Last class: Results about cyclic groups:

Assume $G = \langle a \rangle$, $\text{ord}(a) = n = |G|$

Results: (a) $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$

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

(c) $H \subset G$ a subgroup $\Rightarrow H = \langle a^{n/d} \rangle$ for some divisor d/n and $|H| = d$

If $G = \langle a \rangle$, $\text{ord}(a) = \infty$

$\Rightarrow \text{ord}(a^k) = \infty$

and if $H \subset G$ a subgroup $\Rightarrow H = \langle a^k \rangle$, k positive integer

e.g. If $G = \mathbb{Z}$, $G = \langle 1 \rangle$ and $H \subset G$ subgroup $\Rightarrow H = \langle k \rangle$

e.g. $H = \langle 2 \rangle = \{0, \pm 2, \pm 4, \pm 6 \ldots\}$

$=$ even numbers.

Question: $G = \langle a \rangle$, $|G| = n$.

how many elements of G have order n?

(observe: If $\text{ord}(b) = n$, $b \in G$

$\Rightarrow |\langle b \rangle| = n$ } $\langle b \rangle = G$

as $\langle b \rangle \subset G$ }

i.e. b is a generator of G.

Answer: $b = a^k$ for some k

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

$\Rightarrow$ $\boxed{\text{ord}(a^k) = n \iff \gcd(k,n) = 1}$

Def Euler's ϕ function is defined by

$$\phi(n) = \#\{j,\ 1 \le j < n,\ \gcd(j,n) = 1\}$$

Examples:

(a) $n = p$ prime number.

$\gcd(j,p) = 1$ for $1 \le j < p$.

$$\Rightarrow \boxed{\phi(p) = p-1}$$

(b) $n = 2^k \Rightarrow \gcd(j, 2^k) = 1 \iff j$ odd

$$\Rightarrow \boxed{\phi(2^k) = 2^{k-1}}$$

(c) $n = p^k$, p prime $\Rightarrow$ $\boxed{\phi(p^k) = (p-1)p^{k-1}}$

(d) If $\gcd(n,m) = 1$

$$\Rightarrow \boxed{\phi(nm) = \phi(n)\phi(m)}$$

Ex. Calculate $\phi(100)$

Sol. $\phi(100) = \phi(2^2 \cdot 5^2) \overset{(d)}{=} \phi(2^2)\,\phi(5^2)$

$\overset{(b),(c)}{=} 2 \cdot (5-1) \cdot 5 = \boxed{40}$

$\Rightarrow$ $\mathbb{Z}_{100}$ has 40 generators.

Theorem: $G = \langle a \rangle$ cyclic, $\text{ord}(a) = n$

(a) G has $\phi(n)$ generators

(b) If $d \mid n \Rightarrow$ G has exactly $\phi(d)$ elements whose order $= d$

If $d \nmid n \Rightarrow \text{ord}(b) \neq d$ for all $b \in G$.

Proof. (a) follows from definitions and $\langle a^u \rangle = G \Leftrightarrow \gcd(u,n) =$

(b) assume $d \mid G$

$\Rightarrow$ $\langle a^{n/d} \rangle$ is subgroup of order $|d|$

If $b \in G$ with $\text{ord}(b) = d$

$\langle b \rangle$ is the unique subgroup of G of order d.

$\Rightarrow$ $\langle b \rangle = \langle a^{n/d} \rangle = H$

$\Rightarrow$ all elements of order d are in H

by (a) exactly $\phi(d)$ elements in H of order d.

Chapter 5 Permutation Groups

Def: Let A be a set. A permutation of A is a map $\pi : A \to A$ which is 1-1 and onto

Example: $A = \{1, 2, 3\}$

how many permutations of A?

1 → 3 possibilities, 2 → 2 poss., 3 → 1

$\to 3 \cdot 2 \cdot 1 = 3!$ permutations

notation: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ...

means

$1 \to 1,\ 2 \to 2,\ 3 \to 3$

$1 \to 1,\ 2 \to 3,\ 3 \to 2$

...

Lemma: Let $P(A)$ be the set of all permutations of A. It forms a group under the binary operation of concatenation.

Proof. (a) associativity ✓ for concatenation of maps

(b) identity: identity map $a \to a$ $\forall a \in A$

(c) inverse: inverse map exists because original map is 1-1 and onto

Ex. inverse of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Cycle notation: (less cumbersome)

$(a_1\ a_2 \dots a_m)$ denotes the permutation

$a_1 \to a_2$

$a_2 \to a_3$

$a_3 \to \dots a_4$

$\dots$

$a_m \to a_1$

numbers not in cycle unchanged

Example. $A = \{1,2,3,4,5\}$

$(1\,4\,3\,5) \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$

Lemma Any permutation of $\{1,2,\dots,n\}$ can be written as a product of disjoint cycles

proof Let π be a permutation

pick a number $a_1 \in \{1,2\dots,n\}$ (e.g. $a_1 = 1$)

Define inductively $a_{i+1} = \pi(a_i)$

get subset $\{a_i,\ i=1,2\dots\} \subset \{1,2\dots n\}$

finite.

e.g. $i \neq j$ $\pi^i(a_1) = \pi^j(a_1)$ $\Leftrightarrow$ $\pi^{i-j}(a_1) = a_1$ (assume $i > j$)

let $m = \min\{j>0,\ \pi^j(a_1) = a_1\}$

get cycle $(a_1\, a_2 \dots a_m)$ which describes action of π on $\{a_1,\dots a_m\}$.

Do same for rest of numbers:

pick $b_1 \in \{1, \dots n\} \setminus \{a_1 \dots a_m\}$

$\rightarrow$ get cycle $(b_1\ b_2 \dots b_4)$

repeat until no numbers left.

Example $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 6 & 8 & 2 & 1 & 4 \end{pmatrix}$

pick:

$a_1 = 1$

$a_2 = \pi(1) = 3$

$a_3 = \pi(3) = 7$

$a_4 = \pi(7) = 1$

$\Big\}$ (137)

$b_1 = 2$

$b_2 = 5$

$b_3 = 8$

$b_4 = 4$

$b_5 = 6$ $\quad b_6 = \pi(6) = 2$

$\Big\}$ (25846)

$\pi = (137)(25846)$