Math 3030 Algebra I
Review of basic group theory

1 Groups

Definition 1.1. *A **group** $(G, *)$ is a nonempty set G together with a binary operation*

$$G \times G \to G,$$
$$(a, b) \mapsto a * b,$$

*called the **group operation** or "**multiplication**", such that*

(1) $*$ *is **associative**, i.e.*
$$(a * b) * c = a * (b * c)$$
for any $a, b, c \in G$.

(2) *There exists an element $e \in G$, called an **identity**, such that*
$$a * e = e * a = a$$
for any $a \in G$.

(3) *Each element $a \in G$ has an **inverse** $a^{-1} \in G$, i.e.*
$$a * a^{-1} = a^{-1} * a = e.$$

Remark 1.2. *We often write $a \cdot b$, or simply ab, to denote $a * b$.*

It is straightforward to show that both the identity and inverse of any given element are unique, and also that the **cancellation laws** hold, i.e. for any $a, b, c \in G$, $ab = ac$ implies that $b = c$ and likewise $ba = ca$ implies that $b = c$, which can be used to show that $(ab)^{-1} = b^{-1}a^{-1}$ for any $a, b \in G$ (or more generally, $(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1}$ for any $a_1, a_2, \ldots, a_k \in G$).

Definition 1.3. *The **order** of G, denoted as $|G|$, is the number of elements in G. We call G **finite** (resp. **infinite**) if $|G| < \infty$ (resp. $|G| = \infty$).*

Definition 1.4. *If the group operation is commutative, i.e. $ab = ba$ for any $a, b \in G$, we say that G is **abelian**; otherwise, G is said to be **nonabelian**.*

Remark 1.5. *When G is abelian, we usually use $+$ to denote the group operation, 0 to denote the identity, and $-a$ to denote the inverse of an element $a \in G$.*

Here are some examples of groups:

(1) Given any field F equipped with the addition $+$ and multiplication $\cdot$, both $(F, +)$ and $(F^\times := F \setminus \{0\}, \cdot)$ are abelian groups. Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with the usual addition and multiplication.

(2) Given a commutative ring R with unity, the set of units $R^\times$ is an abelian group under ring multiplication.

(3) The set of integers $\mathbb{Z}$ is an abelian group under addition, but the set of nonzero integers $\mathbb{Z} \setminus \{0\}$ is *not* a group under multiplication.

(4) For any nonzero integer n, the set (of equivalence classes) $\mathbb{Z}_n$ is a finite abelian group under addition mod n.

(5) Any vector space V is an abelian group under the addition. (This is part of the definition of a vector space.)

(6) The set of all $m \times n$ matrices is an abelian group under matrix addition. More generally, given any group G and a nonempty set X, the set of all maps from X to G form a group using the group operation in G, which is abelian if G is so.

(7) The set of all nonsingular $n \times n$ matrices with coefficients in a field F is a group under multiplication, denoted by $GL_n(F)$ and called the **general linear group over** F. For $n \geq 2$, this group is nonabelian.

(8) Let X be a nonempty set, and let S_X be the set of all bijective maps (permutations) $\sigma : X \to X$. Then S_X is a group under composition of maps, called the **symmetric group on** X. For any positive integer n, the group S_{I_n}, where $I_n := \{1, \dots, n\}$, is denoted as S_n and called the n**-th symmetric group**. For $n \geq 3$, S_n is a finite nonabelian group.

(9) If G_1, G_2 are groups, then the Cartesian product $G_1 \times G_2$ is naturally a group whose multiplication is defined componentwise; this is called the **direct product** of G_1 and G_2. Similarly, one can define the direct product of *any* number of groups.

2 Subgroups

Definition 2.1. *Let $(G, *)$ be a group. Let $H \subset G$ be a subset. If H is closed under $*$, i.e. $a * b \in H$ for any $a, b \in H$ and H is a group under the induced group operation $*$, then we call H a* ***subgroup*** *of G, denoted by $H < G$.*

To check that a (nonempty) subset is a subgroup, we have the following very useful criterion:

Proposition 2.2. *A nonempty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for any $a, b \in H$.*

Proposition 2.3. *A finite subset H of a group G is a subgroup if and only if H is nonempty and closed under multiplication.*

Here are some examples of subgroups:

(1) We have $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ under addition, and $\mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$ under multiplication.

(2) For any group G, we have $\{e\} < G$ (called the **trivial subgroup**) and $G < G$. A subgroup $H \lneqq G$ is called **proper** and a subgroup $\{e\} \lneqq H < G$ is called **nontrivial**.

(3) Vector subspaces are additive subgroups.

(4) The subset
$$SL_n(F) := \{M \in GL_n(F) \mid \det M = 1\}$$
is a subgroup of $GL_n(F)$, called the **special linear group**. We also have the subgroups
$$O_n(F) = \{M \in GL_n(F) \mid M^T M = I_n = MM^T\},$$
$$SO_n(F) = \{M \in O_n(F) \mid \det M = 1\}$$
of $GL_n(F)$, called the **orthogonal group** and **special orthogonal group** respectively, where M^T denotes the transpose of M and I_n denotes the $n \times n$ identity matrix. For $F = \mathbb{C}$, we have the subgroups
$$U(n) = \{M \in GL_n \mid M^* M = I_n = MM^*\},$$
$$SU(n) = \{M \in U_n \mid \det M = 1\}$$
of $GL_n(\mathbb{C})$, called the **unitary group** and **special unitary group** respectively, where M^* denotes the conjugate transpose of M. When $n = 1$, this gives the **circle group**
$$U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$$
as a multiplicative subgroup of $\mathbb{C}^\times$.

Remark 2.4. *The above are examples of* ***matrix groups****, which are in turn examples of* ***Lie groups****. When F is a finite field, they for an important class of finite simple groups.*

3 Homomorphisms and isomorphisms

Definition 3.1. *A map $\phi : G \to G'$ from a group G to another group G' is called a* ***homomorphism*** *if*
$$\phi(ab) = \phi(a)\phi(b)$$
for any $a, b \in G$. If ϕ is furthermore bijective, then it is called an ***isomorphism****. We say that G is* ***isomorphic*** *to G', denoted by $G \cong G'$, if there exists an isomorphism ϕ from G to G'. An isomorphism from G onto itself is called an* ***automorphism****; the set of all automorphisms of a group G is a group itself, denoted by Aut(G).*

Remark 3.2. *If ϕ is an isomorphism, then ϕ^{-1} is automatically an isomorphism.*

Isomorphic groups share the same algebraic properties (they only differ by relabeling of their elements). One of the most important questions in group theory is to *classify* all groups up to isomorphism.

Examples of homomorphisms:

(1) A linear map (resp. isomorphism) between two vector spaces V and W is a homomorphism (resp. isomorphism) between the abelian groups $(V, +)$ and $(W, +)$.

(2) The determinant $\det : GL_n(F) \to F^\times$ is a homomorphism.

(3) The exponential function $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ is an isomorphism, whose inverse is the logarithm $\log$.

(4) For any nonzero integer n, $n\mathbb{Z} < \mathbb{Z}$ and the map $\phi : n\mathbb{Z} \to \mathbb{Z}$ defined by $\phi(nk) = k$ is an isomorphism. So $\mathbb{Z}$ and its proper subgroup $n\mathbb{Z}$ (when $|n| \geq 2$) are abstractly isomorphic.

(5) For any positive integer n, the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by mapping k to its reminder when divided by n is a surjective homomorphism.

(6) The map

$$SO_2(\mathbb{R}) \to U(1), \quad \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mapsto e^{\mathbf{i}\theta}$$

is an isomorphism.

(7) The finite groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are *not* isomorphic though they have the same order.

4 Cyclic groups; generating sets

4.1 Cyclic (sub)groups

Definition 4.1. *Let G be a group and $a \in G$ be any element. Then the subset*

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

*is a subgroup of G, called the **cyclic subgroup** generated by a. The **order** of a, denoted by $|a|$, is defined as the order of $\langle a \rangle$.*

Proposition 4.2. *If $|a| < \infty$, then $|a|$ is the smallest positive integer k such that $a^k = e$.*

Definition 4.3. *A group G is called **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$. In this case, we say a **generates** G, or a is a **generator** of G.*

Proposition 4.4. *Every cyclic group is abelian.*

Remark 4.5. *The converse is false.*

Theorem 4.6. *(Classification of cyclic groups) Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. Any cyclic group of finite order n is isomorphic to $(\mathbb{Z}_n, +)$.*

For example, the set of n-th roots of unity $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$ is a cyclic subgroup of $U(1)$. By the above theorem, U_n is isomorphic to $\mathbb{Z}_n$. (This is a better way to visualize the adjective "cyclic".) In fact, U_n is generated by $\exp \frac{2\pi\mathbf{i}}{n}$. (How about the cyclic subgroup generated by $\exp 2\pi\mathbf{i}t$ where $t \in \mathbb{R}$?)

Proposition 4.7. *A subgroup of a cyclic group is also cyclic.*

Corollary 4.8. *Any subgroup of* $\mathbb{Z}$ *is of the form* $n\mathbb{Z}$ *for* $n \in \mathbb{Z}$.

Theorem 4.9. *(Classification of subgroups of a finite cyclic group) Let* $G = \langle a \rangle$ *be a cyclic group of finite order* n. *Let* $a^s \in G$. *Then* $|a^s| = n/d$ *where* $d = \gcd(s, n)$. *Moreover,* $\langle a^s \rangle = \langle a^t \rangle$ *if and only if* $\gcd(s, n) = \gcd(t, n)$.

Corollary 4.10. *All generators of a cyclic group* $G = \langle a \rangle$ *are of the form* a^r *where* r *is relatively prime to* n.

For example, $\mathbb{Z}_{18}$ is generated by 1, 5, 7, 11, 13 or 17.

4.2 Generating sets

Proposition 4.11. *The intersection of any collection of subgroups is also a subgroup.*

Definition 4.12. *Let* G *be a group, and* $A \subset G$ *any subset. The smallest subgroup* $\langle A \rangle$ *of* G *containing* A *is called the* ***subgroup generated by*** A. *By the above proposition, we must have*

$$\langle A \rangle = \bigcap_{\{H<G \mid A \subset H\}} H.$$

If $G = \langle A \rangle$, *then we say that the subset* A ***generates*** G. *If* G *is generated by a finite set* A, *then we say that* G *is* ***finitely generated****.*

Remark 4.13. *In practice, the subgroup generated by a subset* A *is given by the set of all* finite *products of powers of elements in* A, *i.e.*

$$\langle A \rangle = \{a_1^{k_1} \cdots a_n^{k_n} \mid a_i \in A, k_i \in \mathbb{Z}\}.$$

For example, there are 2 distinct groups of order 4: the cyclic group $\mathbb{Z}_4$ and the **Klein 4-group** V, which is not cyclic, but is finitely generated and abelian; in fact, $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is generated by $(1, 0)$ and $(0, 1)$.

Remark 4.14. *All groups of order less than or equal to 3 are cyclic.*

As another example, the group $SL_2(\mathbb{Z})$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Remark 4.15. *Not all abelian groups are finitely generated, e.g.* $\mathbb{Q}$, $\mathbb{R}$.

5 Symmetric groups and dihedral groups

5.1 Symmetric groups

Recall that, given an integer $n \geq 2$, the n-th symmetric group S_n is the set of bijective maps from the set $I_n = \{1, \ldots, n\}$ onto itself equipped with the composition of maps. Elements of S_n are called **permutations** (of I_n).

For example, a permutation in S_{10} is of the form

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 7 & 8 & 9 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

Definition 5.1. *Let $i_1, i_2, \ldots, i_r$ ($r \leq n$) be distinct elements of I_n. Denote by $(i_1, i_2, \ldots, i_r)$ the permutation*

$$i_1 \mapsto i_2,\ i_2 \mapsto i_3,\ \ldots,\ i_{r-1} \mapsto i_r,\ i_r \mapsto i_1$$

*and $j \mapsto j$ for any $j \in I_n \setminus \{i_1,\ i_2, \ldots, i_r\}$. We call $(i_1, i_2, \ldots, i_r)$ an r-**cycle**, and r is the **length** of the cycle. A 2-cycle is also called a **transposition**.*

For example, in S_5, we have

$$(1,3,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (5,4,1,3).$$

Proposition 5.2. *Every permutation $\sigma \in S_n$ is a product of disjoint cycles (unique up to ordering of the terms in the product). In particular, S_n is generated by cycles.*

For example, in S_8, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1,3,6)(2,8)(4,7,5).$$

Remark 5.3. *Composition of disjoint cycles is commutative.*

Proposition 5.4. *For an r-cycle μ, we have $|\mu| = r$. Hence, if we write a permutation σ as a product of disjoint cycles $\sigma = \mu_1\mu_2 \cdots \mu_k$, then*

$$|\sigma| = \mathit{lcm}(r_1, r_2, \ldots, r_k),$$

where $r_i = |\mu_i| =$ length of μ_i.

Since $(i_1, i_2, \ldots, i_r) = (i_1, i_r)(i_1, i_{r-1}) \cdots (i_1, i_3)(i_1, i_2)$, we have

Proposition 5.5. *Every permutation is a product of transpositions. In particular, S_n is generated by transpositions.*

Corollary 5.6. *S_n is generated by $(1,2)$ and $(1, 2, \ldots, n)$.*

Note that the decomposition in Proposition 5.5 is not unique, e.g.

$$(1,2,3) = (1,3)(1,2) = (1,3)(2,3)(1,2)(1,3).$$

However, the *parity* is well-defined:

Proposition 5.7. *No permutation can be expressed both as a product of an even number of transpositions and also as a product of an odd number of transpositions.*

Hence the following definition makes sense.

Definition 5.8. *A permutation $\sigma \in S_n$ is called **even** (resp. **odd**) if it can be expressed as a product of an even (resp. odd) number of transpositions.*

Proposition 5.9. *Let A_n be the subset of all even permutations in S_n. Then A_n is a subgroup, called the n-**th alternating group**. Moreover, the order of A_n is $|S_n|/2 = n!/2$.*

5.2 Dihedral groups

Given an integer $n \geq 3$, we let $\Delta = \Delta_n \subset \mathbb{R}^2$ be a regular n-gon centered at the origin. An **isometry** is a distance-preserving map between metric spaces. If we equip $\mathbb{R}^2$ with the Euclidean metric, then a **symmetry** of Δ is an isometry (or rigid motion) $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ such that $\phi(\Delta) = \Delta$.

Definition 5.10. *The n**-th dihedral group** D_n is the set of symmetries of Δ equipped with composition of maps.*

We make the following observations:

(1) Enumerating the vertices of Δ as $1, 2, \ldots, n$ (say, in the counter-clockwise direction), we can view each element of D_n as a permutation of $I_n = \{1, 2, \ldots, n\}$. Also note that two distinct symmetries will give rise to two distinct permutations of I_n. So we may regard D_n as a subgroup of S_n.

(2) There is a complete classification of isometries of $\mathbb{R}^2$: **translations**, **rotations**, **reflections** and **glide reflections**. But a symmetry of Δ fixes the origin $0 \in \mathbb{R}^2$ and both translations and glide reflections have no fixed points, so that D_n consists of *only* rotations and reflections.

(3) Let $a \in D_n$ be the rotation by the angle $2\pi/n$ in the counter-clockwise direction. Then the set of rotations in D_n is given by $\langle a \rangle = \{\text{id}, a, a^2, \ldots, a^{n-1}\}$. On the other hand, there are n reflections in D_n. So we conclude that

$$|D_n| = 2n.$$

Furthermore, the composition of two reflections is a rotation (which can be seen by flipping a 2-dollar coin). Hence if we let $b \in D_n$ be any reflection, then the set of reflections in D_n is given by $\{b, ab, a^2b, \ldots, a^{n-1}b\}$. In particular,

$$D_n = \langle a, b \rangle.$$

(4) There are three relations among a and b:

$$a^n = 1, \ b^2 = 1, \ ab = ba^{-1}.$$

(Again you can confirm this by playing with a 2-dollar coin.) In fact, they are all the relations, so that we have a **presentation**

$$D_n = \langle a, b \mid a^n = b^2 = abab = 1 \rangle.$$

Remark 5.11. *Some authors use D_{2n} to denote the n-th dihedral group. An excellent reference for dihedral groups and other interesting groups of symmetries is Michael Artin's textbook* Algebra *(Chapter 5).*

Remark 5.12. *The dihedral groups form a class of finite subgroups of $SO_3(\mathbb{R})$. The others are given by: finite cyclic groups and the groups of symmetries of the* Platonic solids *(there are 5 of such solids, corresponding to 3 different groups).*

6 Cosets and the theorem of Lagrange

Given a subgroup $H < G$, we can define two equivalence relations:

$$a \sim_L b \Leftrightarrow a^{-1}b \in H,$$
$$a \sim_R b \Leftrightarrow ab^{-1} \in H.$$

These induce two partitions of G, whose equivalence classes are called cosets of H:

Definition 6.1. *Let $H < G$, and $a \in G$. The sets $aH := \{ah \mid h \in H\}$ and $Ha := \{ha \mid h \in H\}$ are called the* ***left*** *and* ***right coset*** *of H containing a respectively.*

Here are some examples:

(1) Let n be a positive integer. Consider the subgroup $n\mathbb{Z} < \mathbb{Z}$. Then the cosets are given by

$$\{k + n\mathbb{Z} \mid k \in \mathbb{Z}\} = \{k + n\mathbb{Z} \mid k \in \{0, 1, \ldots, n-1\}\},$$

which is in a 1-1 correspondence with elements of $\mathbb{Z}_n$.

Remark 6.2. *When G is abelian, any left coset is equal (as a subset) to the corresponding right coset, and we usually use $a + H$ to denote a coset.*

(2) For $\mathbb{Z} < \mathbb{R}$, the cosets are given by

$$\{t + \mathbb{Z} \mid t \in \mathbb{R}\} = \{t + \mathbb{Z} \mid t \in [0, 1)\},$$

which is in a 1-1 correspondence with the circle group $U(1)$ (by mapping $t + \mathbb{Z}$ to $\exp 1\pi \mathbf{i} t$).

(3) Given a vector subspace $W \subset V$, the cosets of the additive subgroup $(W, +) < (V, +)$ are given by the *affine translates* of the subspace W:

$$\{v + W \mid v \in V\}.$$

If we choose another subspace $Q \subset V$ which is complementary to W, i.e. such that $Q \cap W = \{0\}$ and $\dim(Q) = \dim(V) - \dim(W)$, then each coset is represented by a unique element in Q:

$$\{v + W \mid v \in V\} = \{v + W \mid v \in Q\}.$$

(4) Consider $S_3 = \{\text{id}, \rho, \rho^2, \mu, \rho\mu, \rho^2\mu\}$, where $\rho = (1, 2, 3)$ and $\mu = (1, 2)$. Let H be the cyclic subgroup generated by μ. Then the left cosets are

$$H = \{\text{id}, \mu\},\ \rho H = \{\rho, \rho\mu\},\ \rho^2 H = \{\rho^2, \rho^2\mu\},$$

while the right cosets are

$$H = \{\text{id}, \mu\},\ H\rho = \{\rho, \rho^2\mu\},\ H\rho^2 = \{\rho^2, \rho\mu\}.$$

Note that $\rho H \neq H\rho$ and $\rho^2 H \neq H\rho^2$.

Since any two cosets are of the same cardinality as H, we have the important:

Theorem 6.3. *(Theorem of Lagrange) Suppose that G is a finite group. Then $|H|$ divides $|G|$ for any subgroup $H < G$.*

Corollary 6.4. *Suppose that G is a finite group. Then $a^{|G|} = e$ for any $a \in G$.*

Corollary 6.5. *Every group of prime order is cyclic.*

Definition 6.6. *Let $H < G$. The number of distinct left (or right) cosets of H in G, denoted by $[G : H]$, is called the* ***index*** *of H in G.*

Remark 6.7. *The index $[G : H]$ may be infinite. But if G is finite, then (the proof of) the Theorem of Lagrange implies that*

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