4-1 Groups

Jun Ma

majun@nju.edu.cn

2021 年 3 月 10 日

TJ 3-3

Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$.
How many elements are in each group?
Are the groups the same? Why or why not?

TJ 3-3

Symmetries of a rectangle

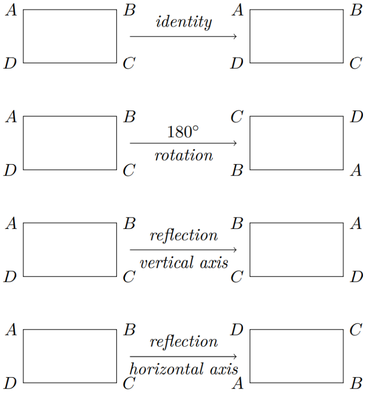

Figure 3.5: Rigid motions of a rectangle

sym	**id**	**180**	**v-ref**	**h-ref**
id	id	180	v-ref	h-ref
180	180	id	h-ref	v-ref
v-ref	v-ref	h-ref	id	180
h-ref	h-ref	v-ref	180	id

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Table 3.29: Addition table for $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$(\mathbb{Z}_4, +)$$

$+$	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

TJ 3-7

Let $S = \mathbb{R} \backslash \{-1\}$ and define a binary operation on S by
$a * b = a + b + ab$.
Prove that $(S, *)$ is an abelian group.

$(S, *)$ is a group

Let $a, b, c \in S$

- **Associative**: $a * (b * c) = (a * b) * c$

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \end{aligned}$$

$(S, *)$ is a group

- **Identity**: $e = 0$ is the identity

$$0 * a = 0 + a + 0a = a$$

$$a * 0 = a + 0 + a0 = a$$

$(S, *)$ is a group

- **Inverse**: for each $a \in S$, $\exists a^{-1}$ s.t. $a * a^{-1} = a^{-1} * a = 0$

$$\begin{aligned} a * \left(\tfrac{-a}{1+a}\right) &= a + \tfrac{-a}{1+a} + a\tfrac{-a}{1+a} \\ &= \tfrac{a+a^2-a-a^2}{1+a} \\ &= 0 \end{aligned}$$

$$\begin{aligned} \left(\tfrac{-a}{1+a}\right) * a &= \tfrac{-a}{1+a} + a + \tfrac{-a}{1+a}a \\ &= \tfrac{-a+a+a^2-a^2}{1+a} \\ &= 0 \end{aligned}$$

$(S, *)$ is an abelian group

- **Communicative**: $a * b = b * a$

$$a * b = a + b + ab = b + a + ba = b * a$$

TJ 3-39

Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.
Hint: $\mathbb{C}^*$: the multiplicative group of nonzero complex numbers.

TJ 3-39

Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.
Hint: $\mathbb{C}^*$: the multiplicative group of nonzero complex numbers.

Proposition 3.31. *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

TJ 3-39

Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.
Hint: $\mathbb{C}^*$: the multiplicative group of nonzero complex numbers.

Proposition 3.31. *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

Obviously, $1 \in \mathbb{T}$ and $\mathbb{T} \neq \emptyset$

TJ 3-39

Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.
Hint: $\mathbb{C}^*$: the multiplicative group of nonzero complex numbers.

Proposition 3.31. *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

Obviously, $1 \in \mathbb{T}$ and $\mathbb{T} \neq \emptyset$

Let $a, b \in \mathbb{T}$, $|a| = |b| = 1$
Then $1 = |a| = |a(b^{-1}b)| = |(ab^{-1})b| = |ab^{-1}||b|$
So, $|ab^{-1}| = 1$, $ab^{-1} \in \mathbb{T}$

TJ 3-42

Let G be the group of 2»2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

Prove that H is a subgroup of G.

TJ 3-42

Let G be the group of 2»2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

Prove that H is a subgroup of G.

Proposition 3.30. *A subset H of G is a subgroup if and only if it satisfies the following conditions.*

1. *The identity e of G is in H.*
2. *If $h_1, h_2 \in H$, then $h_1h_2 \in H$.*
3. *If $h \in H$, then $h^{-1} \in H$.*

TJ 3-42

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

证明.

- Obviously, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in H$

TJ 3-42

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

证明.

- Obviously, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in H$
- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, $\begin{pmatrix} u & v \\ w & x \end{pmatrix} \in H$. So, $a + d = u + x = 0$; then, $a + u + d + x = 0$,
  i.e. $\begin{pmatrix} a+u & b+v \\ c+w & d+x \end{pmatrix} \in H$

TJ 3-42

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}$$

证明.

- Obviously, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in H$
- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, $\begin{pmatrix} u & v \\ w & x \end{pmatrix} \in H$. So, $a + d = u + x = 0$; then, $a + u + d + x = 0$,
  i.e. $\begin{pmatrix} a+u & b+v \\ c+w & d+x \end{pmatrix} \in H$
- Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. As $a + d = 0$, $-a + -d = 0$. Therefore, $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \in H$

TJ 4-49

Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

TJ 4-49

Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

证明.

$$ba = a^4b = (a^3a)b = a^3(ab) = e(ab) = ab$$

□

TJ 3-54

Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup of G.

TJ 3-54

Let H be a subgroup of G. If $g \in G$, show that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is also a subgroup of G.

Proposition 3.31. *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

$$\boxed{gHg^{-1} \neq \emptyset}$$

$$\boxed{gHg^{-1} \neq \emptyset}$$

证明.

$$\text{As } e \in H,\ geg^{-1} = e \in gHg^{-1}.$$

□

$\boxed{\text{Let } a, b \in gHg^{-1}\text{, then } ab^{-1} \in gHg^{-1}}$

$$\boxed{\text{Let } a, b \in gHg^{-1}, \text{ then } ab^{-1} \in gHg^{-1}}$$

证明.

- Assume $a = gxg^{-1}$ and $b = gyg^{-1}$, where $x, y \in H$
- $$\begin{aligned} ab^{-1} &= (gxg^{-1})(gyg^{-1})^{-1} \\ &= (gxg^{-1})(gy^{-1}g^{-1}) \\ &= gxg^{-1}gy^{-1}g^{-1} \\ &= gxy^{-1}g^{-1} \end{aligned}$$

  $y \in H \Rightarrow y^{-1} \in H$. Then $xy^{-1} \in H$. So, $gxy^{-1}g^{-1} \in H$.

□

TJ 4-1

Prove or disprove each of the following statements.

(a) All of the generators of $\mathbb{Z}_{60}$ are prime.

(b) $U(8)$ is cyclic.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of subgroups is finite.

(a)

$\boxed{\text{All of the generators of } \mathbb{Z}_{60} \text{ are prime?}}$

(a)

$\boxed{\text{All of the generators of } \mathbb{Z}_{60} \text{ are prime?}}$ ✗

(a)

$\boxed{\text{All of the generators of } \mathbb{Z}_{60} \text{ are prime?}}$ ✗

Corollary 4.14. *The generators of* $\mathbb{Z}_n$ *are the integers* r *such that* $1 \leq r < n$ *and* $\gcd(r, n) = 1$.

(a)

$\boxed{\text{All of the generators of } \mathbb{Z}_{60} \text{ are prime?}}$ ✗

Corollary 4.14. *The generators of* $\mathbb{Z}_n$ *are the integers* r *such that* $1 \leq r < n$ *and* $\gcd(r, n) = 1$.

49?

(b)

$\boxed{U(8) \text{ is cyclic?}}$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 3.12: Multiplication table for $U(8)$

(b)

$$\boxed{U(8) \text{ is cyclic?}}$$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 3.12: Multiplication table for $U(8)$

- $|1| = 1$
- $|3| = |5| = |7| = 2$

(b)

$\boxed{U(8) \text{ is cyclic?}}$ ✗

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 3.12: Multiplication table for $U(8)$

- $|1| = 1$
- $|3| = |5| = |7| = 2$

(c)

$$\boxed{\mathbb{Q} \text{ is cyclic?}}$$

(c)

$\boxed{\mathbb{Q} \text{ is cyclic?}}$

- $(\mathbb{Q}, +)$: ✗
  - Identity: 0
  - Inverse: $-a$

(c)

$\boxed{\mathbb{Q} \text{ is cyclic?}}$

- $(\mathbb{Q}, +)$: ✗
  - Identity: 0
  - Inverse: $-a$
- $(\mathbb{Q}, *)$: ✗
  - Identity: 1
  - Inverse: $1/a$? If $a = 0$?
  - $(\mathbb{Q}, *)$ is not a group!

(d)

$\boxed{\text{If every proper subgroup of a group } G \text{ is cyclic, then } G \text{ is a cyclic group?}}$

(d)

If every proper subgroup of a group G is cyclic, then G is a cyclic group?

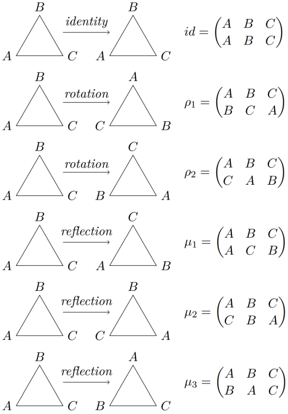

Figure 3.6: Symmetries of a triangle

S_3

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Table 3.7: Symmetries of an equilateral triangle

(d)

If every proper subgroup of a group G is cyclic, then G is a cyclic group? ✗

Example 4.7. Not every group is a cyclic group. Consider the symmetry group of an equilateral triangle S_3. The multiplication table for this group is Table 3.7. The subgroups of S_3 are shown in Figure 4.8. Notice that every subgroup is cyclic; however, no single element generates the entire group.

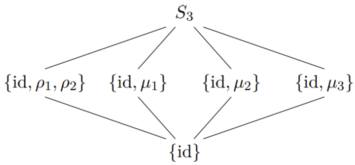

Figure 4.8: Subgroups of S_3

(e)

$\boxed{\text{A group with a finite number of subgroups is finite?}}$

(e)

$\boxed{\text{A group with a finite number of subgroups is finite?}}$

$$\Downarrow$$

$\boxed{\text{An infinite group has infinite number of subgroups}}$

引理-1

引理 (1)

Any group is a union of its cyclic subgroups.

证明.

For any $a \in G$, $\langle a \rangle$ is a subgroup of G $\square$

引理-2

引理 (2)

An infinite cyclic group has infinitely many (cyclic) subgroups.

证明.

- Let a be the generator of G
- Then $\left\langle a^k \right\rangle$ is a cyclic subgroup of G, for $k = 1, 2, \cdots$

□

$\boxed{\text{An infinite group has infinite number of subgroups}}$

An infinite group has infinite number of subgroups

证明.

Let G be an infinite group.

An infinite group has infinite number of subgroups

证明.

Let G be an infinite group.

- G is the union of all its cyclic subgroups. (引理-1)

An infinite group has infinite number of subgroups

证明.

Let G be an infinite group.

- G is the union of all its cyclic subgroups. (引理-1)
- If G has finite number of cyclic subgroups, there must be at least one subgroup H which is **infinite**; Otherwise, G cannot be infinite.

An infinite group has infinite number of subgroups

证明.

Let G be an infinite group.

- G is the union of all its cyclic subgroups. (引理-1)
- If G has finite number of cyclic subgroups, there must be at least one subgroup H which is **infinite**; Otherwise, G cannot be infinite.
- As H is cyclic, H has infinitely many cyclic subgourps.(引理-2)

An infinite group has infinite number of subgroups

证明.

Let G be an infinite group.

- G is the union of all its cyclic subgroups. (引理-1)
- If G has finite number of cyclic subgroups, there must be at least one subgroup H which is **infinite**; Otherwise, G cannot be infinite.
- As H is cyclic, H has infinitely many cyclic subgourps.(引理-2)
- Subgroups of H must be subgruops of G, so G has infinitely many subgroups.

$\square$

Another Problem

$\boxed{\text{How many generators does an infinite cyclic group have?}}$

How many generators does an infinite cyclic group have?

Only 2

Another Problem

How many generators does an infinite cyclic group have?

Only 2

证明.

- If $G = \langle a \rangle = \langle b \rangle$ then $b = a^n$ for some n and $a = b^m$ for some m.

Another Problem

How many generators does an infinite cyclic group have?

Only 2

证明.

- If $G = \langle a \rangle = \langle b \rangle$ then $b = a^n$ for some n and $a = b^m$ for some m.
- Therefore $a = b^m = (a^n)^m = a^{nm}$

How many generators does an infinite cyclic group have?

Only 2

证明.

- If $G = \langle a \rangle = \langle b \rangle$ then $b = a^n$ for some n and $a = b^m$ for some m.
- Therefore $a = b^m = (a^n)^m = a^{nm}$
- Since G is an infinite cyclic group, $nm = 1$, which has only two solutions $(1, 1)$ and $(-1, -1)$.

Another Problem

$\boxed{\text{How many generators does an infinite cyclic group have?}}$

Only 2

证明.

- If $G = \langle a \rangle = \langle b \rangle$ then $b = a^n$ for some n and $a = b^m$ for some m.
- Therefore $a = b^m = (a^n)^m = a^{nm}$
- Since G is an infinite cyclic group, $nm = 1$, which has only two solutions $(1, 1)$ and $(-1, -1)$.
- So, $b = a$ or $b = a^{-1}$.

□

TJ 4-12

(a) Find a cyclic group with exactly one generator.
$\mathbb{Z}_1$: 0
$\mathbb{Z}_2$: 1

(b) Can you find cyclic groups with exactly two generators?
$\mathbb{Z}_3$:1,2
$\mathbb{Z}_4$:1,3
$\mathbb{Z}_6$:1,5
$\mathbb{Z}$:1,-1

(c) Four generators?
$\mathbb{Z}_5$: 1,2,3,4
$\mathbb{Z}_8$: 1,3,5,7
$\mathbb{Z}_{10}$: 1,3,7,9

(d) How about n generators?

How about n generators?

How about n generators?

- **Case 1:** $n > 2$ and n is **odd**. Impossible!!!
  - If a is a generator, then a^{-1} must be a generator other than a.

How about n generators?

- **Case 1:** $n > 2$ and n is **odd**. Impossible!!!
  - If a is a generator, then a^{-1} must be a generator other than a.
- **Case 2:** n is **even**. $\mathbb{Z}_m$, where $m = \varphi(n)$

Euler φ-function

The Euler φ-function is the map $\varphi : \mathbb{N} \to \mathbb{N}$ defined by $\varphi(n) = 1$ for $n = 1$, and, for $n > 1$, $\varphi(n)$ is the number of positive integers m with $1 \leq m < n$ and $gcd(m, n) = 1$.

TJ 4-24

Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

TJ 4-24

Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

How many r are there satisfying $0 \leq r < pq$, and $GCD(pq, r) = 1$?

TJ 4-24

Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

How many r are there satisfying $0 \leq r < pq$, and $GCD(pq, r) = 1$?
Answer: $pq - (p-1) - (q-1) - 1 = pq - p - q + 1$

$$\begin{array}{cc} p & q \\ 2p & 2q \\ \cdots & \cdots \\ (q-1)p & (p-1)q \\ qp & pq \end{array}$$

$$\varphi(p)\varphi(q) = (p-1)(q-1) = pq - p - q + 1$$

TJ 4-32

Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $gcd(k, n) = 1$, then y must be a generator of G.

TJ 4-32

Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $gcd(k, n) = 1$, then y must be a generator of G.

Theorem 4.13. *Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.*

TJ 4-32

Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $gcd(k, n) = 1$, then y must be a generator of G.

Theorem 4.13. *Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where $d = \gcd(k, n)$.*

So, the order of y is $n/gcd(k, n) = n$, i.e. y is a generator of G.

Z_p

证明：设 p 为素数，则 $Z_p = \{1, 2, ..., p-1\}$ 关于 p **乘法**构成的 $p-1$ 阶循环群。（此处的 $1, 2, ..., p-1$ 是模 p 等价类的代表元）

Z_p^* is an (abelian) group

- **Associative**: Obviously.
- **Identity**: $1 \in Z_p$.
- **Inverse**: for any $a \in Z_p$, $ax = 1 \bmod p$ has an unique root.
- **Abelian**: Obviously.

Z_p^* is cyclic?

引理 (1)

Let $a \in G$, with $|a| = n$, Then, for any $k|n$, there exists a $c \in G$ with $|c| = k$.

Z_p^* is cyclic?

引理 (1)

Let $a \in G$*, with* $|a| = n$*, Then, for any* $k|n$*, there exists a* $c \in G$ *with* $|c| = k$*.*

证明.

Let $c = a^{n/k}$ □

Z_p^* is cyclic?

引理 (2)

Let $a, b \in G$, *with* $|a| = n$, $|b| = m$, *and* $\gcd(n, m) = 1$. *Then, there exists a* $c \in G$ *with* $|c| = nm$.

Z_p^* is cyclic?

引理 (2)

Let $a, b \in G$, *with* $|a| = n$, $|b| = m$, *and* $\gcd(n, m) = 1$. *Then, there exists a* $c \in G$ *with* $|c| = nm$.

证明.

- $(ab)^{nm} = (a^n)^m (b^m)^n = 1^m 1^n = 1$. ($G$ is abelian).
- Let $|ab| = k$, then $k|nm$. $(ab)^k = 1 \Rightarrow a^k b^k = 1 \Rightarrow a^k = b^{-k}$.
- Then, $(a^k)^m = (b^{-k})^m \Rightarrow a^{mk} = 1$. Thus, $n|mk$.
- However, as $\gcd(n, m) = 1$, we have $n|k$.
- Similarly, $m|k$.
- So, $nm|k$. And finally $nm = k$

□

Z_p^* is cyclic?

引理 (3)

Let $a, b \in G$, *with* $|a| = n$, $|b| = m$. *Then, there exists a* $c \in G$ *with* $|c| = lcm(n, m)$.

Z_p^* is cyclic?

引理 (3)

Let $a, b \in G$, with $|a| = n$, $|b| = m$. Then, there exists a $c \in G$ with $|c| = lcm(n, m)$.

证明.

- By lemma(1), there exists $c_1, c_2, c_3 \in G$ with

$$|c_1| = \gcd(n, m); |c_2| = \frac{n}{\gcd(n, m)}; |c_3| = \frac{m}{\gcd(n, m)}$$

Z_p^* is cyclic?

引理 (3)

Let $a, b \in G$, with $|a| = n$, $|b| = m$. Then, there exists a $c \in G$ with $|c| = lcm(n, m)$.

证明.

- By lemma(1), there exists $c_1, c_2, c_3 \in G$ with

$$|c_1| = \gcd(n, m); |c_2| = \frac{n}{\gcd(n, m)}; |c_3| = \frac{m}{\gcd(n, m)}$$

- $|c_1|, |c_2|, |c_3|$ are co-primes, by lemma(2), there exists a $c \in G$, s.t.

$$|c| = \gcd(n, m)\frac{n}{\gcd(n, m)}\frac{m}{\gcd(n, m)} = \frac{nm}{\gcd(n, m)}$$

□

Z_p^* is cyclic?

引理 (4)

For $d|p-1$, $x^d - 1 = 0$ *has exactly* d *roots in* Z_p^*.

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))
- As Z_p^* is **not cyclic**, d must be a strict divisor of $p-1$.

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))
- As Z_p^* is **not cyclic**, d must be a strict divisor of $p-1$.
- For every $i \in G$, we have:

$$i^d - 1 = (i^{m_i})^{d/m_i} - 1 = 1^{d/m_i} - 1 = 0$$

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))
- As Z_p^* is **not cyclic**, d must be a strict divisor of $p-1$.
- For every $i \in G$, we have:

$$i^d - 1 = (i^{m_i})^{d/m_i} - 1 = 1^{d/m_i} - 1 = 0$$

- So, every $i \in G$ is a root of $x^d - 1 = 0$. Totally, $p-1$ roots.

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))
- As Z_p^* is **not cyclic**, d must be a strict divisor of $p-1$.
- For every $i \in G$, we have:

$$i^d - 1 = (i^{m_i})^{d/m_i} - 1 = 1^{d/m_i} - 1 = 0$$

- So, every $i \in G$ is a root of $x^d - 1 = 0$. Totally, $p-1$ roots.
- $x^d - 1 = 0$ would have exactly d roots (by Lemma(5))

Z_p^* is cyclic?

- Assume $G = Z_p^*$ is **not cyclic**.
- Assume $|i| = m_i$ for $i \in \{1, 2, \cdots, p-1\}$, let $d = lcm(m_1, m_2, \cdots, m_{p-1})$
- There is a $c \in G$ with $|c| = d$. (by Lemma(3))
- As Z_p^* is **not cyclic**, d must be a strict divisor of $p-1$.
- For every $i \in G$, we have:

$$i^d - 1 = (i^{m_i})^{d/m_i} - 1 = 1^{d/m_i} - 1 = 0$$

- So, every $i \in G$ is a root of $x^d - 1 = 0$. Totally, $p-1$ roots.
- $x^d - 1 = 0$ would have exactly d roots (by Lemma(5))
- As d is a strict divisor of $p-1$, $d < p-1$. **Contradiction!**


Thank
You!