on itself by multiplication on the left, $x \to gx$. In this case, the homomorphism Φ is injective, and we say that the action is faithful.

The trivial action: We take $gx = x$ for all $g \in G$, $x \in X$. This action is highly unfaithful..

Conjugation on elements: For $g, x \in G$, we define $g \bullet x = gxg^{-1}$. The Kernel is

$$\{g : gxg^{-1} = x, x \in X\},$$

that is

$$\{g : gx = xg, x \in X\}.$$

群在集合上的作用示例

The regular action: Every group acts on itself by multiplication on the left, $x \to gx$. In this case, the homomorphism Φ is injective, and we say that the action is faithful.

The trivial action: We take $gx = x$ for all $g \in G$, $x \in X$. This action is highly unfaithful..

Conjugation on elements: For $g, x \in G$, we define $g \bullet x = gxg^{-1}$. The Kernel is

$$\{g : gxg^{-1} = x, x \in X\},$$

that is

$$\{g : gx = xg, x \in X\}.$$

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

群在集合上的作用示例

Definition 3.2

设$a \in G$。若对于任意$x \in G$，有$ax = xa$，则称a为群G的中心元。

群G的所有的中心元集合构成了G的一个子群。

Conjugation on subgroups: If $H \leq G$, we take $g \bullet H = gHg^{-1}$. Note that $gHg^{-1} \leq G$, called the conjugate subgroup of H by g, since $gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1}$ and $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$. We have a legal action of G on the set of subgroups of G.

Conjugation on subsets: let G act by conjugation on the collection of all subsets of G, not just subgroups.

Multiplication on left cosets: Let G act on the set of left cosets of a fixed subgroup G by $g \bullet (xH) = (gx)H$.

Multiplication on subsets: Let G act on all subsets of G by $g \bullet S = gS = \{gx : x \in S\}$.

The Orbit-Stabilizer Theorem

Definition 3.3

Suppose that the group G acts on the set X. If we start with the element $x \in X$ and successively apply group elements in all possible ways, we get $B(x) = \{gx : g \in G\}$, which is called the orbit of x under the action of G.

Definition 3.4

Suppose that the group G acts on the set X. The action is transitive (we also say that G acts transitively on X) if there is only one orbit, in other words, for any $x, y \in X$, there exists $g \in G$ such that $gx = y$.

- Define $y \sim x$ iff $y = gx$ for some $g \in G$. Then $\sim$ is an equivalence relation.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

The Orbit-Stabilizer Theorem

Definition 3.3

Suppose that the group G acts on the set X. If we start with the element $x \in X$ and successively apply group elements in all possible ways, we get $B(x) = \{gx : g \in G\}$, which is called the orbit of x under the action of G.

Definition 3.4

Suppose that the group G acts on the set X. The action is transitive (we also say that G acts transitively on X) if there is only one orbit, in other words, for any $x, y \in X$, there exists $g \in G$ such that $gx = y$.

- Define $y \sim x$ iff $y = gx$ for some $g \in G$. Then $\sim$ is an equivalence relation.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

The Orbit-Stabilizer Theorem

Definition 3.3

Suppose that the group G acts on the set X. If we start with the element $x \in X$ and successively apply group elements in all possible ways, we get $B(x) = \{gx : g \in G\}$, which is called the orbit of x under the action of G.

Definition 3.4

Suppose that the group G acts on the set X. The action is transitive (we also say that G acts transitively on X) if there is only one orbit, in other words, for any $x, y \in X$, there exists $g \in G$ such that $gx = y$.

- Define $y \sim x$ iff $y = gx$ for some $g \in G$. Then $\sim$ is an equivalence relation.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

The Orbit-Stabilizer Theorem

Definition 3.3

Suppose that the group G acts on the set X. If we start with the element $x \in X$ and successively apply group elements in all possible ways, we get $B(x) = \{gx : g \in G\}$, which is called the orbit of x under the action of G.

Definition 3.4

Suppose that the group G acts on the set X. The action is transitive (we also say that G acts transitively on X) if there is only one orbit, in other words, for any $x, y \in X$, there exists $g \in G$ such that $gx = y$.

- Define $y \sim x$ iff $y = gx$ for some $g \in G$. Then $\sim$ is an equivalence relation.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \leq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \leq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \leq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \leq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \preceq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Definition 3.5

The stabilizer of an element $x \in X$ is

$$G(x) = \{g \in G : gx = x\},$$

the set of elements that leave x fixed.

- The stabilizer of x is a subgroup, i.e, $G(x) \preceq G$.
- If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
- Each orbit of an element x is an equivalence class, and the orbits partition X.

Example 3.6

1. The regular action of G on G is transitive, and the stabilizer of x is the subgroup $\{1\}$.
2. The trivial action is not transitive (except in trivial cases), in fact, $B(x) = x$ for every $x \in X$. The stabilizer of x is the entire group G.

Example 3.7

1. Conjugation on elements is not transitive. The orbit of x is the set of conjugates gxg^{-1} of x, that is,

$$B(x) = \{gxg^{-1} : g \in G\},$$

which is known as the conjugacy class of x (x的共轭类). The stabilizer of x is

$$G(x) = \{g : gxg^{-1} = x\} = \{g : gx = xg\}.$$

2. The stabilizer of x under conjugation is the centralizer $C_G(x)$ of x.
3. Let $S \subset G$, the centralizer $C_G(S)$ of S is also a subgroup, i.e., $C_G(S) \preceq G$.

Example 3.7

1. Conjugation on elements is not transitive. The orbit of x is the set of conjugates gxg^{-1} of x, that is,

$$B(x) = \{gxg^{-1} : g \in G\},$$

which is known as the conjugacy class of x (x的共轭类). The stabilizer of x is

$$G(x) = \{g : gxg^{-1} = x\} = \{g : gx = xg\}.$$

2. The stabilizer of x under conjugation is the centralizer $C_G(x)$ of x.
3. Let $S \subset G$, the centralizer $C_G(S)$ of S is also a subgroup, i.e., $C_G(S) \leq G$.

Example 3.7

1. Conjugation on elements is not transitive. The orbit of x is the set of conjugates gxg^{-1} of x, that is,

$$B(x) = \{gxg^{-1} : g \in G\},$$

which is known as the conjugacy class of x (x的共轭类). The stabilizer of x is

$$G(x) = \{g : gxg^{-1} = x\} = \{g : gx = xg\}.$$

2. The stabilizer of x under conjugation is the centralizer $C_G(x)$ of x.
3. Let $S \subset G$, the centralizer $C_G(S)$ of S is also a subgroup, i.e., $C_G(S) \preceq G$.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is

$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$

4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is

$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$

4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is

$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$

4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is
$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$
4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is
$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$
4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.8

1. Conjugation on subgroups is not transitive. The orbit of H is the set of conjugate subgroups $B(H) = \{gHg^{-1} : g \in G\}$.
2. $gHg^{-1} \leq G$.
3. The stabilizer of H is
$$G(H) = \{g : gHg^{-1} = H\} = \{g : gH = Hg\}.$$
4. The stabilizer of a subgroup H under conjugation is also called the Normalizer $N_G(H)$ of H.
5. $H \trianglelefteq K$ iff $gHg^{-1} = H$ for all $g \in K$ iff $K \subset N_G(H)$.
6. $N_G(H)$ is the largest subgroup of G in which H is normal.

Example 3.9

1. Conjugation on subsets is not transitive. The orbit of set S, $S \subset G$, is the set of conjugate subsets $B(S) = \{gSg^{-1} : g \in G\}$.
2. $|gSg^{-1}| = |S|$.
3. The stabilizer of S is the Normalizer $N_G(S)$ of S

$$N_G(S) = \{g : gSg^{-1} = S\} = \{g : gS = Sg\}.$$

Example 3.9

1. Conjugation on subsets is not transitive. The orbit of set S, $S \subset G$, is the set of conjugate subsets $B(S) = \{gSg^{-1} : g \in G\}$.
2. $|gSg^{-1}| = |S|$.
3. The stabilizer of S is the Normalizer $N_G(S)$ of S

$$N_G(S) = \{g : gSg^{-1} = S\} = \{g : gS = Sg\}.$$

Example 3.9

1. Conjugation on subsets is not transitive. The orbit of set S, $S \subset G$, is the set of conjugate subsets $B(S) = \{gSg^{-1} : g \in G\}$.
2. $|gSg^{-1}| = |S|$.
3. The stabilizer of S is the Normalizer $N_G(S)$ of S

$$N_G(S) = \{g : gSg^{-1} = S\} = \{g : gS = Sg\}.$$

Example 3.10

1. Multiplication on left cosets is transitive. Given two cosets xH and yH, $\exists g, g = yx^{-1}$ such that $g(xH) = yH$.
2. The stabilizer of xH is

$$G(xH) = \{g : gxH = xH\} = \{g : x^{-1}gx \in H\} = xHx^{-1}.$$

Example 3.10

1. Multiplication on left cosets is transitive. Given two cosets xH and yH, $\exists g, g = yx^{-1}$ such that $g(xH) = yH$.
2. The stabilizer of xH is

$$G(xH) = \{g : gxH = xH\} = \{g : x^{-1}gx \in H\} = xHx^{-1}.$$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

The Orbit-Stabilizer Theorem

Theorem 3.11

Suppose that a group G acts on a set X. Let $B(x)$ be the orbit of $x \in X$, and let $G(x)$ be the stabilizer of x. Then the size of the orbit is the index of the stabilizer, that is,

$$|B(x)| = [G : G(x)].$$

Thus if G is finite, then $|B(x)| = |G|/|G(x)|$; in particular, the orbit size divides the order of the group.

Proof. Consider the orbit of x, i.e, $B(x)$. We know that $B(x)$ is an equivalence class. Let $G(x)$ be the stabilizer of x.

- $y \in B(x)$ iff $\exists g_1, g_2$, such that $y = g_1 x = g_2 x$;
- $x = g_1^{-1} g_2 x$, hence $g_1^{-1} g_2 \in G(x)$;
- $\{g_i \mid g_i x = y, g_i \in G\} = g_1 G(x) = g_2 G(x) = g_i G(x)$.
- $|B(x)| = [G : G(x)]$

Class Equation for Conjugation on Elements

Theorem 3.12

Consider the conjugation of a group G on G. Let $B(x)$ be the orbit of $x \in G$, and let $G(x)(C_G(x))$ be the stabilizer(centralizer) of x. Let C be the center of G. Then

$$|G| = |C| + \sum_i [G : C_G(x_i)],$$

where x_i is chosen from each conjugacy class of size greater than 1.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

Class Equation for Conjugation on Elements

Theorem 3.13

Let G be a finite group. $H, K \preceq G$. then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Consider the action of subgroup H of G on left cosets of K.

- The orbit of coset K is given by $\{hK, h \in H\}$.
- The Stabilizer is $H \cap K$.
- $\bigcup\{hK, h \in H\} = HK$.
- $|HK|/|K|$ is the orbit size of K.
- According to the Orbit Stabilizer theorem, $B(K) = |HK|/|K| = |H|/|H \cap K|$.

The Orbit-Counting Theorem

Theorem 3.14

Let G be a finite group, and G act on the finite set X. Let $f(g) = |\{x \in X : g \bullet x = x\}|$ be the number of elements of X fixed by g. Then the number of orbits is

$$\frac{1}{|G|}\sum_{g\in G} f(g),$$

the average number of points left fixed by elements of G.

The Orbit-Counting Theorem

Theorem 3.14

Let G be a finite group, and G act on the finite set X. Let $f(g) = |\{x \in X : g \bullet x = x\}|$ be the number of elements of X fixed by g. Then the number of orbits is

$$\frac{1}{|G|}\sum_{g\in G} f(g),$$

the average number of points left fixed by elements of G.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

The Orbit-Counting Theorem

Proof. "Counting two ways". Let $T = \{(g, x) : g \bullet x = x, g \in G, x \in X\}$.

- For a fixed $x \in X$, define $T_x = \{(g, x) : g \bullet x = x, g \in G\}$. Then $T_x = G(x)$.
- $T = \bigcup_{x \in X} T_x$ and $|T| = \sum_{x \in X} |T_x| = \sum_{x \in X} |G(x)|$.
- For a fixed $g \in G$, define $T_g = \{x \in X : g \bullet x = x\}$. Then $T = \bigcup_{g \in G} T_g$. And $|T_g| = f(g)$ and $|T| = \sum_{g \in G} |T_g| = \sum_{g \in G} f(g)$.
- $\frac{1}{|G|} \sum f(g) = \sum_{x \in X} \frac{|G(x)|}{|G|} = \sum_{x \in X} \frac{1}{|B(x)|}$.
- $\sum_{x \in X} \frac{1}{|B(x)|}$ is the number of orbits.

串珠染色问题之一

手链上珠子共6颗，现将每颗珠子染一种色，共有n种颜色，请问：可以得到多少种染色不同的手链？

二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$
\begin{aligned}
\tau_0 &= (1)(2)(3)(4)(5)(6) & r \circ \tau_0 &= (1\ 6)(2\ 5)(3\ 4) \\
\tau_1 &= (1\ 2\ 3\ 4\ 5\ 6) & r \circ \tau_1 &= (1\ 5)(2\ 4)(3)(6) \\
\tau_2 &= (1\ 3\ 5)(2\ 4\ 6) & r \circ \tau_2 &= (1\ 4)(2\ 3)(5\ 6) \\
\tau_3 &= (1\ 3)(2\ 5)(3\ 6) & r \circ \tau_3 &= (1\ 3)(2)(4\ 6)(5) \\
\tau_4 &= (1\ 5\ 3)(2\ 6\ 4) & r \circ \tau_4 &= (1\ 2)(3\ 6)(4\ 5) \\
\tau_5 &= (1\ 6\ 5\ 4\ 3\ 2) & r \circ \tau_5 &= (1)(2\ 6)(3\ 5)(4)
\end{aligned}
$$

$(n^6 + n + n^2 + n^3 + n^2 + n + n^3 + n^4 + n^3 + n^4 + n^3 + n^4)/12$

串珠染色问题之一

手链上珠子共6颗，现将每颗珠子染一种色，共有n种颜色，请问：可以得到多少种染色不同的手链？
二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$\begin{aligned}
\tau_0 &= (1)(2)(3)(4)(5)(6) & r \circ \tau_0 &= (1\ 6)(2\ 5)(3\ 4) \\
\tau_1 &= (1\ 2\ 3\ 4\ 5\ 6) & r \circ \tau_1 &= (1\ 5)(2\ 4)(3)(6) \\
\tau_2 &= (1\ 3\ 5)(2\ 4\ 6) & r \circ \tau_2 &= (1\ 4)(2\ 3)(5\ 6) \\
\tau_3 &= (1\ 3)(2\ 5)(3\ 6) & r \circ \tau_3 &= (1\ 3)(2)(4\ 6)(5) \\
\tau_4 &= (1\ 5\ 3)(2\ 6\ 4) & r \circ \tau_4 &= (1\ 2)(3\ 6)(4\ 5) \\
\tau_5 &= (1\ 6\ 5\ 4\ 3\ 2) & r \circ \tau_5 &= (1)(2\ 6)(3\ 5)(4)
\end{aligned}$$

$(n^6 + n + n^2 + n^3 + n^2 + n + n^3 + n^4 + n^3 + n^4 + n^3 + n^4)/12$

串珠染色问题之二

如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？

二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$\begin{aligned}
\tau_0 &= (1)(2)(3)(4)(5)(6) & r \circ \tau_0 &= (1\ 6)(2\ 5)(3\ 4) \\
\tau_1 &= (1\ 2\ 3\ 4\ 5\ 6) & r \circ \tau_1 &= (1\ 5)(2\ 4)(3)(6) \\
\tau_2 &= (1\ 3\ 5)(2\ 4\ 6) & r \circ \tau_2 &= (1\ 4)(2\ 3)(5\ 6) \\
\tau_3 &= (1\ 3)(2\ 5)(3\ 6) & r \circ \tau_3 &= (1\ 3)(2)(4\ 6)(5) \\
\tau_4 &= (1\ 5\ 3)(2\ 6\ 4) & r \circ \tau_4 &= (1\ 2)(3\ 6)(4\ 5) \\
\tau_5 &= (1\ 6\ 5\ 4\ 3\ 2) & r \circ \tau_5 &= (1)(2\ 6)(3\ 5)(4)
\end{aligned}$$

$(C_3^6 + 0 + 2 + 0 + 2 + 0 + 0 + 4 + 0 + 0 + 4 + 0 + 4)/12 = 3$

串珠染色问题之二

如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？
二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$
\begin{aligned}
\tau_0 &= (1)(2)(3)(4)(5)(6) & r \circ \tau_0 &= (1\ 6)(2\ 5)(3\ 4) \\
\tau_1 &= (1\ 2\ 3\ 4\ 5\ 6) & r \circ \tau_1 &= (1\ 5)(2\ 4)(3)(6) \\
\tau_2 &= (1\ 3\ 5)(2\ 4\ 6) & r \circ \tau_2 &= (1\ 4)(2\ 3)(5\ 6) \\
\tau_3 &= (1\ 3)(2\ 5)(3\ 6) & r \circ \tau_3 &= (1\ 3)(2)(4\ 6)(5) \\
\tau_4 &= (1\ 5\ 3)(2\ 6\ 4) & r \circ \tau_4 &= (1\ 2)(3\ 6)(4\ 5) \\
\tau_5 &= (1\ 6\ 5\ 4\ 3\ 2) & r \circ \tau_5 &= (1)(2\ 6)(3\ 5)(4)
\end{aligned}
$$

$(C_3^6 + 0 + 2 + 0 + 2 + 0 + 0 + 4 + 0 + 0 + 4 + 0 + 4)/12 = 3$

串珠染色问题之二

如果手链上的6颗珠子，必须染成3黄3红，那么有多少种可能性？
二面体群$D_{2n} = D_{12}(n = 6)$的群元素为：

$$
\begin{aligned}
\tau_0 &= (1)(2)(3)(4)(5)(6) & r \circ \tau_0 &= (1\ 6)(2\ 5)(3\ 4) \\
\tau_1 &= (1\ 2\ 3\ 4\ 5\ 6) & r \circ \tau_1 &= (1\ 5)(2\ 4)(3)(6) \\
\tau_2 &= (1\ 3\ 5)(2\ 4\ 6) & r \circ \tau_2 &= (1\ 4)(2\ 3)(5\ 6) \\
\tau_3 &= (1\ 3)(2\ 5)(3\ 6) & r \circ \tau_3 &= (1\ 3)(2)(4\ 6)(5) \\
\tau_4 &= (1\ 5\ 3)(2\ 6\ 4) & r \circ \tau_4 &= (1\ 2)(3\ 6)(4\ 5) \\
\tau_5 &= (1\ 6\ 5\ 4\ 3\ 2) & r \circ \tau_5 &= (1)(2\ 6)(3\ 5)(4)
\end{aligned}
$$

$(C_3^6 + 0 + 2 + 0 + 2 + 0 + 0 + 4 + 0 + 0 + 4 + 0 + 4)/12 = 3$

The Structure of a Finite Group

- Considerable information about the structure of a finite group G can be obtained by factoring the order of G.
- Suppose that $|G| = p^r m$ where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. We will prove that
  - G must have a subgroup of order p^r.
  - Any two such subgroups must be conjugate.
  - $\forall p$, $p||G|$, $\exists a \in G$ s.t. $ord(a) = p$.

The Structure of a Finite Group

- Considerable information about the structure of a finite group G can be obtained by factoring the order of G.
- Suppose that $|G| = p^r m$ where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. We will prove that
  - G must have a subgroup of order p^r.
  - Any two such subgroups must be conjugate.
  - $\forall p$, $p||G|$, $\exists a \in G$ s.t. $ord(a) = p$.

The Structure of a Finite Group

- Considerable information about the structure of a finite group G can be obtained by factoring the order of G.
- Suppose that $|G| = p^r m$ where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. We will prove that
  - G must have a subgroup of order p^r.
  - Any two such subgroups must be conjugate.
  - $\forall p$, $p \| G|$, $\exists a \in G$ s.t. $ord(a) = p$.

The Structure of a Finite Group

- Considerable information about the structure of a finite group G can be obtained by factoring the order of G.
- Suppose that $|G| = p^r m$ where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. We will prove that
  - G must have a subgroup of order p^r.
  - Any two such subgroups must be conjugate.
  - $\forall p$, $p \| G|$, $\exists a \in G$ s.t. $ord(a) = p$.

The Structure of a Finite Group

- Considerable information about the structure of a finite group G can be obtained by factoring the order of G.
- Suppose that $|G| = p^r m$ where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. We will prove that
  - G must have a subgroup of order p^r.
  - Any two such subgroups must be conjugate.
  - $\forall p$, $p||G|$, $\exists a \in G$ s.t. $ord(a) = p$.

Definition 4.1

Let p be a prime number. The group G is said to be a p-group if the order of each element of G is a power of p. If $|G| = p^r m$, where $p \nmid m$, then a subgroup P of G of order p^r is called a Sylow p-subgroup of G.

A Sylow p-subgroup of G is a p-subgroup of G of maximum possible size.

Theorem 4.2

If G is a finite group, then G is a p-group iff the order of G is a power of p.

Proof. $\Leftarrow$: Lagrange's theorem.
$\Rightarrow$: a corollary to the Sylow theorems.

Definition 4.1

Let p be a prime number. The group G is said to be a p-group if the order of each element of G is a power of p. If $|G| = p^r m$, where $p \nmid m$, then a subgroup P of G of order p^r is called a Sylow p-subgroup of G.

A Sylow p-subgroup of G is a p-subgroup of G of maximum possible size.

Theorem 4.2

If G is a finite group, then G is a p-group iff the order of G is a power of p.

Proof. $\Leftarrow$: Lagrange's theorem.
$\Rightarrow$: a corollary to the Sylow theorems.

Definition 4.1

Let p be a prime number. The group G is said to be a p-group if the order of each element of G is a power of p. If $|G| = p^r m$, where $p \nmid m$, then a subgroup P of G of order p^r is called a Sylow p-subgroup of G.

A Sylow p-subgroup of G is a p-subgroup of G of maximum possible size.

Theorem 4.2

If G is a finite group, then G is a p-group iff the order of G is a power of p.

Proof. $\Leftarrow$: Lagrange's theorem.
$\Rightarrow$: a corollary to the Sylow theorems.

Definition 4.1

Let p be a prime number. The group G is said to be a p-group if the order of each element of G is a power of p. If $|G| = p^r m$, where $p \nmid m$, then a subgroup P of G of order p^r is called a Sylow p-subgroup of G.

A Sylow p-subgroup of G is a p-subgroup of G of maximum possible size.

Theorem 4.2

If G is a finite group, then G is a p-group iff the order of G is a power of p.

Proof. $\Leftarrow$: Lagrange's theorem.
$\Rightarrow$: a corollary to the Sylow theorems.

Lemma 4.3

If $n = p^r m$ where p is prime, then

$$\binom{n}{p^r} \equiv m \mod p.$$

Thus if $p \nmid m$ then $p \nmid \binom{n}{p^r}$.

Proof.

- By the binomial expansion modulo p, we have

$$(X+1)^{p^r} \equiv X^{p^r} + 1^{p^r} \equiv X^{p^r} + 1 \mod p.$$

- $(X+1)^n \equiv \left(X^{p^r} + 1\right)^m \mod p.$
- On the left side, the coefficient of X^{p^r} is $\binom{n}{p^r}$ and on the right side, it is m.

Lemma 4.3

If $n = p^r m$ where p is prime, then

$$\binom{n}{p^r} \equiv m \mod p.$$

Thus if $p \nmid m$ then $p \nmid \binom{n}{p^r}$.

Proof.

- By the binomial expansion modulo p, we have

$$(X+1)^{p^r} \equiv X^{p^r} + 1^{p^r} \equiv X^{p^r} + 1 \mod p.$$

- $(X+1)^n \equiv \left(X^{p^r} + 1\right)^m \mod p.$
- On the left side, the coefficient of X^{p^r} is $\binom{n}{p^r}$ and on the right side, it is m.

Lemma 4.3

If $n = p^r m$ where p is prime, then

$$\binom{n}{p^r} \equiv m \mod p.$$

Thus if $p \nmid m$ then $p \nmid \binom{n}{p^r}$.

Proof.

- By the binomial expansion modulo p, we have

$$(X+1)^{p^r} \equiv X^{p^r} + 1^{p^r} \equiv X^{p^r} + 1 \mod p.$$

- $(X+1)^n \equiv \left(X^{p^r} + 1\right)^m \mod p.$
- On the left side, the coefficient of X^{p^r} is $\binom{n}{p^r}$ and on the right side, it is m.

Lemma 4.3

If $n = p^r m$ where p is prime, then

$$\binom{n}{p^r} \equiv m \mod p.$$

Thus if $p \nmid m$ then $p \nmid \binom{n}{p^r}$.

Proof.

- By the binomial expansion modulo p, we have

$$(X+1)^{p^r} \equiv X^{p^r} + 1^{p^r} \equiv X^{p^r} + 1 \mod p.$$

- $(X+1)^n \equiv \left(X^{p^r} + 1\right)^m \mod p.$
- On the left side, the coefficient of X^{p^r} is $\binom{n}{p^r}$ and on the right side, it is m.

The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. Then

1. G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.(西罗第一定理)
2. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p | m$. (西罗第二定理)
3. All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \equiv K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class.(西罗第三定理)

It is obvious if $m = 1$. We only consider the case $m \neq 1$.

The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. Then

1. G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.(西罗第一定理)
2. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p | m$. (西罗第二定理)
3. All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \equiv K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class.(西罗第三定理)

It is obvious if $m = 1$. We only consider the case $m \neq 1$.

The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. Then

1. G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.(西罗第一定理)
2. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p | m$. (西罗第二定理)
3. All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \equiv K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class.(西罗第三定理)

It is obvious if $m = 1$. We only consider the case $m \neq 1$.

The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. Then

1. G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.(西罗第一定理)
2. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p | m$. (西罗第二定理)
3. All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \equiv K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class.(西罗第三定理)

It is obvious if $m = 1$. We only consider the case $m \neq 1$.

The Sylow Theorems

Let G be a finite group of order $p^r m$, where p is prime, $r \in \mathbb{Z}^+$ and $p \nmid m$. Then

1. G has at least one Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.(西罗第一定理)
2. Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p | m$. (西罗第二定理)
3. All Sylow p-subgroups are conjugate. Thus if we define an equivalence relation on subgroups by $H \equiv K$ iff $H = gKg^{-1}$ for some $g \in G$, then the Sylow p-subgroups comprise a single equivalence class.(西罗第三定理)

It is obvious if $m = 1$. We only consider the case $m \neq 1$.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \leq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \leq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \leq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \preceq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \preceq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \preceq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \preceq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

西罗第一定理: G has at least one Sylow p-subgroup

Proof. Let G act on subsets of G of size p^r by left multiplication.

- The number of such subsets is $\binom{n}{p^r}$. Then $p \nmid \binom{n}{p^r}$.
- There is at least one subset S whose orbit size is not divisible by p, i.e, $p \nmid |B(S)|$.
- Let P be the stabilizer of S, then $P \preceq G$, and $|B(S)| = [G : P] = |G|/|P| = p^r m/|P|$.
- $p^r \| P|$.
- Given $x \in S$, consider the map $\phi_x : P \to Px$ with $\phi_x(g) = gx$ for $g \in P$. Then ϕ_x is injective.
- P is the stabilizer of S, hence $xP \subseteq S$.
- $|P| \leq |S| = p^r$.
- $|P| = p^r$, and P is a Sylow p-subgroup.

Cauchy's Theorem

Corollary 4.4

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G. Choose $g \in P$ such that $g \neq 1$. Then $order(g) = p^i$ with $i \geq 1$.
Then $y = g^{p^{i-1}}$ has order p.

Corollary 4.5

The finite group G is a p-group iff the order of G is a power of p.

Proof. If $|G| = p^i m$ with $p \nmid m$, $m > 1$. Then there exists a prime q such that $q||G|$. According to the Sylow Theorem, G has at least a Sylow q-subgroup. Then G has an element of order q. This contradicts with the fact that G is a p-group.

Cauchy's Theorem

Corollary 4.4

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G. Choose $g \in P$ such that $g \neq 1$. Then $order(g) = p^i$ with $i \geq 1$.
Then $y = g^{p^{i-1}}$ has order p.

Corollary 4.5

The finite group G is a p-group iff the order of G is a power of p.

Proof. If $|G| = p^i m$ with $p \nmid m$, $m > 1$. Then there exists a prime q such that $q||G|$. According to the Sylow Theorem, G has at least a Sylow q-subgroup. Then G has an element of order q. This contradicts with the fact that G is a p-group.

Cauchy's Theorem

Corollary 4.4

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G. Choose $g \in P$ such that $g \neq 1$. Then $order(g) = p^i$ with $i \geq 1$.
Then $y = g^{p^{i-1}}$ has order p.

Corollary 4.5

The finite group G is a p-group iff the order of G is a power of p.

Proof. If $|G| = p^i m$ with $p \nmid m$, $m > 1$. Then there exists a prime q such that $q||G|$. According to the Sylow Theorem, G has at least a Sylow q-subgroup. Then G has an element of order q. This contradicts with the fact that G is a p-group.

Cauchy's Theorem

Corollary 4.4

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G. Choose $g \in P$ such that $g \neq 1$. Then $order(g) = p^i$ with $i \geq 1$.
Then $y = g^{p^{i-1}}$ has order p.

Corollary 4.5

The finite group G is a p-group iff the order of G is a power of p.

Proof. If $|G| = p^i m$ with $p \nmid m$, $m > 1$. Then there exists a prime q such that $q||G|$. According to the Sylow Theorem, G has at least a Sylow q-subgroup. Then G has an element of order q. This contradicts with the fact that G is a p-group.

Cauchy's Theorem

Corollary 4.4

If the prime p divides the order of G, then G has an element of order p.

Proof. Let P be a Sylow p-subgroup of G. Choose $g \in P$ such that $g \neq 1$. Then $order(g) = p^i$ with $i \geq 1$.
Then $y = g^{p^{i-1}}$ has order p.

Corollary 4.5

The finite group G is a p-group iff the order of G is a power of p.

Proof. If $|G| = p^i m$ with $p \nmid m$, $m > 1$. Then there exists a prime q such that $q||G|$. According to the Sylow Theorem, G has at least a Sylow q-subgroup. Then G has an element of order q. This contradicts with the fact that G is a p-group.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第二定理: $n_p \equiv 1 \mod p$ and $n_p | m$.

Proof. Let X be the set of all Sylow p-subgroups of G. Then $|X| = n_p$. P is a sylow p-subgroup of G. Let P acts on X by conjugation, i.e., $g \bullet Q = gQg^{-1}$, $g \in P$..

- The size of any orbit divides $|P| = p^r$, hence is a power of p.
- The orbit size of P is 1;
- Suppose that $Q = gQg^{-1}$ for all $g \in P$, then the orbit size of Q is 1.
- $PQ = QP$, hence $PQ = \langle P, Q \rangle \leq G$ and $|PQ| \geq p^r$.
- $|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^r p^r / |P \cap Q|$. Hence $|PQ| = p^i$ Then $|PQ| \leq p^r$ since $PQ \leq G$.
- $|PQ| = p^r$. Hence $P = Q$.
- There is only one sylow p-subgroup of orbit size 1, that is P.
- $n_p = p^0 + \sum_{i>0} p^i$.
- $n_p \equiv 1 \mod p$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p \| G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

西罗第三定理: All Sylow p-subgroups are conjugate.

Proof. Let R be a p-subgroup of G, then its order is a power of p. Let Y be the set of left cosets of P. Let R act by left multiplication on Y.

- $|Y| = m$ and $p \nmid m$; hence is NOT a power of p.
- There exists some orbit size that is not divisible by p, i.e., $\exists g_0 P, p \nmid |B(g_0 P)|$.
- Every orbit size divides $|R|$, hence is a power of p, i.e., $\forall g \in G, \exists i \in \mathbb{N}$ such that $|B(gP)| = p^i$.
- Hence $|B(g_0 P)| = 1$, and the stabilizer of $g_0 P$ is R.
- $r(g_0 P) = g_0 P$ for all $r \in R$, then $g_0^{-1} r g_0 \in P$, i.e., $r \in g_0 P g_0^{-1}$.
- $R \subseteq g_0 P g_0^{-1}$. R is contained in a conjugate of P.
- If R is a sylow p-subgroup. Then $R = g_0 P g_0^{-1}$. i.e., R is a conjugate of P.

Let G act on subgroups by conjugation. The orbit of P has size n_p by (3). By the orbit and stabilizer theorem, $n_p | |G| = p^r m$. But $p \nmid n_p$, so $n_p | m$.

The Sylow Theorems

Definition 4.6

设G为任意群(不一定为有限群)

1. 设G中元素a, b是共轭的，若存在$g \in G$使得$b = gag^{-1}$, 也就是存在$\phi \in InnG$, 使$b = \phi(a)$. 易见共轭关系是一个等价关系，称它为等价类，也就是$\{gag^{-1}, g \in G\}$, 为一个共轭元素类。
2. 群G的中心元a的等价类是$\{a\}$。
3. 共轭关系是一个等价关系，群G的共轭元素类构成G的等价类。
4. 设G的子群H, K共轭，若存在$g \in G$使得$K = gHg^{-1}$, 也即存在$\phi \in InnG$, 使$K = \phi(H)$. 共轭关系是子群间的一个等价关系，称它的一个等价类，亦即$\{gHg^{-1}, g \in G\}$, 为一个共轭子群类。

The Sylow Theorems

Definition 4.6

设G为任意群(不一定为有限群)

1. 设G中元素a, b是共轭的，若存在$g \in G$使得$b = gag^{-1}$, 也就是存在$\phi \in InnG$, 使$b = \phi(a)$. 易见共轭关系是一个等价关系，称它为等价类，也就是$\{gag^{-1}, g \in G\}$, 为一个共轭元素类。
2. 群G的中心元a的等价类是$\{a\}$。
3. 共轭关系是一个等价关系，群G的共轭元素类构成G的等价类。
4. 设G的子群H, K共轭，若存在$g \in G$使得$K = gHg^{-1}$, 也即存在$\phi \in InnG$, 使$K = \phi(H)$. 共轭关系是子群间的一个等价关系，称它的一个等价类，亦即$\{gHg^{-1}, g \in G\}$, 为一个共轭子群类。

The Sylow Theorems

Definition 4.6

设G为任意群(不一定为有限群)

1. 设G中元素a, b是共轭的，若存在$g \in G$使得$b = gag^{-1}$, 也就是存在$\phi \in InnG$, 使$b = \phi(a)$. 易见共轭关系是一个等价关系，称它为等价类，也就是$\{gag^{-1}, g \in G\}$, 为一个共轭元素类。
2. 群G的中心元a的等价类是$\{a\}$。
3. 共轭关系是一个等价关系，群G的共轭元素类构成G的等价类。
4. 设G的子群H, K共轭，若存在$g \in G$使得$K = gHg^{-1}$, 也即存在$\phi \in InnG$, 使$K = \phi(H)$. 共轭关系是子群间的一个等价关系，称它的一个等价类，亦即$\{gHg^{-1}, g \in G\}$, 为一个共轭子群类。

The Sylow Theorems

Definition 4.6

设G为任意群(不一定为有限群)

1. 设G中元素a, b是共轭的，若存在$g \in G$使得$b = gag^{-1}$, 也就是存在$\phi \in InnG$, 使$b = \phi(a)$. 易见共轭关系是一个等价关系，称它为等价类，也就是$\{gag^{-1}, g \in G\}$, 为一个共轭元素类。
2. 群G的中心元a的等价类是$\{a\}$。
3. 共轭关系是一个等价关系，群G的共轭元素类构成G的等价类。
4. 设G的子群H, K共轭，若存在$g \in G$使得$K = gHg^{-1}$, 也即存在$\phi \in InnG$, 使$K = \phi(H)$. 共轭关系是子群间的一个等价关系，称它的一个等价类，亦即$\{gHg^{-1}, g \in G\}$, 为一个共轭子群类。

Definition 4.7

设S是群G的一个子集, 令

$$N(S) = \{g \in G | gSg^{-1} = S\},$$

称为S的正规化子。

- $N(S) \preceq G$。
- 群G的中心元a的正规化子是G。
- 若$S \preceq G$，则$S \trianglelefteq N(S)$。

Definition 4.7

设S是群G的一个子集, 令

$$N(S) = \{g \in G | gSg^{-1} = S\},$$

称为S的正规化子。

- $N(S) \preceq G$。
- 群G的中心元a的正规化子是G。
- 若$S \preceq G$，则$S \trianglelefteq N(S)$。

Definition 4.7

设S是群G的一个子集, 令

$$N(S) = \{g \in G | gSg^{-1} = S\},$$

称为S的正规化子。

- $N(S) \preceq G$。
- 群G的中心元a的正规化子是G。
- 若$S \preceq G$，则$S \trianglelefteq N(S)$。

Definition 4.7

设S是群G的一个子集, 令

$$N(S) = \{g \in G | gSg^{-1} = S\},$$

称为S的正规化子。

- $N(S) \preceq G$。
- 群G的中心元a的正规化子是G。
- 若$S \preceq G$，则$S \trianglelefteq N(S)$。

Lemma 4.8

G是有限群，S是G的一个共轭元素类，$|S| = t$. 则存在G的子群H, 它在G中的指数恰为t.

Proof: 任取$s \in S$而考察s的正规化子$N(s)$. 由子群$N(s)$的定义容易知道：对于任意的$x, y \in G$，则

$$xsx^{-1} = ysy^{-1} \Leftrightarrow s = (x^{-1}y)s(y^{-1}x) = (x^{-1}y)s(x^{-1}y)^{-1}$$

$$\Leftrightarrow x^{-1}y \in N(s) \Leftrightarrow x, y \text{ 属于} N(s) \text{的同一左陪集}$$

亦即用$N(s)$的同一左陪集中的元素去作用s给出s的相同共轭元素，而用不同左陪集中的元素去作用s, 则给出s的不想同的共轭元素。这样s 的不同共轭元素的个数就等于子群$N(s)$的不同左陪集的个数，亦即$|S|$等于子群$N(s)$在群G中的指数。

Lemma 4.8

G是有限群，S是G的一个共轭元素类，$|S| = t$. 则存在G的子群H, 它在G中的指数恰为t.

Proof: 任取$s \in S$而考察s的正规化子$N(s)$. 由子群$N(s)$的定义容易知道：对于任意的$x, y \in G$，则

$$xsx^{-1} = ysy^{-1} \Leftrightarrow s = (x^{-1}y)s(y^{-1}x) = (x^{-1}y)s(x^{-1}y)^{-1}$$

$$\Leftrightarrow x^{-1}y \in N(s) \Leftrightarrow x, y \text{ 属于} N(s) \text{的同一左陪集}$$

亦即用$N(s)$的同一左陪集中的元素去作用s给出s的相同共轭元素，而用不同左陪集中的元素去作用s, 则给出s的不想同的共轭元素。这样s 的不同共轭元素的个数就等于子群$N(s)$的不同左陪集的个数，亦即$|S|$等于子群$N(s)$在群G中的指数。

Sylow定理

Theorem 4.9

设G是一个有限群，其阶为$n = p^r \cdot m$，其中p是一个素数，那么存在G的一个子群H，使得$|H| = p^r$。

Proof.归纳法。对n做归纳。设C是群G的中心，即所有中心元构成的集合，故C是一个子群。
如果$C = G$，则G是可交换群，由定理2.3知结论成立。
如果$C \neq G$，则$C \subset G$。

Sylow定理

Theorem 4.9

设G是一个有限群，其阶为$n = p^r \cdot m$，其中p是一个素数，那么存在G的一个子群H，使得$|H| = p^r$。

Proof.归纳法。对n做归纳。设C是群G的中心，即所有中心元构成的集合，故C是一个子群。

如果$C = G$，则G是可交换群，由定理2.3知结论成立。

如果$C \neq G$，则$C \subset G$。

Sylow定理

Theorem 4.9

设G是一个有限群，其阶为$n = p^r \cdot m$，其中p是一个素数，那么存在G的一个子群H，使得$|H| = p^r$。

Proof.归纳法。对n做归纳。设C是群G的中心，即所有中心元构成的集合，故C是一个子群。
如果$C = G$，则G是可交换群，由定理2.3知结论成立。
如果$C \neq G$，则$C \subset G$。

Sylow定理

Theorem 4.9

设G是一个有限群，其阶为$n = p^r \cdot m$，其中p是一个素数，那么存在G的一个子群H，使得$|H| = p^r$。

Proof.归纳法。对n做归纳。设C是群G的中心，即所有中心元构成的集合，故C是一个子群。
如果$C = G$，则G是可交换群，由定理2.3知结论成立。
如果$C \neq G$，则$C \subset G$。

引理的证明

若$p \| C|$，

- 则引理2.2知，C中存在一个p阶子群$\langle a \rangle$。
- 由于$\langle a \rangle \preceq C \preceq G$，所以$\langle a \rangle \trianglelefteq G$。
- 因此$\overline{G} = G/\langle a \rangle$是一个商群且$p^{r-1} \mid |\overline{G}|$。由归纳假设知：存在$\overline{H} \preceq \overline{G}$，且$|\overline{H}| = p^{r-1}$。
- 设$\overline{H}$在自然满同态下的完全原象为H。
  则$H \prec G$且$|H| = |\langle a \rangle| \cdot |\overline{H}| = p \cdot p^{r-1} = p^r$。结论得证。

引理的证明

若$p \| C|$，

- 则引理2.2知，C中存在一个p阶子群$\langle a \rangle$。
- 由于$\langle a \rangle \preceq C \preceq G$，所以$\langle a \rangle \trianglelefteq G$。
- 因此$\overline{G} = G/\langle a \rangle$是一个商群且$p^{r-1} \mid |\overline{G}|$。由归纳假设知：存在$\overline{H} \preceq \overline{G}$，且$|\overline{H}| = p^{r-1}$。
- 设$\overline{H}$在自然满同态下的完全原象为H。
  则$H \prec G$且$|H| = |\langle a \rangle| \cdot |\overline{H}| = p \cdot p^{r-1} = p^r$。结论得证。

引理的证明

若$p \| C|$，

- 则引理2.2知，C中存在一个p阶子群$\langle a \rangle$。
- 由于$\langle a \rangle \preceq C \preceq G$，所以$\langle a \rangle \trianglelefteq G$。
- 因此$\overline{G} = G/\langle a \rangle$是一个商群且$p^{r-1} \mid |\overline{G}|$。由归纳假设知：存在$\overline{H} \preceq \overline{G}$，且$|\overline{H}| = p^{r-1}$。
- 设$\overline{H}$在自然满同态下的完全原象为H。
  则$H \prec G$且$|H| = |\langle a \rangle| \cdot |\overline{H}| = p \cdot p^{r-1} = p^r$。结论得证。

引理的证明

若$p||C|$，

- 则引理2.2知，C中存在一个p阶子群$\langle a\rangle$。
- 由于$\langle a\rangle \preceq C \preceq G$，所以$\langle a\rangle \trianglelefteq G$。
- 因此$\overline{G} = G/\langle a\rangle$是一个商群且$p^{r-1} \mid |\overline{G}|$。由归纳假设知：存在$\overline{H} \preceq \overline{G}$，且$|\overline{H}| = p^{r-1}$。
- 设$\overline{H}$在自然满同态下的完全原象为H。
  则$H \prec G$且$|H| = |\langle a\rangle| \cdot |\overline{H}| = p \cdot p^{r-1} = p^r$。结论得证。

引理的证明

若$p \nmid |C|$,

- 设$C_i, i = 1, 2, \cdots, t$,是G的所有共轭元素类。则$G = \bigcup_{i=1}^{t} C_i$，则

$$n = |G| = |C_1| + |C_2| + \cdots + |C_t| = n_1 + n_2 + \cdots n_t.$$

- 由于中心元的等价类只有一个元素组成，所以
$n = |G| = |C| + |C_{i_1}| + |C_{i_2}| + \cdots + |C_{i_s}| = |C| + m_1 + m_2 + \cdots m_s.$
- 因此$s \geq 1$。且$m_{i_j} > 1$， $j = 1, 2, \cdots, s$。
- 设$p \nmid |C|$，则至少存在一个C_{i_k}使得$p \nmid m_k, 1 \leq k \leq s$。
- 由引理4.8知，存在一个子群$N \leq G$使得$|C_i| = [G : N]$。因此$p^r \mid |N|$。结论得证。
- 同归纳假设知，存在N的子群H使得$|H| = p^r$，自然H也是G的p^r阶子群。

引理的证明

若$p \nmid |C|$，

- 设$C_i, i = 1, 2, \cdots, t$,是G的所有共轭元素类。则$G = \bigcup_{i=1}^{t} C_i$，则

$$n = |G| = |C_1| + |C_2| + \cdots + |C_t| = n_1 + n_2 + \cdots n_t.$$

- 由于中心元的等价类只有一个元素组成，所以
$n = |G| = |C| + |C_{i_1}| + |C_{i_2}| + \cdots + |C_{i_s}| = |C| + m_1 + m_2 + \cdots m_s.$
- 因此$s \geq 1$。且$m_{i_j} > 1$，$j = 1, 2, \cdots, s$。
- 设$p \nmid |C|$，则至少存在一个C_{i_k}使得$p \nmid m_k, 1 \leq k \leq s$。
- 由引理4.8知，存在一个子群$N \leq G$使得$|C_i| = [G : N]$。因此$p^r \mid |N|$。结论得证。
- 同归纳假设知，存在N的子群H使得$|H| = p^r$，自然H也是G的p^r阶子群。

引理的证明

若$p \nmid |C|$，

- 设$C_i, i = 1, 2, \cdots, t$,是G的所有共轭元素类。则$G = \bigcup_{i=1}^{t} C_i$，则

$$n = |G| = |C_1| + |C_2| + \cdots + |C_t| = n_1 + n_2 + \cdots n_t.$$

- 由于中心元的等价类只有一个元素组成，所以
  $n = |G| = |C| + |C_{i_1}| + |C_{i_2}| + \cdots + |C_{i_s}| = |C| + m_1 + m_2 + \cdots m_s.$
- 因此$s \geq 1$。且$m_{i_j} > 1$，$j = 1, 2, \cdots, s$。
- 设$p \nmid |C|$，则至少存在一个C_{i_k}使得$p \nmid m_k, 1 \leq k \leq s$。
- 由引理4.8知，存在一个子群$N \leq G$使得$|C_i| = [G : N]$。因此$p^r \mid |N|$。结论得证。
- 同归纳假设知，存在N的子群H使得$|H| = p^r$，自然H也是G的p^r阶子群。

引理的证明

若$p \nmid |C|$，

- 设$C_i, i = 1, 2, \cdots, t$,是G的所有共轭元素类。则$G = \bigcup_{i=1}^{t} C_i$，则

$$n = |G| = |C_1| + |C_2| + \cdots + |C_t| = n_1 + n_2 + \cdots n_t.$$

- 由于中心元的等价类只有一个元素组成，所以
  $n = |G| = |C| + |C_{i_1}| + |C_{i_2}| + \cdots + |C_{i_s}| = |C| + m_1 + m_2 + \cdots m_s.$
- 因此$s \geq 1$。且$m_{i_j} > 1$，$j = 1, 2, \cdots, s$。
- 设$p \nmid |C|$，则至少存在一个C_{i_k}使得$p \nmid m_k, 1 \leq k \leq s$。
- 由引理4.8知，存在一个子群$N \leq G$使得$|C_i| = [G : N]$。因此$p^r \mid |N|$。结论得证。
- 同归纳假设知，存在N的子群H使得$|H| = p^r$，自然H也是G的p^r阶子群。

引理的证明

若$p \nmid |C|$，

- 设$C_i, i = 1, 2, \cdots, t$,是G的所有共轭元素类。则$G = \bigcup_{i=1}^{t} C_i$，则

$$n = |G| = |C_1| + |C_2| + \cdots + |C_t| = n_1 + n_2 + \cdots n_t.$$

- 由于中心元的等价类只有一个元素组成，所以
  $n = |G| = |C| + |C_{i_1}| + |C_{i_2}| + \cdots + |C_{i_s}| = |C| + m_1 + m_2 + \cdots m_s.$
- 因此$s \geq 1$。且$m_{i_j} > 1$，$j = 1, 2, \cdots, s$。
- 设$p \nmid |C|$，则至少存在一个C_{i_k}使得$p \nmid m_k, 1 \leq k \leq s$。
- 由引理4.8知，存在一个子群$N \leq G$使得$|C_i| = [G : N]$。因此$p^r \mid |N|$。结论得证。
- 同归纳假设知，存在N的子群H使得$|H| = p^r$，自然H也是G的p^r阶子群。

Sylow 定理

Definition 4.10

如果G是有限群且每个元素的阶是素数p的某次幂，则称G为有限p–群。

Theorem 4.11 (Sylow 第一定理)

G为有限p–群当且仅当G的阶为p的幂。

Definition 4.12

有限群G中阶是素数p的幂的的所有子群中存在在极大者，称为Sylow p-子群。

Sylow 定理

Definition 4.10

如果G是有限群且每个元素的阶是素数p的某次幂，则称G为有限p–群。

Theorem 4.11 (Sylow 第一定理)

G为有限p–群当且仅当G的阶为p的幂。

Definition 4.12

有限群G中阶是素数p的幂的的所有子群中存在在极大者，称为Sylow p-子群。

Sylow 定理

Definition 4.10

如果G是有限群且每个元素的阶是素数p的某次幂，则称G为有限p–群。

Theorem 4.11 (Sylow 第一定理)

G为有限p–群当且仅当G的阶为p的幂。

Definition 4.12

有限群G中阶是素数p的幂的的所有子群中存在在极大者，称为Sylow p-子群。

Sylow 定理

Definition 4.10

如果G是有限群且每个元素的阶是素数p的某次幂，则称G为有限p–群。

Theorem 4.11 (Sylow 第一定理)

G为有限p–群当且仅当G的阶为p的幂。

Definition 4.12

有限群G中阶是素数p的幂的的所有子群中存在在极大者，称为Sylow p-子群。

Sylow 定理

Theorem 4.13 (Sylow 定理)

G为有限群，且G的阶为$n = p^s \cdot m$，其中$\gcd(p, m) = 1$。则

1. 群G中存在t个*Sylow-p*子群，即阶为p^s的子群，其中$t|m$，$t \equiv 1 \mod p$；
2. 群G中所有*Sylow-p*子群彼此共轭，即所有的*Sylow-p*子群组成一个共轭子群类。

Sylow 定理

Theorem 4.13 (Sylow 定理)

G为有限群，且G的阶为$n = p^s \cdot m$，其中$\gcd(p, m) = 1$。则

1. 群G中存在t个*Sylow-p*子群，即阶为p^s的子群，其中$t|m$，$t \equiv 1 \mod p$；
2. 群G中所有*Sylow-p*子群彼此共轭，即所有的*Sylow-p*子群组成一个共轭子群类。

Sylow 定理

Theorem 4.13 (Sylow 定理)

G为有限群，且G的阶为$n = p^s \cdot m$，其中$\gcd(p, m) = 1$。则

1. 群G中存在t个*Sylow-p*子群，即阶为p^s的子群，其中$t|m$，$t \equiv 1 \mod p$；
2. 群G中所有*Sylow-p*子群彼此共轭，即所有的*Sylow-p*子群组成一个共轭子群类。

Direct Product of groups

Definition 5.1 (direct product)

Suppose H and K be two groups, let

$$\overline{G} = H \times K = \{(h,k) : h \in H, k \in K\}.$$

Define multiplication on $\overline{G}$:

$$(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2).$$

Thus $\overline{G}$ with this multiplication is a group, called the external direct product of H and K. 记为$\overline{G} = H \times K$。

- 令$\overline{H} = \{(h, 1_K) : h \in H\}$ 且$\overline{K} = \{(1_H, k) : k \in K\}$.
- 则$\overline{H} \trianglelefteq \overline{G}$, $\overline{K} \trianglelefteq \overline{G}$. $\overline{H} \cap \overline{K} = \{1\} = \{(1_H, 1_K)\}$.
- $\overline{H} \cong H$ and $\overline{K} \cong K$.

Direct Product of groups

Definition 5.1 (direct product)

Suppose H and K be two groups, let

$$\overline{G} = H \times K = \{(h,k) : h \in H, k \in K\}.$$

Define multiplication on $\overline{G}$:

$$(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2).$$

Thus $\overline{G}$ with this multiplication is a group, called the external direct product of H and K. 记为$\overline{G} = H \times K$。

- 令$\overline{H} = \{(h, 1_K) : h \in H\}$ 且$\overline{K} = \{(1_H, k) : k \in K\}$.
- 则$\overline{H} \trianglelefteq \overline{G}$, $\overline{K} \trianglelefteq \overline{G}$. $\overline{H} \cap \overline{K} = \{1\} = \{(1_H, 1_K)\}$.
- $\overline{H} \cong H$ and $\overline{K} \cong K$.

Direct Product of groups

Definition 5.1 (direct product)

Suppose H and K be two groups, let

$$\overline{G} = H \times K = \{(h,k) : h \in H, k \in K\}.$$

Define multiplication on $\overline{G}$:

$$(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2).$$

Thus $\overline{G}$ with this multiplication is a group, called the external direct product of H and K. 记为$\overline{G} = H \times K$。

- 令$\overline{H} = \{(h, 1_K) : h \in H\}$ 且$\overline{K} = \{(1_H, k) : k \in K\}$.
- 则$\overline{H} \trianglelefteq \overline{G}$, $\overline{K} \trianglelefteq \overline{G}$. $\overline{H} \cap \overline{K} = \{1\} = \{(1_H, 1_K)\}$.
- $\overline{H} \cong H$ and $\overline{K} \cong K$.

Direct Product of groups

Example 5.2

Let $H = \{1_H, a\}$, $K = \{1_K, b\}$, then

$$\begin{aligned} H \times K &= \{(1_H, 1_K), (1_H, b), (a, 1_K), (a, b)\} \\ &\cong K_4 \qquad \text{(Klein 4-group).} \end{aligned}$$

Theorem 5.3

设$\overline{G} = H \times K$是群$H$和$K$的外直积。

1. $\overline{G}$是有限群当且仅当H和K都是有限群，且有限群$\overline{G}$有$|\overline{G}| = |H||K|$.
2. $\overline{G}$是*Abel*群当且仅当H和K均为*Abel*群。
3. $H \times K \cong K \times H$。

Direct Product of groups

Example 5.2

Let $H = \{1_H, a\}$, $K = \{1_K, b\}$, then

$$\begin{aligned} H \times K &= \{(1_H, 1_K), (1_H, b), (a, 1_K), (a, b)\} \\ &\cong K_4 \qquad \text{(Klein 4-group).} \end{aligned}$$

Theorem 5.3

设$\overline{G} = H \times K$是群$H$和$K$的外直积。

1. $\overline{G}$是有限群当且仅当H和K都是有限群，且有限群$\overline{G}$有$|\overline{G}| = |H||K|$.
2. $\overline{G}$是*Abel*群当且仅当H和K均为*Abel*群。
3. $H \times K \cong K \times H$。

外直积中元素的阶

Theorem 5.4

设H和K是两个群。且$a \in H, b \in K$是有限阶元素，则$(a, b) \in H \times K$的阶是

$$ord((a, b)) = l.c.m(ord(a), ord(b)).$$

Theorem 5.5

设H和K是两个有限循环群。且$|H| = m, |K| = n$。$H \times K$是循环群当且仅当$\gcd(m, n) = 1$.

Definition 5.6 (internal direct product 内直积)

If group G contains normal subgroups H and K, i.e., $H, K \trianglelefteq G$, such that $G = HK$ and $H \cap K = \{1\}$, thus G is the internal direct product of H and K. Denoted by $G = H \otimes K$.

外直积中元素的阶

Theorem 5.4

设H和K是两个群。且$a \in H, b \in K$是有限阶元素，则$(a, b) \in H \times K$的阶是

$$ord((a, b)) = l.c.m(ord(a), ord(b)).$$

Theorem 5.5

设H和K是两个有限循环群。且$|H| = m, |K| = n$。$H \times K$是循环群当且仅当$\gcd(m, n) = 1$.

Definition 5.6 (internal direct product 内直积)

If group G contains normal subgroups H and K, i.e., $H, K \trianglelefteq G$, such that $G = HK$ and $H \cap K = \{1\}$, thus G is the internal direct product of H and K. Denoted by $G = H \otimes K$.

内直积的等价定义

Theorem 5.7

$G = H \otimes K$等价于下述两个条件：

1. G中的每个元素g可以唯一地表示为$g = hk$，其中$h \in H, k \in K$。
2. 对于任意的$h \in H, k \in K$，有$hk = kh$。

证明：$\Rightarrow$
设$G = H \otimes K$，则$G = HK$，$H, K \trianglelefteq G$，且$H \cap K = \{1\}$。设$g \in G$有两种表示方法：

$$g = hk = h'k', \quad h, h' \in H, \ k, k' \in K.$$

则$h^{-1}h' = kk'^{-1} \in H \cap K = \{1\}$。故$h^{-1}h' = kk'^{-1} = 1$，得$h = h', k = k'$。故表示方法唯一。
任意的$h \in H, k \in K$，由于$H, K \trianglelefteq G$，故

$$(hk)(kh)^{-1} = hkh^{-1}k^{-1} \in H \cap K = \{1\}.$$

因此$(hk)(kh)^{-1} = 1$，即$hk = kh$。

内直积的等价定义

Theorem 5.7

$G = H \otimes K$等价于下述两个条件：

1. G中的每个元素g可以唯一地表示为$g = hk$，其中$h \in H, k \in K$。
2. 对于任意的$h \in H, k \in K$，有$hk = kh$。

证明：$\Rightarrow$
设$G = H \otimes K$，则$G = HK$，$H, K \trianglelefteq G$，且$H \cap K = \{1\}$。设$g \in G$有两种表示方法：

$$g = hk = h'k', \quad h, h' \in H, \ k, k' \in K.$$

则$h^{-1}h' = kk'^{-1} \in H \cap K = \{1\}$。故$h^{-1}h' = kk'^{-1} = 1$，得$h = h', k = k'$。故表示方法唯一。
任意的$h \in H, k \in K$，由于$H, K \trianglelefteq G$，故

$$(hk)(kh)^{-1} = hkh^{-1}k^{-1} \in H \cap K = \{1\}.$$

因此$(hk)(kh)^{-1} = 1$，即$hk = kh$。

内直积的等价定义

Theorem 5.7

$G = H \otimes K$等价于下述两个条件：

1. G中的每个元素g可以唯一地表示为$g = hk$，其中$h \in H, k \in K$。
2. 对于任意的$h \in H, k \in K$，有$hk = kh$。

证明：$\Rightarrow$
设$G = H \otimes K$，则$G = HK$，$H, K \trianglelefteq G$，且$H \cap K = \{1\}$。设$g \in G$有两种表示方法：

$$g = hk = h'k', \quad h, h' \in H, \ k, k' \in K.$$

则$h^{-1}h' = kk'^{-1} \in H \cap K = \{1\}$。故$h^{-1}h' = kk'^{-1} = 1$，得$h = h', k = k'$。故表示方法唯一。
任意的$h \in H, k \in K$，由于$H, K \trianglelefteq G$，故

$$(hk)(kh)^{-1} = hkh^{-1}k^{-1} \in H \cap K = \{1\}.$$

因此$(hk)(kh)^{-1} = 1$，即$hk = kh$。

内直积的性质

Theorem 5.8

$G = H \otimes K$有如下性质：

1. G中的每个元素g可以唯一地表示为$g = hk$，其中$h \in H, k \in K$。
2. 对于任意的$h \in H, k \in K$，有$hk = kh$。

证明：$\Leftarrow$

$\forall g \in G$, there exists $h_1 \in H, k_1 \in K$ such that $g = h_1 k_1$. Hence $G = HK$.

$\forall g \in G$, $\forall h \in H$,

$$ghg^{-1} = h_1 k_1 h (h_1 k_1)^{-1} = h_1 k_1 h k_1^{-1} h_1^{-1} = h_1 k_1 k_1^{-1} h h_1^{-1} \in H.$$

Hence $H \trianglelefteq G$. Similarly, we have $K \trianglelefteq G$.

Finally $\forall w \in H \cap K$, we have $w = 1w = w1$. The unique expression of w gives $w = 1$.

内直积的性质

Theorem 5.8

$G = H \otimes K$有如下性质：

1. G中的每个元素g可以唯一地表示为$g = hk$，其中$h \in H, k \in K$。
2. 对于任意的$h \in H, k \in K$，有$hk = kh$。

证明：$\Leftarrow$

$\forall g \in G$, there exists $h_1 \in H, k_1 \in K$ such that $g = h_1 k_1$. Hence $G = HK$.

$\forall g \in G$, $\forall h \in H$,

$$ghg^{-1} = h_1 k_1 h (h_1 k_1)^{-1} = h_1 k_1 h k_1^{-1} h_1^{-1} = h_1 k_1 k_1^{-1} h h_1^{-1} \in H.$$

Hence $H \trianglelefteq G$. Similarly, we have $K \trianglelefteq G$.

Finally $\forall w \in H \cap K$, we have $w = 1w = w1$. The unique expression of w gives $w = 1$.

Direct Product of groups

Lemma 5.9

If G is the internal direct product of H and K, then $G \cong H \times K$.

Proof.

Define $f : H \times K \mapsto G$ by $f(h,k) = hk$; note that if $h \in H$ and $k \in K$ then $hk = kh$.

1. f is a homomorphism, since

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) \\ &= f(h_1,k_1)f(h_2,k_2). \end{aligned}$$

2. f is surjective, since $G = HK$.
3. f is injective, for if $f(h,k) = 1$ then $hk = 1$, so that $h = k^{-1}$. Thus $h \in H \cap K$, so $h = 1$. $\ker f$ is trivial.

□

Direct Product of groups

Lemma 5.9

If G is the internal direct product of H and K, then $G \cong H \times K$.

Proof.

Define $f : H \times K \mapsto G$ by $f(h,k) = hk$; note that if $h \in H$ and $k \in K$ then $hk = kh$.

1. f is a homomorphism, since

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) \\ &= f(h_1,k_1)f(h_2,k_2). \end{aligned}$$

2. f is surjective, since $G = HK$.
3. f is injective, for if $f(h,k) = 1$ then $hk = 1$, so that $h = k^{-1}$. Thus $h \in H \cap K$, so $h = 1$. $\ker f$ is trivial.

□

Direct Product of groups

Lemma 5.9

If G is the internal direct product of H and K, then $G \cong H \times K$.

Proof.

Define $f : H \times K \mapsto G$ by $f(h,k) = hk$; note that if $h \in H$ and $k \in K$ then $hk = kh$.

1. f is a homomorphism, since

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) \\ &= f(h_1,k_1)f(h_2,k_2). \end{aligned}$$

2. f is surjective, since $G = HK$.
3. f is injective, for if $f(h,k) = 1$ then $hk = 1$, so that $h = k^{-1}$. Thus $h \in H \cap K$, so $h = 1$. $\ker f$ is trivial.

□

群的外直积的一般定义

Definition 5.10

设$H_1, H_2, \cdots, H_n$是任意的n个群。则它们的外直积就是它们的笛卡尔乘积$\overline{G} = H_1 \times H_2 \times \cdots \times H_n$，和如下运算

$$(h_1, h_2, \cdots, h_n)(h_1', h_2', \cdots, h_n') = (h_1h_1', h_2h_2', \cdots, h_nh_n').$$

- 外直积$\overline{G}$中包含了与H_i同构的子群，$\overline{H_i} = \{(1_{H_1}, \cdots 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \cdots, 1_{H_n}), h_i \in H_i\}$。
- $\overline{H_i} \trianglelefteq \overline{G}$且$\overline{G} = \overline{H_1H_2} \cdots \overline{H_n}$。
- 对于$\forall \overline{g} \in \overline{G}$，$\overline{g} = \overline{h_1h_2} \cdots \overline{h_n}$的表示是惟一的。
- 对于$\forall i, j, i \neq j$有$\overline{H_i} \cap \overline{H_j} = \{(1_{H_1}, \cdots 1_{H_n})\}$。

群的外直积的一般定义

Definition 5.10

设$H_1, H_2, \cdots, H_n$是任意的n个群。则它们的外直积就是它们的笛卡尔乘积$\overline{G} = H_1 \times H_2 \times \cdots \times H_n$，和如下运算

$$(h_1, h_2, \cdots, h_n)(h_1', h_2', \cdots, h_n') = (h_1h_1', h_2h_2', \cdots, h_nh_n').$$

- 外直积$\overline{G}$中包含了与H_i同构的子群，$\overline{H_i} = \{(1_{H_1}, \cdots 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \cdots, 1_{H_n}), h_i \in H_i\}$。
- $\overline{H_i} \trianglelefteq \overline{G}$且$\overline{G} = \overline{H_1H_2} \cdots \overline{H_n}$。
- 对于$\forall \overline{g} \in \overline{G}$，$\overline{g} = \overline{h_1h_2} \cdots \overline{h_n}$的表示是惟一的。
- 对于$\forall i, j, i \neq j$有$\overline{H_i} \cap \overline{H_j} = \{(1_{H_1}, \cdots 1_{H_n})\}$。

群的外直积的一般定义

Definition 5.10

设$H_1, H_2, \cdots, H_n$是任意的n个群。则它们的外直积就是它们的笛卡尔乘积$\overline{G} = H_1 \times H_2 \times \cdots \times H_n$，和如下运算

$$(h_1, h_2, \cdots, h_n)(h_1', h_2', \cdots, h_n') = (h_1h_1', h_2h_2', \cdots, h_nh_n').$$

- 外直积$\overline{G}$中包含了与H_i同构的子群，$\overline{H_i} = \{(1_{H_1}, \cdots 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \cdots, 1_{H_n}), h_i \in H_i\}$。
- $\overline{H_i} \trianglelefteq \overline{G}$且$\overline{G} = \overline{H_1H_2} \cdots \overline{H_n}$。
- 对于$\forall \overline{g} \in \overline{G}$，$\overline{g} = \overline{h_1h_2} \cdots \overline{h_n}$的表示是惟一的。
- 对于$\forall i, j, i \neq j$有$\overline{H_i} \cap \overline{H_j} = \{(1_{H_1}, \cdots 1_{H_n})\}$。

群的外直积的一般定义

Definition 5.10

设$H_1, H_2, \cdots, H_n$是任意的n个群。则它们的外直积就是它们的笛卡尔乘积$\overline{G} = H_1 \times H_2 \times \cdots \times H_n$，和如下运算

$$(h_1, h_2, \cdots, h_n)(h_1', h_2', \cdots, h_n') = (h_1h_1', h_2h_2', \cdots, h_nh_n').$$

- 外直积$\overline{G}$中包含了与H_i同构的子群，$\overline{H_i} = \{(1_{H_1}, \cdots 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \cdots, 1_{H_n}), h_i \in H_i\}$。
- $\overline{H_i} \trianglelefteq \overline{G}$且$\overline{G} = \overline{H_1H_2} \cdots \overline{H_n}$。
- 对于$\forall \overline{g} \in \overline{G}$，$\overline{g} = \overline{h_1h_2} \cdots \overline{h_n}$的表示是惟一的。
- 对于$\forall i, j, i \neq j$有$\overline{H_i} \cap \overline{H_j} = \{(1_{H_1}, \cdots 1_{H_n})\}$。

群的外直积的一般定义

Definition 5.10

设$H_1, H_2, \cdots, H_n$是任意的n个群。则它们的外直积就是它们的笛卡尔乘积$\overline{G} = H_1 \times H_2 \times \cdots \times H_n$，和如下运算

$$(h_1, h_2, \cdots, h_n)(h_1', h_2', \cdots, h_n') = (h_1h_1', h_2h_2', \cdots, h_nh_n').$$

- 外直积$\overline{G}$中包含了与H_i同构的子群，$\overline{H_i} = \{(1_{H_1}, \cdots 1_{H_{i-1}}, h_i, 1_{H_{i+1}}, \cdots, 1_{H_n}), h_i \in H_i\}$。
- $\overline{H_i} \trianglelefteq \overline{G}$且$\overline{G} = \overline{H_1H_2} \cdots \overline{H_n}$。
- 对于$\forall \overline{g} \in \overline{G}$，$\overline{g} = \overline{h_1h_2} \cdots \overline{h_n}$的表示是惟一的。
- 对于$\forall i, j, i \neq j$有$\overline{H_i} \cap \overline{H_j} = \{(1_{H_1}, \cdots 1_{H_n})\}$。

群的内直积的一般定义

Definition 5.11

设群$G = H_1H_2\cdots H_n$，且$H_i \trianglelefteq G$，且$\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。称G是H_i的内直积。记为$G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$.

- 设G是$H_1, H_2, \cdots, H_n$的内直积，则$G \cong H_1 \times H_2 \times \cdots \times H_n$。且同构映射为$f(h_1, h_2, \cdots, h_n) = h_1h_2\cdots h_n$。

群的内直积的一般定义

Definition 5.11

设群$G = H_1H_2\cdots H_n$，且$H_i \trianglelefteq G$，且$\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。称G是H_i的内直积。记为$G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$.

- 设G是$H_1, H_2, \cdots, H_n$的内直积，则$G \cong H_1 \times H_2 \times \cdots \times H_n$。且同构映射为$f(h_1, h_2, \cdots, h_n) = h_1h_2\cdots h_n$。

群的内直积的一般定义

Definition 5.11

设群$G = H_1H_2\cdots H_n$，且$H_i \trianglelefteq G$，且$\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。称G是H_i的内直积。记为$G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$.

- 设G是$H_1, H_2, \cdots, H_n$的内直积，则$G \cong H_1 \times H_2 \times \cdots \times H_n$。且同构映射为$f(h_1, h_2, \cdots, h_n) = h_1h_2\cdots h_n$。

群的内直积的判定

Theorem 5.12

设$G = H_1H_2\cdots H_n$且$H_i \trianglelefteq G$。下列条件等价：

1. $\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。
2. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j\neq i}H_j = \{1\}$；
3. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j=1}^{i-1}H_j = \{1\}$；

如果G为Abel群，则条件1等价于单位元1有唯一的表示。

群的内直积的判定

Theorem 5.12

设$G = H_1H_2\cdots H_n$且$H_i \trianglelefteq G$。下列条件等价：

1. $\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。
2. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j\neq i}H_j = \{1\}$；
3. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j=1}^{i-1}H_j = \{1\}$；

如果G为Abel群，则条件1等价于单位元1有唯一的表示。

群的内直积的判定

Theorem 5.12

设$G = H_1H_2\cdots H_n$且$H_i \trianglelefteq G$。下列条件等价：

1. $\forall g \in G$都有惟一的表示：$g = h_1h_2\cdots h_n$，$h_i \in H_i$，$i = 1, 2, \cdots, n$。
2. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j\neq i}H_j = \{1\}$；
3. 对于所有的$i = 1, 2, \cdots, n$，有$H_i \bigcap \Pi_{j=1}^{i-1}H_j = \{1\}$；

如果G为Abel群，则条件1等价于单位元1有唯一的表示。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是$Abel$群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

循环群$< g >$中各元素的级

Lemma 6.1

在群G中，

1. 如果$ord(g) = t$，且$\gcd(t, s) = k$，则$ord(g^s) = t/k$；
2. 如果$ord(g) = t$，且$\gcd(t, s) = 1$，则$ord(g^s) = t$；
3. 如果群G是*Abel*群，$g_1 \cdot g_2 \cdots g_m = 1$且$g_i$的阶$t_i$两两互素，则$g_i = 1, i = 1, 2, \cdots, m$

证明：(3)归纳法。

- $m = 1$时$g_1 = 1$显然成立。
- 假设$m - 1$时结论成立。
- $g_1 \cdot g_2 \cdots g_m = 1$，则$(g_1 \cdot g_2 \cdots g_m)^{t_m} = g_1^{t_m} \cdot g_2^{t_m} \cdots g_{m-1}^{t_m} = 1$。由归纳假设知$g_1^{t_m} = g_2^{t_m} = \cdots = g_{m-1}^{t_m} = 1$。
  由于$\gcd(t_i, t_m) = 1, i = 1, 2, \cdots, m - 1$，由(2)知$g_i = 1$。

有限交换群的直积分解

Theorem 6.2

有限交换群G中，若$|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，其中$p_i$是互不相同的素数，则有

1. $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$，其中$H_i$是Sylow p_i–群，$i = 1, 2, \cdots, t$；
2. 如果$G = H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1' \otimes H_2' \otimes \cdots \otimes H_t'$，其中$H_i, H_i'$是Sylow p_i–群，那么$H_i = H_i'$，$i = 1, 2, \cdots, t$；

证明：(1)

- 对于任意的$1 \le i \le t$，
  令$n_i = p_i^{m_i}, r_i = n/n_i$，$H_i = \{g \in G \mid ord(g) = p_i^u, u \in \mathbb{Z}\}$。
  则$H_i = \{g \in G \mid g^{n_i} = g^{p_i^{m_i}} = 1\}$。$H_i \le G$是Sylow p_i–群。
- $H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1 H_2 \cdots H_t = \{h_1 h_2 \cdots h_t \mid h_i \in H_i, i = 1, 2, \cdots, t\} \le G$。
  如果$h_1 h_2 \cdots h_t = 1$，那么由于$h_1, h_2, \cdots, h_t$的级两两互素，
  由Lemma6.1知，$h_1 = h_2 = \cdots = h_t = 1$。

有限交换群的直积分解

Theorem 6.2

有限交换群G中，若$|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，其中$p_i$是互不相同的素数，则有

1. $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$，其中$H_i$是Sylow p_i–群，$i = 1, 2, \cdots, t$；
2. 如果$G = H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1' \otimes H_2' \otimes \cdots \otimes H_t'$，其中$H_i, H_i'$是Sylow p_i–群，那么$H_i = H_i'$，$i = 1, 2, \cdots, t$；

证明：(1)

- 对于任意的$1 \le i \le t$，
  令$n_i = p_i^{m_i}, r_i = n/n_i$，$H_i = \{g \in G \mid ord(g) = p_i^u, u \in \mathbb{Z}\}$。
  则$H_i = \{g \in G \mid g^{n_i} = g^{p_i^{m_i}} = 1\}$。$H_i \le G$是Sylow p_i–群。
- $H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1 H_2 \cdots H_t = \{h_1 h_2 \cdots h_t \mid h_i \in H_i, i = 1, 2, \cdots, t\} \le G$。
  如果$h_1 h_2 \cdots h_t = 1$，那么由于$h_1, h_2, \cdots, h_t$的级两两互素，
  由Lemma6.1知，$h_1 = h_2 = \cdots = h_t = 1$。

有限交换群的直积分解

Theorem 6.2

有限交换群G中，若$|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，其中$p_i$是互不相同的素数，则有

1. $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$，其中$H_i$是Sylow p_i–群，$i = 1, 2, \cdots, t$；
2. 如果$G = H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1' \otimes H_2' \otimes \cdots \otimes H_t'$，其中$H_i, H_i'$是Sylow p_i–群，那么$H_i = H_i'$，$i = 1, 2, \cdots, t$；

证明：(1)

- 对于任意的$1 \le i \le t$，
  令$n_i = p_i^{m_i}, r_i = n/n_i$，$H_i = \{g \in G \mid ord(g) = p_i^u, u \in \mathbb{Z}\}$。
  则$H_i = \{g \in G \mid g^{n_i} = g^{p_i^{m_i}} = 1\}$。$H_i \le G$是Sylow p_i–群。
- $H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1 H_2 \cdots H_t = \{h_1 h_2 \cdots h_t \mid h_i \in H_i, i = 1, 2, \cdots, t\} \le G$。
  如果$h_1 h_2 \cdots h_t = 1$，那么由于$h_1, h_2, \cdots, h_t$的级两两互素，
  由Lemma6.1知，$h_1 = h_2 = \cdots = h_t = 1$。

有限交换群的直积分解

Theorem 6.2

有限交换群G中，若$|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，其中$p_i$是互不相同的素数，则有

1. $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$，其中$H_i$是Sylow p_i–群，$i = 1, 2, \cdots, t$；
2. 如果$G = H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1' \otimes H_2' \otimes \cdots \otimes H_t'$，其中$H_i, H_i'$是Sylow p_i–群，那么$H_i = H_i'$，$i = 1, 2, \cdots, t$；

证明：(1)

- 对于任意的$1 \le i \le t$，
  令$n_i = p_i^{m_i}, r_i = n/n_i$，$H_i = \{g \in G \mid ord(g) = p_i^u, u \in \mathbb{Z}\}$。
  则$H_i = \{g \in G \mid g^{n_i} = g^{p_i^{m_i}} = 1\}$。$H_i \le G$是Sylow p_i–群。
- $H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1 H_2 \cdots H_t = \{h_1 h_2 \cdots h_t \mid h_i \in H_i, i = 1, 2, \cdots, t\} \le G$。
  如果$h_1 h_2 \cdots h_t = 1$，那么由于$h_1, h_2, \cdots, h_t$的级两两互素，
  由Lemma6.1知，$h_1 = h_2 = \cdots = h_t = 1$。

有限交换群的直积分解

Theorem 6.2

有限交换群G中，若$|G| = n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，其中$p_i$是互不相同的素数，则有

1. $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$，其中$H_i$是Sylow p_i–群，$i = 1, 2, \cdots, t$；
2. 如果$G = H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1' \otimes H_2' \otimes \cdots \otimes H_t'$，其中$H_i, H_i'$是Sylow p_i–群，那么$H_i = H_i'$，$i = 1, 2, \cdots, t$；

证明：(1)

- 对于任意的$1 \le i \le t$，
  令$n_i = p_i^{m_i}, r_i = n/n_i$，$H_i = \{g \in G \mid ord(g) = p_i^u, u \in \mathbb{Z}\}$。
  则$H_i = \{g \in G \mid g^{n_i} = g^{p_i^{m_i}} = 1\}$。$H_i \le G$是Sylow p_i–群。
- $H_1 \otimes H_2 \otimes \cdots \otimes H_t = H_1 H_2 \cdots H_t = \{h_1 h_2 \cdots h_t \mid h_i \in H_i, i = 1, 2, \cdots, t\} \le G$。
  如果$h_1 h_2 \cdots h_t = 1$，那么由于$h_1, h_2, \cdots, h_t$的级两两互素，
  由Lemma6.1知，$h_1 = h_2 = \cdots = h_t = 1$。

- 由于$r_1, r_2, \cdots, r_t$互素，则它们的最大公因子是1。因此，存在整数$s_i \in \mathbb{Z}, i = 1, 2, \cdots, t$，使得$s_1 r_1 + s_2 r_2 + \cdots + s_t r_t = 1$。
- 任取$a \in G$，令$b_i = a^{s_i r_i}$，则$a = a^{(\sum_{i=1}^{t} s_i r_i)} = \Pi_{i=1}^{t} b_i$。
- 由于$|G| = n$，则$a^n = 1$，故$b_i^{n_i} = a^{s_i r_i n_i} = a^{s_i n} = 1$，故$b_i \in H_i$。因此$a \in H_1 H_2 \cdots H_m$。
- $G \leq H_1 \otimes H_2 \otimes \cdots \otimes H_t$。
- $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$。

- 由于$r_1, r_2, \cdots, r_t$互素，则它们的最大公因子是1。因此，存在整数$s_i \in \mathbb{Z}, i = 1, 2, \cdots, t$，使得$s_1 r_1 + s_2 r_2 + \cdots + s_t r_t = 1$。
- 任取$a \in G$，令$b_i = a^{s_i r_i}$，则$a = a^{(\sum_{i=1}^{t} s_i r_i)} = \Pi_{i=1}^{t} b_i$。
- 由于$|G| = n$，则$a^n = 1$，故$b_i^{n_i} = a^{s_i r_i n_i} = a^{s_i n} = 1$，故$b_i \in H_i$。因此$a \in H_1 H_2 \cdots H_m$。
- $G \preceq H_1 \otimes H_2 \otimes \cdots \otimes H_t$。
- $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$。

- 由于$r_1, r_2, \cdots, r_t$互素，则它们的最大公因子是1。因此，存在整数$s_i \in \mathbb{Z}, i = 1, 2, \cdots, t$，使得$s_1 r_1 + s_2 r_2 + \cdots + s_t r_t = 1$。
- 任取$a \in G$，令$b_i = a^{s_i r_i}$，则$a = a^{(\sum_{i=1}^{t} s_i r_i)} = \Pi_{i=1}^{t} b_i$。
- 由于$|G| = n$，则$a^n = 1$，故$b_i^{n_i} = a^{s_i r_i n_i} = a^{s_i n} = 1$，故$b_i \in H_i$。因此$a \in H_1 H_2 \cdots H_m$。
- $G \leq H_1 \otimes H_2 \otimes \cdots \otimes H_t$。
- $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$。

- 由于$r_1, r_2, \cdots, r_t$互素，则它们的最大公因子是1。因此，存在整数$s_i \in \mathbb{Z}, i = 1, 2, \cdots, t$，使得$s_1 r_1 + s_2 r_2 + \cdots + s_t r_t = 1$。
- 任取$a \in G$，令$b_i = a^{s_i r_i}$，则$a = a^{(\sum_{i=1}^{t} s_i r_i)} = \Pi_{i=1}^{t} b_i$。
- 由于$|G| = n$，则$a^n = 1$，故$b_i^{n_i} = a^{s_i r_i n_i} = a^{s_i n} = 1$，故$b_i \in H_i$。因此$a \in H_1 H_2 \cdots H_m$。
- $G \preceq H_1 \otimes H_2 \otimes \cdots \otimes H_t$。
- $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$。

- 由于$r_1, r_2, \cdots, r_t$互素，则它们的最大公因子是1。因此，存在整数$s_i \in \mathbb{Z}, i = 1, 2, \cdots, t$，使得$s_1 r_1 + s_2 r_2 + \cdots + s_t r_t = 1$。
- 任取$a \in G$，令$b_i = a^{s_i r_i}$，则$a = a^{(\sum_{i=1}^{t} s_i r_i)} = \Pi_{i=1}^{t} b_i$。
- 由于$|G| = n$，则$a^n = 1$，故$b_i^{n_i} = a^{s_i r_i n_i} = a^{s_i n} = 1$，故$b_i \in H_i$。因此$a \in H_1 H_2 \cdots H_m$。
- $G \preceq H_1 \otimes H_2 \otimes \cdots \otimes H_t$。
- $G = H_1 \otimes H_2 \otimes \cdots \otimes H_t$。

有限交换群$\Rightarrow$ 有限sylow $p-$群

设$G =< g >$是一个循环群且$|G| = p^m$，则$G = g^{\mathbb{Z}}$。

循环$p-$群G不可能再分解。

反证法：如果G可以分解。不失一般性，设G可以分解为两个真子群的直积，即$G =< g_1 > \otimes < g_2 >$。设$ord(g_1) = p^{m_1}, ord(g_2) = p^{m_2}$，设$m_1 \leq m_2 < m$，则

$$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}}.$$

$\forall g \in G$，有$g = g_1^{t_1} g_2^{t_2}$，因此$g^{p^{m_2}} = g_1^{t_1 p^{m_2}} g_2^{t_2 p^{m_2}} = 1$。如果$g$为$G$生成元，则出现矛盾！

循环$p-$群是群中的最基本的构件！

有限交换群⇒ 有限sylow p–群

设$G =< g >$是一个循环群且$|G| = p^m$，则$G = g^{\mathbb{Z}}$。
循环p–群G不可能再分解。
反证法：如果G可以分解。不失一般性，设G可以分解为两个真子群的直积，即$G =< g_1 > \otimes < g_2 >$。设$ord(g_1) = p^{m_1}, ord(g_2) = p^{m_2}$，设$m_1 \leq m_2 < m$，则

$$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}}.$$

$\forall g \in G$，有$g = g_1^{t_1} g_2^{t_2}$，因此$g^{p^{m_2}} = g_1^{t_1 p^{m_2}} g_2^{t_2 p^{m_2}} = 1$。如果$g$为$G$生成元，则出现矛盾！
循环p–群是群中的最基本的构件！

有限交换群⇒ 有限sylow p–群

设$G =< g >$是一个循环群且$|G| = p^m$，则$G = g^{\mathbb{Z}}$。
循环p–群G不可能再分解。
反证法：如果G可以分解。不失一般性，设G可以分解为两个真子群的直积，即$G =< g_1 > \otimes < g_2 >$。设$ord(g_1) = p^{m_1}, ord(g_2) = p^{m_2}$，设$m_1 \leq m_2 < m$，则

$$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}}.$$

$\forall g \in G$，有$g = g_1^{t_1} g_2^{t_2}$，因此$g^{p^{m_2}} = g_1^{t_1 p^{m_2}} g_2^{t_2 p^{m_2}} = 1$。如果$g$为$G$生成元，则出现矛盾！
循环p–群是群中的最基本的构件！

有限p–群(交换群)的分解

设$\{g_1, g_2, \cdots, g_k\}$和$\{h_1, h_2, \cdots, h_k\}$是有限$p$–群$G$的两个元素个数相等的生成元集，生成元素的相应级为$\{p^{m_1}, p^{m_2}, \cdots, p^{m_k}\}$和$\{p^{l_1}, p^{l_2}, \cdots, p^{l_k}\}$。

如果$m_1 + m_2 + \cdots + m_k < l_1 + l_2 + \cdots + l_k$，我们就称生成元集$\{g_1, g_2, \cdots, g_k\}$小于生成元集$\{h_1, h_2, \cdots, h_k\}$。

Theorem 6.3

设G为有限p–群(交换群)，且$|G| = p^m$，则有

1. $G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$；
2. 如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，则必有$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$，其中$i = 1, 2, \cdots, k$。

有限p–群(交换群)的分解

设$\{g_1, g_2, \cdots, g_k\}$和$\{h_1, h_2, \cdots, h_k\}$是有限$p$–群$G$的两个元素个数相等的生成元集，生成元素的相应级为$\{p^{m_1}, p^{m_2}, \cdots, p^{m_k}\}$和$\{p^{l_1}, p^{l_2}, \cdots, p^{l_k}\}$。
如果$m_1 + m_2 + \cdots + m_k < l_1 + l_2 + \cdots + l_k$，我们就称生成元集$\{g_1, g_2, \cdots, g_k\}$小于生成元集$\{h_1, h_2, \cdots, h_k\}$。

Theorem 6.3

设G为有限p–群(交换群)，且$|G| = p^m$，则有

1. $G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$；
2. 如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，则必有$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$，其中$i = 1, 2, \cdots, k$。

有限p–群(交换群)的分解

设$\{g_1, g_2, \cdots, g_k\}$和$\{h_1, h_2, \cdots, h_k\}$是有限$p$–群$G$的两个元素个数相等的生成元集，生成元素的相应级为$\{p^{m_1}, p^{m_2}, \cdots, p^{m_k}\}$和$\{p^{l_1}, p^{l_2}, \cdots, p^{l_k}\}$。
如果$m_1 + m_2 + \cdots + m_k < l_1 + l_2 + \cdots + l_k$，我们就称生成元集$\{g_1, g_2, \cdots, g_k\}$小于生成元集$\{h_1, h_2, \cdots, h_k\}$。

Theorem 6.3

设G为有限p–群(交换群)，且$|G| = p^m$，则有

1. $G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$；
2. 如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，则必有$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$，其中$i = 1, 2, \cdots, k$。

有限p–群(交换群)的分解

设$\{g_1, g_2, \cdots, g_k\}$和$\{h_1, h_2, \cdots, h_k\}$是有限$p$–群$G$的两个元素个数相等的生成元集，生成元素的相应级为$\{p^{m_1}, p^{m_2}, \cdots, p^{m_k}\}$和$\{p^{l_1}, p^{l_2}, \cdots, p^{l_k}\}$。
如果$m_1 + m_2 + \cdots + m_k < l_1 + l_2 + \cdots + l_k$，我们就称生成元集$\{g_1, g_2, \cdots, g_k\}$小于生成元集$\{h_1, h_2, \cdots, h_k\}$。

Theorem 6.3

设G为有限p–群(交换群)，且$|G| = p^m$，则有

1. $G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$；
2. 如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，则必有$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$，其中$i = 1, 2, \cdots, k$。

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i \mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

证明：(1)有限群必有有限的生成元集。

- 取G中所有生成元集中元素个数最少的，而且按上述的大小关系也是最小的一个生成元集，设为$\{g_1, g_2, \cdots, g_k\}$，设其相应的级为$\{p^{r_1}, p^{r_2}, \cdots, p^{r_k}\}$。
- 则$G = g_1^{\mathbb{Z}} g_2^{\mathbb{Z}} \cdots g_k^{\mathbb{Z}}$。
- 反证法。假设$G \neq g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$。

  则存在$g_i^{l_i}, g_j^{l_j}, g_t^{l_t}$，均不为1，但却使得$g_i^{l_i} g_j^{l_j} g_t^{l_t} = 1$。
- $p|l_i, p|l_j, p|l_t$。如果存在$p \nmid l_i$，则$ord(g_i) = ord(g_i^{l_i})$。因此$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}}$。

  $g_i^{l_i} = g_j^{-l_j} g_t^{-l_t}$，所以$g_i^{\mathbb{Z}} = g_i^{l_i\mathbb{Z}} \subseteq g_j^{\mathbb{Z}} g_t^{\mathbb{Z}}$。

  这样的话去掉生成元集中去掉g_i仍是生成元集。矛盾！

有限p–群(交换群)的分解

- 设$\gcd(l_i, l_j, l_t) = lp^s$且$\gcd(l, p) = 1$，则

$$g_i^{l_i} g_j^{l_j} g_t^{l_t} = \left(g_i^{m_i} g_j^{m_j} g_t^{m_t}\right)^{p^s} = 1$$

- m_i, m_j, m_k中至少有一个不被p整除，不防设为m_j，$p \nmid m_j$。
则$ord(g_j) = ord(g_j^{m_j})$且$g_j^{\mathbb{Z}} = \left(g_j^{m_j}\right)^{\mathbb{Z}}$。
- 令$g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}$，可
知$M = \{g_1, g_2, \cdots, g_{j-1}, g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}, g_{j+1}, \cdots, g_k\}$是$G$的生成元集。
而$g_j'^{p^s} = 1$，而且$g_j^{m_j p^s} \neq 1$可知$p^s < p^{r_j}$，故生成元集M的大小次序比$\{g_1, g_2, \cdots, g_k\}$还要小，矛盾！

有限p–群(交换群)的分解

- 设$\gcd(l_i, l_j, l_t) = lp^s$且$\gcd(l, p) = 1$，则

$$g_i^{l_i} g_j^{l_j} g_t^{l_t} = \left(g_i^{m_i} g_j^{m_j} g_t^{m_t}\right)^{p^s} = 1$$

- m_i, m_j, m_k中至少有一个不被p整除，不防设为m_j，$p \nmid m_j$。
则$ord(g_j) = ord(g_j^{m_j})$且$g_j^{\mathbb{Z}} = \left(g_j^{m_j}\right)^{\mathbb{Z}}$。
- 令$g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}$，可
知$M = \{g_1, g_2, \cdots, g_{j-1}, g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}, g_{j+1}, \cdots, g_k\}$是$G$的生成元集。
而$g_j'^{p^s} = 1$，而且$g_j^{m_j p^s} \neq 1$可知$p^s < p^{r_j}$，故生成元集M的大小次序
比$\{g_1, g_2, \cdots, g_k\}$还要小，矛盾！

有限p–群(交换群)的分解

- 设$\gcd(l_i, l_j, l_t) = lp^s$且$\gcd(l, p) = 1$，则

$$g_i^{l_i} g_j^{l_j} g_t^{l_t} = \left(g_i^{m_i} g_j^{m_j} g_t^{m_t}\right)^{p^s} = 1$$

- m_i, m_j, m_k中至少有一个不被p整除，不防设为m_j，$p \nmid m_j$。
则$ord(g_j) = ord(g_j^{m_j})$且$g_j^{\mathbb{Z}} = \left(g_j^{m_j}\right)^{\mathbb{Z}}$。
- 令$g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}$，可
知$M = \{g_1, g_2, \cdots, g_{j-1}, g_j' = g_i^{m_i} g_j^{m_j} g_t^{m_t}, g_{j+1}, \cdots, g_k\}$是$G$的生成元集。
而$g_j'^{p^s} = 1$，而且$g_j^{m_j p^s} \neq 1$可知$p^s < p^{r_j}$，故生成元集M的大小次序比$\{g_1, g_2, \cdots, g_k\}$还要小，矛盾！

有限p–群(交换群)

如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，现在用归纳法证明下面的结论：设$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$，$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$均为有限交换$p$–群，且$G \cong G'$，那么$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$。

- 当$k = 1$时，由于循环p–群不能再分解，所以$G = g_1^{\mathbb{Z}}$。又因为$G \cong G'$，故$G' = h_1^{\mathbb{Z}}$也是循环群，故$g_1^{\mathbb{Z}} \cong h_1^{\mathbb{Z}}$。
- 设$k - 1$时结论成立。
- 在k的情况下，不失一般性，假设g_k是生成元集$\{g_1, \cdots, g_k\}$中级最大的元素，设$ord(g_k) = p^m$。设$\sigma : G \to G'$是同构映射。则$ord(\sigma(g_k)) = p^m$。假设生成元集$\{h_1, \cdots, h_s\}$中级最大的元素为h_s，其级为p^n。必有$n = m$（若$n < m$，则$\sigma(g_k) \in G'$不能用生成元集$\{h_1, \cdots, h_s\}$表示）。
- 不失一般性，设$ord(h_j) = ord(h_{j+1}) = \cdots = ord(h_s) = p^m$。

$$\sigma(g_k) = h_1^{l_1} h_2^{l_2} \cdots h_s^{l_s}. \tag{4}$$

则上式的$\{l_j, l_{j+1}, \cdots, l_s\}$中定存在一个元素不被$p$整除。否则$\sigma(g_k)$的级就会小于$p^m$。

有限p–群(交换群)

如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，现在用归纳法证明下面的结论：设$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$，$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$均为有限交换$p$–群，且$G \cong G'$，那么$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$。

- 当$k = 1$时，由于循环p–群不能再分解，所以$G = g_1^{\mathbb{Z}}$。又因为$G \cong G'$，故$G' = h_1^{\mathbb{Z}}$也是循环群，故$g_1^{\mathbb{Z}} \cong h_1^{\mathbb{Z}}$。
- 设$k-1$时结论成立。
- 在k的情况下，不失一般性，假设g_k是生成元集$\{g_1, \cdots, g_k\}$中级最大的元素，设$ord(g_k) = p^m$。设$\sigma : G \to G'$是同构映射。则$ord(\sigma(g_k)) = p^m$。假设生成元集$\{h_1, \cdots, h_s\}$中级最大的元素为h_s，其级为p^n。必有$n = m$（若$n < m$，则$\sigma(g_k) \in G'$不能用生成元集$\{h_1, \cdots, h_s\}$表示）。
- 不失一般性，设$ord(h_j) = ord(h_{j+1}) = \cdots = ord(h_s) = p^m$。

$$\sigma(g_k) = h_1^{l_1} h_2^{l_2} \cdots h_s^{l_s}. \tag{4}$$

则上式的$\{l_j, l_{j+1}, \cdots, l_s\}$中定存在一个元素不被$p$整除。否则$\sigma(g_k)$的级就会小于$p^m$。

有限p–群(交换群)

如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，现在用归纳法证明下面的结论：设$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$，$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$均为有限交换$p$–群，且$G \cong G'$，那么$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$。

- 当$k = 1$时，由于循环p–群不能再分解，所以$G = g_1^{\mathbb{Z}}$。又因为$G \cong G'$，故$G' = h_1^{\mathbb{Z}}$也是循环群，故$g_1^{\mathbb{Z}} \cong h_1^{\mathbb{Z}}$。
- 设$k - 1$时结论成立。
- 在k的情况下，不失一般性，假设g_k是生成元集$\{g_1, \cdots, g_k\}$中级最大的元素，设$ord(g_k) = p^m$。设$\sigma : G \to G'$是同构映射。则$ord(\sigma(g_k)) = p^m$。假设生成元集$\{h_1, \cdots, h_s\}$中级最大的元素为h_s，其级为p^n。必有$n = m$（若$n < m$，则$\sigma(g_k) \in G'$不能用生成元集$\{h_1, \cdots, h_s\}$表示）。
- 不失一般性，设$ord(h_j) = ord(h_{j+1}) = \cdots = ord(h_s) = p^m$。

$$\sigma(g_k) = h_1^{l_1} h_2^{l_2} \cdots h_s^{l_s}. \tag{4}$$

则上式的$\{l_j, l_{j+1}, \cdots, l_s\}$中定存在一个元素不被$p$整除。否则$\sigma(g_k)$的级就会小于$p^m$。

有限p–群(交换群)

如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，现在用归纳法证明下面的结论：设$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$，$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$均为有限交换$p$–群，且$G \cong G'$，那么$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$。

- 当$k = 1$时，由于循环p–群不能再分解，所以$G = g_1^{\mathbb{Z}}$。又因为$G \cong G'$，故$G' = h_1^{\mathbb{Z}}$也是循环群，故$g_1^{\mathbb{Z}} \cong h_1^{\mathbb{Z}}$。
- 设$k - 1$时结论成立。
- 在k的情况下，不失一般性，假设g_k是生成元集$\{g_1, \cdots, g_k\}$中级最大的元素，设$ord(g_k) = p^m$。设$\sigma : G \to G'$是同构映射。则$ord(\sigma(g_k)) = p^m$。假设生成元集$\{h_1, \cdots, h_s\}$中级最大的元素为h_s，其级为p^n。必有$n = m$（若$n < m$，则$\sigma(g_k) \in G'$不能用生成元集$\{h_1, \cdots, h_s\}$表示）。
- 不失一般性，设$ord(h_j) = ord(h_{j+1}) = \cdots = ord(h_s) = p^m$。

$$\sigma(g_k) = h_1^{l_1} h_2^{l_2} \cdots h_s^{l_s}. \tag{4}$$

则上式的$\{l_j, l_{j+1}, \cdots, l_s\}$中定存在一个元素不被$p$整除。否则$\sigma(g_k)$的级就会小于$p^m$。

有限p–群(交换群)

如果$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}} = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$，现在用归纳法证明下面的结论：设$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \cdots \otimes g_k^{\mathbb{Z}}$，$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \cdots \otimes h_s^{\mathbb{Z}}$均为有限交换$p$–群，且$G \cong G'$，那么$k = s$且$g_i^{\mathbb{Z}} \cong h_i^{\mathbb{Z}}$。

- 当$k = 1$时，由于循环p–群不能再分解，所以$G = g_1^{\mathbb{Z}}$。又因为$G \cong G'$，故$G' = h_1^{\mathbb{Z}}$也是循环群，故$g_1^{\mathbb{Z}} \cong h_1^{\mathbb{Z}}$。
- 设$k - 1$时结论成立。
- 在k的情况下，不失一般性，假设g_k是生成元集$\{g_1, \cdots, g_k\}$中级最大的元素，设$ord(g_k) = p^m$。设$\sigma : G \to G'$是同构映射。则$ord(\sigma(g_k)) = p^m$。假设生成元集$\{h_1, \cdots, h_s\}$中级最大的元素为h_s，其级为p^n。必有$n = m$（若$n < m$，则$\sigma(g_k) \in G'$不能用生成元集$\{h_1, \cdots, h_s\}$表示）。
- 不失一般性，设$ord(h_j) = ord(h_{j+1}) = \cdots = ord(h_s) = p^m$。

$$\sigma(g_k) = h_1^{l_1} h_2^{l_2} \cdots h_s^{l_s}. \tag{4}$$

则上式的$\{l_j, l_{j+1}, \cdots, l_s\}$中定存在一个元素不被$p$整除。否则$\sigma(g_k)$的级就会小于$p^m$。

有限p–群(交换群)

- 不妨设$(l_s, p) = 1$，则$ord(\sigma(g_k)) = ord(h_s^{l_s})$，则

$$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}} \otimes \sigma(g_k)^{\mathbb{Z}}.$$

  同时，我们知道

$$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \ldots \otimes g_{k-1}^{\mathbb{Z}} \otimes g_k^{\mathbb{Z}}.$$

- 考虑商群

$$\overline{G} = G/ < g_k > \cong g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes g_{k-1}^{\mathbb{Z}}, \ \overline{G'} = G'/ < \sigma(g_k) > \cong h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}}$$

- 由于σ为同构映射，则$G/ < g_k > \cong G'/ < \sigma(g_k) >$，即

$$g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \ldots \otimes g_{k-1}^{\mathbb{Z}} \cong h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}}.$$

- 由归纳假设知$s - 1 = k - 1$，故$s = k$，且$h_i^{\mathbb{Z}} \cong g_i^{\mathbb{Z}}$，$i = 1, 2, \cdots, k - 1$。
- 同时$g_k^{\mathbb{Z}}$和$h_s^{\mathbb{Z}}$均为阶为p^m的循环群，故$g_k^{\mathbb{Z}} \cong h_s^{\mathbb{Z}}$。

有限p–群(交换群)

- 不妨设$(l_s, p) = 1$，则$ord(\sigma(g_k)) = ord(h_s^{l_s})$，则

$$G' = h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}} \otimes \sigma(g_k)^{\mathbb{Z}}.$$

同时，我们知道

$$G = g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \ldots \otimes g_{k-1}^{\mathbb{Z}} \otimes g_k^{\mathbb{Z}}.$$

- 考虑商群

$$\overline{G} = G/ < g_k > \cong g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes g_{k-1}^{\mathbb{Z}}, \quad \overline{G'} = G'/ < \sigma(g_k) > \cong h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}}$$

- 由于σ为同构映射，则$G/ < g_k > \cong G'/ < \sigma(g_k) >$，即

$$g_1^{\mathbb{Z}} \otimes g_2^{\mathbb{Z}} \otimes \ldots \otimes g_{k-1}^{\mathbb{Z}} \cong h_1^{\mathbb{Z}} \otimes h_2^{\mathbb{Z}} \otimes \ldots \otimes h_{s-1}^{\mathbb{Z}}.$$

- 由归纳假设知$s - 1 = k - 1$，故$s = k$，且$h_i^{\mathbb{Z}} \cong g_i^{\mathbb{Z}}$，$i = 1, 2, \cdots, k - 1$。
- 同时$g_k^{\mathbb{Z}}$和$h_s^{\mathbb{Z}}$均为阶为p^m的循环群，故$g_k^{\mathbb{Z}} \cong h_s^{\mathbb{Z}}$。

有限交换群的结构定理

Theorem 6.4

在有限交换群G可以惟一分解为阶为素数的幂的循环群的直积，即
设$|G| = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$，那么

1. $G = G_{11} \otimes \cdots \otimes G_{1s_1} \otimes G_{21} \otimes \cdots \otimes G_{22} \otimes G_{t1} \otimes G_{t_2} \otimes G_{t_{s_t}}$。其中$|G_{ij}| = p_i^{m_{ij}}$。
2. 自然数集$(p_1^{m_{1i}}, \cdots, p_1^{m_{1,s_1}}, \cdots, p_t^{m_{t1}}, \cdots, p_t^{m_{ts_t}})$由群$G$惟一确定。

乘法群$Z_N^*(N = pq)$的分解

设$N = pq$，其中p, q是素数且$p = 2p' + 1, q = 2q' + 1$。
则$\phi(N) = (p-1)(q-1) = 4p'q'$。设$p', q'$也为素数。

- $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$（加法群同构）。$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$（乘法群同构）。
- 定义映射$\theta_p : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$：$\theta_p(a) := a^2 \mod p$。则$\theta_p$是$\mathbb{Z}_p^*$上的自同态；定义模$p$的平方剩余$\mathbb{QR}_p$

$$\mathbb{QR}_p := \theta_p(\mathbb{Z}_p^*) = \{a' \mid \exists a \in \mathbb{Z}_p^*,\ a^2 = a' \mod p\}.$$

$$Ker(\theta_p) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_p \cong \mathbb{Z}_{p'}.$$

$$\mathbb{Z}_p^* = Ker(\theta_p) \otimes \mathbb{QR}_p$$

- 定义映射$\theta_q : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$：$\theta_q(b) := b^2 \mod q$。则$\theta_q$是$\mathbb{Z}_q^*$上的自同态；定义模$q$的平方剩余$\mathbb{QR}_q$

$$\mathbb{QR}_q := \theta_q(\mathbb{Z}_q^*) = \{a' \mid \exists a \in \mathbb{Z}_q^*,\ a^2 = a' \mod q\}.$$

$$Ker(\theta_q) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_q \cong \mathbb{Z}_{q'}.$$

$$\mathbb{Z}_q^* = Ker(\theta_q) \otimes \mathbb{QR}_q.$$

乘法群$Z_N^*(N = pq)$的分解

设$N = pq$，其中p, q是素数且$p = 2p' + 1, q = 2q' + 1$。
则$\phi(N) = (p-1)(q-1) = 4p'q'$。设$p', q'$也为素数。

- $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$（加法群同构）。$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$（乘法群同构）。
- 定义映射$\theta_p : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$：$\theta_p(a) := a^2 \mod p$。则$\theta_p$是$\mathbb{Z}_p^*$上的自同态；定义模$p$的平方剩余$\mathbb{QR}_p$

$$\mathbb{QR}_p := \theta_p(\mathbb{Z}_p^*) = \{a' \mid \exists a \in \mathbb{Z}_p^*,\ a^2 = a' \mod p\}.$$

$$Ker(\theta_p) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_p \cong \mathbb{Z}_{p'}.$$

$$\mathbb{Z}_p^* = Ker(\theta_p) \otimes \mathbb{QR}_p$$

- 定义映射$\theta_q : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$：$\theta_q(b) := b^2 \mod q$。则$\theta_q$是$\mathbb{Z}_q^*$上的自同态；定义模$q$的平方剩余$\mathbb{QR}_q$

$$\mathbb{QR}_q := \theta_q(\mathbb{Z}_q^*) = \{a' \mid \exists a \in \mathbb{Z}_q^*,\ a^2 = a' \mod q\}.$$

$$Ker(\theta_q) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_q \cong \mathbb{Z}_{q'}.$$

$$\mathbb{Z}_q^* = Ker(\theta_q) \otimes \mathbb{QR}_q.$$

乘法群$Z_N^*(N = pq)$的分解

设$N = pq$，其中p, q是素数且$p = 2p' + 1, q = 2q' + 1$。
则$\phi(N) = (p-1)(q-1) = 4p'q'$。设$p', q'$也为素数。

- $\mathbb{Z}_N \cong \mathbb{Z}_p \times \mathbb{Z}_q$（加法群同构）。$\mathbb{Z}_N^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$（乘法群同构）。
- 定义映射$\theta_p : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$：$\theta_p(a) := a^2 \mod p$。则$\theta_p$是$\mathbb{Z}_p^*$上的自同态；定义模$p$的平方剩余$\mathbb{QR}_p$

$$\mathbb{QR}_p := \theta_p(\mathbb{Z}_p^*) = \{a' \mid \exists a \in \mathbb{Z}_p^*,\ a^2 = a' \mod p\}.$$

$$Ker(\theta_p) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_p \cong \mathbb{Z}_{p'}.$$

$$\mathbb{Z}_p^* = Ker(\theta_p) \otimes \mathbb{QR}_p$$

- 定义映射$\theta_q : \mathbb{Z}_q^* \to \mathbb{Z}_q^*$：$\theta_q(b) := b^2 \mod q$。则$\theta_q$是$\mathbb{Z}_q^*$上的自同态；定义模$q$的平方剩余$\mathbb{QR}_q$

$$\mathbb{QR}_q := \theta_q(\mathbb{Z}_q^*) = \{a' \mid \exists a \in \mathbb{Z}_q^*,\ a^2 = a' \mod q\}.$$

$$Ker(\theta_q) = \{1, -1\} \cong \mathbb{Z}_2 \quad \mathbb{QR}_q \cong \mathbb{Z}_{q'}.$$

$$\mathbb{Z}_q^* = Ker(\theta_q) \otimes \mathbb{QR}_q.$$

乘法群$Z_N^*(N = pq)$的分解

设$N = pq$，其中p, q是素数且$p = 2p' + 1, q = 2q' + 1$。
则$\phi(N) = (p-1)(q-1) = 4p'q'$。设$p', q'$也为素数。

- 定义映射$\theta_N : \mathbb{Z}_N^* \to \mathbb{Z}_N^*$：$\theta_N(x) := x^2 \mod N$。则$\theta_N$是$\mathbb{Z}_N^*$上的自同态；定义模$N$的平方剩余$\mathbb{QR}_N$

$$\mathbb{QR}_N := \theta_N(\mathbb{Z}_N^*) = \{x' \mid \exists x \in \mathbb{Z}_N^*,\ x^2 = x' \mod N\}.$$

$$Ker(\theta_N) = \{1, -1, w, -w\} \cong K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

$$\mathbb{Z}_N^* = Ker(\theta_N) \otimes \mathbb{QR}_N = \langle -1 \rangle \otimes \langle w \rangle \otimes \mathbb{QR}_N.$$

Notes

- About automorphism: $f : G \to G$.
  $G = Ker(f) \otimes Img(f)$ iff $Img(f) = Img(f^2)$ and $Img(f) \trianglelefteq G$.
- About linear transformation over vector space. If $M_{n\times m}$ is a matrix over a field F, then

$$V^m = Ker(M) \oplus Img(M^T),\ V^n = Ker(M^T) \oplus Img(M).$$

- n次二面体群D_n 的生成元集为(a, b)，其中a为$2\pi/n$旋转，b为沿某中轴翻转。

$$D_n =< a, b >,\ \ a^n = b^2 = 1, ba = a^{-1}b.$$

1. $D_n =< a > \cdot < b >$;
2. $< a > \cap < b >= \{1\}$;
3. $< a > \trianglelefteq D_n$;
4. $< b > \trianglelefteq D_2$； $n > 2$, $< b > \ntrianglelefteq D_n$;
5. $n = 2$时, $D_2 =< a >=< b >$， $n > 2$时, $D_n \neq < a > \otimes < b >$。

作业(群II)

1. P.71 习题2-1：1，8，11，12，20，22
2. P.79 习题2-2：2，5，6，9，10，11
3. P.88 习题2-3：1，6，7，16，18，19
4. P.88 习题2-3：12, 20
5. P.104 习题2-5：1, 3, 4, 6
6. Group G acts on set X. Let $G(x)$ denote the stabilizer of $x \in X$. Prove: If $y = ax$ for $a \in G, x, y \in X$, then $G(y) = aG(x)a^{-1}$.
7. P.111 习题2-6：1, 2, 3, 4, 6
8. P.96 习题2-4：1, 3, 5, 7, 8, 14

1. Let G be a finite *abelian* group, show that $f : g \mapsto g^k$ is isomorphism iff $(k, |G|) = 1$.
2. Show that a group with order 145 is a cyclic group.