Permutations

$\varepsilon = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $\sigma_2 = \sigma_1^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\text{syn} = -1$ (odd)

$\sigma_2 = \begin{matrix}1&2&3\\\downarrow&\downarrow&\downarrow\\2&3&1\\\downarrow&\downarrow&\downarrow\\3&1&2\end{matrix}$ $\sigma_2\sigma = \begin{matrix}1&2&3\\\downarrow&\downarrow&\downarrow\\3&1&2\\\downarrow&\downarrow&\downarrow\\1&2&3\end{matrix}$ $\Rightarrow$

multiplication table

$\circ$	ε	σ_1	σ_2
ε	ε	σ_1	σ_2
σ_1	σ_1	σ_2	ε
σ_2	σ_2	ε	σ_1

"multiplicative" group of integers modulo m, $G_m^\times$

$G_m^\times = \{a \mid (1 \le a \le m) \wedge (gdc(a,m) = 1)\}$ forms w.r.t. multiplication modulo m

$\varphi(m) = |G_m^\times|$ — Euler totient function

a) Closure: $\forall a,b \mid gcd(a,m) \wedge gdc(b,m) = 1 \rightarrow gcd(a\cdot b, m) = 1$

b) associativity is there

c) neutral $gcd(1,m) = 1$

d) invertibility $\forall a \in G_m^\times$, there is a $y \in G_m^\times$ such that $a \cdot y = 1 \pmod m$, $y = a^{-1}$

subgroups

Let G be a group & $H \subseteq G$ iff

i) Closure $\forall x,y \mid x \in H \wedge y \in H \rightarrow x \cdot y \in H$

ii) Neutral $\varepsilon \in H$

iii) Invertibility $\forall x \in H \; (x^{-1} \in H)$

Cyclic subgroups — group that can be generated by a single element

let $H = \{a^k \mid k \in \mathbb{Z}\}$ H is a subgroup, because a can generate the entire group

ex. $\{\ldots, a^{-2}, a^{-1}, \varepsilon, a^1, a^2, \ldots\}$, $\varepsilon = a^0$

Lagrange Theorem

Let $G = \{g_1, g_2, g_3, \ldots, g_n\}$ of order n

and $H \subseteq G = \{h_1, h_2, \ldots, h_k\}$ of order k

$\Big\}$ $\frac{n}{k} = \ell$ (disjoint subsets) of same size

$\Downarrow$

$k\ell = n$

example: $x \cdot y \pmod{10}$ group

$G = \{1, 3, 7, 9\}$

$H = \{1, 9\}$

$\Downarrow$

$*\pmod{10}$	1	9
$1 * H$	1	9
$3 * H$	3	7
$7 * H$	7	3
$9 * H$	9	1

$\Rightarrow \ell = 2 \times k = 4 = n$

$\{1,9\}$ $\{3,7\}$