0. The handout is a continuation of the Handout *Abelian groups, integral domains and fields*. We introduce an algebraic structure, namely, groups, slightly more general than abelian groups.

   For a more extensive treatment on the notion of groups, refer to your *algebraic structures* course.

1. Inspect Theorem (1), Theorem (2), Theorem (3) below:

   - Theorem (1) follows trivially from the definition for the notion of abelian groups. (Refer to the Handout *Abelian groups, integral domains and fields*.)
   - Theorem (2) follows from the various properties for the notion of bijectivity and inverse functions.
   - Theorem (3) follows from the various properties for the notion of non-singularity of square matrices with real entries.

   Theorem (1).

   Let A be a set, and $\bullet$ be a closed binary operation on A. Suppose A forms an abelian group under $\bullet$. Then the statements below hold:

   (a) *For any $x, y \in A$, $x \bullet y \in A$.*

   (b) *For any $x, y, z \in A$, $(x \bullet y) \bullet z = x \bullet (y \bullet z)$.*

   (c) *There exists some $e \in A$ such that for any $x \in A$, $e \bullet x = x = x \bullet e$.*

   (d) *For any $x \in A$, there exists some $v \in A$ such that $v \bullet x = e = x \bullet v$.*

   Theorem (2).

   Let S be a set. Define $\mathsf{Bij}(S)$ by $\mathsf{Bij}(S) = \{\varphi \in \mathsf{Map}(S, S) : \varphi$ is a bijective function from S to $S\}$.

   The statements below hold:

   (a) For any $\varphi, \psi \in \mathsf{Bij}(S)$, $\varphi \circ \psi \in \mathsf{Bij}(S)$.

   (b) For any $\varphi, \psi, \xi \in \mathsf{Bij}(S)$, $(\varphi \circ \psi) \circ \xi = \varphi \circ (\psi \circ \xi)$.

   (c) There exists some $\varepsilon \in \mathsf{Bij}(S)$, namely $\varepsilon = \mathsf{id}_S$, and for any $\varphi \in \mathsf{Bij}(S)$, $\varepsilon \circ \varphi = \varphi = \varphi \circ \varepsilon$.

   (d) For any $\varphi \in \mathsf{Bij}(S)$, there exists some $\zeta \in \mathsf{Bij}(S)$, namely, $\zeta = \varphi^{-1}$, such that $\zeta \circ \varphi = \mathsf{id}_S = \varphi \circ \zeta$.

   Theorem (3).

   Let n be a positive integer. Define $\mathsf{GL}(\mathbb{R}^n)$ by $\mathsf{GL}(\mathbb{R}^n) = \{K \in \mathsf{Mat}_{n\times n}(\mathbb{R}) : \det(K) \neq 0.\}$.

   ($\mathsf{GL}(\mathbb{R}^n)$ is the set of all non-singular $(n \times n)$-square matrices with real entries.)

   The statements below hold:

   (a) For any $J, K \in \mathsf{GL}(\mathbb{R}^n)$, $JK \in \mathsf{GL}(\mathbb{R}^n)$.

   (b) For any $J, K, L \in$, $(JK)L = J(KL)$.

   (c) There exists some $E \in \mathsf{GL}(\mathbb{R}^n)$, namely $E = \mathbf{1}_n$, and for any $K \in \mathsf{GL}(\mathbb{R}^n)$, $EK = K = KE$.

   (d) For any $K \in \mathsf{GL}(\mathbb{R}^n)$, there exists some $L \in \mathsf{GL}(\mathbb{R}^n)$, namely, $L = K^{-1}$, such that $LK = \mathbf{1}_n = KL$.

   Theorem (1), Theorem (2), Theorem (3) suggest the presence of some common algebraic structure for various mathematical objects. This mathematical structure is usually referred to as **group structure**.

2. **Definition**.

   Let G be a non-empty set, and $\bullet$ be a closed binary operation on G. We say $(G, \bullet)$ is a **group** *(or, G forms a group under $\bullet$,) if it satisfies the conditions* (GR1)-(GR3) *below:*

   (GR1) *For any $r, s, t \in A$, $(r \bullet s) \bullet t = r \bullet (s \bullet t)$.*

   (GR2) *There exists some $e \in A$ such that for any $r \in A$, $e \bullet r = r = r \bullet e$.*

   (GR3) *For any $r \in A$, there exists some $v \in A$ such that $v \bullet r = r \bullet v = e$.*

   Remarks on terminologies. We usually refer to the closed binary operation $\bullet$ on G as the **group operation** for (the group) G.

- By virtue of (GR1), we say the **Law of Associativity** holds in $(G, \bullet)$.
- By virtue of (GR2), we say the **Law of Existence of Identity** holds in $(G, \bullet)$, and e is called an **identity element** of $(G, \bullet)$.
- By virtue of (GR3), we say the **Law of Existence of Inverse** holds in $(G, \bullet)$, and each such v is called an **inverse** of the corresponding r in $(G, \bullet)$.

3. **Examples on groups.**

   Theorem (1), Theorem (2), Theorem (3) gives rise to three basic examples on groups.

   (a) Every abelian group is a group.

   A group is an abelian group exactly when the group operation for the group is commutative.

   (b) For each set S, the set $\mathsf{Bij}(S)$ of all bijective functions from S to itself forms a group under the group operation $\circ$, which is the composition of functions

   $(\mathsf{Bij}(S), \circ)$ is not an abelian group whenever S has three or more elements.

   When S is a finite set, we refer to $(\mathsf{Bij}(S), \circ)$ as the group of permutations on S. Each bijective function from S to itself is called a permutation on S.

   (c) For each positive integer n, the set $\mathsf{GL}(\mathbb{R}^n)$ of all non-singular $(n \times n)$-square matrices with real entries form a group under the group operation which is matrix multiplication.

   $(\mathsf{GL}(\mathbb{R}^n), \cdot)$ is not an abelian group whenever $n \geq 2$.

   In fact, every group can be 'visualized' as a group of bijective functions from some set to itself. Many interesting groups arise as groups of matrices with entries in some field.

4. **Basic properties of groups.**

   Basic 'rules of arithmetic' which are valid for abelian groups remain valid for groups as long as they do not depend on the Law of Commutativity for abelian groups.

   Theorem (4).

   Let $(G, \bullet)$ be a group. The following statements hold:

   (a) *$(G, \bullet)$ has a unique identity element.*

   (b) *Every element of G has a unique inverse in $(G, \bullet)$.*

   (c) *For any $r, s \in G$, there exists some unique $t \in G$ such that $r = s \bullet t$.* (Or equivalent, *for any $r, s \in G$, the equation $r = s \bullet u$ with unknown u in G has a unique solution.*)

   (d) *For any $r, s \in G$, there exists some unique $t \in G$ such that $r = t \bullet s$.* (Or equivalent, *for any $r, s \in G$, the equation $r = u \bullet s$ with unknown u in G has a unique solution.*)

   Remarks.

   - We tend to write '$r \bullet s$' as 'rs', omitting the symbol for the closed binary operation altogether.
     We tend to denote its identity element denoted by '1' and call it 'one'.

     We tend to denote the inverse of any r in the group as r^{-1} and call it 'r-inverse'.

     For any $r, s \in G$, we present the unique solution to equation $r = su$ with unknown u in G as $u = s^{-1}r$, and we present the unique solution to the equation $r = us$ with unknown u in G as $u = rs^{-1}$. Note that $s^{-1}r$, rs^{-1} are not necessarily equal because the group G is not necessarily an abelian group.

   Theorem (5).

   Let $(G, \bullet)$ be a group. The statements below hold:

   (a) *For any $r, s, t \in A$, if $r \bullet t = s \bullet t$ then $r = s$.*

   (b) *For any $r, s, t \in A$, if $t \bullet r = t \bullet s$ then $r = s$.*

   (c) *For any $r \in G$, $\left(r^{-1}\right)^{-1} = r$.*

   (d) *For any $r, s \in G$, $(r \bullet s)^{-1} = s^{-1} \bullet r^{-1}$.*