Math 541 Modern Algebra

Fall 2024

Contents

1 Introduction **2**
- 1.1 Syllabus . . . 2
- 1.2 Some General Suggestions . . . 4
- 1.3 Some examples of applications of algebra . . . 4

2 A Review of Set Theory **6**
- 2.1 Sets, Subsets, Empty Sets and Power Sets . . . 6
- 2.2 Unions, intersections and set differences . . . 7
- 2.3 Ordered Pairs, Cartesian products and Relations . . . 7
- 2.4 Functions . . . 8
- 2.5 Equivalence relations . . . 10

3 Groups **12**
- 3.1 Groups, subgroups, homomorphisms . . . 12
- 3.2 Basic Properties, Automorphism Groups . . . 14
- 3.3 Kernels, Quotients, Isomorphism Theorem . . . 16

4 Group Actions **20**
- 4.1 Left G sets, invariant subsets, equivariant maps . . . 20
- 4.2 Basic Properties, Stablizers . . . 21
- 4.3 Permutation representation, Caylay's Theorem . . . 22
- 4.4 Orbit decomposition, Cosets . . . 23
- 4.5 Applications . . . 25
  - 4.5.1 Cycle Notation . . . 25
  - 4.5.2 Lagrange's Theorem . . . 25

5 Rings and Modules **26**

6 Congurence Problem **26**

1 Introduction

1.1 Syllabus

Institution Name: University of Wisconson-Madison

Credits: 3

Course Designation: Breadth - Natural Science
Level - Advanced
L&S Credit - Counts as Liberal Arts and Science credit in L&S
Grad 50% - Counts toward 50% graduate coursework requirement

Official course description: Groups, normal subgroups, Cayley's theorem, rings, ideals, homomorphisms, polynomial rings, abstract vector spaces.

Requisites: (MATH 234 or 375), (MATH 320, 340, 341, or 375), and (MATH 341, 375, 421, 467, or 521), or graduate/professional standing or member of the Pre-Masters Mathematics (Visiting International) Program

Instructor: Chenxi Wu

Email: cwu367@wisc.edu

Modes of Instruction: In person.

Lecture: 1:00-2:15pm Tu Th VV B139.

Office Hours: 10-11 am Wednesday and Thursday at Van Vleck 517, or by appointment.

This is an introductory course on algebra. We will cover basic properties of groups, rings, fields a, and their applications.

Learning goal:

1. Understand the definitions and basic properties of groups, rings, fields and modules.

2. Practice reading and writing mathematical proofs.

3. Able to apply concepts and ideas in abstract algebra to other areas of mathematics.

4. Able to define and recognize simple algebraic structures, investigate their structures and classify them.

Textbook: Dummit and Foote, *Abstract Algebra*. I will also post detailed lecture notes on Canvas.

How Credit Hours are met: This class meets for two, 75-minute class periods each week over the fall/spring semester and carries the expectation that students will work on course learning activities (reading, writing, problem sets, studying, etc) for about 3 hours out of the classroom for every class period. The syllabus includes more information about meeting times and expectations for student work.

Canvas Support: `https://kb.wisc.edu/luwmad/page.php?id=66546`

Grades: We will have weekly homework (10%), one in-class midterm exam (35%) and one final exam (55%). HW problems will be posted on Canvas every weekend, due on the Monday after the next weekend. Please submit your solution as a single pdf file via Canvas.

All HW or midterm grades that are lower than final grades will be replaced by final grades. For example, if one has 0/10 in HW1, 9/10 in HW2, 50/100 in midterm and 80/100 in final, then the HW1 grade will be replaced by 8/10 and midterm grade will be replaced by 80/100. HW2 grade will remain unchanged. Since all missing HW grades have been automatically replaced by final grades, no late HW will be accepted. The final exam will be cumulative. All exams will be open book and open notes but electronic devices will not be allowed.

If the cumulative grade is ≥ 90 then one gets A, if ≥ 75 one gets B or above, if ≥ 60 one gets C or above.

This is a tentative list of topics we may cover in this semester:

1. A review of set theory notations.

2. Groups, group actions and examples.

3. Orbit decomposition and Permutation Representation.

4. Isomorphism theorem.

5. Rings, fields, modules and examples.

6. Ideals and left ideals.

7. Chinese remainder theorem, Euclidean domains and PIDs.

Institutional Level Academic Policies: `https://teachlearn.wisc.edu/course-syllabi/course-credit-information-required-for-syllabi/`

1.2 Some General Suggestions

We all have different academic backgrounds and different learning styles, so what works for one may not work for another. However the following are some things I did when I was in college which I found helpful at the time:

1. Understand every definition and proofs and summarize the key ideas behind each in one sentence.
2. If there is extra time after finishing the weekly homework, do as many exercises as possible. There is no need to actually write down the full solution, just go through the problems in the textbook and make sure you know how to do them.
3. Focus on the connections between different concepts in this course as well as their connections with ideas in your other math courses.

Dummit and Foote is a very comprehensive and readable introductory textbook on algebra. Another textbook that I read while learning the subject myself was Jacobson's *Basic Algebra*.

1.3 Some examples of applications of algebra

Example 1.3.1. Consider a linear map from the set of continuous functions to the set of continuous functions $I : C(\mathbb{R}) \to C(\mathbb{R})$ defined as:

$$(I(f))(x) = \int_0^x f(t)dt$$

We know that $(e^x)' = e^x$. So, by fundamental theorem of calculus, $\int_0^x e^t dt = e^x - 1$, i.e. $I(e^x) = e^x - 1$,

$$e^x = 1/(1 - I) = 1 + I + I^2(1) + I^3(1) + \cdots = 1 + x + x^2/2! + x^3/3! + \dots$$

which is the Taylor series expansion of e^x. The reason this argument works is because $z \mapsto I$ gives a **homomorphism** from the ring of convergent power series to the ring of linear self maps on $C(\mathbb{R})$.

Example 1.3.2.

$$1/3 = 0.333333\dots$$

$$1/6 = 0.166666\dots$$

$$1/7 = 0.142857142857\dots$$

$$1/9 = 0.111111\ldots$$

$$1/11 = 0.09090909\ldots$$

$$1/12 = 0.0833333\ldots$$

$$1/13 = 0.076923076923076923\ldots$$

$$\ldots$$

In general, the the period of the decimal expansion of $1/n$ is a factor of Euler's function $\varphi(n)$ which is the number of integers from 1 to $n-1$ which is coprime to n. (In particular, if n is a prime, $\varphi(n) = n-1$) This is called **Euler's Theorem** which is a generalization of **Fermat's Little Theorem**, and a special case of **Lagrange's Theorem** which we will prove later in the semester.

Example 1.3.3. Consider the following two questions:

1. Find integer N such that $N-2$ is a multiple of 3, $N-1$ is a multiple of 4 and $N-3$ is a multiple of 5. (Answer: $N = 20+45+48+60k$ where k is an arbitrary integer.)

2. Find polynomial p such that $p(0) = 1$, $p(1) = 0$, $p(2) = 2$. (Answer: $p = (x-1)(x-2)/2 + (x-1)x + x(x-1)(x-2)h$, where h is any polynomial)

These are both examples of **Chinese Remainder Theorem**.

Example 1.3.4.

1. Any real valued function on $\mathbb{R}$ can be written as a sum of an even function and an odd function.

2. Fourier series for periodic functions.

3. Spherical harmonics.

These all come from the theory of **group representations** which we will mention but not cover this semester.

2 A Review of Set Theory

A complete treatment of predicate logic and axiomatic set theory may take a whole semester. So we will just review some notations and concepts from set theory which we will use this semester.

2.1 Sets, Subsets, Empty Sets and Power Sets

1. Let S be a set. If x is an **element**, or **member** of S, we write $x \in S$.
2. We say A is a **subset** if for any $x \in A$, $x \in S$. We denote it as $A \subseteq S$. In particular, $S \subseteq S$.
3. Two sets are **equal** if they have the same elements. In other words, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.
4. If $A \subseteq B$ and $A \neq B$ we say that A is a **proper subset** of B, denoted as $A \subsetneq B$.
5. To describe a set, one can write down its elements and put a $\{\}$ around them, for example:
$$A = \{0, 1, 2\}$$
When there are multiple elements between the $\{\}$ that are identical, we ignore all but one of them. One can also use the terminology of **specification** to describe a set consisting of elements that satisfy a certain property. For example:
$$A = \{n \in \mathbb{N} : n \leq 2\}$$
means "A is a set consists of natural numbers that are no more than 2"; or the terminology of **replacement**, for example:
$$B = \{\{n, \emptyset\} : n \in Z\}$$
means "B is a set consisting of sets of the form $\{n, \emptyset\}$ where n is an integer". Here the ":" notation may be replaced with | in some texts.
6. There is a unique set called the **empty set**, denoted as $\emptyset$, which contains no elements. The empty set is a subset of any set.
7. For every set A, there is a set consisting of all subsets of A, called the **power set**, denoted as $P(A)$ or 2^A.

Remark 2.1.1. $\emptyset \in P(A)$ for any A, hence $P(A) \neq \emptyset$. Furthermore, if A is a set with n elements, then $P(A)$ has 2^n elements.

Notations for some common sets of numbers:

1. $\mathbb{N}$: set of natural numbers. In mathematics we usually think of 0 as a natural number.

2. $\mathbb{Z}$: set of integers.

3. $\mathbb{Q}$: set of rationals.

4. $\mathbb{R}$: set of real numbers. This is a key concept for this semester which we will discuss in more details later.

5. $\mathbb{C}$: set of complex numbers.

Example 2.1.2. $P(P(\{\emptyset\})) = P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.

Example 2.1.3. $A = \{P(B) : B \in P(\mathbb{Z}), 2 \in B\}$ is a set. $\{\emptyset, \{2\}\} = P(\{2\}) \in A$. $\{P(B) : B \in P(\mathbb{Z}), \{1, 2\} \subseteq B\}$ is a proper subset of A.

2.2 Unions, intersections and set differences

Definition 2.2.1. 1. Let A be a set of sets. The **union** of elements in A, denoted as $\bigcup A$ or $\bigcup_{B \in A} B$, is a set such that $x \in \bigcup A$ iff there is some $B \in A$ such that $x \in B$. When $A = \{U, V\}$, we denote $\bigcup A$ as $U \cup V$.

2. Let A be a non-empty set of sets. The **intersection** of elements in A, denoted as $\bigcap A$ or $\bigcap_{B \in A} B$, is defined as $\{x \in \bigcup A : x \in B \text{ for all } B \in A\}$. When $A = \{U, V\}$, we denote $\bigcap A$ as $U \cap V$.

3. Let A and B be two sets, the **set difference** $A \backslash B$ is defined as $\{x \in A : x \notin B\}$.

Example 2.2.2. 1. $A \cup A = A \cap A = A \cup \emptyset = A$, $A \cap \emptyset = A \backslash A = \emptyset$.

2. $(\bigcup_{n \in \mathbb{N}} (1/(n+2), 1/(n+1)]) \backslash [0, 1/3) = (0, 1] \backslash [0, 1/3) = [1/3, 1]$.

2.3 Ordered Pairs, Cartesian products and Relations

Definition 2.3.1. Given two objects a and b, one can form an **ordered pair**, denoted as (a, b), such that $(a, b) = (c, d)$ iff $a = c$ and $b = d$. This can be done by various set-theoretic constructions, e.g. one may define $(a, b) = \{\{a\}, \{a, b\}\}$.

Definition 2.3.2. Let A and B be two sets (can be identical), the **Cartesian product** between A and B is defined as the set of ordered pairs of one element in A and another element in B. We write this as

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Definition 2.3.3. A subset of $A \times B$ is called a **relation** between A and B.

Example 2.3.4. 1. If A or B is empty, then $A \times B = \emptyset$.

2. $\{(a, a) : a \in A\}$ is a relation between A and A, which we called the **identity relation**, denoted as id_A.

We will mostly focus on two special kinds of relations: functions and equivalence relations.

2.4 Functions

Definition 2.4.1. 1. A relation $f \in P(A \times B)$ is called a **function**, or a **map** from A to B, denoted as $f : A \to B$, if for every $a \in A$, **there is a unique** $b \in B$ such that $(a, b) \in f$. When f is a function, we can write $(a, b) \in f$ as $a \mapsto b$ or $b = f(a)$.

2. The set of functions from A to B is denoted as $Map(A, B)$.

3. Let f be a function from A to B. For every $C \in P(A)$, define $f(C) = \{f(c) : c \in C\}$. For every $D \in P(B)$, define $f^{-1}(D) = \{a \in A : f(a) \in D\}$.

4. Let f be a function from A to B, A is called the **domain**, B is called the **codomain**, $\{f(a) : a \in A\} \subseteq B$, denoted as $f(A)$, is called the **range** or the **image**.

5. Let $f : A \to B$ be a function. We call f an **injection** if $f(a) = f(b)$ implies $a = b$, a **surjection** if $f(A) = B$, a **bijection** if it is both an injection and a surjection.

Example 2.4.2. 1. id_A is a function from A to A, called the **identity function**. The identity function is always a bijection.

2. Let B be a non-empty set, $b \in B$, $C_b = \{(a, b) : a \in A\}$ is a function from A to B, called a **constant function**.

3. Let $A \subseteq B$, the function $i = \{(a, a) : a \in A\} \subseteq A \times B$ is called the **inclusion function**. These are injections but not necessarily surjections.

4. Let A be a set, $f : A \to P(A)$ defined as $f(a) = A \backslash \{a\}$ is a function which is a injection but not a surjection.

Definition 2.4.3. Let $f : A \to B$, $g : B \to C$ be functions. The **composition** between f and g, denoted as $g \circ f$, is a function from A to C defined as $c = (g \circ f)(a)$ iff $c = g(f(a))$. If A is a subset of B and f is the inclusion function, the composition is called the **restriction** of g on A, denoted as $g|_A$.

Remark 2.4.4.

1. Let $f : A \to B$ be a function, then $f = f \circ id_A = id_B \circ f$.

2. Compositions of injections are injections, compositions of surjections are surjections, compositions of bijections are bijections.

Theorem 2.4.5. Any function can be written as the composition of a surjection and an injection.

Proof. Let $f : A \to B$ be a function, then $g : A \to f(A)$ defined as $g(a) = f(a)$ is a surjection, and f is the composition of g and the inclusion $f(A) \to B$ which is an injection. □

Theorem 2.4.6. $f : A \to B$ is a bijection iff there is a function $g : B \to A$, such that $f \circ g = id_B$, $g \circ f = id_A$. We call such an f **invertable**, such a g its **inverse**, denoted as $g = f^{-1}$.

Proof. Suppose f is a bijection. Define $g = \{(b, a) \in B \times A : b = f(a)\}$. Surjectivity and injectivity of f implies that g is a function, and by construction $f \circ g = id_B$ and $g \circ f = id_A$. Suppose f has an inverse g, then $f(a) = f(b)$ implies $a = g(f(a)) = g(f(b)) = b$, hence f is an injection. For every $b \in B$, $b = f(g(b)) \in f(A)$, hence f is a surjection. □

Theorem 2.4.7. There is a bijection between $Map(A \times B, C)$ and $Map(A, Map(B, C))$, defined as

$$f \mapsto (a \mapsto (b \mapsto f(a, b))$$

Proof. It is easy to show that the map from $Map(A \times B, C)$ to $Map(A, Map(B, C))$ defined above is well defined.

We can also verify that the map from $Map(A, Map(B, C))$ to $Map(A \times B, C)$ defined by $g \mapsto ((a, b) \mapsto (g(a))(b))$ is its inverse, so by Theorem 2.4.6 it is a bijection. □

Remark 2.4.8. This is called **Currying** after the American logician Haskell Curry. It is often used in computer science to reduce multi variable functions to single variable ones. For example, the binary operator $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ can be seen as a function sending integer a to a function $b \mapsto a + b$.

One can use the concept of functions to define Cartesian products of potentially infinitely many sets.

Definition 2.4.9.

1. By a **parametrized family of sets**, we mean a set I, a set U, and a function $I \to P(U)$ which we denote as $\alpha \mapsto U_\alpha$. We can write this as $\{U_\alpha : \alpha \in I\}$. Note that this is **NOT** a set despite the superficial similarity in notations.

2. The Cartesian product of a family of sets $\{U_\alpha : \alpha \in I\}$ is defined as

$$\prod_{\alpha \in I} U_\alpha = \{f \in Map(I, \bigcup_{\alpha \in I} U_\alpha) : f(\alpha) \in U_\alpha \text{ for all } \alpha \in I\}$$

Remark 2.4.10. If $U_\alpha \neq \emptyset$ for every $\alpha \in I$, the **axiom of choice** says that $\prod_{\alpha \in I} U_\alpha \neq \emptyset$.

Furthermore, one can also define the concept of **cardinality** via bijections:

Definition 2.4.11.

Two sets are said to have the same **cardinality** if there is a bijection between them. A set A is said to have cardinality no more than B, if there is an injection from A to B, denoted as $|A| \leq |B|$.

A set with the same cardinality as $\{1, 2, \ldots, n\}$ is called a **finite set**, and we say that it has cardinality n, denoted as $|A| = n$.

2.5 Equivalence relations

Definition 2.5.1. Let A be a set, an **equivalence relation** on A is a relation $\sim$ between A and A, that satisfies:

1. ("identity") For any $a \in A$, $(a, a) \in \sim$.
2. ("symmetry") $(a, b) \in \sim$ iff $(b, a) \in \sim$.
3. ("transitivity") If $(a, b) \in \sim$, $(b, c) \in \sim$, then $(a, c) \in \sim$.

We usually write $(a, b) \in \sim$ as $a \sim b$.

Definition 2.5.2. When $\sim$ is an equivalence relation on a set A, the **quotient set** is defined as

$$A/\sim = \{\{b \in A : b \sim a\} : a \in A\}$$

Here the set $\{b \in A : b \sim a\}$ is called the **equivalence class containing (or represented by)** a, denoted as $[a]$. There is a surjection from A to $A/\sim$ called the **quotient map** defined as $a \mapsto [a]$.

Remark 2.5.3. Let $\sim$ be an equivalence relation on a set A. Then $A = \bigcup(A/\sim)$ and elements of $A/\sim$ are **disjoint**, in the sense that $a, b \in A/\sim$ then either $a = b$ or $a \cap b = \emptyset$. In other words, A a **disjoint union** of elements of $A/\sim$.

Example 2.5.4.

1. $id_A = \{(a, a) : a \in A\}$ is an equivalence relation. The corresponding quotient set is $\{\{a\} : a \in A\}$ and the quotient map is a bijection.
2. $A \times A$ is an equivalence relation. The corresponding quotient set is $\{A\}$.
3. Let $f : A \to B$ be a map, then $\sim_f$ defined as $a \sim_f b$ iff $f(a) = f(b)$ is an equivalence relation. The corresponding quotient set is $\{f^{-1}(\{b\}) : b \in B\}$.
4. Let T be the set of triangles in an Euclidean 2-plane, then "similarity" is an equivalence relation.
5. Let M be the set of $n \times n$ matrices over $\mathbb{C}$, $A \sim B$ iff there is some invertible matrix U such that $A = UBU^{-1}$, then $\sim$ is an equivalence relation, the quotient set can be described via, for example, the Jordan normal form.
6. Let n be an integer, $\sim$ be a relation between $\mathbb{Z}$ and $\mathbb{Z}$ such that $a \sim b$ iff $a - b$ divides n (a is congurent to b mod n). The quotient set has $|n|$ elements if $n \neq 0$ and infinitely many elements if $n = 0$. This quotient set is denoted as $\mathbb{Z}/n$.

The ideas in Example 2.5.4 Part 3 gives a way to relate equivalence relations and surjections:

Theorem 2.5.5. Let A be a set, $f : A \to B$ a map, $g : A \to Q$ a surjection. Let $\sim_f$ and $\sim_g$ be the equivalence relations defined in Example 2.5.4 Part 3. Then

1. There is a map $h : Q \to B$ such that $h \circ g = f$ iff $\sim_g \subseteq \sim_f$.
2. When such an h exist it is unique.
3. When such an h exist, it is injective iff $\sim_g = \sim_f$, surjective iff f is surjective.
4. In particular, if f is a surjection, there is a unique bijection $j : A/\sim_f \to B$ such that $f = j \circ p$, where $p : A \to A/\sim_f$ is the quotient map.

Proof. 1. When such an h exist, $g(a) = g(b)$ implies $f(a) = f(b)$, hence $\sim_g \subseteq \sim_f$. When $\sim_g \subseteq \sim_f$, for every $q \in Q$, let $a \in A$ be such that $g(a) = q$, and define $h(q) = f(a)$. This is well defined because if $g(a) = g(a')$ then $a \sim_g a'$ which implies that $a \sim_f a'$, i.e. $f(a) = f(a')$.

2. Suppose there is some other h' such that $h' \circ g = f$. For any $q \in Q$, let $a \in A$ such that $g(a) = q$, then $h'(q) = h'(g(a)) = f(a) = h(g(a)) = h(q)$, hence $h = h'$.

3. h is an injection iff $h(q) = h(q')$ implies $q = q'$. Let $q = g(a)$, $q' = g(a')$, then this is the same as saying $f(a) = f(a')$ implies $g(a) = g(a')$, i.e. $\sim_f \subseteq \sim_g$. From Part 1 above we already have $\sim_g \subseteq \sim_f$, so this is equivalent to $\sim_g = \sim_f$. If h is a surjection, f must be a surjection due to Remark 2.4.4. If f is a surjection, for every $y \in B$, let $a \in A$ such that $y = f(a)$, then $y = h(g(a)) \in h(Q)$.

4. Let g be the quotient map p and apply Parts 1, 2, and 3 above.

□

3 Groups

3.1 Groups, subgroups, homomorphisms

Definition 3.1.1.

1. A **group** is a pair $(G, *)$, where G is a set, $* : G \times G \to G$ a map called the **group operation**, such that:
   (a) ("associativity") For any $a, b, c \in G$, $*(*(a, b), c) = *(a, *(b, c))$.
   (b) ("identity") There is an element $e \in G$, such that for any $a \in G$, $*(e, a) = *(a, e) = a$.
   (c) ("inverse") For any $a \in G$, there is a $b \in G$, such that $*(a, b) = *(b, a) = e$.
2. If G has finite cardinality we call it a **finite group**, otherwise we call it an **infinite group**.
3. If for any $a, b \in G$, $*(a, b) = *(b, a)$, we call $(G, *)$ a **commutative** or **abelian** group.

Remark 3.1.2.
1. When $(G, *)$ is a group we can also say "G is a group under $*$". When there is no ambiguity on $*$ we can also say "G is a group".
2. $*(a, b)$ can be written as $a * b$, $a \cdot b$ or ab. When the group is abelian we may also write the group operation as $+$.
3. The identity element can be written as 1 or 0 (when we use $+$ to denote the group operation).
4. The inverse of $a \in G$ can be written as a^{-1} or $-a$ (when we use $+$ to denote the group operation).
5. When checking $(G, *)$ is a group, don't forget to make sure that $*$ is really a function from $G \times G$ to G.

Definition 3.1.3.

1. Let $(G, *)$ and $(H, *')$ be two groups, $f : G \to H$ is called a **homomorphism**, if for any $a, b \in G$, $f(a * b) = f(a) *' f(b)$. A homomorphism from a group to itself is called an **endomorphism**, and the set of homomorphisms between two groups G and H is denoted as $Hom(G, H)$.
2. Let $(G, *)$ be a group. A subset $H \subseteq G$ is called a **subgroup**, denoted as $H \leq G$, if
   (a) The identity element of G belongs to H.
   (b) If $a, b \in H$, $a * b \in H$.
   (c) If $a \in H$, the inverse $a^{-1} \in H$.

Remark 3.1.4. 1. The first condition on subgroup can be replaced by "H is non-empty".

2. If $H \leq G$, then $(H, *|_{H\times H})$ is a group, and the inclusion map is an injective group homomorphism. Here, H being closed under $*$ implies that $*|_{H\times H}$ is a function from $H \times H$ to H, associativity follows from the associativity of $(G, *)$, $e_G \in H$ is the identity element, and the existence of inverse is due to H being closed under inverse in G.

Example 3.1.5. 1. $(\{e\}, (e, e) \mapsto e)$ is a group called the **trivial group**, often denoted as 0 or 1.

2. Let G be a group, then both G and $\{e_G\}$ are subgroups of G.

3. Let G and H be two groups, id_G is a homomorphism from G to itself, $g \mapsto e_H$ is a homomorphism from G to H.

4. Let A be a set, the set of bijections from A to itself is a group under $\circ$, called the **permutation group**, denoted as S_A. If $B \subseteq A$, the bijections which are identity when restricted to B is a subgroup. If $A = \{1, \dots n\}$, we also write S_A as S_n.

5. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ under $+$ are all abelian groups, and each is a subgroup of the next. $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ and $\mathbb{C}\backslash\{0\}$ are all abelian groups under $\times$, and each is a subgroup of the next. exp is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}, \times)$.

6. From linear algebra we have the classical matrix groups $GL(n)$, $SL(n)$, $O(n)$, $SO(n)$, $U(n)$, $SU(n)$, $SP(n)$, ... det is a homomorphism from these groups to $\mathbb{R}\backslash\{0\}$ or $\mathbb{C}\backslash\{0\}$.

7. Any vector space is a group under $+$.

8. The set of invertable 3×3 upper triangular matrices form a group.

9. A non-empty set X with a metric $d : X \times X \to \mathbb{R}_{\geq 0}$ is called a metric space, the set of bijections from X to itself that preserves the metric form a subgroup of S_X, called the **isometry group**. For example, under the usual Euclidean metric, the isometry group of a equilaterial triangle has 6 elements while the isometry group of a sphere has infinitely many.

10. The set of increasing bijections from $\mathbb{R}$ to $\mathbb{R}$ form a subgroup of $S_{\mathbb{R}}$.

Some non-examples:

Example 3.1.6. 1. $(\mathbb{N}, +)$ is not a group (no inverse).

2. $(\mathbb{R}\backslash\mathbb{Q}, +)$ is not a group (group operation is not well defined).

3. $(\mathbb{Z}, \max)$ is not a group (no inverse, no identity).

Some special groups, subgroups and homomorphisms:

Example 3.1.7.

1. $(\{e\}, (e,e) \mapsto e)$ is a group called the **trivial group**, often denoted as 0 or 1.
2. Let G be a group, then both G and $\{e_G\}$ are subgroups of G.
3. Let G and H be two groups, id_G is a homomorphism from G to itself, $g \mapsto e_H$ is a homomorphism from G to H.
4. Let G be a group, $g \in G$, then $x \mapsto gxg^{-1}$ is a homomorphism from G to G, called an **inner automorphism**.

Remark 3.1.8. Let G be a group, $S \subseteq G$, the smallest subgroup containing elements of S is called the **subgroup generated by** S, denoted as $\langle S \rangle$. The elements in S are called the **generating set** of this subgroup. For example, if $G = (\mathbb{Z}, +)$, $\langle n \rangle = \langle \{n\} \rangle$ consists of all integers divisible by n.

There are some more ways of constructing groups via other groups:

Definition 3.1.9.
1. Let $(G, *)$ be a group, define $*'$ as $a *' b = b * a$, then $(G, *')$ is also a group, which we call the **opposite group**, denoted as G^{op}.
2. Let $(G, *)$, $(H, *')$ be two groups, one can define $\cdot : (G \times H) \times (G \times H) \to G \times H$ by $(a,b) \cdot (c,d) = (a * c, b *' d)$. Then $(G \times H, \cdot)$ is a group, called the **direct product** between G and H, denoted as $G \times H$. One can similarly define the direct product of more than 2, or even arbitrarily many groups.

3.2 Basic Properties, Automorphism Groups

Below are some elementary properties of groups and group homomorphisms:

Theorem 3.2.1. Let G be a group, then

1. When multiplying a sequence of elements in G, we can add parenthesis at any order, e.g. $(ab)(cd) = (a(bc))d$.
2. The identity is unique.
3. The inverse is unique.
4. $(a^{-1})^{-1} = a$.
5. $(ab)^{-1} = b^{-1}a^{-1}$.
6. (Cancellation Law) $ab = ac$ or $ba = ca$ implies $b = c$.

Proof.
1. Repeatedly apply associativity law.
2. Suppose e, e' are identities, then $e = ee' = e'$.

3. Suppose $a \in G$, b, b' are its inverses, then $b = be = b(ab') = (ba)b' = eb' = b'$.

4. This is because $aa^{-1} = a^{-1}a = e$.

5. This is because $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = e$.

6. Multiply a^{-1} to both sides from the left or from the right.

□

Theorem 3.2.2. Let $f : G \to H$ be a group homomorphism, then

1. f sends identity element e_G of G to identity element e_H.
2. For any $a \in G$, $f(a^{-1}) = (f(a))^{-1}$.
3. If $N \leq G$, then $f(N) \leq H$.
4. If $M \leq H$, then $f^{-1}(M) \leq G$.
5. If $h : H \to L$ is another group homomorphism, then $h \circ f$ is a group homomorphism.
6. If f is a bijection, the inverse map f^{-1} (see Theorem 2.4.6) is also a group homomorphism. We call such an f an **isomorphisms**.

Proof. 1. $e_G e_G = e_G$, hence $f(e_G)f(e_G) = f(e_G)$. Now apply the cancellation law.

2. $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H$, $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H$.

3. (a) $N \leq G$ hence $e_G \in N$, so $e_H = f(e_G) \in f(N)$.
   (b) If $a, b \in f(N)$, there are $c, d \in N$ such that $a = f(c)$, $b = f(d)$. Hence $ab = f(c)f(d) = f(cd) \in f(N)$.
   (c) If $a \in f(N)$, there is some $c \in N$ such that $a = f(c)$, hence $a^{-1} = (f(c))^{-1} = f(c^{-1}) \in f(N)$.

4. (a) $f(e_G) = e_H \in M$, so $e_G \in f^{-1}(M)$.
   (b) If $a, b \in f^{-1}(M)$, $f(ab) = f(a)f(b) \in M$, hence $ab \in f^{-1}(M)$.
   (c) If $a \in f^{-1}(M)$, then $f(a) \in M$, hence $f(a^{-1}) = (f(a))^{-1} \in M$, which implies that $a^{-1} \in f^{-1}(M)$.

5. Let $a, b \in G$, $h(f(ab)) = h(f(a)f(b)) = h(f(a))h(f(b))$.

6. For any $a, b \in H$, $f^{-1}(ab) = f^{-1}(f(f^{-1}(a))f(f^{-1}(b))) = f^{-1}(f(f^{-1}(a)f^{-1}(b))) = f^{-1}(a)f^{-1}(b)$.

□

Remark 3.2.3. If there is an isomorphism f between groups G and H, we say G is **isomorphic to** H, denoted as $G \cong H$.

Theorem 3.2.4. Let G be a group, the set of bijective group homomorphisms from G to itself form a subgroup of S_G, called the **automorphism group**, denoted as S_G. Elements of this subgroup are called **automorphisms**.

Proof. By definition id_G is a bijective group homomorphism. Theorem 3.2.2 Part 5 and Remark 2.4.4 Part 2 implies that this subset is closed under function composition (which is the group operation of S_G). Theorem 3.2.2 Part 6 shows that it is closed under inverses. □

Example 3.2.5. The automorphism group of $(\mathbb{Z}, +)$ has 2 elements: $n \mapsto n$ or $n \mapsto -n$.

3.3 Kernels, Quotients, Isomorphism Theorem

Definition 3.3.1. Let $f : G \to H$ be a group homomorphism. Theorem 3.2.2 Part 3 and 4, and Example 3.1.7 Part 2 implies that $f(G) \leq H$, $f^{-1}(\{e_H\}) \leq G$. The former is called the **image** of f, denoted as $im(f)$, while the latter called the **kernel** of f, denoted as $\ker(f)$.

Example 3.3.2.

1. When G and H are vector spaces and f a linear map, the concept of kernels and images defined here is compatible with those in linear algebra.
2. $x \mapsto e^{ix}$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{C}\backslash\{0\}, \times)$. Its kernel is $\{2\pi n : n \in \mathbb{Z}\}$, and its image is $\{z \in \mathbb{C} : |z| = 1\}$.
3. Let $G = GL(n, \mathbb{R})$ which is the group of $n \times n$ real invertible matrices under matrix multiplication. det is a homomorphism from G to $(\mathbb{R}\backslash\{0\}, \times)$, and the kernel is the special linear group $SL(n, \mathbb{R})$.

We can characterize group homomorphisms via their kernels and images:

Theorem 3.3.3. Let $f : G \to H$ be a group homomorphism. Then

1. f can be written as the composition of a surjective group homomorphism $f_1 : G \to f(G)$ and an injective group homomorphism i which is the inclusion from $f(G)$ to H.
2. $f(a) = f(b)$ iff $a^{-1}b \in \ker(f)$.
3. If $g : G \to Q$ is a surjective group homomorphism, then:
   (a) There is a unique map $h : Q \to H$ such that $f = h \circ g$ iff $\ker(g) \subseteq \ker(f)$.
   (b) When such an h exist, it is unique and a group homomorphism.
   (c) When such an h exist, it is surjective iff f is surjective, injective iff $\ker(g) = \ker(f)$.

(d) In particular, if $\ker(g) = \ker(f)$ and both f and g are surjections, then there is a unique group isomorphism $h : Q \to H$, such that $f = h \circ g$.

Proof. 1. $f = i \circ f_i$ by construction, and one can easily verify that both f_1 and i are group homomorphisms.

2. $f(a) = f(b)$ iff $e_H = (f(a))^{-1} f(b) = f(a^{-1}) f(b) = f(a^{-1}b)$ iff $a^{-1}b \in \ker(f)$.

3. This is basically Theorem 2.5.5 combined with Part 2 above. The only thing remains to show is that if such an h exist it is a group homomorphism. To see this, let $q, q' \in Q$, $a, a' \in G$ such that $q = g(a)$, $q' = g(a')$, then $h(qq') = h(g(a)g(a')) = h(g(aa')) = f(aa') = f(a)f(a') = h(g(a))h(g(a')) = h(q)h(q')$.

□

The Theorem above shows that to study surjections from a given group G to another group, up to isomorphisms between the codomain, one need to only study their kernels. So we have the following:

Theorem 3.3.4. Let G be a group, $H \leq G$ a subgroup. The followings are equivalent:

1. There is a surjective homomorphism $f : G \to Q$ such that $H = \ker(f)$.
2. For any $g \in G$, any $h \in H$, $ghg^{-1} \in H$ (we write this as $gHg^{-1} = H$).

Proof.

- From 1 to 2: Let $H = \ker(f)$ for some group homomorphism f, then for any $h \in H$, any $g \in G$, $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = e_Q$, so $ghg^{-1} \in H$.
- From 2 to 1: Suppose $H \leq G$ satisfies $gHg^{-1} = H$. We construct the f and Q via the following steps:
  1. Firstly we define an equivalence relation $\sim_H$ on G, such that $a \sim_H b$ iff $a^{-1}b \in H$. We now check that this is indeed an equivalence relation:
     (a) For any $a \in G$, $a^{-1}a \in H$.
     (b) For any $a, b \in G$, if $a^{-1}b \in H$, then $b^{-1}a = (a^{-1}b)^{-1} \in H$.
     (c) For any $a, b, c \in G$, if $a^{-1}b \in H$, $b^{-1}c \in H$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.
  2. Now let $Q = G/\sim_H$, define the group operation $\cdot : Q \times Q \to Q$ as $([a], [b]) \mapsto [ab]$.
     (a) Firstly we show that $\cdot$ is well defined. Suppose $[a] = [a']$, $[b] = [b']$, then $a^{-1}a' \in H$, $b^{-1}b' \in H$, and $(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = (b^{-1}(a^{-1}a')b)(b^{-1}b') \in H$. Hence $[ab] = [a'b']$.

(b) Associativity follows from the associativity of group operation on G, $e_Q = [e_G]$, $[a]^{-1} = [a^{-1}]$.

It is evident from the construction that the quotient map $G \to G/\sim_H = Q$ is now a surjection and a group homomorphism, and its kernel is H.

□

Remark 3.3.5. When $H \leq G$, the $\sim_H$ in the proof of Theorem 3.3.4 is an equivalence relation. The equivalence classes are called **left cosets**, denoted as $[a] = aH$, and the quotient set $G/\sim_H$ is denoted as G/H.

Remark 3.3.6. Subgroups that satisfy the condition in Theorem 3.3.4 are called **normal subgroups**, denoted as $N \trianglelefteq G$. The corresponding Q with surjection $f : G \to Q$ constructed in the proof of Theorem 3.3.4 are called **quotient groups**, denoted as $Q = G/N$.

Remark 3.3.7. Any subgroup of an abelian group is a normal subgroup.

Example 3.3.8.

1. Let G and H be two groups, $G \times H$ their direct product, then $p_1 : G \times H \to G$ defined as $p_1(a, b) = a$ is a surjective homomorphism, its kernel is $\{(e_G, b) : b \in H\}$ which is isomorphic to H.

2. Let n be an integer, $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ is a normal subgroup of $(\mathbb{Z}, +)$, the quotient group is denoted as $\mathbb{Z}/n$. These are called the **cyclic groups**.

3. There is an injective homomorphism i from S_n to $GL(n, \mathbb{R})$, such that any $\sigma \in S_n$ is sent to a linear map T_σ which sends the i-th standard basis e_i to $e_{\sigma(i)}$. Then $\det \circ i$ is a homomorphism from S_n to $(\mathbb{R}\backslash\{0\}, \times)$, whose image is $\{\pm 1\}$ and the kernel is a normal subgroup of S_n called the **alternating group**, denoted as A_n.

Theorem 3.3.9 (Isomorphism Theorem)**.** Let $f : G \to H$ be a group homomorphism. Then $f(G)$ is isomorphic to the quotient group $G/\ker(f)$. In particular, when $\ker(f) = \{e_G\}$, G is isomorphic to $f(G)$.

Proof. By Theorem 3.3.4, $\ker(f) \trianglelefteq G$. Let $q : G \to G/\ker(f)$ be the quotient map, then $\ker(q) = \ker(f)$, hence by Theorem 3.3.3, $G/\ker(f) \cong f(G)$. When $\ker(f) = \{e_G\}$, q is a bijection hence by Theorem 3.2.2 Part 6, it is an isomorphism. Hence $G \cong f(G)$. □

Theorem 3.3.10. If $H \trianglelefteq G$, $p : G \to G/H$ the quotient map, and there is a group homomorphism $s : G/H \to G$ such that $s(G/H) \trianglelefteq G$ and $p \circ s = id_{G/H}$, then G is isomorphic to $H \times G/H$.

Proof. Define $i : G \to H \times G/H$ as $i(g) = (g(s(p(g)))^{-1}, p(g))$.

1. Firstly we show this is well defined, in particular $g(s(p(g)))^{-1} \in H$. This is because $p(g(s(p(g)))^{-1}) = p(g)p(g)^{-1} = e_{G/H}$.

2. Next we show that this is a bijection, which is because it has inverse $j : (h, q) \mapsto hs(q)$.

3. Finally we show that the i is indeed a group homomorphism: for any $g, g' \in G$, $i(gg') = ((gg')s(p(gg'))^{-1}, p(gg')) = (gg's(p(g'))^{-1}s(p(g))^{-1}, p(g)p(g'))$. Because H and $s(G/H)$ are both normal subgroups of G,

$$(g's(p(g'))^{-1})s(p(g))^{-1}(g's(p(g'))^{-1})^{-1}s(p(g))$$

lies in both H and $s(G/H)$ hence equals e_G. So

$$(gg's(p(g'))^{-1}s(p(g))^{-1}, p(g)p(g'))$$

$$= ((gs(p(g))^{-1})(g's(p(g'))^{-1}), p(g)p(g')) = i(g)i(g')$$

□

Remark 3.3.11. The map s is called a **section**. If we require that a section is group homomorphism but do not require its image to be a normal subgroup, we call G a **semidirect product** between H and G/H.

4 Group Actions

4.1 Left G sets, invariant subsets, equivariant maps

Definition 4.1.1.

1. Let G be a group, X a set. A **(left) G-action** on X is a map $c : G \times X \to X$, such that

   (a) For any $x \in X$, $c(e_G, x) = x$.

   (b) For any $x \in X$, $a, b \in G$, $c(a, c(b, x)) = c(ab, x)$.

   The pair (X, c) is called a **left G-set**.

2. A subset $Y \subseteq X$ is called a **G-invariant subset** if for any $y \in Y$, any $g \in G$, $c(g, y) \in Y$.

3. Let (X, c), (Z, c') be two left G-sets. A map $f : X \to Z$ is called **G-equivariant** if for any $g \in G$, any $x \in X$, $f(c(g, x)) = c'(g, f(x))$.

Remark 4.1.2.

1. Similar to the case of groups, instead of "(X, c) is a left G-set" we can also say "X is a left G-set under action c" or, when there is no ambiguity, X is a left G set.

2. When there is no ambiguity we can write $c(g, x)$ as $g \cdot x$ or gx.

3. Similar to the case of groups, if $Y \subseteq X$ is a G-invariant subset of left G-set X with left G-action c, then $(Y, c|_{G \times Y})$ is a left G-set and the inclusion map is G-equivariant.

Example 4.1.3.

1. $G = S_X$, $gx = g(x)$.

2. If $f : X \to X$ is a bijection, X has a left $\mathbb{Z}$ action defined by $nx = f^{\circ n}(x)$, where $f^{\circ -n}(x) = (f^{-1})^{\circ n}(x)$.

3. $(G, *) = (\mathbb{R}\backslash\{0\}, \times)$, X is a $\mathbb{R}$-vector space, then the scalar multiplication is a left G-action. A subspace is an invariant subset and a linear map between vector spaces is an equivariant map.

4. G is the same as above, X is the set of functions from $\mathbb{R}$ to $\mathbb{R}$, $c(g, f) = (x \mapsto f(g^{-1}x))$ is a left G-action. The set of functions of the form $x \mapsto kx$ is a G-invariant subset.

Example 4.1.4.

1. $X = \{a\}$, $ga = a$ for all $g \in G$ is a left G-action.

2. Let X be a left G-set, $\emptyset$ and X are both G-invariant subsets, and id_X is G-equivariant.

3. Any group $(G, *)$ can be seen as a left G-set by $c(g, a) = g * a$. This is called the **left action**.

4. Any group $(G, *)$ can be seen as a left G-set by $c(g, a) = g * a * g^{-1}$. This is called the **conjugate action**.

5. Let G be a group, there is a left $Aut(G)$ action on G by $fg = f(g)$.

6. Let G be a group, S the set of subgroups of G. There is a left G action on S defined by $gH = gHg^{-1} = \{ghg^{-1} : h \in H\}$.

7. Let $f : G \to H$ be a group homomorphism, any left H-set X can be seen as a left G-set by $gx = f(g)x$.

8. Let $f : G \to H$ be a group homomorphism, then H can be seen as a left G set by $c(g, h) = f(g)h$.

4.2 Basic Properties, Stablizers

Analogous to Theorem 3.2.2 and Theorem 3.2.4, we have:

Theorem 4.2.1. Let $f : X \to Y$ be a G-equivariant map between left G sets.

1. If $Z \subseteq X$ is a G-invariant subset, then $f(Z) \subseteq Y$ is a G-invariant subset.

2. If $W \subseteq Y$ is a G-invariant subset, then $f^{-1}(W) \subseteq X$ is a G-invariant subset.

3. If $h : Y \to U$ is another G-equivariant map, then $h \circ f$ is a G-equivariant map.

4. If f is a bijection, the inverse map f^{-1} (see Theorem 2.4.6) is also G-equivariant. We call such an f an **isomorphisms**.

As a consequence, the set of isomorphisms from a left G-set X to itself forms a subgroup of S_X, denoted as $Aut(X)$.

Proof. 1. For any $y \in f(Z)$, there is some $x \in Z$ such that $y = f(x)$. Hence, for any $g \in G$, $gy = gf(x) = f(gx) \in f(Z)$.

2. For any $x \in f^{-1}(W)$, $f(x) \in W$. For any $g \in G$, $f(gx) = gf(x) \in W$, hence $gx \in f^{-1}(W)$.

3. For any $g \in G$, $x \in X$, $h(f(gx)) = h(gf(x)) = gh(f(x))$.

4. For any $g \in G$, $y \in Y$, $f^{-1}(gy) = f^{-1}(gf(f^{-1}(y))) = f^{-1}(f(gf^{-1}(y))) = gf^{-1}(y)$.

$Aut(X) \leq S_X$ is due to Part 2 of Example 4.1.4 and Part 3 and 4 above. □

Remark 4.2.2. If there is an isomorphism f between left G-sets X and Y, we say X is **isomorphic to** Y, denoted as $X \cong Y$.

Theorem 4.2.3. Let X be a left G-set, $x \in G$, then $\{g \in G : gx = x\} \leq G$. This subgroup is called the **stablizer** of x, denoted as G_x.

Proof. We show that G_x satisfies the three conditions in Definition 3.1.3 Part 2:

1. $e_G \in G_x$ because $e_G x = x$.
2. If $a, b \in G_x$, $ax = x$ and $bx = x$, hence $(ab)x = a(bx) = ax = x$, hence $ab \in G_x$.
3. If $a \in G_x$, $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$, hence $a^{-1} \in G_x$.

□

Definition 4.2.4. If X is a left G-set, for any $x \in X$, $G_x = \{e_g\}$, then we say the left G action on X is **free**.

4.3 Permutation representation, Caylay's Theorem

Theorem 4.3.1. Let X be a left G-set, then:

1. For any $g \in G$, $x \mapsto gx$ is a bijection from X to X.
2. The map $g \mapsto (x \mapsto gx)$ is a group homomorphism from G to S_X. This homomorphism is called the **permutation representation**

Proof. 1. By Theorem 2.4.6, we only need to show that this map $h_g : x \mapsto gx$ has an inverse. Let h'_g be $x \mapsto g^{-1}x$, then $h_g(h'_g(x)) = g(g^{-1}x) = (gg^{-1})x = x$, $h'_g(h_g(x)) = g^{-1}(gx) = (g^{-1}g)x = x$, hence h'_g is the inverse of h_g, which shows that h_g is a bijection from X to X, namely $h_g \in S_X$.

2. The map $\rho : g \mapsto h_g \in S_X$ is well defined due to Part 1 above. To show that it is a group homomorphism, let $g, g' \in G$, then for any $x \in X$, $(\rho(gg'))(x) = h_{gg'}(x) = (gg')x = g(g'(x)) = h_g(h_{g'}(x)) = (\rho(g) \circ \rho(g'))(x)$, hence $\rho(gg') = \rho(g) \circ \rho(g')$, ρ is a group homomorphism.

□

Definition 4.3.2. Let X be a left G-set. The kernel of the corresponding permutation representation is called the **kernel** of the left G action, and if this kernel equals $\{e_G\}$ we say the action is **effective**.

Remark 4.3.3. If X is non-empty and the left G action on X is free, then the action is also effective, because the kernel equals $\{g \in G : gx = x \text{ for all } x\} \subseteq \{g \in G : gx = x\} = G_x$.

Theorem 4.3.4. (Caylay's Theorem) Let G be a group, the left action is free hence effective. Hence, G is isomorphic to a subgroup of S_G.

Proof. Let $c(g, x) = gx$, then the permutation representation is $\rho : g \mapsto (x \mapsto gx)$, and for every $a \in G$, $G_a = \{g \in G : ga = a\} = \{e_G\}$. By Isomorphism Theorem 3.3.9, $G \cong \rho(G) \leq S_G$. □

Theorem 4.3.5. Let G be a group and X a set. There is a bijection between the set of left G-actions on X and the set $Hom(G, S_X)$, defined as follows:

$$(c : G \times X \to X) \mapsto (\rho : G \to S_X, \rho(g) = (x \mapsto c(g, x)))$$

$$(\rho : G \to S_X) \mapsto (c : G \times X \to X, c(g, x) = (\rho(g))(x))$$

Proof. The two maps above are restrictions of the two bijections in Theorem 2.4.7, hence we only need to show that both are well defined. The first one being well defined is due to Theorem 4.3.1. To show that the second is well defined, let $\rho \in Hom(G, S_X)$, $c : G \times X \to X$ be $c(g, x) = (\rho(g))(x)$, then by Theorem 3.2.2 Part 1, $c(e_G, x) = (\rho(e_G))(x) = id_X(x) = x$, and if $a, b \in G$, $c(a, c(b, x)) = \rho(a)(\rho(b)(x)) = (\rho(a) \circ \rho(b))(x) = (\rho(ab))(x) = c(ab, x)$, hence c is a left G action on X. □

4.4 Orbit decomposition, Cosets

Definition 4.4.1. We say a left G action on a non-empty set X is **transitive**, if for every $x, y \in X$, there is some $g \in G$ such that $y = gx$.

Remark 4.4.2. An equivalent definition of transitivity is that there is some $x \in X$, such that for every $y \in Y$, there is some $g \in G$ such that $y = gx$. To show that this seemingly weaker definition is actually equivalent to Definition 4.4.1, if there is some x such that every $y \in Y$ can be written as $y = gx$ for some $g \in G$, then for any $y, z \in X$, there are $g, g' \in G$ such that $y = gx$ and $z = g'x$, hence $x = g'x = g'(g^{-1}y) = (g'g^{-1})y$.

Theorem 4.4.3. Let X be a left G set. Then

1. $\sim = \{(x, y) \in X \times X : \text{ there exists } g \in G, y = gx\}$ is an equivalence relation on X.

2. The equivalence classes are non-empty G-invariant subsets, where the G action is transitive. We call them **G-orbits**.

The decomposition of X into disjoint unions of elements of $X/\sim$ (see Remark 2.5.3), is called the **orbit decomposition**.

Proof. 1. $x = e_G x$, hence $\sim$ contains id_X as a subset. Symmetry is because if $y = gx$ then $x = g^{-1}y$, and transitivity is because if $y = gx$, $z = g'y$, then $z = g'(gx) = (g'g)x$.

2. By definition, $[x] = \{gx : g \in G\}$. Hence for any $g' \in G$, $gx \in [x]$, $g'(gx) = (g'g)x \in [x]$, hence $[x]$ is G-invariant. For any $y \in [x]$, $y = g''x$ for some $g'' \in G$, hence the G action on $[x]$ is transitive.

□

The orbit decomposition shows that any left G set is a disjoint union of non-empty transitive left G sets. Now we will investigate their structures.

Theorem 4.4.4. Let G be a group, $H \leq G$ a subgroup. The set of left cosets G/H has a transitive left G action by $g(aH) = (ga)H$, and the stablizer of eH is H.

Proof. 1. Firstly we show that this left G-action is well defined. If $aH = bH$, then $b^{-1}a \in H$, hence for any $g \in G$, $(gb)^{-1}(ga) = (b^{-1}g^{-1})(ga) = b^{-1}a \in H$, so $g(aH) = g(bH)$.

2. Now we verify that this map satisfies Definition 4.1.1 Part 1: $e_G(aH) = (e_G a)H = aH$; for any $g, g' \in G$, $g(g'(aH)) = (gg'a)H = (gg')(aH)$.

3. Next we show that this left G action is transitive: for any $aH \in G/H$, $aH = a(eH)$.

4. Lastly we calculate the stablizer: $G_{eH} = \{g \in G : g(eH) = eH\} = \{g \in G : gH = eH\} = \{g \in G : e^{-1}g \in H\} = H$.

□

Theorem 4.4.5. Let X and Y be two non-empty transitive left G-sets. The followings are equivalent:

1. $X \cong Y$.
2. There are $x \in X$, $y \in Y$, such that $G_x = G_y$.
3. For all $x \in X$, $y \in Y$, there is some $g \in G$ such that $G_x = gG_y g^{-1} = \{ghg^{-1} : h \in G_y\}$.
4. There are $x \in X$, $y \in Y$, such that there is some $g \in G$ and $G_x = gG_y g^{-1} = \{ghg^{-1} : h \in G_y\}$.

Proof.

- 1 $\implies$ 2: Let $f : X \to Y$ be an isomorphism, pick $x \in X$, $y = f(x)$, then $G_y = \{g \in G : gy = y\} = \{g \in G : gf(x) = f(x)\} = \{g \in G : f(gx) = f(x)\} = \{g \in G : gx = x\} = G_x$.
- 2 $\implies$ 3: Suppose $a \in X$, $b \in Y$, $G_a = G_b$. Because the G action on both X and Y are transitive, for any $x \in X$, $y \in Y$, there are $c, c' \in G$ such that $x = ca$, $y = c'b$. Hence $G_x = \{g \in G : gca = ca\} = \{g \in G : c^{-1}gca = a\} = \{g \in G : c^{-1}gc \in G_a\} = \{g \in G : c^{-1}gc \in G_b\} = \{g \in G : c^{-1}gcb = b\} = \{g \in G : c'c^{-1}gcc'^{-1}c'b = c'b\} = \{g \in G : c'c^{-1}gcc'^{-1} \in G_y\} = cc'^{-1}G_y(cc'^{-1})^{-1}$.
- 3 $\implies$ 4: This is obvious.
- 4 $\implies$ 1: Let $x \in X$, $y \in Y$ satisfies $G_x = gG_y g^{-1}$. Because the G-action on X is transitive, for any $x' \in X$, there is some g' such that $x' = g'x$. Define $f : X \to Y$ such that $f(x') = g'gy$.
  1. Firstly we show that this is well defined: if $g''x = g'x$, then $g'^{-1}g'' \in G_x = gG_y g^{-1}$, hence there is some $b \in G_y$ such that $g'^{-1}g'' = gbg^{-1}$, hence $(g'g)^{-1}(g''g) = b \in G_y$, which implies that $g''gy = g'gy$.

2. Next we show that this is G-equivariant: for any $a \in G$, $x' = g'x \in X$, $f(ax') = f((ag')x) = ag'gy = a(gg'y) = af(x')$.
3. Next we show that this map is an injection: if $f(g'x) = f(g''x)$, then $g'gy = g''gy$, which shows that $g^{-1}g''^{-1}g'gy = y$. Hence $g^{-1}g''^{-1}g'g \in G_y$, which implies that $g''^{-1}g \in gG_yg^{-1} = G_x$.
4. Lastly we show that this map is a surjection. Because G action on Y is also transitive, for every $y' \in Y$, there is some $b \in G$ such that $y' = by$. Hence $y' = f(bg^{-1}x)$.

□

Theorem 4.4.6. Let X be a non-empty transitive left G-set, $x \in X$, then there is a left G-set isomorphism from G/G_x to X, sending eG_x to x.

Proof. This is an immediate consequence of Theorem 4.4.4 and Theorem 4.4.5. □

4.5 Applications

4.5.1 Cycle Notation

Let $\sigma \in S_n$, there is a left $\mathbb{Z}$ action on $\{1, \ldots, n\}$ defined by $tx = \sigma^t(x)$. One can write down σ by specifying the orbits of this action that has more than one element, in the order of $a, \sigma(a), \sigma^2(a), \ldots$. For example, $\sigma \in S_6$ that sends 1 to 3, 2 to 6, 3 to 4, 4 to 1, 5 to 5 and 6 to 2 can be written as $(1, 3, 4)(5, 6)$. This is called the **cycle notation**.

4.5.2 Lagrange's Theorem

Theorem 4.5.1 (Lagrange's Theorem)**.** Let G be a finite group, $H \leq G$, then $|G| = |H||G/H|$. In particular, $|H|$ is a factor of $|G|$.

Proof. Consider the left H^{op} action on G, $h \cdot g = gh$. Because $g' = gh$ iff $g^{-1}g' = h$, the orbits of this action are exactly the left cosets. The stablizer at any $g \in G$ equals $H_g^{op} = \{h \in H : gh = g\} = \{e_H\}$, hence each orbit is isomorphic to $H^{op}/\{e\} = \{\{h\} : h \in H\}$, which has the same number of elements as $|H|$. So $|G| = |H^{op}||G/H| = |H||G/H|$. □

Theorem 4.5.2. Let G be a finite group, $g \in G$. Then:

1. There is a positive integer n such that $g^n = e_G$. The smallest such positive integer is called the **order** of g, denoted as $ord(g)$.
2. The subgroup generated by g is $\langle g \rangle = \{e, g, \ldots, g^{ord(g)-1}\}$, and is a group of $ord(g)$ elements.
3. $ord(g)$ is a factor of $|G|$.

Proof. 1. Finiteness of G implies that g^n, $n \in \mathbb{N}$ can not all be distinct. If there are natural numbers $a < b$ such that $g^a = g^b$, then $g^{b-a} = e$.

2. Firstly show that the $ord(g)$ elements, $e = g^0, g, g^2, \ldots, g^{ord(g)-1}$ are all distinct. If not, there are $0 \leq a < b \leq ord(g) - 1$ such that $g^a = g^b$, then $g^{b-a} = e$ and $0 < b - a \leq ord(g) - 1 < ord(g)$, which contradicts with the assumption on $ord(g)$. Now it is easy to verify that this set is closed under product and inverse.

3. This follows from Part 2 above and Theorem 4.5.1.

□

5 Rings and Modules

6 Congurence Problem