Mathematics for Computer Science – Group, Subgroup and Cyclic Group

Libin Wang

Shool of Computer Science, South China Normal University

April 2, 2025

Table of contents

Motivation.

抽象.

抽象：发现已知的世界中事物的共性与区别，忽略掉某些细节，得到一种更通用、更宽泛、可以描述更广阔世界的框架或语言，从而探求未知世界的知识。

Motivation.

抽象.

抽象：发现已知的世界中事物的共性与区别，忽略掉某些细节，得到一种更通用、更宽泛、可以描述更广阔世界的框架或语言，从而探求未知世界的知识。

Question.

更给出（或找出）更适合你自己的“抽象”的定义。

Motivation.

重新审视“消去律”.

In last chapter, we extremely rely on *Cancellation Law*.
If $\gcd(c, m) = 1$ and $ac \equiv bc \pmod{m}$, then

$$a \equiv b \pmod{m}.$$

Motivation.

重新审视“消去律”.

In last chapter, we extremely rely on *Cancellation Law*.
If $\gcd(c, m) = 1$ and $ac \equiv bc \pmod{m}$, then

$$a \equiv b \pmod{m}.$$

Question.

Actually, what is cancellation?

Motivation.

Ideas.

From $ac \equiv bc \pmod{m}$ to $a \equiv b \pmod{m}$, seemingly, we need division, actually we need multiplication:

$$acc^{-1} \equiv bcc^{-1} \pmod{m}.$$

Hence by $cc^{-1} \equiv 1 \pmod{m}$, we have

$$a \equiv b \pmod{m}.$$

Why c^{-1} exists? Because of $\gcd(c, m) = 1$!

Motivation.

Additional conditions.

Need more conditions?

Motivation.

Additional conditions.

Need more conditions?

Yes, we need *association*:

$$(ac)c^{-1} \equiv a(cc^{-1}) \pmod{m},$$

and *closure*, which means we only consider numbers from 1 to $m-1$.

Motivation.

Additional conditions.

Need more conditions?

Yes, we need *association*:

$$(ac)c^{-1} \equiv a(cc^{-1}) \pmod{m},$$

and *closure*, which means we only consider numbers from 1 to $m-1$.

Question.

什么数学操作不满足结合律?

Motivation.

Wrap up.

Wrap these up. For a set $\mathbb{G}$ and an operator $\cdot$ on the elements, we need:

- *Closure*: $\forall a, b \in \mathbb{G}, \quad a \cdot b \in \mathbb{G}$.
- *Association*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- An element "1" called *identity*, s.t. $1 \cdot a = a \cdot 1 = a$.
- $\forall a \in G$, there exists $a^{-1} \in G$, such that $a \cdot a^{-1} = 1 = a^{-1}a$, called *inverse*.

Group（群）.

Definition.

Definition(Group). A group is a set $\mathbb{G}$ and an operator $\cdot$ on the elements, satisfies the following axioms:

- *Closure(封闭性)*: $\forall a, b \in \mathbb{G}, \quad a \cdot b \in \mathbb{G}$.
- *Association(结合律)*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- There is an element "$e \in \mathbb{G}$" called *identity(单位元)*, s.t. $e \cdot a = a \cdot e = a$.
- $\forall a \in G$, there exists $a^{-1} \in G$ called *inverse(逆元)*, such that $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Examples of groups.

Groups.

- $(\mathbb{Z}, +)$ is a group, while $(\mathbb{Z}, \times)$ is not a group.
- $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are groups.
- $(\mathbb{Q}^*, \times)$ and $(\mathbb{R}^*, \times)$ are groups.

Examples of groups.

Groups.

- $(\mathbb{Z}, +)$ is a group, while $(\mathbb{Z}, \times)$ is not a group.
- $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are groups.
- $(\mathbb{Q}^*, \times)$ and $(\mathbb{R}^*, \times)$ are groups.

Check.

Please check and know why.

Examples of some important groups.

$\mathbb{Z}_n$

Let n be an integer, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ forms a group under the operation of addition. However, $(\mathbb{Z}_n, \times)$ is not a group.

Examples of some important groups.

$\mathbb{Z}_n$

Let n be an integer, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ forms a group under the operation of addition. However, $(\mathbb{Z}_n, \times)$ is not a group.

$\mathbb{Z}_p^*$

Let p be a prime number, $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ forms a group under the operation of multiplication. (Recall Fermat's Little Theorem.)

Examples of some important groups.

$\mathbb{Z}_n$

Let n be an integer, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ forms a group under the operation of addition. However, $(\mathbb{Z}_n, \times)$ is not a group.

$\mathbb{Z}_p^*$

Let p be a prime number, $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ forms a group under the operation of multiplication. (Recall Fermat's Little Theorem.)

$\mathbb{Z}_n^*$

Let n be an integer, $\mathbb{Z}_n^* = \{a \in [1..n-1] \text{ and } gcd(a, n) = 1\}$ forms a group under the operation of multiplication. (Recall Euler's Theorem.)

An important group: nth root of unity.

Example

设 n 为正整数，称方程 $z^n = 1$ 在复数上的所有解为 n 次单位根，记为 $\mathbb{U}_n = \{z^n = 1, z \in \mathbb{C}\}$。根据高等数学相关知识可知，$\mathbb{U}_n = \{e^{\frac{2\pi ik}{n}}, k = 0, 1, \cdots, n-1\}$，并且

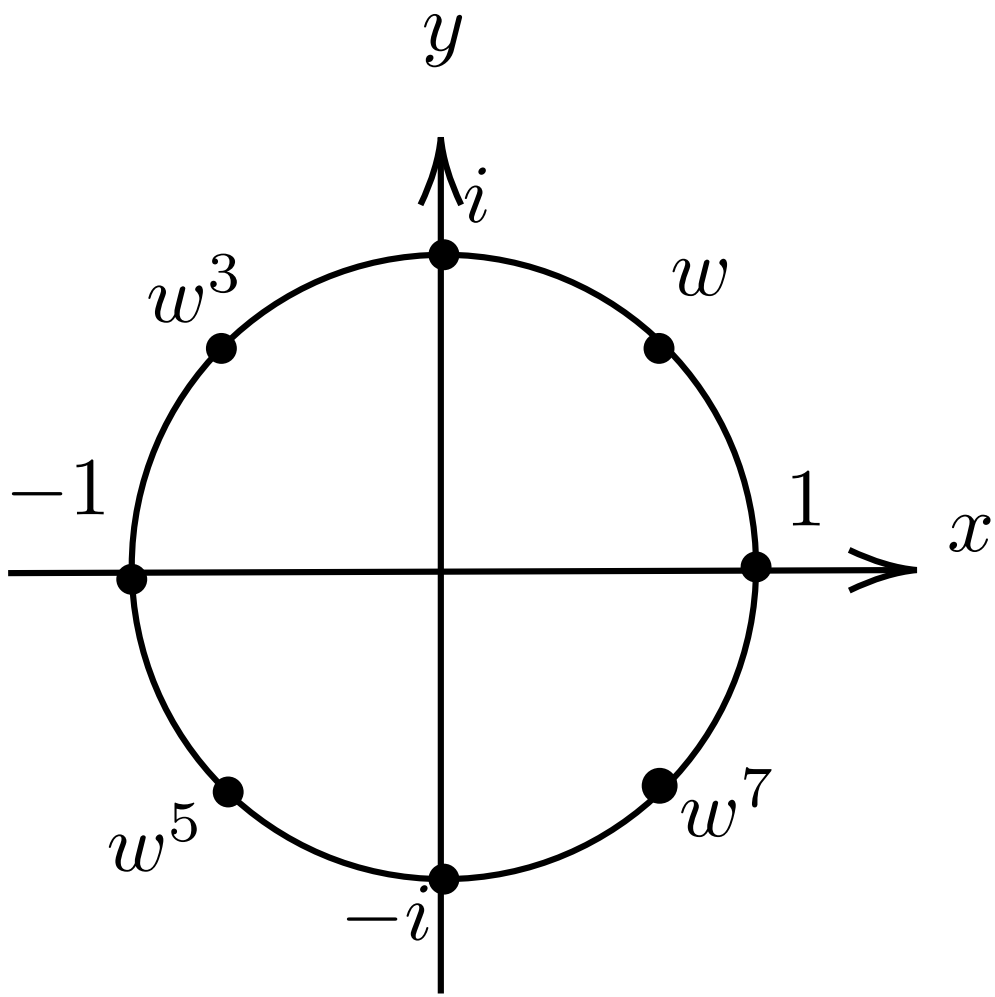
$$e^{\frac{2\pi ik}{n}} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}), k = 0, 1, \cdots, n-1$$

如果记 $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$，则可更简洁地表示 n 次单位根为

$$\mathbb{U}_n = \{\omega^i, i = 0, 1, \cdots, n-1\}$$

可证明 $\mathbb{U}_n$ 在复数的乘法上形成群 (这是课后习题)，并称 $\mathbb{U}_n$ 为 n 次*单位根群*。

8th root of unity.



思考

Thinking.

$\mathbb{Z}_n$ 与 $\mathbb{U}_n$ 的操作行为很类似吗？这会意味什么呢？另外，$\mathbb{U}_n$ 的操作行为与 $\mathbb{Z}_p^*$ 不很类似，是吗？

Basic Properties of Groups.

Proposition

Proposition 1. The identity element in a group $\mathbb{G}$ is unique; that is, there exists only one element $e \in \mathbb{G}$ s.t. $eg = ge = g$ for all $g \in \mathbb{G}$.

Basic Properties of Groups.

Proposition

Proposition 1. The identity element in a group $\mathbb{G}$ is unique; that is, there exists only one element $e \in \mathbb{G}$ s.t. $eg = ge = g$ for all $g \in \mathbb{G}$.

Proof.

Suppose $\exists e, e' \in \mathbb{G}$ are identities. Then:

- $ee' = e'$
- $ee' = e$

Combining these two equations, we have $e = ee' = e'$. □

Proposition 2.

Proposition

Proposition 2. If $\forall g \in \mathbb{G}$, then the inverse of g, g^{-1}, is unique.

Proof.

如果 g^{-1} 和 g' 都是 g 的逆元，则有

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Proposition 3.

Proposition

Proposition 3. Let $\mathbb{G}$ be a group. If $a, b \in \mathbb{G}$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

By construction.

- $ab(b^{-1}a^{-1}) = e$.
- $(b^{-1}a^{-1})ab = e$.

Combining these two equations, we know, the inverse of (ab) is $b^{-1}a^{-1}$. □

Proposition 4.

Proposition

Proposition 4. Let $\mathbb{G}$ be a group, $\forall g \in \mathbb{G}$, $(g^{-1})^{-1} = g$.

Proposition 4.

Proposition

Proposition 4. Let $\mathbb{G}$ be a group, $\forall g \in \mathbb{G}$, $(g^{-1})^{-1} = g$.

Proof.

By definition, $gg^{-1} = e$ and $g^{-1}(g^{-1})^{-1} = e$. Hence:

$$(g^{-1})^{-1} = (gg^{-1})(g^{-1})^{-1} = g(g^{-1}(g^{-1})^{-1}) = ge = g.$$

Proposition 4.

Proposition

Proposition 4. Let $\mathbb{G}$ be a group, $\forall g \in \mathbb{G}$, $(g^{-1})^{-1} = g$.

Proof.

By definition, $gg^{-1} = e$ and $g^{-1}(g^{-1})^{-1} = e$. Hence:

$$(g^{-1})^{-1} = (gg^{-1})(g^{-1})^{-1} = g(g^{-1}(g^{-1})^{-1}) = ge = g.$$

□

另一种思路.

该命题要证明的是 g^{-1} 的逆元是 g。根据 g^{-1} 的定义，“交换” g 与 g^{-1} 的位置，即得!

Proposition 5.

Proposition

Proposition 5. Let $\mathbb{G}$ be a group, for any two elements $a, b \in \mathbb{G}$. Then the equation $ax = b$ and $xa = b$ have unique solutions in $\mathbb{G}$.

Proposition 5.

Proposition

Proposition 5. Let $\mathbb{G}$ be a group, for any two elements $a, b \in \mathbb{G}$. Then the equation $ax = b$ and $xa = b$ have unique solutions in $\mathbb{G}$.

Proof.

- Existence. Such an x exists.
- Uniqueness. Suppose that x_1 and x_2 are both solutions.....

Left as an exercise. □

Proposition 6.

Proposition

Cancellation Law. Let $\mathbb{G}$ *be a group, and* $a, b, c \in \mathbb{G}$. *Then* $ba = ca$ *implies* $b = c$ *and* $ab = ac$ *implies* $b = c$.

Proposition 6.

Proposition

Cancellation Law. Let $\mathbb{G}$ be a group, and $a, b, c \in \mathbb{G}$. Then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Proof.

Left as an exercise. □

Proposition 6.

Proposition

Cancellation Law. Let $\mathbb{G}$ be a group, and $a, b, c \in \mathbb{G}$. Then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

Proof.

Left as an exercise. □

A little thought.

Where does "*Cancellation Law*" come from?

思考一.

置换与消去律

在费尔马小定理和欧拉定理的证明中，依赖消去律可得：
对任意素数 p 和与 p 互素的正整数 a，
$\mathbb{Z}_p^* = a\mathbb{Z}_p^* = \{ai : \forall i \in \mathbb{Z}_p^*\}$;
对任意合数 n 和与 n 互素的正整数 a，$a\mathbb{Z}_n^* = \mathbb{Z}_n^*$。
请问，对任意的群 $\mathbb{G}$ 和群元 a，是否有
$\mathbb{G} = a\mathbb{G} = \{ag : \forall g \in \mathbb{G}\}$? 为什么?

思考二.

逆元的唯一性源自什么?

回忆，模 n 的乘法逆元源自 Bezout 定理，然后我们分析过为什么乘法逆元唯一。请问，对任意的群 $\mathbb{G}$，我们也有“逆元唯一”的结论，此时，逆元唯一源自于什么？这样的思考能给我们什么启发?

Notations.

Let $\mathbb{G}$ be a group, and $g \in \mathbb{G}$. For $n \in \mathbb{N}$.

Notations.

- $g^0 = e$
- $g^n = \underbrace{g \cdot g \cdots g}_{\text{n times}}$
- $g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{\text{n times}}$

Order.

The order of a finite group is the number of elements that it contains. If $\mathbb{G}$ is a group containing n elements, we write $|\mathbb{G}| = n$.

Defintions

Definition

(Subgroup.)（子群）
Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subset of $\mathbb{G}$. If $\mathbb{H}$ is a group under group operation in $\mathbb{G}$, then $\mathbb{H}$ is said to be a subgroup of $\mathbb{G}$, denoted by $\mathbb{H} \leq \mathbb{G}$.

Examples of Subgroup.

Examples of Subgroup.

- For any group $\mathbb{G}$, there is a trivial subgroup $\{e\}$.
- The additive groups: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
- $\forall n \in \mathbb{Z}$, $n\mathbb{Z} = \{kn | k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

Examples of Subgroup.

Subgroup of $\mathbb{Z}_p^*$.

Let p be a prime, for all $i \in \mathbb{Z}_p^*$, compute $i^2 \bmod p$, form a set $\mathbb{S} = \{i^2 \bmod p, \forall i \in \mathbb{Z}_p^*\}$. Check that $\mathbb{S}$ is a group under the operation of multiplication, namely $\mathbb{S}$ is a subgroup of $\mathbb{Z}_p^*$. What is the order of $\mathbb{S}$?

Properties of Subgroup.

Exercise.

Write a program to play with $\mathbb{Z}_n^*$.

- Given an integer n, construct the multiplicative group $\mathbb{Z}_n^*$;
- Find a subgroup of the group $\mathbb{Z}_n^*$;
- Find a relation between the size of subgroup and the size of $\mathbb{Z}_n^*$.

Properties of subgroup.

Proposition

(Subgroup.) A nonempty subset $\mathbb{H}$ of a group $\mathbb{G}$ is a subgroup of $\mathbb{G}$ if and only if $\mathbb{H} \neq \emptyset$, and $ab^{-1} \in \mathbb{H}$ for all $a, b \in \mathbb{H}$.

Proof.

Two directions. The $\rightarrow$ part is easy. For $\leftarrow$ part, you need to check that $\mathbb{H}$ satisfies all the axioms of a group. $\square$

子群判定方法.

有多少种判定子群的方法?

给定群 $\mathbb{G}$ 和其子集 $\mathbb{H}$，如何判断 $\mathbb{H}$ 是否 $\mathbb{G}$ 的子群?

- 验证四条群公理.
- 命题 6.8：封闭性、有逆元.
- 命题 6.9：$\mathbb{H} \neq \emptyset$, and $ab^{-1} \in \mathbb{H}$ for all $a, b \in \mathbb{H}$.
- 命题 6.10：针对有限群，只需要验证封闭性.

子群判断.

练习题.

- 证明：任意群 $\mathbb{G}$ 的两个子群的交集也是群 $\mathbb{G}$ 的子群。
- 证明或证伪：任意群 $\mathbb{G}$ 的两个子群的并集也是群 $\mathbb{G}$ 的子群。
- $\mathbb{G}$ 是阿贝尔群，$\mathbb{H}$ 和 $\mathbb{K}$ 是 $\mathbb{G}$ 的子群。请证明 $\mathbb{HK} = \{hk : h \in \mathbb{H}, k \in \mathbb{K}\}$ 是群 $\mathbb{G}$ 的子群。如果 $\mathbb{G}$ 不是阿贝尔群，结论是否依然成立?
- 设 $\mathbb{G}$ 是阿贝尔群，m 是任意整数，记 $\mathbb{G}^m = \{g^m : g \in \mathbb{G}\}$。请证明 $\mathbb{G}^m$ 是 $\mathbb{G}$ 的一个子群。
- 设 $\mathbb{G}$ 是阿贝尔群，m 是任意整数，记 $\mathbb{G}[m] = \{g \in \mathbb{G} : g^m = e\}$。请证明 $\mathbb{G}[m]$ 是 $\mathbb{G}$ 的一个子群。

习题.

证明题.

证明：阿贝尔群 $\mathbb{G}$ 中的有限阶元素形成子群。该子群有一个特殊的名字，称为*挠子群*（*Torsion Subgroup*）。

Cyclic Groups（循环群）.

Example of cyclic group.

Consider the following computation: Choose a number g from Z_p^* randomly, p is a prime, and compute:

$$\mathbb{S} = \{g, g^2, g^3, \cdots, g^j, \cdots\}$$

Cyclic Groups（循环群）.

Example of cyclic group.

Consider the following computation: Choose a number g from Z_p^* randomly, p is a prime, and compute:

$$\mathbb{S} = \{g, g^2, g^3, \cdots, g^j, \cdots\}$$

Questions:

- May $\mathbb{S}$ be finite?
- May $\mathbb{S}$ be a group? Why or why not?
- May $\mathbb{S}$ equals Z_p^*?

Cyclic Groups.

Example of cyclic group.

For example: For $p = 11$, choose $g = 4$, and compute:

$$\mathbb{S} = \{4, 4^2, 4^3, \cdots, g^j, \cdots\}$$

Cyclic Groups.

Example of cyclic group.

For example: For $p = 11$, choose $g = 4$, and compute:

$$\mathbb{S} = \{4, 4^2, 4^3, \cdots, g^j, \cdots\}$$

We will have:

$$\mathbb{S} = \{4, 5, 9, 3, 1\}$$

Certainy, it is finite and it is a group.

Cyclic Groups.

Example of cyclic group.

For example: For $p = 11$, choose $g = 4$, and compute:

$$\mathbb{S} = \{4, 4^2, 4^3, \cdots, g^j, \cdots\}$$

We will have:

$$\mathbb{S} = \{4, 5, 9, 3, 1\}$$

Certainy, it is finite and it is a group.Questions:

- What will we get if $g = 2$?
- What will we get if $g = 3$?

Cyclic Groups.

Theorem

Let $\mathbb{G}$ be a group and g be any element in $\mathbb{G}$. Then the set

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{G}$. We call $\langle g \rangle$ the cyclic group generated by g, and g is a generator of the group.

Proof.

Check the axioms. □

Examples of Cyclic groups.

Some cyclic groups.

- $(\mathbb{Z}, +)$ is a cyclic group, while 1 is the generator.
- $(\mathbb{Z}_n, +)$ is a cyclic group, while 1 is the generator.
- $\langle i \rangle$ is a cyclic group, while i is the generator.

Examples of Cyclic groups.

Some cyclic groups.

- $(\mathbb{Z}, +)$ is a cyclic group, while 1 is the generator.
- $(\mathbb{Z}_n, +)$ is a cyclic group, while 1 is the generator.
- $\langle i \rangle$ is a cyclic group, while i is the generator.

Check.

Please check and know why.

Examples of Cyclic groups.

Some cyclic groups.

- Z_p^* is a cyclic group, while p is a prime.
- $\mathbb{Z}_n^*$ is *NOT* a cyclic group, while n is composite.

Examples of Cyclic groups.

Some cyclic groups.

- Z_p^* is a cyclic group, while p is a prime.
- $\mathbb{Z}_n^*$ is *NOT* a cyclic group, while n is composite.

Check.

Please check and know why.

习题

单位根群.

$\mathbb{U}_n$ 是循环群吗？为什么，或者为什么不?

Primitive Root（原根）

Definition

Let a and n be relatively prime integers with $n > 0$. The order of a modulo n is the smallest exponent $e \geq 1$ such that $a^e \equiv 1 \pmod{n}$. If the order of a modulo n equals to the largest possible order modulo n, then a is called a primitive root modulo n.

Primitive Root

原根

From last example, we know the order of 4 modulo 11 is 5, and the order of 2 and 6 modulo n is 10. Since the largest possible order modulo 11 is 10, thus 2 and 6 are two primitive roots modulo 11. Using language of group, we may say that $\mathbb{Z}_{11}$ is a cyclic group generated by 2 or 6, and 2 and 6 are generators of $\mathbb{Z}_{11}$.

Properties of Cyclic Groups.

Proposition

所有的循环群都是阿贝尔群。

Proposition

循环群 $\mathbb{G} = \langle g \rangle$ 的每一个子群都是循环群。

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. Then $g^k = e$ if and only if n divides k.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. Then $g^k = e$ if and only if n divides k.

Proof.

Note that, n is the least positive number s.t. $g^n = e$.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. Then $g^k = e$ if and only if n divides k.

Proof.

Note that, n is the least positive number s.t. $g^n = e$.

1. The $\leftarrow$ part is trivial, since $g^k = g^{ns} = e$.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. Then $g^k = e$ if and only if n divides k.

Proof.

Note that, n is the least positive number s.t. $g^n = e$.

1. The $\leftarrow$ part is trivial, since $g^k = g^{ns} = e$.
2. The $\rightarrow$ part. Suppose $g^k = e$. By division algorithm, $k = nq + r$, where $0 \leq r < n$. Hence,

$$e = g^k = g^{nq+r} = g^{nq} g^r = g^r.$$

Thus, $r = 0$. □

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. If $h = g^k$ then the order of h is n/d, where $d = gcd(k, n)$.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. If $h = g^k$ then the order of h is n/d, where $d = gcd(k, n)$.

Proof.

Let m be the least positive number s.t. $h^m = g^{km} = e$.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. If $h = g^k$ then the order of h is n/d, where $d = gcd(k, n)$.

Proof.

Let m be the least positive number s.t. $h^m = g^{km} = e$.
1. Then $n \mid km$, equivalently, $(n/d) \mid (k/d)m$.

Properties of Cyclic Groups.

Theorem

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n. If $h = g^k$ then the order of h is n/d, where $d = gcd(k, n)$.

Proof.

Let m be the least positive number s.t. $h^m = g^{km} = e$.

1. Then $n \mid km$, equivalently, $(n/d) \mid (k/d)m$.
2. Since $d = gcd(k, n)$, n/d and k/d are relatively prime. Thus, $(n/d) \mid (k/d)m$ implies $(n/d) \mid m$. The smallest such m is n/d. □

Properties of Cyclic Groups.

强调!

循环群元素的阶.

n 阶循环群 $\mathbb{G} = \langle g \rangle$ 中的元素 g^k 的阶为:

$$\text{ord}(g^k) = \frac{n}{\gcd(k, n)}$$

Properties of Cyclic Groups.

通过生成元找生成元

已知 2 是群 $\mathbb{Z}_{11}^*$ 的生成元，群 $\mathbb{Z}_{11}^*$ 的阶是 10，$2^3 = 8 \in \mathbb{Z}_{11}^*$，且 $gcd(3, 10) = 1$，所以 8 的阶是 10，即 8 也是一个生成元。5 不是生成元，因为 $5 = 2^4 \bmod 11$，$gcd(4, 10) = 2$。请读者自行验证以上结论。以上命题告诉我们，在知道某个元是生成元时，如何找到另一个生成元。

Properties of Cyclic Groups.

练习题.

请找出群 $\mathbb{Z}_{11}^*$ 的所有生成元。

Properties of Cyclic Groups.

思考题.

已知 g 的阶为 n，则 g^s 的阶 k 必然整除 n。你能立即想到理由吗？如果 n 为素数，那么任意 g^s 的阶会是什么？

Properties of Cyclic Groups.

Corollary

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n then there are exactly $\phi(n)$ generators in $\mathbb{G}$.

Properties of Cyclic Groups.

Corollary

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order n then there are exactly $\phi(n)$ generators in $\mathbb{G}$.

Proof.

There are n elements in $\mathbb{G}$ with the form g^i, for all $i \in \mathbb{Z}_n$. For arbitrary g^i, its order is n/d, where $d = gcd(i, n)$, then g^i is a generator when $d = 1$ which means i is relatively prime to n. There are $\phi(n)$ elements in $\mathbb{Z}_n$ are relatively prime to n, therefore there are $\phi(n)$ generators in $\mathbb{G}$. □

Properties of Cyclic Groups.

Corollary

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of order p, where p is a prime, then all elements in $\mathbb{G}$ except e are generators.

Proof.

Trivially from Corollary 16. □

Properties of Cyclic Groups.

Corollary

设群 $\mathbb{G} = \langle g \rangle$ 是阶为 n 的循环群，则任意 $h \in \mathbb{G}$ 的阶必整除 n。

Proof.

该结论的正确性可直接由命题 7.5 得出。 □

Properties of Cyclic Groups.

以下是一种常见的思考方式，请大家注意。

强调!

任意群中阶为 n 的元素 g，可将群元素 g 的阶视为循环子群 $\langle g \rangle$ 的阶:

$$\text{ord}(g) = |\langle g \rangle| = n.$$

Properties of Cyclic Groups.

Exercise-1.

- 请心算列举出群 $\mathbb{Z}_{10}$ 的所有生成元。
- 群 $\mathbb{Z}_{17}^*$ 有多少个生成元？已知 3 是其中一个生成元，请问 9 和 10 是否生成元？
- p 和 q 是两个不同的素数，请问 $\mathbb{Z}_{pq}$ 都多少个生成元？r 是任意正整数，请问 $\mathbb{Z}_{p^r}$ 都多少个生成元？
- 请问 $\mathbb{U}_n$ 中有多少个生成元，它们分别具有什么形式？
- 证明：如果 p 是素数，则 $\mathbb{Z}_p$ 没有非平凡子群。

Properties of Cyclic Groups.

Exercise.

- 证明：设 n 为正整数，对任意阶为 n 的循环群 $\mathbb{G}$，如果存在整数 d 是 n 的因子，则群 $\mathbb{G}$ 中存在 d 阶元素，且有 $\phi(d)$ 个 d 阶元素。
- 设 n 是正整数，加法群 $\mathbb{Z}_n$ 是一个循环群。你能否利用本章的知识来证明第四章最后一道习题呢？即：$\Sigma_{d|n}(\phi(d)) = n$。

Primitive Root Theorem

Theorem

(Primitive Root Theorem.) Every prime p has a primitive root modulo p, and there are exactly $\phi(p-1)$ *primitive roots modulo p.*

General Primitive Root Theorem

Theorem

If $n \in \mathbb{Z}$ are 2, 4, p^e and $2p^e$, for all primes $p > 2$ and all possitive integers e, then $\mathbb{Z}_n^*$ is cyclic.

原根判定算法

目标与思路.

- 目标：输入 a 和 p，判断 a 是模 p 的原根
- 算法基础：命题 7.5 展示，任意元素 a 的阶都是 $p-1$（群阶）的因子；反之，只要 a 的阶不是小于 $p-1$ 的因子，那么 a 的阶就是 $p-1$，即为原根。
- 思路：排除法，对群阶的所有因子 d 进行判断，如果有 $a^d \equiv 1 \pmod{p}$，则 a 不是原根。
- 实现过程：找出群阶的所有素因子，然后...

原根判定算法

Listing 1: 原根判定算法

```
# 输入素数p和一个小于p的正整数a
# 输出Ture，如果a是模p的原根，否则输出False
def is_primitive_root(a, p):
    flist = prime_fators_list(p-1) #求p-1的所有素因子
    for f in flist:
        if pow(a, (p-1)//f, p) == 1:
            return False
    return True
```

原根判定算法

若干值得注意的问题.

- 该算法的效率该如何衡量？该算法效率的瓶颈在哪里？
- 注意：排除法是枚举所有的因子；但是，算法第一步求的是 $p-1$ 的素因子，不是求出所有因子。
- 算法中求所有素因子的函数如何用 SageMath 方便地实现？

Coset（陪集）

Definition of Coset.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. Define a left coset of $\mathbb{H}$ with representative $g \in \mathbb{G}$ to be the set

$$g\mathbb{H} = \{gh : h \in \mathbb{H}\}.$$

Right coset can be defined similarly by

$$\mathbb{H}g = \{hg : h \in \mathbb{H}\}.$$

Coset

Examples of Coset.

Recall our previous proof of Fermat's Little Theorem, we randomly choose a number $a \in \mathbb{Z}_p^*$, and prove

$$a\mathbb{Z}_p^* = \mathbb{Z}_p^*$$

It is similar in Eurler's Theorem. $\forall a \in \mathbb{Z}_n^*$,

$$a\mathbb{Z}_n^* = \mathbb{Z}_n^*$$

Coset

Examples of Coset.

Let $p = 11$, let $g = 4$, then $\mathbb{H} = \{g^i : i \in \mathbb{Z}\}$ is a subgroup of a $\mathbb{Z}_p^*$. Actually, $\mathbb{H} = \{1, 3, 4, 5, 9\}$. Compute:

- $\forall a \in \mathbb{H}$, what is $a\mathbb{H}$?
- $\forall a \notin \mathbb{H}$ and $a \in \mathbb{Z}_p^*$, what is $a\mathbb{H}$?

Properties of Coset.

The number of the elements in a coset.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. $\forall g \in \mathbb{G}$, the number of elements in $\mathbb{H}$ is the same as the number of elements in $g\mathbb{H}$.

Proof.

Define a map $\psi : \mathbb{H} \to g\mathbb{H}$ by $\psi(h) = gh$. Show the map is one-to-one（单射）and onto（满射）. (Please recall what we have done in the proof of Fermat's Little theorem.) □

Properties of Coset.

Identical or isolation（相等或不相交）.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. $\forall g_1, g_2 \in \mathbb{G}$, then $g_1\mathbb{H} = g_2\mathbb{H}$ or $g_1\mathbb{H} \cap g_2\mathbb{H} = \emptyset$.

Properties of Coset.

Identical or isolation（相等或不相交）.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. $\forall g_1, g_2 \in \mathbb{G}$, then $g_1\mathbb{H} = g_2\mathbb{H}$ or $g_1\mathbb{H} \cap g_2\mathbb{H} = \emptyset$.

Proof.

Suppose $\exists h_1, h_2 \in \mathbb{H}$ s.t. $g_1 h_1 = g_2 h_2$, we prove the $g_1\mathbb{H} \subseteq g_2\mathbb{H}$. Similarly, $g_2\mathbb{H} \subseteq g_1\mathbb{H}$. Then $g_1\mathbb{H} = g_2\mathbb{H}$. Note that:

$$\forall g_1 h \in g_1\mathbb{H}, g_1 h = g_1(h_1 h_1^{-1})h = g_2(h_2 h_1^{-1} h) \in g_2\mathbb{H}$$

Properties of Coset.

Partitioning of group $\mathbb{G}$.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. Then the left cosets of $\mathbb{H}$ in $\mathbb{G}$ partition $\mathbb{G}$.

Properties of Coset.

Partitioning of group $\mathbb{G}$.

Let $\mathbb{G}$ be a group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. Then the left cosets of $\mathbb{H}$ in $\mathbb{G}$ partition $\mathbb{G}$.

Proof.

Nothing! Convince yourself that the cosets $g\mathbb{H}$ cover $\mathbb{G}$, and then recall the last proposition. Why cover? Note that $e \in \mathbb{H}$! □

Lagrange's Theorem

Notation.

Let $\mathbb{G}$ be a finite group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. Define the index of $\mathbb{H}$ in $\mathbb{G}$ to be the number of left cosets of $\mathbb{H}$ in $\mathbb{G}$. We denote the index by $[\mathbb{G} : \mathbb{H}]$.

Lagrange's Theorem（拉格朗日定理）.

Let $\mathbb{G}$ be a finite group and $\mathbb{H}$ a subgroup of $\mathbb{G}$. Then $|\mathbb{G}|/|\mathbb{H}| = [\mathbb{G} : \mathbb{H}]$ is the number of distinct left cosets of $\mathbb{H}$ in $\mathbb{G}$.

Proof.

The group $\mathbb{G}$ is partitioned in $[\mathbb{G} : \mathbb{H}]$ distinct left cosets. Each left coset has $|\mathbb{H}|$ elements; therefore, $|\mathbb{G}| = [\mathbb{G} : \mathbb{H}]|\mathbb{H}|$ □

Corollaries from Lagrange's Theorem

Corollary

Suppose that $\mathbb{G}$ is a finite group and $g \in \mathbb{G}$. Then the order of g must divide $|\mathbb{G}|$.

Corollary

Let $\mathbb{G}$ be a group and $|\mathbb{G}| = p$ where p is a prime. Then $\mathbb{G}$ is cyclic and any $g \in \mathbb{G}$ such that $g \neq e$ is a generator.

Corollary

Let $\mathbb{H}$ and $\mathbb{K}$ be subgroups of a finite group $\mathbb{G}$ such that $\mathbb{K} \subset \mathbb{H} \subset \mathbb{G}$. Then

$$[\mathbb{G} : \mathbb{K}] = [\mathbb{G} : \mathbb{H}][\mathbb{H} : \mathbb{K}]$$

Corollaries from Lagrange's Theorem

Corollary

Fermat's Little Theorem.

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary

Euler's Theorem.

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

Abstract Fermat's Little Theorem.

Theorem

(Abstract Fermat's Little Theorem.) Let $\mathbb{G}$ be a finite group with order n. Then for any $a \in \mathbb{G}$, $a^n = e$.

Exercises.

(练习题.)

- 设 $\mathbb{G}$ 是群，$\mathbb{H}$ 是 $\mathbb{G}$ 的子群。任取 $g_1, g_2 \in \mathbb{G}$，则 $g_1\mathbb{H} = g_2\mathbb{H}$ 当且仅当 $g_1^{-1}g_2 \in \mathbb{H}$。
- 如果 $\mathbb{G}$ 是群，$\mathbb{H}$ 是群 $\mathbb{G}$ 的子群，且 $[\mathbb{G} : \mathbb{H}] = 2$，请证明对任意的 $g \in \mathbb{G}$，$g\mathbb{H} = \mathbb{H}g$。
- 如果 $\mathbb{G}$ 是有限群，$\mathbb{H}$ 和 $\mathbb{K}$ 是群 $\mathbb{G}$ 的子群，且子群 $\mathbb{H}$ 的阶与子群 $\mathbb{K}$ 的阶互素。请证明，$\mathbb{H}$ 与 $\mathbb{K}$ 只有一个共同元素–单位元。
- 设 $\mathbb{G}$ 是阶为 pq 的群，其中 p 和 q 是素数。请证明 $\mathbb{G}$ 的任意非平凡子群是循环群。
- 设 $\mathbb{G}$ 是阶为 pq 的阿贝尔群，其中 p 和 q 是素数。已知群元 g_1 的阶为 p，群元 g_2 的阶为 q，请问群元 g_1g_2 的阶为多少？请说明理由。