1. GROUPS

Proposition 1. *Let $*$ be an operation on G. If there is a $*$-identity, then it is unique.*

Proposition 2. *Let $*$ be an associative operation on G which has an identity, say e. If $x \in G$ has an inverse, then this inverse is unique.*

Proposition 3. *Let $(G, *, e_G)$ be a group. In a Cayley table for G, each row and each column contains each element of G exactly once.*

Proposition 4. *For each $n \in \mathbb{N}$, the set of multiples of n*

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$. In particular, the set of even integers is a subgroup. Moreover, any subgroup of $(\mathbb{Z}, +, 0)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$.

Theorem 5 (Well-Ordering Principle of the Naturals)**.** *Any non-empty subset of $\mathbb{N}$ has a least element.*

Theorem 6 (Mathematical induction)**.** *Suppose $S \subseteq \mathbb{N}$ is a subset satisfying the following two properties:*

(1) $1 \in S$,
(2) if $n \in S$, then $n+1 \in S$.

Then $S = \mathbb{N}$.

Proposition 7. *Let G be a group and $a, b, c \in G$. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.*

Proposition 8. *Let G be a group and $g \in G$. For all $m, n \in \mathbb{Z}$,*

$$g^m g^n = g^{m+n} = g^{n+m} = g^n g^m.$$

Definition 9. Let G be a group and $h \in G$. A *conjugate* of h is an element of the form ghg^{-1}. The set of all conjugates is denoted by $\mathrm{Conj}(h)$ and

$$\mathrm{Conj}(h) = \{x \in G : \exists g \in G, x = ghg^{-1}\}.$$

The set $\mathrm{Conj}(h)$ is called a conjugacy class containing h.

Proposition 10. *Let G be a group. For all $g, h \in G$, and for all $n \in \mathbb{Z}$,*

$$(ghg^{-1})^n = gh^n g^{-1}.$$

Theorem 11. *Let G be a group. Define $g \sim h$ if $g \in \mathrm{Conj}(h)$. This is a relation on G which is reflexive, symmetric, and transitive. Consequently, conjugation is an equivalence relation on G. Therefore, the collection of conjugacy classes of G forms a partition of G.*

Definition 12. Let G be a group and $g \in G$. We define the *order* of g to be the least (positive) natural number $n \in \mathbb{N}$ such that $g^n = e$, if it exists. If such a number does not exist then we say g has *infinite order*. We denote the order of g by $o(g)$. (Some books write $|g|$.)

Theorem 13. *Let G be a group and $g, h \in G$. Suppose that $g \in \mathrm{Conj}(h)$. Then $o(g) = o(h)$.*

Proposition 14. *We gave many examples of how to prove a subset H of G is a subgroup. Remember that you need to show the following three properties.*

1. *$H \neq \emptyset$.*
2. *$\forall g, h \in H$, $gh \in H$.*
3. *$\forall h \in H$, $h^{-1} \in H$.*

Alternatively, you can also show the "One Step Subgroup Test"; that $H \neq \emptyset$ and that $\forall g, h \in H, gh^{-1} \in H$.

Definition 15. Let $H \leq G$ and $g \in G$. Denote

$$gHg^{-1} = \{x \in G : \exists h \in H, x = ghg^{-1}\}.$$

Proposition 16. *let $H \leq G$ and $g \in G$. then gHg^{-1} is also a subgroup of G and $|H| = |gHg^{-1}|$ (i.e. they have the same cardinality).*

Proof. The map $F : H \to ghg^{-1}$ defined by $F(h) = ghg^{-1}$ is one-to-one and onto, i.e. F is a bijection. □

Definition 17. Let $H \leq G$ and $g \in G$. Denote

$$gH = \{x \in G : \exists h \in H, x = gh\}.$$

The set gH is called the *left coset of H with representative g*.

Proposition 18. *let $H \leq G$ and $g \in G$. The set of left cosets of H gH satisfies $|H| = |gH|$. Moreover, the collection $\{gH\}_{g \in G}$ forms a partition of G. The number of left cosets of H is called the index of H and is denoted by $[G : H]$. The set of left cosets of H is denoted by G/H ("G mod H").*

Theorem 19 (Lagrange's Theorem)**.** *Suppose G is a finite group and $H \leq G$. Then*

$$|G| = |H| \cdot [G : H].$$

In other words, the order of a subgroup divides the order of a group. Furthermore, it follows that the order of an element of G divides the order of G.

Definition 20. Recall that a *permutation on a set A* is a bijection from A to A. The set of all permutation on A is denoted by S_n and $(S_n, \circ, id_A)$ is a group under composition. When $A = \{1, 2, \ldots, n\}$, then we instead write S_n. Observe that $|S_n| = n!$.

A permutation $\sigma \in S_n$ is called a k-cycle if it has the form $(a_1\ a_2\ \cdots\ a_k)$ for distinct $a_i \in \{1, \ldots, n\}$. The order of a k-cycle is k. Two different k-cycles, say $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (b_1\ b_2\ \cdots\ b_j)$ are said to be disjoint if $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_j\} = \emptyset$.

Lemma 21. *Disjoint cycles commute.*

Theorem 22. *Each $\sigma \in S_n$ can be written as a product of disjoint cycles.*

Definition 23. A k-cycle is said to be even if k is odd, and said to be odd if k is even. The identity is an even permutation. To each k-cycle σ we define the signature of σ, denoted $\text{sgn}(\sigma)$ as 1 or -1 depending on whether it is even or odd, respectively. We then can define the signature of an arbitrary permutation by setting $\text{sgn}(\sigma) = -1$ if there is an odd number of even-cycles in its unique cycle decomposition. Define $\text{sgn}(\sigma) = 1$ otherwise.

Define σ to be *even* if $\text{sgn}(\sigma) = 1$, and odd otherwise. The set of all even permutations in S_n is denoted by A_n and called the alternating group.

Proposition 24. *For each $n \geq 3$, $A_n \leq S_n$.*

Definition 25. Let H be a subgroup of G. We say *H is a normal subgroup of G*and write $H \trianglelefteq G$ if H satisfies $\forall g \in G, gHg^{-1} = H$.

The trivial subgroups of G are both normal.

Theorem 26. *Suppose $H \leq G$. Then the following statements are equivalent.*

1. *$H \trianglelefteq G$.*
2. *$\forall g \in H$, $gHg^{-1} \subseteq H$.*
3. *$\forall h \in H$, $gH = Hg$.*

Remark 27. In each of the following cases we can conclude that H is a normal subgroup of G.

1) If H is a the unique subgroup of G of size $|H|$.

2) $[G : H] = 2$. In particular $A_n \trianglelefteq S_n$.

3) $H \subseteq Z(G)$. In particular, $Z(G) \trianglelefteq G$.

Definition 28. Let $(G,\cdot,e_G)$ and $(H,\triangle,e_H)$ be two groups. A function $\varphi : G \to H$ is called a *group homomorphism* if for all $g_1, g_2 \in G$,

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \triangle \varphi(g_2).$$

A group homomorphism which is also a bijection is called an *isomorphism*.

Proposition 29. *Suppose $\varphi : G \to H$ is a group homomorphism and $g \in G$. Then*
1) $\varphi(e_g) = e_H$
2) For all $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.
3) $o(\varphi(g)) \mid o(g)$.
4) If G is cyclic and φ is onto, then H is cyclic.
5) If G is abelian and φ is onto, then H is abelian.
6) If φ is an isomorphism, then $|G| = |H|$. But not conversely.

Definition 30. let $\varphi : G \to H$ be a group homomorphism. The *kernel of* φ is the set

$$\ker\varphi = \{g \in G : \varphi(g) = e_H\}.$$

Proposition 31. *Suppose $\varphi : G \to H$ is a group homomorphism. Then* $\ker\varphi \trianglelefteq G$.

Proposition 32. *Suppose $N \trianglelefteq G$. Then the map $\pi : G \to G/N$ defined by*

$$\pi(g) = gN$$

is a group homomorphism and $\ker\pi = N$.

Proposition 33. *If $G/Z(G)$ is cyclic, then G is abelian.*

Theorem 34 (First Isomorphism Theorem)**.** *Suppose $\varphi : G \to H$ is a group homomorphism. Then* $\ker\varphi \trianglelefteq G$, *$\varphi(G) \leq H$, and there is an isomorphism $\bar{\varphi} : G/\ker\varphi \to \varphi(G)$ such that*

$$\bar{\varphi} \circ \pi_{\ker\varphi} = \varphi$$

Definition 35. An isomorphism from a group onto itself is called an *automorphism*. The set of all automorphisms from G onto G is denoted by $\mathrm{Aut}(G)$ and it is a group under composition with identity the identity function.

Let $g \in G$. The map $\phi^g : G \to G$ defined by conjugation $\phi^g(x) = gxg^{-1}$ is an automorphism. An an automorphism that is given by conjugation is called an *inner automorphism*. The set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Proposition 36. *For any group G,* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. *Moreover,* $G/Z(G) \cong \mathrm{Inn}(G)$.

Theorem 37 (Cauchy's Theorem for finite Abelian Groups)**.** *Suppose G is an abelian group and p is a prime. If $p \mid\mid G|$, then G has an element of order p.*

Definition 38. Let G be a group and A a set. We say G acts on A is there is a map $\cdot : G \times A \to A$ such that

(1) $e_g \cdot a = a$ for all $a \in A$;
(2) for all $g_1, g_2 \in G$, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$.

Suppose G acts on A. For $a \in A$, call the set $G_a = \{g \in G : g \cdot a = a\}$ the *stabilizer of a*. For each $a \in A$, $G_a \leq G$. We also define the *orbit of a* to be the set $\mathcal{O}_a = \{b \in A : \exists g \in G, g \cdot a = b\}$.

Theorem 39 (Orbit-stabilizer Theorem)**.** *Suppose G acts on A. For any $a \in A$,*

$$|\mathcal{O}_a| = [G : G_a].$$

Example 40. The following are groups under addition +:

(1) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
(2) $Z_n = \{0, 1, 2, \ldots, n-1\}$
(3) $M_2(\mathbb{R})$
(4) $\mathbb{R}[x]$ the set of real polynomials.

Example 41. The following are groups under addition multiplication:

(1) $\mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$
(2) F^* for any field F.
(3) $SL_2(\mathbb{R}) \leq GL_2(\mathbb{R})$.

Example 42. Suppose $(G, *, e_G)$ and $(H, \triangle, e_H)$ are groups. then $G \times H$ is a group with operation defined by

$$(g_1, h_1) \otimes (g_2, h_2) = (g_1 * g_2, h_1 \triangle h_2).$$

The identity of this group is (e_G, e_H) and for any $(g, h) \in G \times H$,

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

Example 43. Let $1 < n$ and denote bu $U(n)$ the group of units of $\mathbb{Z}_n$ under multiplication. Specifically,

$$U(n) = \{k \in \mathbb{Z}_n | gcd(k, n) = 1\}.$$

Also note that the elements of $U(n)$ are precisely the generators of the group $\mathbb{Z}_n$.

Example 44. The group of rigid motions on a regular n-sided polygon is called a dihedral group and we denote it by D_n. We can label the vertices in a counter-clockwise fashion $1, 2, \ldots, n$. The rotation by $\frac{360^\circ}{n}$ is denoted by r and the flip through the line of symmetry through 1 is denoted by s.

Observe that if $n = 2k$ is even then the line of symmetry goes through the vertex $k+1$, while if n is odd then it goes through the mid-point of the vertices $\frac{n+1}{2}$ and $\frac{n+3}{2}$.

Now you can show that $srs^{-1} = r^{-1}$. Next,

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

In terms of generators and relations

$$D_n = < r, s | r^n = e = s^2 \text{ and } srs^{-1} = r > .$$

Example 45. 1) If G is abelian then the collection of singleton sets of G, $\{ \{g\} : g \in G\}$ is the collection of the conjugacy classes of G.

2) The set of conjugacy classes of D_3 is $\{\{e\}, \{r, r^2\}, \{s, sr, sr^2\}\}$.

Example 46. The following are examples of subgroups of a given group G.

1. The *center* of G
$$Z(G) = \{x \in G | \forall g \in G \ (xg = gx)\}.$$
2. For $g \in G$, the *cyclic subgroup generated by g*
$$< g >= \{x \in G | \exists n \in \mathbb{Z} \ (x = g^n)\}.$$
3. For a given subgroup $H \leq G$, the *centralizer of H*
$$C(H) = \{x \in G | \ \forall h \in H \ (xh = hx)\}.$$
4. For a family of subgroups $\{H_i\}_{i \in I}$, the intersection $\bigcap_{i \in I} H_i$.
5. If G is abelian, then the set of finite order (i.e. *torsion*) elements
$$t(G) = \{x \in G | \ o(x) < \infty\}.$$

6. For a given subgroup $H \leq G$ and $g \in G$, the *g-conjugates of H*
$$gHg^{-1} = \{x \in G | \ \exists h \in H \ (x = ghg^{-1})\}.$$
7. For a given subgroup $H \leq G$, the *normalizer of H*
$$N(H) = \{x \in G | \ xHx^{-1} = H\}.$$