2. Groups and Functions between Groups

2.1 Groups

A group is a nonempty set G with a law of composition $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$, satisfying:

1. Associative: $\forall g1, g2, g3 \in G$, $(g1g2)g3 = g1(g2g3)$
2. Identity: $1 \in G$ s.t. $\forall g \in G$, $g1 = 1g = g$
3. Inverse: $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = 1$

Examples: $\mathbb{Z}^+$, $\mathbb{Q}^\times$, S_n, A_n, $\mathbb{Z}/n\mathbb{Z}$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$

If the law of composition is commutative, i.e. $\forall g_1, g_2 \in G$, $g_1 g_2 = g_2 g_1$, then G is an abelian group. $\iff$ multiplication table is symmetric along diagonal

Prop. A group G admits the Cancellation Law: $ac = bc \to a = b$

The order of a group G is the number of elements in its underlying set, and is denoted by $|G|$. If $|G| < \infty$, G is a finite group; otherwise infinite group.

2.2 Permutations

Let X be a set. The set of all bijections of X, $P(X) = \{f : X \to X | f \text{ is bijective}\}$ with the law of composition the composition of functions form a group, called the permutation group on X:

1. Composition of functions is associative
2. The identity element is the identity function on X
3. The inverse of $f \in P(X)$ is its inverse function f^{-1}

If $X = \{1, 2, ..., n\}$, we call the permutation group of n letters S_n.

A cycle $(a_1, ..., a_k) \in S_n$, where $a_1, ..., a_k$ are distinct numbers between 1 and n, is the function sending a_1 to a_2, a_2 to a_3,..., a_k to a_1, while keeping the other numbers fixed.

Two cycles $(a_1, ..., a_k)$ and $(b_1 ... b_m)$ in S_n are disjoint if $a_1, ..., a_k, b_1, ..., b_m$ are all distinct numbers.

$S_2 = \{id, (12)\}$

$S_3 = \{id, (12), (13), (23), (123), (132)\}$

2.3 Subgroups

A subgroup H of a group G is a subset of G satisfying:

1. Closure: $\forall a, b \in H \to ab \in H$
2. Identity: $1 \in H$
3. Inverse: $\forall a \in H \to a^{-1} \in H$

Prop. A nonempty subset H is a subgroup of $G \iff \forall a, b \in H \to a^{-1}b \in H.$

Examples: G and $\{1\}$; $G = \mathbb{R}^+$, $H = \mathbb{Z}$

$GL_n(\mathbb{R})$; $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | \det(A) = 1\}$ is a subgroup, since $\det(A^{-1}B) = \det(A^{-1})\det(B) = 1$

2.4 Subgroups of Z

If H is a subgroup of $\mathbb{Z}$, then $H = a\mathbb{Z}$ for some $a \in \mathbb{N}$.

Given two integers a, b. Define the greatest common divisor of a and b to be the positive integer d such that $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ (which is a subgroup of $\mathbb{Z}$).

Prop. If $d = \gcd(a, b)$ then:

1. $d \mid a$, $d \mid b$.
2. $\exists r, s \in \mathbb{Z}$ s.t. $ar + bs = d$.
3. If $c \mid a$, $c \mid b$, then $c \mid d$.

Two nonzero integers a, b are relatively prime if their $\gcd(a, b) = 1$, i.e., $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

Cor. relatively prime $\iff \exists r, s \in \mathbb{Z}$ s.t. $ar + bs = 1$

Cor. p is a prime number and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

2.5 Cyclic Groups and Cyclic Subgroups

G is a group. $x \in G$. The cyclic subgroup of G generated by x is the set of all powers of x: $< x >= \{x^k \in G | k \in \mathbb{Z}\}$.

Prop. $x \in G$. Let $S = \{k \in \mathbb{Z} | x^k = 1\}$, then S is a subgroup of $\mathbb{Z}$.

H is a subgroup of G. Define the order of H to be the number of elements in H, denoted by $|H|$.

The order of an element g in G is defined as the order of the cyclic subgroup it generates, i.e.,$|g| = |< g >|$.

$$|g| = \begin{cases} \min\{k \in \mathbb{Z} | k > 0, g^k = 1\} & \text{if the set is nonempty and thus has a min} \\ \infty & \text{otherwise} \end{cases}$$

When $|g| < \infty$, $< g >= \{1, g, g^2, ..., g^{|g|-1}\}$.

When $|g| = \infty$, $< g >= \{..., g^{-2}, g^{-1}, 1, g, g^2, ...\}$.

Prop. If $|g| = n$, then $g^k = 1 \iff n \mid k$. $g^l = g^m \iff n \mid l - m$.

If $G =< g >$ for some $g \in G$, we say G is a cyclic group generated by g, and g is a generator of G.

Examples: $\mathbb{Z}^+ =< 1 >=< -1 >$; K_4 (4 elements) and S_3 (6 elements) are not cyclic

Prop. Every subgroup of a cyclic group is a cyclic subgroup. (pf. S is a subgroup of $\mathbb{Z}$.)

2.6 Homomorphisms and Normal Subgroups

G and G' are groups. A homomorphism $f : G \to G'$ is a function sayisfying $\forall a, b \in G$, $f(ab) = f(a)f(b)$. That is, the function is compatible with the group structures.

Prop. A homomorphism $f : G \to G'$ maps identity to identity, and inverse to inverse:

1. $f(1) = 1'$

2. $\forall g \in G$, $f(g)^{-1} = f(g^{-1})$

$f : G \to G'$ is a homomorphism, define

the kernel of f to be $\ker(f) = \{g \in G | f(g) = 1'\}$

the image of f to be $Im(f) = \{f(g) \in G' | g \in G\}$

Prop. $\ker(f)$ is a subgroup of G, $\operatorname{Im}(f)$ is a subgroup of G'.

Prop. $f : G \to G'$ is a homomorphism, then f is injective $\iff \ker(f) = \{1\}$.

Example: $x \in G$, $f : Z \to G$, $f(k) = x^k$ is a homomorphism

$$\ker(f) = \{k \in \mathbb{Z} | x^k = 1\} = \begin{cases} \{0\}, & |x| = \infty \\ |x|\mathbb{Z}, & |x| < \infty \end{cases}$$

$$\operatorname{Im}(f) = \{x^k \in G | k \in \mathbb{Z}\} =< x >$$

Example: $f : G \to G'$, $f(g) = 1'$ $\forall g \in G$ is a homomorphism

$$\ker(f) = G, \operatorname{Im}(f) = \{1'\} \qquad \text{Note: } |\ker(f)| \cdot |\operatorname{Im}(f)| = |G|$$

G is a group. The conjugation of $x \in G$ by $g \in G$ is the element $gxg^{-1} \in G$. We say x and gxg^{-1} are conjugate elements.

A subgroup N of G is called a normal subgroup if $\forall n \in N, \forall g \in G, gng^{-1} \in N$.

For a subgroup N of G, the following are equivalent:

1. N is a normal subgroup of G
2. $\forall g \in G$, $gNg^{-1} \subseteq N$ (equivalent to 1 by definition)
3. $\forall g \in G$, $gNg^{-1} = N$

Example: If G is an abelian group, then any subgroup of G is a normal subgroup of G.

Example: We have shown that $SLn(R) = \ker \det$, so by the above proposition, $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$.

The centre of a group G is the subset $Z(G) = \{g \in G | gx = xg \text{ for any } x \in G\}$.

G is abelian $\iff Z(G) = G$.

$Z(G)$ is a normal subgroup of G.

2.7 Isomorphisms and Automorphisms

An isomorphism is a bijective homomorphism.

Two groups G and G' are called isomorphic if there exists an isomorphism $\phi : G \to G'$, and we write $G \cong G'$. Intuitively, isomorphic groups have the same algebraic structures, and share all the algebraic properties. We can interpret an isomorphism as "a change of name" for the elements in the group.

Example: If $G =< x >$ in an infinite cyclic group, then $\phi : \mathbb{Z} \to G$, $k \mapsto x^k$ is an isomorphism. We've proved ϕ is a homomorphism. $\ker(f) = \{k \in \mathbb{Z} | a^k = 1\} = \{0\}$ $\to$ injective. Definition of $G =< x >$ $\to$ surjective. So bijective homomorphism.

Examples: $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$Aut(\mathbb{Z}) \cong \{\pm 1\}$

$Aut(S_3) \cong S_3$

Prop. The inverse of an isomorphism is also an isomorphism.

An isomorphism $\phi : G \to G$ of a group to itself is called an automorphism of G.

Example: $\phi : \mathbb{Z} \to \mathbb{Z}$, $k \mapsto -k$ is an automorphism.

Example: If G is a group, $g \in G$, then there is an automorphism of G given by conjugation $\phi : G \to G$, $x \mapsto gxg^{-1}$.

The group of automorphisms of G, denoted by $Aut(G)$, is the set of all automorphisms of G with the law of composition to be composition of functions,

Note: The identity of $Aut(G)$ is id_G. The inverse of $f \in Aut(G)$ is its inverse function f^{-1}.

The inner automorphism group of a group G is the subgroup $Inn(G) = \{\phi_g \in Aut(G) | g \in G\}$.

where $\phi_g : G \to G$, $x \mapsto gxg^{-1}$.

$Inn(G)$ is a normal subgroup of $Aut(G)$.