Groups and Symmetry

Group

A group $(G, \oplus)$ where G is a set and $\oplus$ satisfies
1. Associative, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
2. Identity, there exist an $e \in G$ where $xe = x = ex$
3. Inverse, each element x has an inverse, $xx^{-1} = e = x^{-1}x$

A group is **abelian** if $\oplus$ is commutative.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups over addition of number.
- $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+, \{+1, -1\}, \mathbb{C} - \{0\}, \{z \in \mathbb{C} : |z| = 1\}, \{\pm 1, \pm i\}$ are groups over multiplication.

Dihedral Groups

Modulo arithmetic

Let $a, b \in \mathbb{Z}_n$

$$a +_n b = \begin{cases} a + b & a + b < n \\ a + b - n & a + b \geq n \end{cases}$$

$$a \times_n b = \begin{cases} 0 & b = 0 \\ a +_n a \times (b - 1) & b > 0 \end{cases}$$

The **dihedral groups** D_n is the family of symmetry groups formed by regular n-gons.

$$\begin{aligned} r^a r^b &= r^k \\ r^a (r^b s) &= r^k \\ (r^a s) r^b &= r^l s \\ (r^a s)(r^b s) &= r^l \end{aligned}$$

where $k = a +_n b$ and $l = a +_n (n - b)$

Subgroups and Generators

Subgroup

$H < G$ if $H \subseteq G$ and H is a group.

Cyclic group

If all elements in H can be written as x^m where $x \in G$, then H is a cyclic group, that is the **subgroup generated by** x.

$$G = <x>$$

- If G has order n, then $x^n = e$.
- $\mathbb{N} = <1>$ with infinite order.

Let $X = \{x_1, x_2, ..., x_k\}$, then $x_1^{m_1} x_2^{m_2} ... x_k^{m_k}$ is a word. Let H be the set of all words, H is called the subgroup generated by X.

- Translate by 1 t $(+1)$ and reflect about 0 s $(-x)$ generates the **infinite dihedral group** $D_\infty = <s, t>$

Theorem 5.1: one step subgroup test
Let H be a non-empty subgroup of G.

$$H < G \Longleftrightarrow (x, y \in H \Longrightarrow xy^{-1} \in H)$$

Theorem 5.2: interseciton of subgroups
Let $H < G$ and $K < G$.

$$H \cap K < G$$

Theorem 5.3:
1. Every subgroup of $\mathbb{Z}$ is cyclic.
2. Every subgroup of a cyclic group is cyclic.

Permutations

Permutation
A permutation is a bijection $\alpha : X \mapsto X$.

- S_X is the set of all permutations from X to X.
- S_X is a group under function composition.
- $S_n = S_X$ where $X = \{1, 2, ..., n\}$
- The order of S_n is $n!$

Cyclic permutation
A cyclic permutation $(abcd...z)$ sends $a \to b$, $b \to c$, etc, and $z \to a$.
- A cyclic permutation of length k is called a k-cycle.
- A 2-cycle is called a **transposition**.

Theorem 6.1: transposition in S_n generates S_n

$$(a_1 a_2 ... a_k) = (a_1 a_k)...(a_1 a_3)(a_1 a_2)$$

Theorem 6.2: more transpositions generates S_n
1. $(12), (13), ..., (1n)$ generates S_n
$$(ab) = (1a)(1b)(1a)$$
2. $(12), (23), ..., (n-1\ n)$ generates S_n
$$(1k) = (k-1\ k)...(23)(12)(23)...(k-1\ k)$$

Theorem 6.3: cyclic permutation generates S_n
(12) and $(123...n)$ generates S_n

$$(k\ k+1) = (123...n)(12)(123...n)^{1-k}$$

Theorem 6.4: even permutations

Even transpositions
Even transpositions can be written as the composition of an even number of transpositions.

The even permutations in S_n forms a subgroup of order $n!/2$ called A_n

Theorem 6.5: 3-cycles generates A_n

For $n \geq 3$, the 3-cycles generates A_n

Isomorphism

Isomorphism

G and G' are isomorphic if there is a bijection $\varphi : G \mapsto G'$ which satisfies $\varphi(xy) = \varphi(x)\varphi(y)$.

- $\varphi(x^{-1}) = \varphi(x)^{-1}$
- $\varphi(e) = e'$
- G albelian $\Longrightarrow x'y' = y'x'$

Plato's Solids

- The tetrahedron is isomorphic to A_4
- The cube and octahedron is isomorphic to S_4
- The dodecahedron and icosahedron is isomorphic to A_5

Theorem 8.1: Cayley's Theorem

Let G be a group, then G is isomorphic to a subgroup of S_G

Theorem 8.2: Cayley's with integer permutations

Let G be a group, then G is isomorphic to a subgroup of $S_{|G|}$

Matrix Groups

Let $f_A(\boldsymbol{x}) = \boldsymbol{x}A^t$ such that it is a group under function composition: $f_{AB}(x) = x(AB)^t = xB^tA^t$ (notice B is applied first).

General Linear Group

$GL_{n(T)}$ is the set of all $n \times n$ matrices such that $f_A : T^n \mapsto T^n$ is invertible.

E.g. $GL_n(\mathbb{R})$ and $GL_n(\mathbb{C})$

- Orthogonal matrices satisfies $A^tA = I$ where $A \in GL_{n(\mathbb{R})}$ (the dot product of column m and n is 1 if $m = n$, 0 otherwise).
- O_n is the set of all orthogonal matrices in $GL_n(\mathbb{R})$, $|A| = +1 \text{ or } -1$
- SO_n is the set of all orthogonal matrices where $|A| = +1$ only.

Orthogonal matricies preserves length and angles.

- Orthogonal matrices in complex numbers satisfies $A^{*t}A = I$, this is because the distance between two points in complex number is given by z^*z.
- U_n is the set of all orthogonal matrices in $GL_n(\mathbb{C})$
- SU_n is the set of all orthogonal matrices where $|A| = +1$

Products

Direct product

The **direct product** $G \times H$ is (g, h), with multiplication $(g, h)(g', h') = (gg', hh')$

Theorem 10.1: Cyclic direct product

$$\mathbb{Z}_m \times \mathbb{Z}_n \text{ cyclic} \Longleftrightarrow \gcd(m, n) = 1$$

Then $\mathbb{Z}_m \times \mathbb{Z}_n = <(1, 1)>$

Theorem 10.2: Subgroup isomorphic
Let $H < G$, $K < G$, $HK = G$, $H \cap K = \{e\}$, every $h \in H$ commutes with $g \in G$, then

$$H \times K \cong G$$

Theorem 11.1: Legrange's theorem
The order of a subgroup of a finite group is always a divisor of the order of the group.

Corollaries
1. The order of every $g \in G$ is a divisor of $|G|$
2. If $|G|$ is prime, then G is cyclic.
3. If $x \in G$ then $x^{|G|} = e$

R_n
- Let R_n be the set of all $x \in \mathbb{Z}_n$ where $\gcd(x, n) = 1$
- Let $\varphi(n) = |R_n|$

Theorem 11.5: Euler's theorem

$$\gcd(x, n) = 1 \Longrightarrow x^{\varphi(n)} \equiv 1 \pmod{n}$$

Theorem 11.6: Fermat's little theorem
If p prime and x is not a multiple of p, then

$$x^{p-1} \equiv 1 \pmod{p}$$