Content:

Theorem Let $a \in G$ with $\circ(a) = n$, then $\circ(a^k) = \dfrac{n}{GCD(n,k)}$.

Theorem Let $\alpha \in S_n$. (1) If $\alpha$ is an $r$-cycle, $\circ(\alpha) = r$. (2) If $\alpha = \beta_1 \cdots \beta_n$ is a complete factorization, then $\circ(\alpha) = \text{lcm}(r_1, \ldots, r_n)$. (3) If $p$ is prime and $\circ(\alpha) = p$, then $\alpha$ is a $p$-cycle or a product of disjoint $p$-cycles.

Definition Subgroup

Definition Conjugate

Theorem If $H \subseteq G$ (a group) such that $H \neq \varnothing$, then $H \leq G$ iff $ab^{-1} \in H$, $\forall\ a, b \in H$.

Definition Cyclic subgroup generated by $a$

Lemma $G$ is a group and $a \in G$. If $\circ(a) = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ where $e, a, a^2, \ldots, a^{n-1}$ are $n$ distinct elements in $G$.

**Warm-Up** Find the order of all elements in

1) $\mu_4 = \{\pm 1, \pm i\}$

| $z \in \mu_4$ | Powers of $z$ | $\circ(z)$ |
|---|---|---|
| 1 | $1^1 = 1$ | 1 |
| $-1$ | $(-1)^1 = -1, (-1)^2 = 1$ | 2 |
| $i$ | $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ | 4 |
| $-i$ | $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$ | 4 |

2) $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.

| $a \in \mathbb{Z}_6$. | Powers of $a$ | $\circ(a)$ |
|---|---|---|
| [0] | [0] | 1 |
| [1] | [1] + [1] + [1] + [1] + [1] + [1] = [6] = [0] | 6 |
| [2] | [2] + [2] + [2] = [6] = [0] | 3 |
| [3] | [3] + [3] = [6] = [0] | 2 |
| [4] | [4] + [4] + [4] = [12] = [0] | 3 |
| [5] | [5] + [5] + [5] + [5] + [5] + [5] = [30] = [0] | 6 |

**Example** Suppose $\circ(a) = 6$, what is $\circ(a^8)$?

We know $(a^8)^6 = 1$. We know $(a^8)^3 = 1$.

Does $a^8 = 1$? No. $a^8 = a^6 \bullet a^2 = a^2$.

Does $(a^8)^2 = 1$? No. $(a^8)^2 = a^{12} \bullet a^4 = a^4$.

So, $\circ(a^8) = 3$.

Let $\circ(a^8) = k$.

Note that $1 = (a^8)^k = a^{8k}$. $8k$ is a multiple of 8 and a multiple of 6; LCM (6,8)

To find $k$, divide LCM (6,8) by 8.

By number theory, we have $\dfrac{LCM(6,8)}{8} = \dfrac{6}{GCD(6,8)}$

**Theorem** Let $a \in G$ with $\circ(a) = n$, then $\circ(a^k) = \dfrac{n}{GCD(n,k)}$.

**Proof**:
Let $d = \gcd(n,k)$. Then there are integers $s, t$ such that $n = ds$ and $k = dt$ where $\gcd(s, t) = 1$ (since we are only guaranteed that $c \mid n$ and $c \mid k \Rightarrow c \mid d$ if $\gcd(s, t) = 1$).
$\therefore\ 1 = (a^k)^r = a^{kr} \Leftrightarrow n \mid kr \Leftrightarrow ds \mid dtr \Leftrightarrow s \mid tr \Leftrightarrow s \mid r$.
This implies that $(a^k)^s = 1$ (since $s \mid s$).
And since $s$ is the smallest integer that $s$ divides, then
$\circ(a^k) = s = \dfrac{n}{d} = \dfrac{n}{GCD(n,k)}$.

---

**Examples**
1) $\circ(\ (13426)\ ) = ?$ 5 (since it's a 5-cycle)
2) $\circ(\ (23)(145)\ ) = ?$ $2 \bullet 3 = 6$
3) $\circ(\ (23)(14)\ ) = ?$ 2
4) $\circ(\ (23)(142)\ ) = ?$ $= \circ(\ (1432)\ ) = 4$

**Theorem** Let $\alpha \in S_n$.
(1) If $\alpha$ is an $r$-cycle, $\circ(\alpha) = r$.
(2) If $\alpha = \beta_1 \cdots \beta_n$ is a complete factorization, then $\circ(\alpha) = \text{lcm}(r_1, \ldots, r_n)$.
(3) If $p$ is prime and $\circ(\alpha) = p$, then $\alpha$ is a $p$-cycle or a product of disjoint $p$-cycles.

**Proof** (1):
We first show that $\alpha^r = (1)$.
If $\alpha$ is an $r$-cycle, then $\alpha^i(a_1) = \alpha_{i+1}$ for all $i < r$.
Since $\alpha^{r-1}(a_1) = a_r$, then $\alpha^r(a_1) = \alpha(\alpha^{r-1}(a_1)) = \alpha(\ a_r) = a_1$.
And $\alpha^r(a_i) = \alpha^r(\alpha^{i-1}(a_1)) = \alpha^{i-1}(\alpha^r(a_1)) = \alpha^{i-1}(a_i) = a_i$.
Thus $\alpha^r(a_i) = a_i$ for all $i$, hence $\alpha^r = (1)$.
We now show, by contradiction, that $r$ is the smallest positive integer $k$ such that $\alpha^k = (1)$.
Let $\circ(\alpha) = k$ and suppose $k < r$. Then $\alpha^k(a_1) = a_{k+1}$ and $k + 1 \le r$.
But $\alpha_{k+1} \ne a_1$, hence $\alpha^k \ne (1)$; and we have our contradiction.
$\therefore\ k = r$. And $\circ(\alpha) = r$.

**Proof** (2):
Each $\beta_i$ has order $r_i$ by part (1).
Suppose that $\alpha^M = (1)$
Then $(\beta_1 \cdots \beta_t)^M = (1)$
$\beta_1^M \cdots \beta_t^M = (1)$ (since $\beta_i$ commute)
So $\beta_1^M = (1) \cdots \beta_t^M = (1)$ (by disjointness of $\beta$'s, Ex 2.11 (ii))
$r_1 \mid M \quad \cdots \quad r_t \mid M$ (by Theorem 2.24)
That is, $M$ is a common multiple of $r_1, \ldots, r_t$.
If $m = \text{lcm}\{\ r_1, \ldots, r_t\}$, then $\alpha^m = (1)$.
Therefore, $\alpha$ has order $m$.

**Proof**: (3):
Every permutation can be written as a cycle or product of disjoint cycles.
If $\alpha$ is a cycle, then $\alpha$ is a $p$-cycle by part (2).
If $\alpha$ is a product of disjoint cycles, then $p = \text{lcm}\{ r_1, \ldots, r_t\}$, hence $r_i = p$ for each $i$.

---

**Examples** 1) How many elements in $S_5$ have order 2?
Elements of order 2 in $S_5$ have the form (12) or (12)(34). so we need to know how many of each there are. Recall

(12) $\quad \frac{5 \cdot 4}{2} = 10$

(12)(34) $\quad \frac{5 \cdot 4 \cdot 3 \cdot 2}{2 \cdot 2 \cdot 2} = 15$

Total: 25

2) How many elements in $S_6$ have order 2?
Elements of order 2 in $S_5$ have the form (12), (12)(34), or (12)(34)(56).

(12) $\quad \frac{6 \cdot 5}{2} = 15$

(12)(34) $\quad \frac{6 \cdot 5 \cdot 4 \cdot 3}{2 \cdot 2 \cdot 2} = 45$

(12)(34)(56) $\quad \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 2 \cdot 2 \cdot 6} = 15$

Total: 75

---

## 2.4 Lagrange's Theorem

$\text{SL}(n, \mathbb{R}) \subseteq \text{GL}(n, \mathbb{R})$.
We know $\text{SL}(n, \mathbb{R})$ is a group AND a subset of another group.

**Definition** Let $G$ be a group and $H \subseteq G$. Then $H$ is a *subgroup* of $G$ if it is a group with respect to the same operation as defined in $G$ (notated $H \leq G$).

**Examples** $G \leq G, \{e\} \leq G, \mathbb{Z} \leq \mathbb{R}$ (with respect to +).

**Non-examples** $\sim(\mathbb{Z}_6 \leq \mathbb{Z})$ as $\sim(\mathbb{Z}_6 \subseteq \mathbb{Z})$. Also + in $\mathbb{Z}_6 \neq$ + in $\mathbb{Z}$.

$\sim(\mathbb{Z}_5 \leq \mathbb{Z}_6)$ as $\sim(\mathbb{Z}_5 \subseteq \mathbb{Z}_6)$
Note: $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, $[0] = \{n : 6 \mid n\}$
And $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, $[0] = \{n : 5 \mid n\}$.

$\sim(\text{GL}(2, \mathbb{R}) \leq \text{M}(2, \mathbb{R})$ as operations are not the same.
$\text{GL}(2, \mathbb{R})$ is a group with respect to +
$\text{M}(2, \mathbb{R})$ is a group with respect to $\cdot$ .

Technically $\sim(S_3 \leq S_4)$ as technically $\sim(S_3 \subseteq S_4)$.
$S_3$ is the set of bijections on $\{1, 2, 3\}$.
$S_4$ is the set of bijections on $\{1, 2, 3, 4\}$.

**Note**: If $H \leq G$, $1_G = 1_H$. This is not due to uniqueness of identity, it is due to the cancellation property.

**Proof**:

$1_G \bullet 1_H = 1_H \in G$.

$1_H \bullet 1_H = 1_H \in G$.

$\therefore\ 1_G \bullet 1_H = 1_H \bullet 1_H$, and by cancellation, $1_G = 1_H$.

**Note**: To show $H$ is a subgroup of $G$, we need to check

1) $1 \in H$.
2) Inverses $\in H$.
3) $H$ is closed.

(Associativity is inherited)

**Theorem** Let $H$ be a nonempty subset of a group $G$.
Then $H \leq G$ iff $ab^{-1} \in H$, $\forall\ a, b \in H$.

**Proof**:

$\Rightarrow$: If $H$ is a group, then $\forall\ a, b \in H$, we have inverses and closure, hence $ab^{-1} \in H$.

$\Leftarrow$: Assume $\forall\ a, b \in H$.

1) Since $H \neq \varnothing$, $\exists\ x \in H$. So $xx^{-1} = 1 \in H$.
2) Let $x \in H$, then $1x^{-1} = x^{-1} \in H$.
3) Let $x, y \in H$. Then $y^{-1} \in H$, hence $x(y^{-1})^{-1} = xy \in H$.

$\therefore\ H$ is a group.

**Note** If $H$ is finite and $a, b \in H \Rightarrow ab \in H$, then $H$ is a group.
That is, all we need is finite and closure.

## Cyclic Groups

**Definition** Let $G$ be a group and $a \in G$. The *cyclic subgroup generated by a* is the smallest subgroup of $G$ containing $a$, denoted $\langle a \rangle$. i.e. If $a \in H$, $H \leq G$, then $\langle a \rangle \in H$.

**Question** How do we know it exists?
Take the collection of subgroups containing $a$.
$H, K \leq G$. Is $H \cap K \leq G$? (Homework exercise)
$\cap$ of all the subgroups $= \langle a \rangle$.

**Question** $\langle e \rangle = \{e\}$? Yes.

**Question** Suppose $a \neq e$, does $\langle a \rangle$ ever equal $\{a\}$? No, it must have $e$, also.

**Question** What must be in $\langle a \rangle$? $\{e, a, a^{-1}, a^n\}$ where $a^n$ is any integer power of $a$.

**Examples** 1) $\mu_4 = \{\pm 1, \pm i\}$;
$\langle i \rangle = \{\ldots, i^{-2}, i^{-1}, i^0, i, i^2, i^3, i^4, i^5, \ldots\} = \mu_4$; we only really need $i, i^2, i^3, i^4$.
$\langle -1 \rangle = \{\pm 1\}$
2) $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$;
$\langle [1] \rangle = \{[0], [1], [2], [3], [4], [5]\} = \mathbb{Z}_6$.
$\langle [2] \rangle = \{[0], [2], [4]\}$

**Lemma** $G$ is a group and $a \in G$. If $\circ(a) = n < \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ where $e, a, a^2, \ldots, a^{n-1}$ are $n$ distinct elements in $G$.

The order of a group = the number of elements in the group, $|G|$. So $\circ(a) = |\langle a \rangle|$.
We will prove this on Wednesday.