5th abstract algebra

Monday, 11. October 2021 14:02

Lemma: Let G be a cyclic group, generated by a then

i) G is abelian. $\frac{a^m}{a^m} \cdot \frac{a^n}{a^n} = a^{m+n} = a^n \cdot a^m$

ii) If G is infinite.

$\dots \; a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, a^3 \dots$

iii) If G is finite.

$a^n = e, a, a^2 \dots a^{n-1}$

① Cyclic group of n = The group of rotation of an n-gon

any rotation can be expressed by a power of a rotation R through $\frac{2\pi}{n}$, $R^n = 1$.

② $n\mathbb{Z}$ take integers $\mathbb{Z}$

subgroup $[0], [1], [2] \dots [n-1] \leftarrow$ group $+$.

$[a] + [b] = [a+b]$ ✱ well-defined ?

$n=5$ $[3]+[4] = [7]$ not closed.

$[a]$ $[a'] = [a]$ if $a' - a = kn$

$[15] = [5] = [10]$

Suppose $a' = a + pn$, $b' = b + qn$ p. q integers.

$b' = b + qn$

$a' + b' = (a+pn) + (b+qn) = (a+b) + pn + qn = (p+q)n.$

$[a+b] = [a'+b']$ well-defined.

$a+b+kn$

The set of left cosets

$\mathbb{Z}/n\mathbb{Z}$: the integers modulo n.

associativity

identity $[a] + [0] = [a] = [a+0]$ $[0]$

inverse. $[a] + [-a] = [0] = [a-a]$ $[-a]$

abelian. $[a] + [b] = [a+b] = [b] + [a]$

cyclic group generated by $[1]$.

② The integers module n under multiplication.

$[a] \cdot [b] = [ab]$ well defined.

associativity ✓

identity $[a] \cdot [1] = [a \cdot 1]$ ✓

inverse: $[a] \cdot \quad [1]$

$[0] \cdot [?] \neq [1]$

$n=5$ ✓

$\exists \cdot \mathbb{Z} = 1$

$a \frac{1}{a} = 1$

$[1]\ [2]\ \cdots\ [n-1]$ $n=4$.

$[2]\ [2] = [4] = [0]$

throw away all those integer that are not coprime to n.

Lemma: Let n be a positive integer.

The group of units U_n for the integers modulo n is

The group of units U_n for the integers modulo n is the subset of $\mathbb{Z}/n\mathbb{Z}$ of integers coprime to n. under multiplication.

proof: U_n is a group

Closed under multiplication ✓

$[a] \in U_n \qquad [b] \in U_n. \qquad a \cdot b$ coprime to n.

$\forall p.$ if $p \mid n \Rightarrow p \nmid a \quad p \nmid b \Rightarrow p \nmid ab \Rightarrow [ab] \in U_n.$

$$[a] \cdot [b] = [ab]$$

associative.

$$[a] \quad [b] \quad [c] \quad \in U_n$$

$$([a][b])[c] = [abc]$$

$$= [a]([b][c]) \quad \checkmark$$

1 is coprime to n. $[1] \in U_n$. identity.

$[a] \in U_n$. need $[b]$ such that $[ab] = [1]$

$$ab + mn = 1$$

a, b coprime by n. by Euclid's algorithm.

such m. exists. $\square$.

Definition: The Euler function ϕ is the function $\phi(n)$ which assigns the order of U_n to n.

Lemma: Let a be any integer which is coprime to the positive integer n.

integer n.

Then $a^{\phi(n)} = 1 \mod n$.

Proof: Let $g = [a] \in U_n$.

$g^{\phi(n)} = e$ from Lemma. ✓

$[a]^{\phi(n)} = e = [1]$

$[a^{\phi(n)}] = [1] \Rightarrow a^{\phi(n)} = 1 \mod n$ □

Lemma. ϕ is multiplicative.

$\phi(mn) = \phi(m)\phi(n)$. if m, n coprime positive integers.

$\phi(p^k) = \phi(p) \cdot \phi(p) \cdots \phi(p) = \phi(p)$ where p is a prime.

$p-1$. $[1], \cdots [p-1]$ coprime to p

$\phi(p) = p-1$. if p is prime.

Fermat's little theorem: Let a be any integer Then.

$a^p = a \mod p$.

$a^{p-1} = 1 \mod p$ if a is coprime to p.

$\phi(p^k)$ $p=3$. $k=2$. $p^k = 9$ $[0] \cdots [8]$

△ how many numbers are coprime to p. $1, 2, \cdots 8$ ✗

multiples of 3: 3. 6
1×3 2×3.

$\phi(p^k)$ 1. p^{k-1}.

$p = 1\cdot p \cdot 2\cdot p \cdots (p^{k-1}-1)p$. $\boxed{p^{k-1}\cdot p = p^k > p^k - 1}$

$p^k - 1 - (p^{k-1}-1) = p^k - p^{k-1}$

$$p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}.$$

Lemma. $\phi(p^k) = p^k - p^{k-1}$.

$9 - 3 = 6$ $\{1, 2, 4, 5, 7, 8\}$.

$U_{5000} = ?$

$5000 = 5 \cdot 10^3 = 5 \cdot 2^3 \cdot 5^3 = 5^4 \cdot 2^3$.

$\phi(5^4) = 5^4 - 5^3 = 5^3(5-1) = 125 \times 4$

$\phi(2^3) = 2^3 - 2^2 = 4$

$\phi(5000) = \phi(5^4) \cdot \phi(2^3) = 16 \times 125 = 2000$.

U_6 $\phi(6) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2$. ✗

▷ get a cyclic group of order 2. $\{1, 5\}$. ✓

$1^2 = 1$ $5^2 = 25 = 24 + 1 = 1 \bmod 6$.

U_8. $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$ ✗ $\{1, 3, 5, 7\}$.

either cyclic of order 4 or every element has order 2.

min order 6 non-abelian. $\{1, 2, 3, 4, 5\}$

$3^2 = 9 = 1 \bmod 8$. $\{1, 3\}$.

$5^2 = 25 = 1 \bmod 8$.

$7^2 = 49 = 1 \bmod 8$. $= [1]$.

U_8 cannot be cyclic.

$a^p = 1$

$a^4 = 1$

$(a^2)^2 = 1$

↑ $a^{\phi(p)} = 1$

Permutation Group.

Definition: Let S be a set. A permutation of S is simply a bijection. $f: S \to S$

Definition: Let S be a set. A permutation of S is simply a bijection: $f: S \to S$.

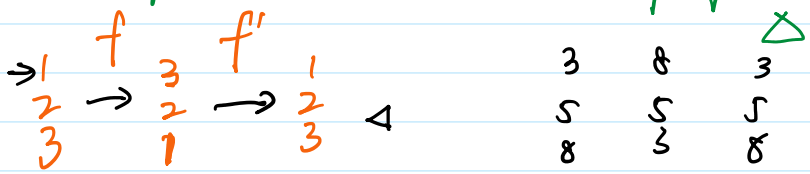
$g: S \to S$

Lemma: Let S be a set.

(1). f, g are permutations, composition of f and g are permutation.

$f \cdot g$ gf.

(2) f is a permutation. inverse of f is a permutation.



Lemma. Let S be a set. The set of all permutations under the operation of composition of permutations, form a group $A(S)$.

proof: Closed under multiplication: $f \cdot g \in A(S)$

associative. $S \xrightarrow{f} S \xrightarrow{g} S \xrightarrow{h} S$ $f \cdot (g \cdot h) = (f \cdot g) \cdot h$

identity. $f \cdot i = i \cdot f = f$. i ✓

$S \xrightarrow{i} S$

inverse ✓ $f \cdot f' = f' \cdot f = i$ □

Lemma: $Ord(A(S)) = n!$ ⋮ $\begin{matrix} n \\ n-1 \\ n-2 \\ \vdots \end{matrix}$

S has n element.

Definition: The group S_n is the set of permutation of first n natural numbers $\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$ $\{1, \dots, n\}$ $\{1, \dots, n\}$

natural numbers $\begin{matrix}1\\2\\3\\\vdots\\n\end{matrix}$ $\{1,\cdots n\}$ $\{1,\cdots n\}$

S_n $n=5$ $\sigma=\begin{pmatrix}1&2&3&4&5\\3&1&5&4&2\end{pmatrix}\in S_5$.

$\tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix}\in S_5$

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

$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\4&5&3&1&2\end{pmatrix}$ non-abelian.

Definition: Let τ be an element of S_n.

We say that τ is a k-cycle if there are integers $a_1\cdots a_k$ such that

$\tau(a_1)=a_2$.

$\tau(a_2)=a_3$ τ fixes every other integers.

$\vdots$

$\tau(a_k)=a_1$

$$\tau(a_i)=\begin{cases}a_{i+1} & i<k\\ a_1 & i=k\\ a_i & \text{otherwise.}\end{cases}$$

$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ 4-cycle. $(1,2,3,4)$

$\begin{pmatrix}1&2&3&4&5\\1&5&3&2&4\end{pmatrix}$ 3-cycle. $(2,5,4)=(5,4,2)$

$=(4,2,5)$

k cycle: $\tau=(a_1a_2\cdots a_k)$.

10.30 下午四点.