Math 541 Modern Algebra

Fall 2024

Contents

1 Introduction

1.1 Syllabus

Institution Name: University of Wisconson at 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 Approximated correspondence with textbook sections

Sections in this notes	Sections in the textbook
3.1, 3.2	1.1-1.6, 2.1, 2.3-2.5, 3.1, 4.4
3.3	3.2-3.5, 5.1, 5.4
4.1	1.7, 4.1-4.3
4.2	2.2
4.3	4.1
4.4, 4.5	3.2, 4.1, 4.5, 5.3, 5.5
6.1, 6.2	7.1-7.4, 10.1, 10.2
7.1	8.1-8.3
7.2	7.6

1.4 Some examples of applications of algebra

Example 1.4.1. 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 1.4.2.

$$\begin{gathered}
1/3 = 0.333333\dots \\
1/6 = 0.166666\dots \\
1/7 = 0.142857142857\dots \\
1/9 = 0.111111\dots \\
1/11 = 0.09090909\dots \\
1/12 = 0.0833333\dots \\
1/13 = 0.076923076923076923\dots \\
\dots
\end{gathered}$$

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 1.4.3. 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 1.4.4. 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.

Example 2.3.5. As a non mathematical example, if A is a finite set whose elements represent the students in UW Madison, B a finite set whose elements represent the courses offered at UW Madison, then $\{(a,b) : a \in A, b \in B, \text{ student } a \text{ took course } b\}$ is a relation.

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 $Map(A,B)$ or B^A.

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.

Remark 2.4.2. $f : A \to B$ is a function, $C \subseteq A$, $D \subseteq B$, then $f(f^{-1}(D)) \subseteq D$, $C \subseteq f^{-1}(f(C))$.

Example 2.4.3.

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. $\{(n,2n) : n \in \mathbb{N}\} \in Map(\mathbb{N},\mathbb{N})$, but $\{(2n,n) : n \in \mathbb{N}\} \notin Map(\mathbb{N},\mathbb{N})$.

5. Let A be a set, $f : A \to P(A)$ defined as $f(a) = A \backslash \{a\}$ and $h : A \to P(P(A))$ defined as $h(a) = \{B \in P(A) : a \notin B\}$ are both functions which are injections but not surjections, while $g : P(P(A)) \to P(A)$ where $g(B) = \bigcup B$ is a surjection but not an injection.

6. $Map(\emptyset, A) = \{\emptyset\}$.

Definition 2.4.4. 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 2.4.5.

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 2.4.6. 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 2.4.7. $f : A \to B$ 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. □

Remark 2.4.8. The notation of inverse functions is similar to the notation of preimages.

Theorem 2.4.9. 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 2.4.7 it is a bijection. □

Example 2.4.10. For example, the bijection in Theorem 2.4.9 sends $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ to $n \mapsto (x \mapsto n + x)$.

Remark 2.4.11. 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 $b \mapsto a + b$. For example in JavaScript:

```
curry=(f=>(x=>(y=>f(x, y))))
f=(curry(((x, y)=>x+y)))(3)
console.log(f(2))
```

or Python 3:

```
def curry(f): return (lambda x: (lambda y: f(x, y)))
f=(curry((lambda x, y: x+y)))(3)
print(f(2))
```

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

Definition 2.4.12.

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 2.4.13. 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 2.4.14.

1. 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 $|A| \leq |B|$.

2. 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. Let A be a set and $\sim$ an equivalence relation on A. For every $a \in A$, we call the subset $[a] = \{b \in A : a \sim b\}$ the **equivalence class represented by** a. The set of equivalence classes $\{[a] : a \in A\}$ is called the **quotient set**, denoted as $A/\sim$.

Example 2.5.3.

1. $id_A = \{(a,a) : a \in A\}$ is an equivalence relation. The corresponding quotient set is $\{\{a\} : a \in A\}$.

2. $A \times A$ is an equivalence relation. The corresponding quotient set is $\{A\}$.

3. If A represents the students at UW-Madison, then

$$\sim = \{(a,b) : a \text{ and } b \text{ have the same first name}\}$$

is an equivalence relation.

4. Let $f : A \to B$ be a map, then $\sim_f = \{(a,b) : f(a) = f(b)\}$ is an equivalence relation. The corresponding quotient set is $\{f^{-1}(\{b\}) : b \in f(A)\}$.

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 $\mathbb{Z}/n$.

Theorem 2.5.4. Let A be a set and $\sim$ an equivalence relation on A. Then every element in A belongs to a unique element of $A/\sim$. The map $p : A \to A/\sim$, defined by $p(a) = [a]$, which we call the **quotient map**, is a surjection, and $\sim = \sim_p$ where $\sim_p$ is as defined in Part 4 of Example 2.5.3.

Proof. Every $a \in A$ belongs to $[a] \in A/\sim$ because $a \sim a$. If $a \in [b]$, then $b \sim a$ hence $a \sim b$. On the other hand, for every $c \in [b]$, we have $b \sim c$, so $a \sim c$ which implies that $[b] \subseteq [a]$. Similarly one can show that $[a] \subseteq [b]$, hence $[a] = [b]$.

To show the second part of the Theorem, surjectivity of quotient map is because every $[a] \in A/\sim$ equals $p(a)$. If $p(a) = p(b)$ then $b \in p(b) = p(a) = [a]$, hence $a \sim b$. If $a \sim b$, then $b \in [a]$, the argument above shows that $[b] = [a]$, hence $p(a) = p(b)$. □

Remark 2.5.5. Let $\sim$ be an equivalence relation on a set A. Then Theorem 2.5.4 implies that $A = \bigcup(A/\sim)$ 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 $A/\sim$.

The ideas in Example 2.5.3 Part 4 gives a way to relate equivalence relations and surjections:

Theorem 2.5.6. Let A, B, Q be sets, $f : A \to B$ a map, $g : A \to Q$ a surjection. Let $\sim_f$ and $\sim_g$ be the equivalence relations defined in Example 2.5.3 Part 4. 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 2.4.5. 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.

Example 3.1.3. 1. $(\mathbb{R}\backslash\mathbb{Q}, +)$ is not a group (group operation is not well defined).

2. $(\mathbb{R}, *)$ where $a * b = \begin{cases} a + b & ab = 0 \\ 0 & ab \neq 0 \end{cases}$ is not a group (no associativity, $1 * (1 * 2) \neq (1 * 1) * 2$).

3. $(\{2n : n \in \mathbb{Z}\}, \times)$ is not a group (no identity).

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

5. $(\mathbb{Z}, (a, b) \mapsto a + b - 1)$ is a group.

Definition 3.1.4.

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 3.1.5. 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 a group homomorphism, see Theorem 3.2.2.

Example 3.1.6. 1. 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. S_n are non abelian if $n \geq 3$.

2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ 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.

3. exp is a homomorphism from $(\mathbb{R}, +)$ to $(\{x \in \mathbb{R} : x > 0\}, \times)$, but $x \mapsto 2\exp(x)$ isn't.

4. From linear algebra we have the classical matrix groups $GL(n) = \{n \times n \text{ invertible matrices}\}$, $SL(n)$, $O(n)$, $SO(n)$, $U(n)$, $SU(n)$, $SP(n)$, $\dots$ which are all groups under matrix multiplication. det is a homomorphism from these groups to $\mathbb{R}\backslash\{0\}$ (or $\mathbb{C}\backslash\{0\}$).

5. Any vector space is a group under $+$, and linear transformations are group homomorphisms.

6. The set of invertible 3×3 upper triangular matrices form a group.

7. 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 equilateral triangle has 6 elements while the isometry group of a sphere has infinitely many.

8. Let V be a n dimensional vector space, the set of bijective linear transformations from V to itself is a subgroup of S_V, and by linear algebra it is isomorphic to $GL(n)$.

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

10. The set of smooth bijections from $\mathbb{R}$ to $\mathbb{R}$, which sends 0 to 0 and the inverse is also smooth, form a group under composition. The map $f \mapsto f'(0)$ is a homomorphism from this group to $(\mathbb{R}\backslash\{0\}, \times)$.

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**.

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

Definition 3.1.8.

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. More generally, let $\{(G_\alpha, *_\alpha) : \alpha \in I\}$ be a family of groups, $\prod_{\alpha \in I} G_\alpha$ is a group under $* : (f, g) \mapsto (\alpha \mapsto f(\alpha) *_\alpha g(\alpha))$, called the **direct product** of this family of 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. (Cancellation Law) $ab = ac$ implies $b = c$, $ba = ca$ implies $b = c$.

3. The identity is unique.

4. The inverse is unique.

5. $(ab)^{-1} = b^{-1}a^{-1}$.

6. $(a^{-1})^{-1} = a$.

Proof. 1. Repeatedly apply associativity law.

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

3. Suppose e, e' are identities, then $e = ee' = e'$.

4. Suppose $a \in G$, b, b' are its inverses, then $ab = e = ab'$, now apply Part 2 (Cancellation Law).

5. $(ab)^{-1}(ab) = e = b^{-1}b = b^{-1}(a^{-1}a)b = (b^{-1}a^{-1})(ab)$, now apply Cancellation Law.

6. $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$, now apply Cancellation Law.

□

Theorem 3.2.2. Let $(G, *)$ be a group, $H \subseteq G$. Then:

1. If H is a subgroup.

2. There is a map $*_H : H \times H \to H$, such $(H, *_H)$ is a group, and the inclusion map from H to G is a group homomorphism.

And when they are true, the map $*_H = *|_{H\times H}$, hence is unique.

Proof.

- $1 \implies 2$: Let $*_H = *|_{H\times H}$. Condition (b) of Definition 3.1.4 Part 2 implies that $*_H$ is a map, Condition (a) implies the existence of identity and Condition (c) implies the existence of inverse. Associativity follows from the associativity of $*$.

- $2 \implies 1$: Let $a, b \in H$, the inclusion map i is a group homomorphism implies that $a *_H b = i(a *_H b) = i(a) * i(b) = a * b$, so $*_H = *|_{H\times H}$. This is a well defined map implies Condition (b) of Definition 3.1.4 Part 2. To show Condition (a), let e_H be the identity element of $(H, *_H)$, then $e_H *_H e_H = e_H = e_H * e = e_H *_H e_H$, so $e = e_H \in H$. To show Condition (c), let $a \in H$, b be its inverse under $*_H$, then $a *_H b = a * b = e$, hence b equals the inverse of a under $*$.

The uniqueness follows from the argument of $2 \implies 1$. □

Theorem 3.2.3. 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 2.4.7) 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. $f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H = (f(a))^{-1}f(a)$, now apply cancellation law (Theorem 3.2.1 Part 2).

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 3.2.4.

1. Theorem 3.2.3 Part 3 implies that if $N \leq H$, $H \leq G$ then $N \leq G$.

2. Theorem 3.2.3 Part 4 implies that the intersection of two subgroups is a subgroup.

3. More generally, one can show from the definition of subgroups (Definition 3.1.4 Part 2), that the intersection of a non empty set of subgroups of a given group is a subgroup.

Remark 3.2.5. Let G be a group, $S \subseteq G$, the intersection of all subgroups which contain all 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.

Example 3.2.6. S_n where $n \geq 3$ can be generated by 2 elements.

Remark 3.2.7. If there is an isomorphism f between groups G and H, we say G is **isomorphic to** H, denoted as $G \cong H$.

Theorem 3.2.8. 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 3.2.3 Part 5 and Remark 2.4.5 Part 2 implies that this subset is closed under function composition (which is the group operation of S_G). Theorem 3.2.3 Part 6 shows that it is closed under inverses. □

Example 3.2.9. Consider the group $(\mathbb{Z}, +)$.

1. Group homomorphisms from $\mathbb{Z}$ to itself are of the form $f_a(x) = ax$ where $a = f(1) \in \mathbb{Z}$.

2. $f_2(\langle 3 \rangle) = \langle 6 \rangle \leq \mathbb{Z}$, $f_2^{-1}(\langle 3 \rangle) = \langle 3 \rangle \leq \mathbb{Z}$.

3. $Aut(\mathbb{Z}) = \{f_1, f_{-1}\}$, any subgroup of $\mathbb{Z}$ will get sent to itself by either of the two automorphisms.

3.3 Kernels, Quotients, Isomorphism Theorem

Definition 3.3.1. Let $f : G \to H$ be a group homomorphism. Theorem 3.2.3 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 $\langle 2\pi \rangle = \{2\pi n : n \in \mathbb{Z}\}$, 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 2.5.6 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.

Theorem 3.3.4. Let G be a group, $H \leq G$ a subgroup, then:

1. $\sim_H = \{(a, b) \in G \times G : a^{-1}b \in H\}$ is an equivalence relation on G.
2. The equivalence class represented by $g \in G$ is $[g] = \{gh : h \in H\}$ (which we denote as gH).

Proof. We first check that $\sim_H$ is indeed an equivalence relation:

1. For any $a \in G$, $a^{-1}a \in H$.
2. For any $a, b \in G$, if $a^{-1}b \in H$, then $b^{-1}a = (a^{-1}b)^{-1} \in H$.
3. For any $a, b, c \in G$, if $a^{-1}b \in H$, $b^{-1}c \in H$, then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

Now $[g] = \{g' \in G : g^{-1}g' \in H\} = \{g' \in G : g^{-1}g' = h \text{ for some } h \in H\} = \{gh : h \in H\}$. □

Definition 3.3.5. The equivalence classes under $\sim_H$ are called **left cosets**, and the set of left cosets, $G/\sim_H$, is denoted as G/H.

Theorem 3.3.6. 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 $gHg^{-1} \subseteq H$).

Proof. 1. 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 $ghg^{-1} \in H$.

2. From 2 to 1: Suppose $H \leq G$ satisfies $gHg^{-1} = H$. Let $Q = G/H$ as in Definition 3.3.5 and f be the quotient map, and 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 $aH = a'H$, $bH = b'H$, 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 $(ab)H = (a'b')H$.

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

   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 3.3.7. Condition 2 in Theorem 3.3.6 can also be written as "for every $g \in G$, $h \in H$ iff $ghg^{-1} \in H$", or "$gHg^{-1} = H$". Subgroups that satisfy either condition in Theorem 3.3.6 are called **normal subgroups**, denoted as $N \trianglelefteq G$. The corresponding Q with surjection $f : G \to Q$ constructed in the proof of Theorem 3.3.6 are called **quotient groups**, denoted as $Q = G/N$.

Example 3.3.8.

1. Any subgroup of an abelian group is a normal subgroup.

2. 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.

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

4. 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 3.3.6, $\ker(f) \trianglelefteq G$. 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 3.2.3 Part 6, it is an isomorphism. Hence $G \cong f(G)$. □

The following theorem provides a condition under which one can "reverse" the construction in Example 3.3.8 Part 2:

Theorem 3.3.10. Let G, H, N be three groups. The followings are equivalent:

1. $G \cong H \times N$.

2. There are normal subgroups H' and N' of G, such that $H \cong H'$, $N \cong N'$, $H' \cap N' = \{e_G\}$, and every element in G can be written as hn where $h \in H'$, $n \in N'$.

3. There is a surjective homomorphism $p : G \to H$, such that $\ker(p) \cong N$, and there is a $s \in Hom(H, G)$ such that $s(H) \trianglelefteq G$, and $p \circ s = id_H$.

Proof. (1) $1 \implies 3$: Let $\phi : H \times N \to G$ be the isomorphism, $p_1 : (h, n) \mapsto h$, $p_2 : (h, n) \mapsto n$ are two surjective homomorphisms from $H \times N$ to H and N respectively. Then let $p = p_1 \circ \phi^{-1}$, and $s(h) = \phi(h, e_N)$. It is easy to verify that all the conditions are satisfied.

(2) $3 \implies 2$: Let $N' = \ker(p)$, $H' = s(H)$. Because $p \circ s = id_H$, s is an injection, hence $H' \cong H$. Let $a \in H' \cap N'$, then $a = s(h)$ for some $h \in H$ and $p(a) = e_H$, hence $h = p(s(h)) = e_H$, which implies that $a = e_G$. Lastly, every $g \in G$ can be written as $g = s(p(g))(s(p(g))^{-1}g)$, the first factor is in H' and the second in N'.

(3) $2 \implies 1$: Let i_1, i_2 be the isomorphisms from H to H' and N to N' respectively. Define $\psi : H \times N \to G$ as $\psi(h, n) = i_1(h)i_2(n)$.

   (a) Firstly we show that ψ is a group homomorphism: let $(h, n), (h', n') \in H \times N$,
$$\psi((h,n)(h',n')) = i_1(h)i_1(h')i_2(n)i_2(n')$$
$$= i_1(h)i_2(n)(i_2(n)^{-1}i_1(h')i_2(n)i_1(h')^{-1})i_1(h')i_2(n')$$
   However,
$$i_2(n)^{-1}i_1(h')i_2(n)i_1(h')^{-1} = (i_2(n)^{-1}i_1(h')i_2(n))i_1(h)'^{-1} \in H'$$
$$i_2(n)^{-1}i_1(h')i_2(n)i_1(h')^{-1} = i_2(n)^{-1}(i_1(h')i_2(n)i_1(h')^{-1}) \in N'$$
   Hence $i_2(n)^{-1}i_1(h')i_2(n)i_1(h')^{-1} = e_G$, $\psi((h,n)(h',n')) = \psi(h,n)\psi(h',n')$.

   (b) If $(h, n) \in \ker(\psi)$, then $i_1(h)i_2(n) = e_G$, hence $i_1(h) = i_2(n)^{-1} \in H' \cap N'$, so $i_1(h) = i_2(n) = e_G$, $(h, n) = e_{H\times N}$. This shows that ψ is an injection.

   (c) Surjectivity of ψ follows from the fact that elements of G can be written as a product of an element in H' and an element in N'.

$\square$

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 N, denoted as $G \cong N \rtimes H$.

Example 3.3.12. When $n \geq 3$, $S_n \cong A_n \rtimes \mathbb{Z}/2$, where p is defined as in Example 3.3.8 and s sends -1 to the element in S_n that permutes 1 and 2.

4 Group Actions

4.1 Left Gsets, 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.

Example 4.1.3.

1. $G = S_X$, $gx = g(x)$. The only possible G-invariant subsets are X and $\emptyset$.

2. If $f : X \to X$ is a bijection, X has a left $\mathbb{Z}$ action defined by $nx = f^n(x)$. Here f^0 is the identity map, f^n when $n > 0$ is the composition of n copies of f, and f^n when $n < 0$ is the composition of $-n$ copies of f^{-1}.

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. There are of course G-invariant subsets which are not subspaces, for example $V\backslash\{0\}$.

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.

5. Let $G = GL(n, \mathbb{R})$, the set of $n \times k$ matrices $M_{n\times k}(\mathbb{R})$ has a left G action by matrix multiplication. Multiplication from the right by a $k \times k$ matrix is a G equivariant self map.

Example 4.1.4.

1. X a non empty set, $ga = a$ for all $g \in G$, $a \in X$ is a left G-action called the **trivial action**. If Y is a left G_Y set as in Part 1 of Example 4.1.3, then a map from Y to X is G-equivariant iff it is constant.

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 $c(g, h) = f(g)h$, and f is a G-equivariant map from G with left action to H with this action.

4.2 Basic Properties, Stablizers

Analogous to Theorem 3.2.2, we have:

Theorem 4.2.1. Let X be a left G-set. The followings are equivalent:

1. $Y \subseteq X$ is a G invariant subset.

2. There is a left G action on Y such that the inclusion map is G-equivariant.

And when they are true, the left G-action is unique and equals the original left G-action restricted to $G \times Y$.

Proof.

- $1 \implies 2$: Let the left G-action be the restriction of the left G action on X to $G \times Y$. Y being G-invariant implies that it is well defined, and it satisfies the definition of left G action because it is the restriction of a left G action.

- $2 \implies 1$: Inclusion being G-equivariant implies that the left G action on Y is the restriction of the left G-action on X. Now Y being G invariant because this left G action is well defined.

□

Analogous to Theorem 3.2.3 and Theorem 3.2.8, we have:

Theorem 4.2.2. 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 2.4.7) 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. □

Example 4.2.3. Let G be a left G set under the left action, $Aut(G) \cong G^{op}$.

Remark 4.2.4. 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 4.2.5. 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 3.1.4 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 $a^{-1} \in G_x$.

□

Example 4.2.6.

1. Consider the left S_X action on X as defined in Example 4.1.3 Part 1. For every $a \in X$, $(S_X)_a \cong S_{X\backslash\{a\}}$.

2. Consider the left $(\mathbb{R}\backslash\{0\}, \times)$ action in Example 4.1.3 Part 3, then $G_v = \begin{cases} G & v = 0 \\ \{0\} & v \neq 0 \end{cases}$.

Definition 4.2.7. 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**.

Example 4.2.8. Let $G = (\mathbb{R}\backslash\{0\})$, V be an R-vector space, the left G action on $V\backslash\{0\}$ via scalar multiplication 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 2.4.7, 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**.

Definition 4.3.3. The kernel of the conjugate action is a subgroup $\{g \in G : \text{ for all } h \in G, hg = gh\}$, called the **center**, denoted as $C(G)$.

Example 4.3.4.

1. $C(GL(n, \mathbb{R}))$ consists of multiples of the identity matrix.

2. $C(S_3)$ consists of only the identity element.

Remark 4.3.5. Let X be a left G set, the kernel of the left G action equals

$$\{g \in G : gx = x \text{ for all } x \in X\} = \bigcap_{x \in X} \{g \in G : gx = x\} = \bigcap_{x \in X} G_x$$

Hence if X is non-empty and the left G action is free then it is also effective.

Example 4.3.6. The S_X action on X in Example 4.1.3 Part 1 is not free as long as X has more than 2 elements. However, the permutation representation is the identity map, hence it is effective.

Theorem 4.3.7. (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 4.3.8. 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 2.4.9, 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 3.2.3 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 G-orbit represented by x is denoted as Gx.

The decomposition of X into disjoint unions of elements of $X/\sim$ (see Remark 2.5.5), 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.

□

Example 4.4.4.

1. Let G be a group, the left action of G on G is transitive, hence it has a single orbit which is G itself.

2. Let G be a group with more than 1 elements, the conjugate action of G on G is not transitive. The G-orbits are called **conjugacy classes**.

3. The S_X action on X defined as $(g, x) \mapsto g(x)$ (see Example 4.1.3 Part 1) is transitive and has a single G orbit.

4. The $(\mathbb{R} \backslash \{0\}, \times)$-orbits of Example 4.1.3 Part 3 are $\{0\}$, $\{kv : k \in \mathbb{R}, k \neq 0\}$.

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 4.4.5. Let G be a group, $H \leq G$ a subgroup. The set of left cosets G/H (see Definition 3.3.5) 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 4.4.6. 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 $G_x = gG_yg^{-1} = \{ghg^{-1} : h \in G_y\}$.

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

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 $G_x = gG_yg^{-1}$. 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 $g'^{-1}g'' \in G_x = gG_yg^{-1}$, 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 4.4.7. 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 4.4.5 and Theorem 4.4.6. □

4.5 Applications

4.5.1 Cycle Notation

Let $\sigma \in S_n$, there is a left $\mathbb{Z}$ action on $\{1, \dots, n\}$ defined by $tx = \sigma^t(x)$ (See Example 4.1.3 Part 2). One can write down σ by specifying the orbits of this action that has more than one element, in the order of $a, \sigma(a), \sigma^2(a), \dots$. 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 $(1, 3, 4)(2, 6)$. This is called the **cycle notation**.

4.5.2 Lagrange's Theorem

Theorem 4.5.1 (Lagrange's Theorem, or Orbit-Stablizer 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} (see Definition 3.1.8 Part 1) 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 $H^{op}_g = \{h \in H : gh = g\} = \{e_H\}$, 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 $\langle g \rangle = \{e, g, \dots, g^{ord(g)-1}\}$, 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, $e = g^0, g, g^2, \dots, g^{ord(g)-1}$ 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.

□

Example 4.5.3. Let p be a prime number, the set $A = (\mathbb{Z}/p)\backslash\{[0]\}$ is a group of $n-1$ elements under multiplication $[a][b] = [ab]$. To show that this is a group we need to check the following:

1. The group operation is well defined: if $[a] \neq [0]$, $[b] \neq [0]$, then p divides neither a nor b. Because p is a prime, it would not divide ab, hence $[ab] \in A$. If $[a] = [a']$, $[b] = [b']$, then p divides both $a - a'$ and $b - b'$, hence divides $ab - a'b' = a(b - b') + b'(a - a')$ which implies that $[ab] = [a'b']$.

2. Associativity follows from the associativity of inter multiplication.

3. The identity element is $[1]$.

4. For any $[a] \in A$, the map $m_a : A \to A$ defined as $m_a([b]) = [ab]$ is an injection, because if $[ab] = [ab']$ then p divides $ab - ab' = a(b - b')$, which together with the assumption that $[b] = [b']$. Because A is a finite set, any injective self map is also a bijection, hence we can let $[a]^{-1} = m_a^{-1}([1])$.

Now apply Theorem 4.5.2 Part 3, we know that for any $[x] \in A$, $[x]^n = [x^n] = [1]$. Hence for any integer x which not a multiple of p, $x^{p-1} - 1$ is a power of p. This is called **Fermat's Little Theorem**.

4.5.3 Semidirect Products

Recall that in Remark 3.3.11, if G is a group, $H \trianglelefteq G$, $Q = G/H$, $p : G \to Q$ the quotient map, and there is $s \in Hom(Q, G)$ such that $p \circ s = id_Q$, then we say G is a semidirect product between H and Q.

1. $H \cap s(Q) = \{e_G\}$. This follows from the same argument in the "$3 \implies 2$" part of the proof of Theorem 3.3.10.

2. There is a bijection from the Cartesian product $H \times Q$ to G, defined as $(h, q) \mapsto hs(q)$.

   (a) To show that this is an injection, if $hs(q) = h's(q')$, then $q = p(hs(q)) = p(hs(q')) = q'$, which implies that $h = h'$.

   (b) The surjectivity of this map follows from the same argumnt in the "$3 \implies 2$" part of the proof of Theorem 3.3.10.

3. Let $h, h' \in H$, $q, q' \in Q$, then

$$hs(q)h's(q') = (hs(q)h's(q)^{-1})s(qq')$$

   Consider the left Q action on H defined by $q \cdot h = s(q)hs(q)^{-1}$, let ψ be its permutation representation, which is a homomorphism from Q to $Aut(H)$, then

$$(hs(q))(h's(q')) = h((\psi(q))(h'))s(qq')$$

4. From the computation above, we see that the group operation of G is determined by $\psi : Q \to Aut(H)$. Hence we can write G as $G \cong H \rtimes_\psi Q$.

4.5.4 Some Properties of Finite Groups

Definition 4.5.4. 1. The number of elements of a group is called its **order**.

2. If G is a group and $H \leq G$, $|G/H|$ is called the **index** of subgroup H, denoted as $[G : H]$

Theorem 3.3.9, 4.3.1 and 4.5.1 together can be used to deduce various properties of finite groups and finite index subgroups:

Theorem 4.5.5. Let G be a group, $H \leq G$ and $[G : H] = n < \infty$. Let N be the kernel of the left G-set G/H, then

1. $N \leq H$

2. $[G : H] = kn$ where k is a factor of $(n-1)!$.

Proof. 1. By construction, $N = \{g \in G : (ga)H = aH \text{ for all } a \in G\} \subseteq \{g : g \in G : (ge)H = eH\} = H$.

2. Let $\rho : G \to S_{G/H}$ be the permutation representation, then $N = \ker(\rho)$. Hence, $[G : N] = |G/N|$, and by Theorem 3.3.9, G/N is isomorphic to a subgroup of $S_{G/H}$, hence by Theorem 4.5.1, $|G/N|$ is a factor of $|S_{G/H}|$ which is $n!$. On the other hand, G/H has a transitive left G/N action by $(aN)(bH) = (ab)H$, hence by Theorem 4.4.7 and Theorem 4.5.1, n is a factor of $|G/N|$.

□

Example 4.5.6. Let G be a group, H a subgroup of finite index, then there is a normal subgroup of G which is contained in H and also has finite index. This is an immediate consequence of Theorem 4.5.5.

Example 4.5.7. Let G be a group, $H \leq G$ and $[G : H] = 2$, then H is a normal subgroup of G. By Theorem 4.5.5, there is some $N \subseteq H$, such that $N \trianglelefteq G$ and $[G : N] = 2$. If $N \neq H$, there is some element $h \in H$ such that $hN \neq eN$. Yet $G = eN \cup hN$, hence $H = G$, a contradiction. Hence $H = N$.

Example 4.5.8. If G is a group of p elements where p is a prime number, then pick an element x which is not an identity, by Theorem 4.5.2 Part 3 its order must be p, hence G must be isomorphic to $(\mathbb{Z}/p, +)$.

Theorem 4.5.9. Let G be a finite abelian group, p be a prime that divides $|G|$, then G has a subgroup isomorphic to $\mathbb{Z}/p$.

Proof. Induction on $|G|$. If $|G| = 1$ it is trivially true, if $|G|$ is prime then it follows from Example 4.5.8. Now suppose the theorem is valid for all groups with fewer elements than $|G|$ but not for G. If $ord(g)$ is a multiple of p, then a subgroup can be found as $\langle g^{ord(g)/p} \rangle$, a contradiction. So we can now assume that for all $g \in G$, $ord(g)$ is not a multiple of p. Now pick $g \in G$, $g \neq e$, let $m = ord(g)$. Now $|G/\langle g \rangle| = |G|/m < |G|$, and p is not a factor of m which means that it is a factor of $|G|/m$. So by inductive hypothesis, there is some $h \in |G|/\langle g \rangle$ such that $ord(h) = p$. Let $h' \in G$ be a preimage of h under the quotient map, then $h'^{ord(h')} = e$ which implies $h^{ord(h')} = e$ which implies that p is a factor of $ord(h')$, a contradiction. □

Theorem 4.5.10. Let G be a finite group, p a prime number that divides $|G|$. Then G has a subgroup isomorphic to $\mathbb{Z}/p$.

Proof. Induction on $|G|$ similar to the proof of Theorem 4.5.9. Suppose the Theorem fails for a group G but is true for all groups with order less than G, then no proper subgroup of G may have an order which is a multiple of p, which means that, by Theorem 4.4.7 -and Theorem 4.5.1, the cardinality of all transitive left G sets are either 1 or a multiple of p.

Now consider the conjugate action of G on G. By orbit decomposition, the number of orbits of length 1 must be a multiple of p. The union of these orbits are the center (see Definition 4.3.3), so $|C(G)|$ is a multiple of p, which is only possible when $G = C(G)$ hence G is abelian. Now it follows from Theorem 4.5.9. □

Example 4.5.11. Let G be a group of 21 elements, we shall show that it must be a semidirect product between $\mathbb{Z}/7$ and $\mathbb{Z}/3$. By Theorem 4.5.10, G has a subgroup N isomorphic to $\mathbb{G}/7$, and a subgroup H isomorphic to $\mathbb{G}/3$. It is easy to see that $N \cap H = \{e\}$. Now it remains to show that N is a normal subgroup. Let ρ be the permutation representation of the left G action on G/N, which is a homomorphism from G to $S_{G/N}$ which has $3! = 6$ elements. By Theorem 4.5.5, $[G : \ker(\rho)] = 3$ or 6, but 6 is not a factor of G, so $[G : \ker(\rho)] = 3$. By the same argument as in Example 4.5.7, $N = \ker(\rho) \trianglelefteq G$.

5 Midterm Review

Groups	Left G sets
Group homomorphisms	G-equivariant maps
Subgroups	G-invariant subsets
Image and preimage of subgroups under homomorphisms are subgroups	Image and preimage of G-invariant subsets under G-equivariant maps are G-invariant
Composition and inverse of homomorphisms are homomorphisms	Composition and inverse of G-equivariant maps are G-equivariant
Kernel, normal subgroups, quotients, Isomorphism Theorem	
Permutation Representation	
	Orbit decomposition, set of left cosets

Practice Problems:

1. Show that if $g \in G$ is an element with infinite order, the stablizer of g under the conjugate action has infinitely many elements.

2. Find a group G, two subgroups N and H, such that the set $\{nh : n \in N, h \in H\}$ is not a subgroup. Hint: can let $G = S_3$.

3. Show that the set of rational numbers that can be written as p/q where both p and q are odd, form a group under ×. Find all subgroups of this group with finitely many elements.

4. Let G be a group, H a subgroup, show that $\cdot : (H \times H) \times G \to G$ defined as $((a, b), x) \mapsto axb^{-1}$ is a left $H \times H$-action. Show that when G is a finite group, H is normal iff the stablizer at every $x \in G$ is isomorphic to H.

Answer:

1. Because all g^n, $n \in \mathbb{Z}$, are in this stablizer.

2. Let $G = S_3$, $N = \langle (1, 2) \rangle$, $H = \langle (1, 3) \rangle$.

3. Denote this set as A, then if $r, r' \in A$, we can write $r = p/q$, $r' = p'/q'$ where p, p', q, q' are all odd, hence $rr' = (pp')/(qq') \in A$. Associativity follows from the associativity of multiplication in $\mathbb{Q}$, identity element is $1 = 1/1$, and if $p/q \in A$ where p, q are both odd, its inverse under × is q/p, which is also in A. The only finite subgroups are $\{1\}$ and $\{\pm 1\}$, because any element with absolute value not 1 has infinite order under ×.

4. $(e,e)\cdot g = ege^{-1} = g$, $(a,b)\cdot((c,d)\cdot g) = a(cgd^{-1})b^{-1} = (ac)g(bd)^{-1} = (ac,bd)\cdot g$. $(H\times H)_g = \{(a,b)\in H\times H : agb^{-1} = g\} = \{(a,b)\in H\times H : a = gbg^{-1}\}$. If H is normal, there is an isomorphism from H to $(H\times H)_g$ defined as $h\mapsto (ghg^{-1},h)$. If H is not normal, there is some $g\in G$ such that $H\cap(gHg^{-1})$ is a proper subgroup of H. Denote this subgroup as H', then H' can not be isomorphic to H as it has fewer elements, and H' is isomorphic to $(H\times H)_g$ by $h\mapsto (h, g^{-1}hg)$.

6 Rings and Modules

6.1 Definitions and Examples

Definition 6.1.1.

1. A **ring** is a triple $(R, + : R \times R \to R, \times : R \times R \to R)$, such that:

   (a) $(R, +)$ is an abelian group.

   (b) (Associativity) For any $a, b, c \in R$,

   $$\times(\times(a, b), c) = \times(a, \times(b, c))$$

   (c) (Distribution) For any $a, b, c \in R$,

   $$\times(+(a, b), c) = +(\times(a, c), \times(b, c))$$
   $$\times(a, +(b, c)) = +(\times(a, b), \times(a, c))$$

2. A subset $S \subseteq R$ is called a **subring**, if $(S, +) \leq (R, +)$, and for any $a, b \in S$, $\times(a, b) \in S$.

3. Let $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ be two rings. A map $f : R \to S$ is called a **ring homomorphism**, if for any $a, b \in R$, $f(+_R(a, b)) = +_S(f(a), f(b))$, $f(\times_R(a, b)) = \times_S(f(a), f(b))$.

Definition 6.1.2. Let $(R, +, \times)$ be a ring.

1. If there is some $u \in R$, which is not the identity of $(R, +)$, such that for any $r \in R$, $\times(u, r) = \times(r, u) = r$, R is said to **have identity**, and u is the **multiplicative identity**.

2. If for any $a, b \in R$, $\times(a, b) = \times(b, a)$, we say R is a **commutative ring**.

3. If R is a commutative ring with identity and $\times(a, b)$ equals the identity of $(R, +)$ implies either a or b equals the identity of $(R, +)$, then we call R an **integral domain**.

4. Let R' be R with the identity of abelian group $(R, +)$ removed. If $(R', \times)$ is an abelian group, we say R is a **field**.

5. The set of homomorphisms from a ring R to a ring S is denoted as $Hom(R, S)$.

Remark 6.1.3. 1. When $(R, +, \times)$ is a ring and there is no ambiguity on $+$ and $\times$, we can also say "R is a ring".

2. $+(a, b)$ can also be written as $a + b$, the inverse of $a \in R$ under $(R, +)$ can be written as $-a$, and the identity element of the group $(R, +)$ is often denoted as 0. $\times(a, b)$ can be written as $a \times b$ or ab. The multiplicative identity, when exists, is often denoted as 1. When R is a field, the inverse of $a \in R\backslash\{0\}$ in $(R\backslash\{0\}, \times)$ is denoted as a^{-1}.

Definition 6.1.4. Let $(R, +, \times)$ be a ring.

1. A **(left)** R**-module** is a triple $(M, + : M \times M \to M, \cdot : R \times M \to M)$, where $+ : (a, b) \mapsto a + b$ and **scalar multiplication** $\cdot : (r, x) \mapsto r \cdot x$, such that:
   (a) $(M, +)$ is an abelian group.
   (b) (Associativity) For any $a, b \in R$, $x \in M$
   $$(a \times b) \cdot x = a \cdot (b \cdot x)$$
   (c) (Distribution) For any $a, b \in R$, $x, y \in M$
   $$(a + b) \cdot x = a \cdot x + b \cdot x$$
   $$a \cdot (x + y) = a \cdot x + a \cdot y$$
2. A subset $N \subseteq M$ is called a **submodule**, if $(N, +) \leq (M, +)$, and for any $a \in R$, $x \in N$, $a \cdot x \in N$.
3. Let $(M, +_M, \cdot_M)$ and $(N, +_N, \cdot_N)$ be two R-modules. A map $f : M \to N$ is called a R**-module homomorphism**, if for any $x, y \in M$, $a \in R$, $f(x +_M y) = f(x) +_N f(y)$, $f(a \cdot_M x) = a \cdot_N f(x)$.

Remark 6.1.5.

1. When there are no ambiguities, "$(M, +, \cdot)$ is an R-module" can be written as "M is an R-module".
2. The inverse of $a \in M$ under $(M, +)$ is written as $-a$, and the identity element denoted as 0.
3. If M is an R-module, $a \in R$, $x \in M$, $a \cdot m$ can also be written as am.
4. The set of R-module homomorphisms between M and N is denoted as $Hom_R(M, N)$.

Remark 6.1.6. In the textbook, they require further that if R has identity, then an R-module M has to have $1 \cdot x = x$ for all $x \in M$. We will specify when we want our modules to satisfy this further condition.

Definition 6.1.7. If F is a field, M an F module such that for any $x \in M$, $1 \cdot x = x$, then we call M an F vector space. This is compatible with the definition in linear algebra.

Some elementary properties of rings and modules:

Theorem 6.1.8. Let R be a ring.

1. If R has multiplicative identity, then such multiplicative identity is unique.
2. For any $a \in R$, $0 \times a = a \times 0 = 0$.

3. If M is a left R module and 0_M the identity of $(M, +)$, then for any $a \in R$, $m \in M$, $0 \cdot m = a \cdot 0_M = 0_M$.

Proof. 1. (See proof of Theorem 3.2.1 Part 3) Suppose 1 and $1'$ are both multiplicative identities, then $1 = 1 \times 1' = 1'$.

2. $0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a$, now apply cancellation law in $(R, +)$. The proof of $a \times 0 = 0$ is similar

3. Similar to the proof of Part 2 above.

□

Remark 6.1.9. Theorem 6.1.8 Part 2 implies that a field must be an integral domain.

Example 6.1.10.

1. $(\{0\}, + : (0, 0) \mapsto 0, \times : (0, 0) \mapsto 0)$ is a ring. We denote it as 0.

2. Let $(A, +)$ be an abelian group, define $\times : A \times A \to A$ sending everything to 0, then $(A, +, \times)$ is a commutative ring.

3. Let R be a ring, then, by Theorem 6.1.8 Part 2, $\{0\}$ (denoted as 0) and R itself are both subrings of R, id_R and the constant map that sends every element to 0 are both homomorphisms from R to R.

4. Let R be a ring, M an R-module, then, by Theorem 6.1.8 Part 3, both $\{0\}$ and M itself are submodules of M, id_M and the map that sends every element to 0 are both R-module homomorphisms from M to itself.

5. Let R be a ring, then R is an R module by $r \cdot x = r \times x$.

6. If $f : R \to S$ is a ring homomorphism, then S is an R-module by $r \cdot s = f(r) \times_S s$. In particular, S is an R module.

Example 6.1.11.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are rings under the usual addition and multiplication, they are all integral domains, each is a subring of the next, and the latter 3 are also fields.

2. $\{2n : n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$ and also a commutative ring without identity.

3. The set of $n \times n$ real matrices, denoted as $M_{n\times n}(\mathbb{R})$, is a ring under matrix addition and multiplication. $\mathbb{R}^n$ is a $M_{n\times n}(\mathbb{R})$ module under the matrix to (column) vector multiplication.

4. Let A be a set, define $\times : P(A) \times P(A) \to P(A)$ as $(B, C) \mapsto B \cap C$, $+ : P(A) \times P(A) \to P(A)$ as $(B, C) \mapsto (B \cup C) \backslash (B \cap C)$.

5. Any abelian group $(A, +)$ is a $\mathbb{Z}$-module, via scalar multiplication

$$n \cdot x = \begin{cases} \underbrace{x + x + \cdots + x}_{n\text{-times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{-n\text{-times}} & n < 0 \end{cases}$$

Example 6.1.12. The set of compactly supported continuous functions $C_c(\mathbb{R})$ is a ring under function addition $+$ and convolution $*$ which is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(t)g(x-t)dt$$

Here a function f is called **compactly supported** if there is some $M > 0$ such that $|x| > M$ implies $f(x) = 0$.

1. To show $+$ and $*$ are both well defined, if f equals 0 outside $[-M, M]$, g equals 0 outside $[-M', M']$, then $f + g$ equals 0 outside

$$[-\max(M, M'), \max(M, M')]$$

and $f * g$ equals 0 outside $[-M - M', M + M']$. It is easy to see, from analysis, that both $f + g$ and $f * g$ are continuous, hence they are both in $C_c(\mathbb{R})$.

2. $(C_c(\mathbb{R}), +)$ is an abelian group follows from the $\mathbb{R}$-vector space structure on $C_c(\mathbb{R})$.

3. Distribution laws follow from the fact that $f \mapsto f * g$ and $g \mapsto f * g$ are both $\mathbb{R}$-linear.

4. To show associativity of $*$, let $f, g, h \in C_c(\mathbb{R})$, then

$$((f * g) * h)(x) = \int_{\mathbb{R}} \left(\int_{\mathbb{R}} f(t)g(s-t)dt \right) h(x-s)ds$$

$$= \int_{\mathbb{R}^2} f(t)g(s-t)h(x-s)dtds = \int_{\mathbb{R}} f(t) \left(\int_{\mathbb{R}} g(s-t)h(x-s)ds \right) dt$$

$$\int_{\mathbb{R}} f(t) \left(\int_{\mathbb{R}} g(s')h(x-t-s')ds' \right) dt = (f * (g * h))(x)$$

Theorem 6.1.13. Let $(A, +)$ be an abelian group. Let $+ : Hom(A, A) \times Hom(A, A) \to Hom(A, A)$ be $(f + g)(a) = f(a) + g(a)$, $\times : Hom(A, A) \times Hom(A, A) \to Hom(A, A)$ be $f \times g = f \circ g$. Then $(Hom(A, A), +, \times)$ is a ring with multiplicative identity, called the **endormorphism ring**, denoted as $End(A)$. A is a left $End(A)$ module by $f \cdot a = f(a)$.

Proof.

1. First show that both $+$ and $\times$ are well defined. The well definedness of $\times$ follows from Theorem 3.2.3 Part 5. To show $+$ is well defined, let $f, g \in Hom(A, A)$, for any $a, b \in A$, $(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b) = (f(a) + g(a)) + (f(b) + g(b)) = (f+g)(a) + (f+g)(b)$, so $f + g \in Hom(A, A)$.

2. To show $(Hom(A, A), +)$ is an abelian group. We can see that associativity and commutativity of $(Hom(A, A), +)$ are due to the associativity and commutativity of $(A, +)$. It is also easy to see that the identity element of $(Hom(A, A), +)$ is the constant map sending every element of A to the identity element 0_A, and if $f \in Hom(A, A)$, $-f$ is defined as $(-f)(a) = -f(a)$ for all $a \in A$.

3. Associativity of $\times$ follows from the associativity of function compositions.

4. Let $f, g, h \in Hom(A, A)$. For any $a \in A$,

   $$(f \times (g+h))(a) = f(g(a)+h(a)) = f(g(a)) + f(h(a)) = (f \times g + f \times h)(a)$$

   So $f \times (g + h) = f \times g + f \times h$. The other distribution law can be proved similarly.

5. $1_{End(A)} = id_A$.

6. By checking the definition as above, we can also show that $(A, +, \cdot)$ is a left $End(A)$-module.

□

Example 6.1.14. If $(A, +) = (\mathbb{Z}, +)$, elements of $End(A)$ are f_k, where $k \in \mathbb{Z}$, and $f_k + f_{k'} = f_{k+k'}$, $f_k \times f_{k'} = f_{kk'}$. So $f_k \mapsto k$ is a bijective ring homomorphism from $End(A)$ to $(\mathbb{Z}, +, \times)$.

Definition 6.1.15. Let R be a ring, G a group, the **group ring**, denoted as $R[G]$, consists of maps from G to R such that all but finitely many $g \in G$ is sent to 0, and $(a+b)(g) = a(g) + b(g)$, $(a \times b)(g) = \sum_{h \in G, a(h) \neq 0} a(h)b(h^{-1}g)$. When R has multiplicative identity 1, so is $R[G]$, and the multiplicative identity of $R[G]$ equals $1_{R[G]}(g) = \begin{cases} 1 & g = e \\ 0 & g \neq e \end{cases}$ When R is a field, a module M of $R[G]$ such that for any $x \in M$, $1_{R[G]} \cdot x = x$, is called an R-**linear representation** of group G.

Remark 6.1.16. The proof that $R[G]$ is a ring is similar to Example 6.1.12, with integration replaced by summation.

Example 6.1.17. $R[\mathbb{Z}]$ can be seen as the ring of Laurent polynomials with coefficients in R (denoted as $R[z, z^{-1}]$), via $a \mapsto \sum_n a(n)z^n$. The subring where $a(n) = 0$ for all $n < 0$ can be seen as the **polynomial ring** $R[z]$.

Definition 6.1.18. If R is an integral domain, Let $Q = R\times(R\backslash\{0\})/\sim$, where $(a, b)\sim(c, d)$ iff $ac = bd$. Let $+_Q : Q\times Q\to Q$ be defined as $([(a, b)], [(c, d)])\mapsto [(ad + bc, bd)]$, $\times_Q : Q\times Q\to Q$ be $([(a, b)], [(c, d)])\mapsto[(ac, bd)]$, then one can show that Q is a field (remember to check $+_Q$, $\times_Q$ being well defined first), called the **field of fractions** of R. $0_Q = [(0, 1)]$, $1_Q = [(1, 1)]$.

Example 6.1.19. When k is a field, we can show that $k[z]$ is an integral domain. The field of fractions of $k[z]$ is called the **field of rational functions**, denoted as $k(z)$.

Remark 6.1.20. One can define R^{op}, as well as direct product of rings and modules, similar to Definition 3.1.8. Furthermore, there is an important concept called **direct sum**, which is a subring (or submodule) of the direct product of a family of rings (or modules), where the function takes 0 for all but finitely elements in the index set.

6.2 More Basic Properties

Theorem 6.2.1. Let $(R, +, \times)$ be a ring, $(M, +, \cdot)$ an R module. Then

1. For any $a, b\in R$, $x\in M$, $(-a)\times b = a\times(-b) = -(a\times b)$, $(-a)\cdot x = a\cdot(-x) = -(a\cdot x)$.
2. For any $a, b\in R$, $x\in M$, $(-a)\times(-b) = a\times b$, $(-a)\cdot(-x) = a\cdot x$.

Proof.
1. By Theorem 6.1.8, $(-a)\times b + (a\times b) = (-a + a)\times b = 0_R\times b = 0$, hence $(-a)\times b = -(a\times b)$. The other three statements are analogous.
2. This follows from Part 1 above and Theorem 3.2.1 Part 6.

□

Many Theorems in Sections 3.2, 3.3, 4.2, 4.3, 4.4 have their analogies in the setting of rings and modules. We will list them below. We will omit most of the proofs as they are similar to the proofs in those sections.

6.2.1 Subrings and submodules, automorphism groups

Theorem 6.2.2 (Analogy of Theorem 3.2.2)**.** Let $(R, +, \times)$ be a ring, $S\subseteq R$ a subset. Then S is a subring iff there are $+_S : S\times S\to S$, $\times_S : S\times S\to S$, such that the inclusion map is a ring homomorphism. When this is true, $+_S = +|_{S\times S}$, $\times_S = \times|_{S\times S}$

Theorem 6.2.3 (Analogy of Theorem 4.2.1)**.** Let R be a ring, $(M, +, \cdot)$ a left R module, $N\subseteq M$ a subset. Then N is a submodule of M iff there are $+_M : M\times M\to M$, $\cdot_M : R\times M\to M$, such that $(M, +_M, \cdot_M)$ is a left R module and the inclusion map is an R module homomorphism.

Theorem 6.2.4 (Analogy of Theorems 3.2.3, 3.2.8, 4.2.2)**.**

1. Let $f : R\to S$ be a ring homomorphism.

   (a) Let R', S' be subrings of R and S respectively, then $f(R')$ is a subring of S and $f^{-1}(S')$ is a subring of R.

   (b) If $g : S \to Q$ is another ring homomorphism, then $g \circ f$ is a ring homomorphism from R to Q.

   (c) If f is a bijection, then f^{-1} is a ring homomorphism. Such a homomorphism is called an **ring isomorphism** and the domain and codomain are said to be **isomorphic**.

   (d) $Aut(R)$, which consists of bijective ring homomorphisms from R to itself, called the **group of ring automorphisms**, is a subgroup of the permutation group S_R.

2. Let R be a ring, M, N be R-modules, $f : M \to N$ an R-module homomorphism.

   (a) Let M', N' be submodules of M and N respectively, then $f(M')$ is a submodule of N and $f^{-1}(N')$ is a submodule of M.

   (b) If $g : N \to Q$ is another R-module homomorphism, then $g \circ f$ is an R-module homomorphism from M to Q.

   (c) If f is a bijection, then f^{-1} is an R-module homomorphism. Such a homomorphism is called an **R-module isomorphism** and the domain and codomain are said to be **isomorphic**.

   (d) $Aut_R(M)$, which consists of bijective R-module homomorphisms from M to itself, called the **group of R-module automorphisms**, is a subgroup of the permutation group S_M.

Remark 6.2.5.

1. Let R be a ring, then both $\{0\}$ and R are subrings. Hence, if $f : R \to S$ is a ring homomorphism, then the **image** $f(R)$ and the **kernel** $f^{-1}(\{0\})$ are subrings of S and R respectively.

2. Let R be a ring, M an R-module, then both $\{0\}$ and M are submodules. Hence, if $f : M \to N$ is an R-module homomorphism, then the **image** $f(M)$ and the **kernel** $f^{-1}(\{0\})$ are submodules of N and M respectively.

3. Intersection of subrings are subrings. If T is a subring of S, S is a subring of R, then T is a subring of R.

4. Intersection of submodules are submodules. If N is a submodule of M, Q a submodule of N, then Q is a submodule of M.

Example 6.2.6. The only automorphism from the ring of real numbers $\mathbb{R}$ to itself is the identity map. This is because such a map f must send 1 to 1, hence is identity when restricted to $\mathbb{Q}$. On the other hand, if $a \geq 0$, $f(a) = f(\sqrt{a})^2 \geq 0$. Hence $a \leq b$ implies $f(a) \leq f(b)$. Now suppose $f(r) > r$, there is some rational q in between, which implies that $r < q$ and $f(r) > q = f(q)$, a contradiction. Similarly $f(r) < r$ can never happen, this implies that $f = id_{\mathbb{R}}$.

Example 6.2.7. Let K be a field, K is an R-module as in Example 6.1.10 Part 4, then $Aut_K(K) = \{x \mapsto xc : c \in K\backslash\{0\}\}$, $Aut_K(K \times K) \cong GL(2, K)$.

Example 6.2.8. Any ring can be made into a subring with multiplicative identity. Let R be a ring, $R' = (R \times \mathbb{Z}, +', \times')$ such that $(a, n) +' (b, m) = (a + b, n + m)$, $(a, n) \times' (b, m) = (ab + nb + ma, mn)$.

6.2.2 Isomorphism Theorems

The analogy of Theorem 3.3.3 and Theorem 3.3.6 in the settings of modules and rings are as follows:

Theorem 6.2.9 (Analogy of Theorem 3.3.6)**.** Let R be a ring, M an R-module, N a subgroup of $(M, +)$. The followings are equivalent:

1. M is a submodule.
2. The quotient group M/N has a R-module structure where the scalar multiplication defined as $r \cdot (x + N) = rx + N$.
3. There is a left R module Q, and an R module homomorphism f from M to Q, such that N is its kernel $\ker(f) = f^{-1}(\{0\})$.

Proof.

- $1 \implies 2$: N is a normal subgroup of $(M, +)$ so M/N is an abelian group under addition. N being closed under scalar multiplication implies that this $\cdot$ is well defined, and $a \cdot (b \cdot (x + N)) = abx + N = (ab) \cdot (x + N)$, $(a+b) \cdot (x+N) = (a+b)x+N = (ax+bx)+N = a \cdot (x+N)+b \cdot (x+N)$.
- $2 \implies 3$: Let $Q = M/N$ and f be the quotient map $x \mapsto x + N$.
- $3 \implies 1$: This follows from Theorem 6.2.4 Part 2(a).

□

Theorem 6.2.10 (Analogy of Theorem 3.3.6)**.** Let R be a ring, I a subgroup of $(R, +)$. The followings are equivalent:

1. For any $a \in R$, $c \in I$, $a \times c \in I$ and $c \times a \in I$.
2. The quotient group R/I has a ring structure with $\times$ defined as $(a + I) \times (b + I) = a \times b + I$.
3. There is a ring S, and a ring homomorphism f from R to S, such that $I = \ker(f) = f^{-1}(\{0\})$.

Proof.

- $1 \implies 2$: I is a normal subgroup of $(R, +)$ so R/I is an abelian group under addition. To show that $\times$ on R/I is well defined, if $a + I = a' + I$, $b + I = b' + I$, then $a'b' - ab = a'(b' - b) + (a' - a)b \in I$, so $ab + I = a'b' + I$. Associativity of $\times$ and distribution law follows from the associativity and distribution laws of R.
- $2 \implies 3$: Let $S = R/I$, f be the quotient map.

- $3 \implies 1$: By Theorem 6.2.4 Part 1(a), $\ker(f)$ is a subring of R. We only need to show that for any $r \in R$, any $a \in \ker(f)$, $ar \in \ker(f)$, $ra \in \ker(f)$. This is because $f(ar) = 0 \times f(r) = 0$, $f(ra) = f(r) \times 0 = 0$.

□

Definition 6.2.11. Subrings that satisfies the conditions in Theorem 6.2.10 are called **ideals**. If R is a commutative ring with identity, I an ideal of R, then:

1. If R/I is an integral domain we call I a **prime** ideal.

2. If R/I is a field, we call I a **maximal** ideal.

Example 6.2.12. Let $\mathbb{Z}$ be the ring of integers, $(a) = \{na : n\mathbb{Z}\}$ is an ideal, the quotient $\mathbb{Z}/(a)$ is an integral domain iff $a = 0$ or $\pm p$ where p is a prime.

Theorem 6.2.13 (Analogy of Theorem 3.3.3)**.** Let R be a ring, M, N, Q are R-modules, $f : M \to Q$ a surjective R-module homomorphism, $g : M \to N$ an R-module homomorphism. Then:

1. There is an R-module homomorphism h from Q to N such that $g = h \circ f$, if and only if $\ker(f) \subseteq \ker(g)$.

2. If h exists, it is unique.

3. If h exists, it is surjective iff g is surjective, injective iff $\ker(f) = \ker(g)$.

Theorem 6.2.14 (Analogy of Theorem 3.3.3)**.** Let R, S, Q be rings, $f : R \to Q$ a surjective ring homomorphism, $g : R \to S$ a ring homomorphism. Then:

1. There is a ring homomorphism h from Q to S such that $g = h \circ f$, if and only if $\ker(f) \subseteq \ker(g)$.

2. If h exists, it is unique.

3. If h exists, it is surjective iff g is surjective, injective iff $\ker(f) = \ker(g)$.

As a consequence of the above theorems, we have:

Theorem 6.2.15 (Analogy of Theorem 3.3.9)**.**

1. Let R be a ring, M, N are R-modules, $f : M \to Q$ an R-module homomorphism, then $f(M) \cong M/\ker(f)$.

2. Let R and S be rings and $f : R \to S$ a ring homomorphism, then $f(R) \cong R/\ker(R)$.

Example 6.2.16. Let $R = \mathbb{R}[t]$, $S = \mathbb{C}$. Let $f : R \to S$ be defined as $f(g) = g(\sqrt{-1})$, then $\ker(f) = \{(t^2 + 1)h(t) : h \in R\}$, which we denote as $(t^2 + 1)$, and $\mathbb{C} = R/(t^2 + 1)$.

6.2.3 Annihilators and Cyclic Modules

Definition 6.2.17. Let R be a ring. A subring A satisfying the condition that for all $a \in A$, $r \in R$, $ra \in A$, is called a **left ideal**.

Remark 6.2.18. If we see R as an R-module as in Example 6.1.10 Part 5, then a subset A is a left ideal iff it is a sub R-module of R.

Theorem 6.2.19 (Analogy of Theorem 4.2.5)**.** Let R be a ring, M an R-module, $x \in M$. The set $\{r \in R : rx = 0\}$ is a left ideal of R. We call it the **annihilator** of x, denoted as $Ann_R(x)$.

Definition 6.2.20. Let R be a ring with identity. We say an R-module M is **cyclic**, if there is $a \in M$ such that for every $x \in M$, there is some $r \in R$ such that $x = ra$. We call a the **generator** of this cyclic module, denoted by $M = Ra$.

Theorem 6.2.21. [Analogy of 4.4.6] Let R be a ring with identity, M, N two cyclic R-modules. Then $M \cong N$ as R-modules iff there are generators x of M, y of N, such that $Ann_R(x) = Ann_R(y)$.

It is easy to see that if R is a ring with mutiplicative identity, L a left ideal, then the quotient module R/L is cyclic with generator $1 + L$ whose annihilator equals L. Hence:

Theorem 6.2.22 (Analogy of Theorem 4.4.7)**.** Let R be a ring with identity and M a cyclic R module with generator a, then there is an R-module isomorphism $f : M \to R/Ann_R(a)$ sending a to $1 + Ann_R(a)$.

Proof. Consider surjective R-module homomorphism $R \to M$ defined by $r \mapsto ra$, apply Theorem 6.2.15 Part 1. □

Example 6.2.23. Let R be the ring of 2×2 real matrices, M be the R-module consisting of column vectors in $\mathbb{R}^2$, then $M = R[1,0]^T \cong R/Ann_R([1,0]^T)$.

6.2.4 Endomorphism Rings

Theorem 6.2.24 (Analogy of Theorem 4.3.8)**.** Let R be a ring, $(M,+)$ an abelian group. There is a one-to-one correspondence between R-module structures on M and $Hom(R, End(M))$, defined by:

$$(\cdot : R \times M \to M) \mapsto (r \mapsto (x \mapsto r \cdot x))$$

$$(\rho : R \to End(M)) \mapsto ((r,x) \mapsto (\rho(r))(x))$$

Example 6.2.25. Consider R as a left R module as in Example 6.1.10 Part 5, then there is a ring homomorphism $i : R \to End((R,+))$. What is the kernel?

Example 6.2.26. If R is the ring of even integers (2), $End((R,+)) \cong \mathbb{Z}$ by $(2n \mapsto 2kn) \mapsto k$. Then the left R module structure of R as in Example 6.1.10 Part 5 induces a homomorphism from R to $\mathbb{Z} \cong End((R,+))$ which is the embedding of (2) into $\mathbb{Z}$.

7 Euclidean Domains and Congurence Problems

7.1 Euclidean Domains

We learned in grade school that for integers we have "division with remainders", for example, given 13 and 3, we have $13 = 3 \times 4 + 1$. We shall formalize this property and look at its consequences:

Definition 7.1.1. An integral domain D is called **Euclidean**, if there is a map $v : D \backslash \{0\} \to \mathbb{N}$, such that for any $a, b \in D$, $b \neq 0$, there are $q, r \in D$, $a = qb + r$, such that either $r = 0$ or $v(r) < v(b)$. The process of finding such q and r is called **division with remainder** and v is called the **Euclidean function**.

Example 7.1.2.

1. $\mathbb{Z}$ is an Euclidean domain with Euclidean function $|\cdot|$.
2. $\mathbb{R}[x]$ is an Euclidean domain with Euclidean function being *deg*.
3. The Gaussian integer ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ is an Euclidean domain with Euclidean function $a^2 + b^2$. To see this, note that elements of $(a + bi) = \{(a + bi)(c + di) : c + di \in \mathbb{Z}[i]\}$ form a square lattice on the complex plane where the length of a side of the square is $\sqrt{a^2 + b^2}$. So the distance from any point in $\mathbb{C}$ to the closest lattice point is no more than $\sqrt{a^2 + b^2}$ which is strictly smaller than $\sqrt{a^2 + b^2}$.

7.1.1 PIDs, Euclid's algorithm

Theorem 7.1.3. Let D be an Euclidean domain, then any ideal I of D can be written as $I = \{ra : r \in D\}$ for some $a \in I$.

Proof. If there are no non-zero element in I, then $I = \{r0 : r \in D\}$. Suppose there are some non-zero element in I, let a be the one where the Euclidean function is minimized. For any $b \in I$, $b = ca + r$, then $r \in I$, which implies that $r = 0$. So $I = \{ra : r \in D\}$. □

Definition 7.1.4. Let D be a commutative ring with identity. An ideal of the form $\{ra : r \in D\}$ is called a **principal ideal**, denoted as (a), a is called its **generator**. More generally, let $\{a_i : i \in I\} \subseteq D$, then the ideal consisting of elements of the form $\sum_i r_i a_i$, where $r_i = 0$ for all but finitely many i, is called the **ideal generated by** $\{a_i\}$, denoted as $(a_i, i \in I)$, and $\{a_i : i \in I\}$ is called its **generating set**.

Definition 7.1.5. An integral domain whose every ideal is principal is called a **principal ideal domain** (PID).

Let D be a PID, by Theorem 7.1.3 given $a, b \in D$, the ideal $\{ra + r'b : r, r' \in D\}$, denoted as (a, b), equals some ideal (c). c is called the **greatest common divisor** of a and b, denoted as $c = gcd(a, b)$.

Lemma 7.1.6. Let D be a PID, $c = gcd(a, b)$ iff there exists $t, s, m, n \in D$ such that $c = ta + sb$, $a = mc$, $b = nc$.

Proof. For the "only if" part, existence of t and s is due to $c \in (a, b)$, existence of m and n are due to $a \in (c)$ and $b \in (c)$ respectively.

For the "if" part, existence of t and s implies that $(c) \subseteq (a, b)$, and existence of m and n implies that $(a, b) \subseteq (c)$. □

The question of finding these t, s, m, n is called **Bezout's Problem**. For Euclidean domains, this problem can be solved via an algorithm called **Euclid's Algorithm** (which is where the name "Euclidean domain" came from), first described by Euclid in c. 300 BCE:

Algorithm 1: Euclid's Algorithm

```
Data: $a, b \in R$, $ab \neq 0$
Result: $t, t', m \in R$, such that $m = \gcd(a, b)$, $m = ta + t'b$
$x \leftarrow a$; $t \leftarrow 1$; $t' \leftarrow 0$;
$x' \leftarrow b$; $s \leftarrow 0$; $s' \leftarrow 1$;
while $x' \neq 0$ do
    Find $q, r \in R$ such that $x = qx' + r$, where $r = 0$ or $h(r) < h(b)$;
    $u \leftarrow t - qs$; $u' \leftarrow t' - qs'$;
    $x \leftarrow x'$; $t \leftarrow s$; $t' \leftarrow s'$;
    $x' \leftarrow r$; $s \leftarrow u$; $s' \leftarrow u'$;
end
$m \leftarrow x$;
```

An example of this algorithm on $\mathbb{Z}$, implemented by Python, is as below:

```
import sys
a=int(sys.argv[1])
b=int(sys.argv[2])
if a*b==0:
    exit()

def euclid(a, b):
    x=[a, b]; t=[1, 0]; s=[0, 1]
    while x[1]!=0:
        r=x[0]%x[1]
        q=(x[0]-r)//x[1]
        u=[u-q*v for u, v in zip(t, s)]
        x[0]=x[1]; t=s
        x[1]=r; s=u
    return t[0], t[1], x[0]

print(euclid(a, b))
```

Definition 7.1.7. Let R be a commutative ring with identity 1. We say two ideals I and J are **coprime**, if the ideal $I + J = \{a + b : a \in I, b \in J\}$ equals $(1) = R$. We call two elements $a, b \in R$ **coprime** if the ideals (a) and (b) are coprime.

Remark 7.1.8. It is easy to see that if R is a PID then a and b are coprime iff $\gcd(a,b)$ has multiplicative inverse. In other words, if R is Euclidean, $a, b \in R$ coprime, by Euclid's Algorithm one can find $m = ra + sb$ such that $m^{-1} \in R$, hence $1 = (m^{-1}r)a + (m^{-1}s)b$.

Example 7.1.9. Let $R = \mathbb{Q}[x]$, $a = x^2 - x$, $b = x^2 + 1$. Then

$$\begin{bmatrix} x^2 - x \\ x^2 + 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

$$x^2 - x = 1 \times (x^2 + 1) + (-x - 1)$$

$$-x - 1 = a - b$$

$$\begin{bmatrix} -x - 1 \\ x^2 + 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

$$x^2 + 1 = (-x + 1) \times (-x - 1) + 2$$

$$2 = x^2 + 1 - (-x + 1) \times (-x - 1) = b - (-x + 1)(a - b) = (x - 1)a + (-x + 2)b$$

$$\begin{bmatrix} -x - 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ x - 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ x - 1 & -x + 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

$$-x - 1 = (-x/2 - 1/2) \times 2 + 0$$

Hence

$$2 = \gcd(a, b)$$

$$2 = (x - 1)a + (2 - x)b$$

$$1 = \frac{x - 1}{2}a + \frac{2 - x}{2}b$$

Remark 7.1.10. From the example above we see that if we write Euclid's algorithm in matrix form, then at each step the column vector $[x, x']^T$ is the column vector of the previous step multiplies with an elementary matrix, which is always invertible, hence when the computation terminates, we have $[x, 0]^T = M[a, b]^T$ where M is an invertible matrix in $M_{2\times2}(R)$, which implies that x is a linear combination of a and b and also both a and b are multiples of x. This is why the Euclid's algorithm works.

7.1.2 Unique Factorization

Definition 7.1.11. Let D be a commutative ring with identity. We say that $u \in D$ is a **unit** if it has multiplicative inverse. We say $p \in D$ is a **prime** if $(p) = \{rp : r \in D\}$ is a prime ideal, i.e. $D/(p)$ is an integral domain.

Remark 7.1.12. p is a prime iff p is not a unit, and if ab is a multiple of p then either a or b is a multiple of p. If $R = \mathbb{Z}$, the non-zero primes are prime numbers and their negations.

Lemma 7.1.13. Let v be an Euclidean function on Euclidean domain D, then $v'(a) = \min_{x \in D, x \neq 0} v(xa)$ is another Euclidean function, and for any non-zero $a, b \in D$, $v'(ab) \geq v'(a)$.

Proof. Given a, b, $b \neq 0$, let $v(cb) = v'(b)$, then there are q, r such that $a = qcb + r$, $r = 0$ or $v(r) < v(cb)$. In the latter case we have $v'(r) \leq v(r) < v(cb) = v'(b)$. This shows that v' is another Euclidean function. $v'(ab) \geq v'(a)$ is by construction. □

Definition 7.1.14. We say a domain D is a **unique factorization domain** (UFD), if every non-zero element $x \in D$ which is not a unit can be written as the product of finitely many primes (possibly with duplications) $x = p_1 \dots p_k$, which is called a **prime factorization**; and if x can be written as prime factorizations in two ways, $x = p_1 \dots p_k$, $x = q_1 \dots q_{k'}$, then $k = k'$, and after rearrangement, there are units u_j such that $q_j = u_j p_j$ for all j.

Theorem 7.1.15. An Euclidean domain is a UFD.

Proof. Let v be the Euclidean function on the Euclidean domain D such that $v(a) \leq v(ab)$ (they always exist due to Lemma 7.1.13). We first show that any non-zero element of D is either a unit or has a prime factorization. Suppose otherwise, let $x \in D$ be a non-zero element in D which is neither a unit nor a product of primes, and also has the smallest Euclidean functions among elements of this kind. Then there are $a', b' \in D$, such that $a' \notin (x)$, $b' \notin (x)$ and $a'b' \in (x)$. Let a and b be the remainders of a and b divide x respectively, then $v(a) < v(x)$, $v(b) < v(x)$, and $ab \in (x)$ hence there is $w \in D$ such that $ab = wx$. Now let $m = gcd(a, x)$, then $v(m) \leq v(a) < v(x)$. Furthermore, there is some $q \in D$ such that $x = mq$. Suppose $m = sa + tx$, then $mb = x(sw + tb) = mq(sw + tb)$, so $b = q(sw + tb)$. Hence we have $v(q) \leq v(b) < v(x)$. By assumption, both q and m are either unit or products of primes, a contradiction.

Suppose $x = p_1 \dots p_r$ and $x = q_1 \dots q_{r'}$ are two prime factorizations, because p_1 is a prime, there must be some q_j which is its multiple. And because q_j is a prime, it equals p_1 multiplying with a unit. Delete the common p_1, move the remaining unit into another $q_{j'}$, and continue. □

Example 7.1.16. As a consequence, the Gaussian integer ring $\mathbb{Z}[i]$ is Euclidean, hence a UFD. We can use this to study the integer solution of $x^2 + y^2 = n$.

7.2 Chinese Remainder Theorem

Theorem 7.2.1 (Chinese Remainder Theorem)**.** Let R be a commutative ring with identity, $I_1, \dots, I_n$ is a set of ideals that are pairwise coprime. Then the map:

$$Q : R \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$$

Defined by

$$Q(r) = (r + I_1, r + I_2, \dots, r + I_n)$$

is a surjection.

Proof. For any $a = (a_1 + I_1, \ldots, a_n + I_n) \in (R/I_1) \times \ldots (R/I_n)$, we will write down some $r \in R$ such that $Q(r) = a$.

For any pair $i \neq j$, by assumption, one can find $a_{ij} \in I_i$, $b_{ij} \in I_j$, such that $a_{ij} + b_{ij} = 1$. Let $w_i = \prod_{j \neq i} b_{ij}$, and $r = \sum_{i=1}^n a_i w_i$.

For any $1 \leq i \leq n$, $r - a_i = a_i(w_i - 1) + \sum_{j \neq i} a_j w_j$. Because for any $j \neq i$, $b_{ji} \in I_i$ is a factor of w_j, we have $\sum_{j \neq i} a_j w_j \in I_i$.

Furthermore,

$$w_i - 1 = \prod_{j \neq i} b_{ij} - 1 = \prod_{j \neq i}(1 - a_{ij}) - 1 = \sum_{\{j_1, \ldots, j_k\} \subseteq (\{1, \ldots, n\} \backslash \{i\}), k > 0} \prod_{l=1}^{k}(-a_{ij_l}) \in I_i$$

Hence $r - a_i \in I_i$, which implies that $Q(r) = a$. □

Remark 7.2.2. Given ideals $I_1, \ldots, I_n$, the problem of finding r such that $r - a_i \in I_i$ is called a **congruence problem**. The first known congruence problem dates back to 3-5th century CE China and is the following:

Find integer $n \in \mathbb{Z}$ such that $n - 2 \in 3\mathbb{Z}$, $n - 3 \in 5\mathbb{Z}$, $n - 2 \in 7\mathbb{Z}$.

The first known proof of the existence of solution, together with an algorithm, was described by Indian mathematician Aryabhata (476-550 CE).

Now you should be able to answer the questions in Example 1.4.3.

Example 7.2.3. Let $x_1, \ldots, x_n$ be n distinct real numbers, finding a polynomial in $\mathbb{R}[x]$ whose graph passes through $(x_1, y_1), \ldots, (x_n, y_n)$, is the same as solving congruence problem $f - y_i \in \{(x - x_i)g(x) : g \in \mathbb{R}[x]\}$. It is easy to see that we can set $a_{ij} = \frac{x_i - x}{x_i - x_j}$, $b_{ij} = \frac{x - x_j}{x_i - x_j}$, hence

$$f(x) = \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

which is called **Lagrange's interpolation formula**.

Remark 7.2.4. The map Q in Theorem 7.2.1 is a ring homomorphism and its kernel is $\bigcap_j I_j$. One can further show that the set of units (elements with multiplicative inverse) of $R/\bigcap_j I_j$, as a group under ×, is isomorphic to the direct product of groups of units of R/I_j. If the prime factorization of a natural number n is $n = \prod_j p_j^{n_j}$, then the group of units of $\mathbb{Z}/(n)$ has $\varphi(n) = \prod_j (p_j^{n_j} - p_j^{n_j - 1})$. (See Example 1.4.2).

8 Further Topics in Algebra

In 542:

- Modules over PIDs, rational normal form and Jordan normal form for matrices.
- Field extensions and Galois theory

Further topics:

- Algebraic number theory, commutative algebra, algebraic geometry
- Homological algebra, category theory
- Classification of finite simple groups
- Geometric group theory
- Lie Theory, K-theory, functional analysis
- ...

9 Final Review

9.1 Topics

Objects	Rings	Modules	Groups	Left G-sets
Subobjects	Subrings	Submodules	Subgroups	Invariant Subsets
Morphisms	Ring homomorphisms	Module homomorphisms	Group homomorphisms	Equivariant Maps
Basic Properties	Morphisms send subobjects to subobjects. Compositions of morphisms are morphisms. Inverses of morphisms which are morphisms. Bijective morphisms form groups, called Automorphism Groups. Intersections of subobjects are subobjects.			
	$f : A \to B$ surjective morphism, $g : A \to C$ morphism, there is morphism $h : B \to C$ such that $g = h \circ f$ iff $ker(f) \subseteq \ker(g)$. h is unique if exists. h injective iff $ker(f) = \ker(g)$.			
	Subring is kernel iff is ideal.	All submodule can be kernels.	Subgroup is kernel iff normal	
Quotient objects	Quotient Rings	Quotient Modules	Quotient Groups	
Isomorphism Theorem	$f : A \to B,\ f(A) \cong A/\ker(A)$			
	Scalar multiplications correspond to elements of $Hom(R, End(M))$		Left actions correspond to elements of $Hom(G, S_X)$	
		Annihilator Cyclic Modules		Stablizer Transitive Actions

Other topics:

- Effective and free actions.
- Orbit decomposition, Lagrange's Theorem, finite groups and finite index subgroups
- Direct product.
- Semidirect product of groups
- Euclidean domain, PID, UFD, Euclid's algorithm
- Chinese remainder theorem

9.2 Practice Problems

1. Let R be a ring, consider the $Aut(R)$ action on R. Is it transitive? Is it free? Is it effective?

2. Let R be a ring, I, J two ideals of R.

   (a) Is $\{ab : a \in I, b \in J\}$ an ideal of R?

   (b) Can you describe the smallest ideal containing this set?

   (c) Let IJ be this minimal ideal, what's the relationship between IJ and $I \cap J$?

   (d) Show that if R is commutative with multiplicative identity, $I+J = R$, then $IJ = I \cap J$.

3. Let M be an R module, f a module homomorphism from M to itself such that $f = f \circ f$. Show that there is a module N such that M is isomorphic to $\ker(f) \times N$.

Answer:

1. It is transitive iff $R = \{0\}$. It is free iff $Aut(R) = \{id_R\}$. For example, when $R = \mathbb{R}$ it is free and when $R = \mathbb{C}$ it isn't. It is always effective because if $\sigma \in Aut(R)$ has $\sigma(x) = x$ for all $x \in R$, then $\sigma = id_R$.

2. (a) No. For example, if $R = \mathbb{Z}[x]$, $I = J = (x, 2)$, x^2 and 4 are both in this set but $x^2 + 4$ isn't.

   (b) It is $\{\sum_i a_i b_i : a_i \in I, b_i \in J\}$.

   (c) $IJ \subseteq I \cap J$.

   (d) By assumption, there are $a \in I$, $b \in J$ such that $a + b = 1$. For any $x \in I \cap J$, $x = x \cdot 1 = x(a + b) = ax + xb \in IJ$.

   Remark 9.2.1. One can similarly define $I_1 \cdot I_n$, the kernel of the ring homomorphism Q in Theorem 7.2.1 then equals $I_1 I_2 \cdot I_n$, and we have

   $$R/(I_1 \cdot I_n) \cong (R/I_1) \times \cdots \times (R/I_n)$$

3. $N = \{x \in M : f(x) = x\}$, then for any $x \in M$, $x = (x - f(x)) + f(x)$, $x - f(x) \in \ker(f)$, $f(x) \in N$. One can verify that the map $x \mapsto (x - f(x), f(x))$ is an R-module isomorphism.

A HW

A.1 HW1

1. Let A be a set.

   (a) Let S be a non empty set of equivalence relations on A. Show that $\bigcap S$ is an equivalence relation on A.

   (b) Let R be a relation between A and A. Show that there is a unique equivalence relation on A, called $\sim_R$, such that $R \subseteq \sim_R$, and any equivalence relation $\sim$ on A which contains R has $\sim_R$ as a subset ($R \subseteq \sim \implies \sim_R \subseteq \sim$).

2. Let A and B be two sets, $f : A \to B$ a function. Define function $F : P(B) \to P(A)$ as $F(C) = f^{-1}(C)$. Show that F is an injection iff f is a surjection, F is a surjection iff f is an injection.

3. Show that $\sim = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Q}\}$ is an equivalence relation on $\mathbb{R}$.

4. Let A and B be two sets. $C = \{(x, i) \in (A \cup B) \times \{0, 1\} : x \in A \text{ if } i = 0, x \in B \text{ if } i = 1\}$. Show that there are injections $k : A \to C$, $j : B \to C$, such that $C = k(A) \cup j(B)$ and $k(A) \cap j(B) = \emptyset$.

5. Let $f : A \to B$ be a function. Show that there is a set C, an injection $g : A \to C$, and a surjection $h : C \to B$, such that $f = h \circ g$. (Hint: You may want to use the solution for the previous problem).

Answer:

1. (a) For every $C \in S$, because C is an equivalence relation, we have $id_A \subseteq C$, hence $id_A \subseteq \bigcap S$. For any $a, b \in A$, if $(a, b) \in \bigcap S$ then $(a, b) \in C$ for all $C \in S$, hence $(b, a) \in C$ for all $C \in S$, which implies that $(b, a) \in \bigcap S$. Lastly, for any $a, b, c \in A$, $(a, b) \in \bigcap S$, $(b, c) \in \bigcap S$ implies that for every $C \in S$, $(a, b) \in C$ and $(b, c) \in C$, hence $(a, c) \in C$, which implies that $(a, c) \in \bigcap S$.

   (b) Let S_R be the set of equivalence relations on A which has S as a subset. $R \subseteq A \times A$ so $A \times A \in S_R$, S_R is non-empty. Let $\sim_R$ be $\bigcap S_R$. Then due to (a), $\sim_R$ is an equivalence relation. By construction, $R \subseteq \sim_R$, and any equivalence relation $\sim$ that satisfies $R \subseteq \sim$ must be in S_R, hence $\sim_R \subseteq \sim$. Lastly, suppose there is some equivalence relation $\sim'$ such that $R \subseteq \sim'$ and $\sim' \subseteq \sim$ for every equivalence relation $\sim$ such that $R \subseteq \sim$, then $\sim' \subseteq \sim_R$ and $\sim_R \subseteq \sim'$, hence they must be equal.

2. (a) i. Suppose f is not a surjection, there must be some $b \in B$ which is not in $f(A)$, then $F(\emptyset) = \emptyset = F(\{b\})$, hence F is not an injection.

ii. Suppose F is not an injection, then there must be some $C, D \in P(B)$ such that $F(C) = F(D)$ and $C \neq D$. Suppose $C \backslash D \neq \emptyset$ (swap C and D if $D \backslash C \neq \emptyset$), let $b \in C \backslash D$. If there is some $a \in A$ such that $f(a) = b$, then $a \in F(C)$ and $a \notin F(D)$, a contradiction, hence $b \notin f(A)$, f is not a surjection.

(b) i. Suppose f is an injection, then for every $E \in P(A)$, $F(f(E)) = f^{-1}(f(E)) = \{a \in A : \text{ there exists } a' \in E, f(a) = f(a')\} = \{a \in A : \text{ there exists } a' \in E, a = a'\} = E$, hence F is a surjection.

ii. Suppose f is not an injection, there must be $a, b \in A$, $f(a) = f(b)$ and $a \neq b$. Consider $\{a\} \in P(A)$. If $\{a\} = F(C)$, then $f(a) \in C$, hence $f(b) \in C$, $b \in F(C)$, a contradiction. Hence F can not be a surjection.

3. For any $x, y, z \in \mathbb{R}$, $x - x = 0 \in \mathbb{Q}$, hence $x \sim x$. If $x \sim y$, then $x - y \in \mathbb{Q}$, hence $y - x = -(x - y) \in \mathbb{Q}$, $y \sim x$. If $x \sim y, y \sim z$, then $x - y \in \mathbb{Q}$, $y - z \in \mathbb{Q}$, hence $x - z = (x - y) + (y - z) \in \mathbb{Q}$, $x \sim z$.

4. Let k ad j be defined as $k : a \mapsto (a, 0)$, $j : b \mapsto (b, 1)$. By the construction of C both are well defined, and every element in C is of the form $(a, 0)$ where $a \in A$ or $(b, 1)$ where $b \in B$, in the former case it would be in $k(A)$ and in the latter case it would be in $j(B)$, hence $C = k(A) \cup j(B)$. If $(x, i) \in k(A) \cap j(B)$, $(x, i) \in k(A)$ implies $i = 0$, $(x, i) \in j(B)$ implies $i = 1$, contradiction. Hence $k(A) \cap j(B) = \emptyset$.

5. Let $C = \{(x, i) \in (A \cup B) \times \{0, 1\} : x \in A, i = 0 \text{ or } x \in B \backslash f(A), i = 1\}$, g be $a \mapsto (a, 0)$, and h be $h((x, i)) = \begin{cases} f(x) & i = 0 \\ x & i = 1 \end{cases}$. Then one can easily verify that g is an injection, h is a surjection, and $h \circ g = f$.

A.2 HW2

1. Let A be a set. $+_A : P(A) \times P(A) \to P(A)$ defined as $(B, C) \mapsto (B \cup C) \backslash (B \cap C)$. Then:

   (a) Show that $(P(A), +_A)$ is an abelian group.

   (b) Let $A' \subseteq A$, show that $B \mapsto B \cap A'$ is a homomorphism from $(P(A), +_A)$ to $(P(A'), +_{A'})$.

   (c) Let $F = \{B \in P(A) : B \text{ is finite or } A \backslash B \text{ is finite}\}$. Show that F is a subgroup of $(P(A), +_A)$.

2. Let G be a group, H_1, H_2 be two subgroups.

   (a) Show that $H_1 \cap H_2 \leq G$.

   (b) Show that $H_1 \cup H_2 \leq G$ iff $H_1 \leq H_2$ or $H_2 \leq H_1$.

   (c) Let G be the group of integers and the group operation is addition. Write down two subgroups whose union is no longer a subgroup.

3. Show that the set of $n \times n$ matrices with integer entries and determinant 1 form a group under matrix multiplication. (These groups are denoted as $SL(n, \mathbb{Z})$.

4. Let G be a group, show that G has only the identity element iff for any group H, $Hom(H, G)$ has exactly one element.

5. Show that for any group G, any $g \in G$, there is a unique group homomorphism from $(\mathbb{Z}, +)$ to G, sending 1 to g.

6. Let M be a set, $* : M \times M \to M$ be a function, such that for any $a, b, c \in M$, $*(a, *(b, c)) = *(*(a, b), c)$, $*(a, b) = *(b, a)$, and there is an element $e \in M$ such that for any $a \in M$, $*(e, a) = *(a, e) = a$. Let $\cdot : (M \times M) \times (M \times M) \to M \times M$ be $((a, b), (c, d)) \mapsto (*(a, c), *(b, d))$, $\sim$ a relation on $M \times M$ defined as $\sim = \{((a, b), (c, d)) \in (M \times M) \times (M \times M) :$ there exists $k \in M, *(*(a, d), k) = *(*(b, c), k)\}$

   (a) Show that $\sim$ is an equivalence relation.

   (b) Let $G = (M \times M)/\sim$. Show that $([a], [b]) \mapsto [\cdot(a, b)]$ is a function from $G \times G$ to G. Denote it as $\cdot'$.

   (c) Show that $(G, \cdot')$ is an abelian group. This is called the Grothendieck group of $(M, *)$.

   (d) Show that there is a bijective homomorphism from the Grothendieck group of $(\mathbb{Z}\backslash\{0\}, \times)$ to the group $(\mathbb{Q}\backslash\{0\}, \times)$.

Answer:

1. (a) $+_A$ is clearly well defined, and from definition one can see that $B +_A C = C +_A B$ for any $B, C \in P(A)$.

      i. Associativity: if $B, C, D \in P(A)$, $a \in A$ lies in $B +_A C$ iff a is in B or C but not both, hence a is in $(B +_A C) +_A D$ iff a is in B but not C or D, C but not B or D, D but not B or C, or in all three sets B, C and D. Similarly $a \in B +_A (C +_A D)$ can be shown to have the same meaning, hence $(B +_A C) +_A D = B +_A (C +_A D)$.

      ii. Identity element is $\emptyset$, because $(\emptyset \cup B)\backslash(\emptyset \cap B) = B\backslash\emptyset = B$.

      iii. The inverse of $B \in P(A)$ is the element B itself.

   These show that $(P(A), +_A)$ is an abelian group.

   (b) Denote this map as r, then for every $B, C \in P(A)$, $r(B) +'_A r(C) = ((B \cap A') \cup (C \cap A'))\backslash((B \cap A') \cap (C \cap A')) = ((B \cup C\backslash(B \cap C)) \cap A' = r(B +_A C)$.

   (c) Clearly $\emptyset \in F$. If $B \in F$, because $-B = B$, $-B \in F$, hence F is closed under inverse. To show that F is closed under group operation, suppose $B, C \in F$. Then there are three cases:

i. Both B and C are finite, then $B +_A C \subseteq B \cup C$ is finite hence in F.

ii. Both $A\backslash B$ and $\backslash C$ are finite, then $B +_A C = (B +_A (A +_A A)) +_A (C +_A (A +_A A)) = ((B +_A A) +_A A) +_A ((C +_A A) +_A A) = (A\backslash B) +_A (A\backslash C) \subseteq (A\backslash B) \cup (A\backslash C)$ is finite, hence in F.

iii. B or C is finite, and the complement of the other is finite as well. Suppose B and $A\backslash C$ are both finite, then $A\backslash(B +_A C) = A +_A (B +_A C) = B +_A (A +_A C) = B +_A (A\backslash C) \subseteq B \cup (A\backslash C)$ is finite, hence $B +_A C \in F$.

2. (a) Let i be the inclusion map from H_1 to G, then $H_1 \cap H_2 = i^{-1}(H_2)$, hence $H_1 \cap H_2 \leq H_1$. Because the group operation on H_1 is the restriction of the group operation on G, $H_1 \cap H_2$ is non-empty and closed under this group operation and inverse, hence is a subgroup of G.

   (b) If $H_1 \leq H_2$ or $H_2 \leq H_1$, $H_1 \cup H_2 = H_2$ or H_1, hence is a subgroup of G. On the other hand, if neither $H_1 \leq H_2$ nor $H_2 \leq H_1$, there are $a \in H_1\backslash H_2$ and $b \in H_2\backslash H_1$. Suppose $H_1 \cup H_2 \leq G$, then $ab \in H_1 \cup H_2$. If $ab \in H_1$, then $b = a^{-1}(ab) \in H_1$, a contradiction. If $ab \in H_2$, then $a = (ab)b^{-1} \in H_2$, also a contradiction.

   (c) By (b) above, we can pick for example $\langle 2\rangle$ and $\langle 3\rangle$.

3. (a) The product of two integer matrices has integer entries, and the determinant equals the product of their determinant, hence matrix multiplication is a well defined function from $SL(n,\mathbb{Z}) \times SL(n,\mathbb{Z})$ to $SL(n,\mathbb{Z})$.

   (b) Associativity follows from the associativity of matrix multiplications.

   (c) The identity element is the identity matrix $I_n \in SL(n,\mathbb{Z})$.

   (d) By Cramer's rule, the inverse of a matrix is $\frac{1}{det}$ times the matrix of cofactors. If $A \in SL(n,\mathbb{Z})$, $\frac{1}{\det(A)} = 1$, and the matrix of cofactors is an integer matrix, hence A^{-1} is an integer matrix. $det(A^{-1}) = 1/det(A) = 1$, hence $A^{-1} \in SL(n,\mathbb{Z})$.

4. If G has only the identity, the only map from H to G must be the constant map sending everything to the identity, which is a group homomorphism. If G has more elements than the identity, $Hom(G,G)$ has at least two elements, one being the identity map $g \mapsto g$, one being the constant map $g \mapsto e$.

5. It is easy to check that the map $f(n) = \begin{cases} g^n & n > 0 \\ e & n = 0 \\ (g^{-n})^{-1} & n < 0 \end{cases}$ is such a group homomorphism. To show that it is unique, if f' is a homomorphism sending 1 to g, then if $n > 0$, $f'(n) = f'(1+1+\cdots+1) = f'(1)f'(1)\ldots f'(1) =$

$f'(1)^n = g^n$, and if $n < 0$ then $f'(-(-n)) = f'(-n)^{-1} = (g^{-n})^{-1}$, hence $f' = f$.

6. For convenience we write $*(a, b)$ as ab

   (a) i. If $(a, b) \in M \times M$, $ab = ab$, hence $(a, b) \sim (a, b)$.

   ii. If $(a, b), (c, d) \in M \times M$, $(a, b) \sim (c, d)$, then $adk = bck$, which implies $cbk = dak$, hence $(c, d) \sim (a, b)$.

   iii. If $(a, b), (c, d), (s, t) \in M \times M$, $(a, b) \sim (c, d)$, $(c, d) \sim (s, t)$, then $adk = bck$, $ctk' = dsk'$, hence $adkctk = bckdsk'$ which implies that $at(cdkk') = bs(cdkk')$, which shows that $(a, b) \sim (s, t)$.

   (b) To show this is well defined, we only need to show the value doesn't depend on the exact choice of the representative. In other words, suppose $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$, we need to show that $(ac, bd) \sim (a'c', b'd')$. $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$ implies that $ab'k = ba'k$, $cd'k' = dc'k'$, hence $(acb'd'kk' = bda'c'kk'$ which finishes the proof.

   (c) Associativity and commutativity follows from the associativity and commutativity of M, $[(a, a)]$ is the identity element, and $[(a, b)] = [(b, a)]$.

   (d) The homomorphism can be defined as $[(p, q)] = p/q$.

   i. To show that it is well defined, if $(p, q) \sim (p', q')$, then $pq'k = qp'k$, hence $p/q = p'/q'$.

   ii. To show that it is an injection, $p/q = p'/q'$ implies $pq' = qp'$ which implies $(p, q) \sim (p', q')$.

   iii. To show that it is a surjection, every $p/q \in \mathbb{Q}\backslash\{0\}$ is the image of $[(p, q)]$.

A.3 HW3

1. Recall that by S_n we mean the permutation group of $\{1, 2, \ldots, n\}$.

   (a) Find all the automorphisms of S_2.

   (b) Find all the automorphisms of S_3.

   Hint: If $f : G \to G$ is a group isomorphism, $g \in G$, then $g^n = e$ iff $f(g)^n = e$, because $f(g)^n = f(g^n)$ and f is a bijection that sends the identity e to itself.

2. Let G be a group, $f : G \to G$ a function, and $\sim$ an equivalence relation on G. Let $G \times G$ be the direct product of G with itself, i. e. with group operation defined as $((a, b), (c, d)) \mapsto (ac, bd)$

   (a) Show that $G_f = \{(g, f(g)) : g \in G\}$ is a subgroup of $G \times G$ iff f is a group homomorphism.

(b) Show that $G_\sim = \{(a,b) \in G \times G : a \sim b\}$ is a subgroup of $G \times G$ iff there is a normal subgroup H of G, such that $\sim = \{(a,b) \in G \times G : b^{-1}a \in H\}$.

3. Let G be a group, S a subset of G. For every $g \in G$, define S^g as $S^g = \{gsg^{-1} : s \in S\}$. Suppose for every $g \in G$, $S^g \subseteq S$, show that for every $g \in G$, $S^g = S$.

4. Let G be a group, S a subset of G. Let H_S be a subset of G consisting of identity e together with all elements of the form $s_1 s_2 \dots s_n$, where each s_j is either in S or its inverse is in S. Show that H_S is a subgroup of G, and any subgroup of G containing all elements in S must have H_S as a subgroup, i. e. $H_S = \langle S \rangle$

5. Recall that if group G satisfies $G = \langle S \rangle$, we say S is a generating set of G. Let $n > 2$ be an integer.

   (a) Let S be a finite subset of $(\mathbb{Q}, +)$, show that $\langle S \rangle \neq \mathbb{Q}$.

   (b) Show that S_n, which is the group of bijections from $\{1, \dots, n\}$ to itself, with group operation being the composition, has a generating set with no more than $n-1$ elements.

   (c) Write down a generating set of S_n with only two elements.

Answer:

1. (a) S_2 has only 2 elements and any group homomorphism sends identity to identity, hence if it is also bijective it has to be id_{S_2}.

   (b) Let the 6 elements of S_3 be $\sigma_0 = id_{\{1,2,3\}}$, $\sigma_1 = \{(1,2),(2,1),(3,3)\}$, $\sigma_2 = \{(1,3),(3,1),(2,2)\}$, $\sigma_3 = \{(2,3),(3,2),(1,1)\}$, $\sigma_4 = \{(1,2),(2,3),(3,1)\}$, $\sigma_5 = \{(1,3),(3,2),(2,1)\}$. Then by the hint, any automorphism must permute the three elements σ_1, σ_2 and σ_3. On the other hand, $\sigma_4 = \sigma_2\sigma_1$, $\sigma_5 = \sigma_3\sigma_1$, so an automorphism is determined by its value on σ_1, σ_2 and σ_3. The six inner automorphisms $x \mapsto gxg^{-1}$ where $g \in S_3$ provides all the possible permutations of $\{\sigma_1, \sigma_2, \sigma_3\}$, hence they are all the automorphisms of S_3.

2. (a) Assume $G_f \leq G \times G$. For any $a, b \in G$, $(a, f(a)), (b, f(b)) \in G_f$, hence their product, $(ab, f(a)f(b)) \in G_f$, which implies that $f(a)f(b) = f(ab)$, i.e. $f \in Hom(G,G)$.

   If $f \in Hom(G,G)$, then $f(e) = e$, hence $(e,e) = (e, f(e)) \in G_f$. Let $(a, f(a)), (b, f(b))$ be any two elements of G_f, then their product in $G \times G$, $(ab, f(a)f(b)) = (ab, f(ab)) \in G_f$, and $(a, f(a))^{-1} = (a^{-1}, f(a)^{-1}) = (a^{-1}, f(a^{-1})) \in G_f$. So $G_f \leq G \times G$.

   (b) Assume $G_\sim \leq G_\sim$. Let $H = [e]$, we first show that H is a normal subgroup of G:

      i. $e \sim e$ hence $e \in H$.

ii. If $a, b \in H$, $(a, e), (b, e) \in G_\sim$, hence $(ab, e) \in G_\sim$, which implies that $ab \in H$.

iii. If $a \in H$, $(a, e) \in G_\sim$, hence $(a, e)^{-1} = (a^{-1}, e) \in G_\sim$, which implies that $a^{-1} \in H$.

iv. If $a \in H$, $g \in G$, then $(a, e), (g, g), (g^{-1}, g^{-1}) \in G_\sim$, hence $(g, g)(a, e)(g^{-1}, g^{-1}) = (gag^{-1}, e) \in G_\sim$, which implies that $gHg^{-1} \subseteq H$. Now apply the conclusion of Problem 3.

Now $(a, b) \in \sim$ iff $(a, b) \in G_\sim$ iff $(b^{-1}, b^{-1})(a, b) \in G_\sim$ iff $b^{-1}a \in H$.

In the other direction, if H is a normal subgroup of G, one can easily verify (see lecture notes) that $\sim = \{(a, b) : b^{-1}a \in H\}$ is an equivalence relation. If $(a, b), (c, d) \in G_\sim$, then $b^{-1}a \in H$, $d^{-1}c \in H$, hence $(bd)^{-1}(ac) = d^{-1}(b^{-1}a)d(d^{-1}c) \in H$, which implies that $G_\sim$ is a subgroup.

3. By assumption, for every $s \in S$, $g^{-1}s(g^{-1})^{-1} = g^{-1}sg \in S$, hence $s = g(g^{-1}sg)g^{-1} \in S^g$, which implies that $S = S^g$.

4. By construction, H_S contains identity, and is closed under multiplication as well as inverse ($(s_1 \dots s_n)^{-1} = s_n^{-1} \dots s_1^{-1}$), hence is a subgroup of G that contains S. Any subgroup of G containing S must also contain the elements of S, their inverses and their finite products, hence it is the smallest such subgroup, $H_S = \langle S \rangle$.

5. (a) Let $S = \{p_1/q_1, \dots, p_n/q_n\}$ where $p_i, q_i \in \mathbb{Z}$, then $1/2 \prod_n q_n \notin \langle S \rangle$ because $\langle S \rangle$ consists of finite sums or differences of p_i/q_i by Problem 4, which can always be written as $p/lcm(q_1, \dots, q_n)$.

   (b) Let σ_i be the element in S_n which switches i and $i+1$ and keeps the other numbers the same. We will now show that $S_n = \langle \sigma_1, \dots, \sigma_{n-1} \rangle$. Given $g \in S_n$, let $k(g)$ be the largest natural number such that $g(i) = i$ for all $i > k(g)$. We shall use induction to show that all g such that $k(g) \leq n$ lies in $\langle \sigma_1, \dots, \sigma_{n-1} \rangle$

   i. If $k(g) = 0$, $g = e \in \langle \sigma_1, \dots, \sigma_{n-1} \rangle$

   ii. Suppose all g' with $k(g') < k$ are in $\langle \sigma_1, \dots, \sigma_{n-1} \rangle$. Let $g \in S_n$, $k(g) = k+1$, then $g(k+1) < k+1$, $(\sigma_k \sigma_{k-1} \dots \sigma_{g(k+1)} g)(k+1) = k+1$, hence $\sigma_k \sigma_{k-1} \dots \sigma_{g(k+1)} g \in \langle \sigma_1, \dots, \sigma_{n-1} \rangle$ by inductive hypothesis, which implies that $g \in \langle \sigma_1, \dots, \sigma_{n-1} \rangle$.

   (You may recognize that what I wrote here is basically Selection Sort. You can prove this via other sorting algorithms as well.)

   (c) One element can be σ_1, and the other element can be chosen as the one sending 1 to 2, 2 to 3, etc, n to 1, which we denote as τ. By Part (b) above, any element in S_n can be written as a finite product of the σ_is, and $\sigma_i = \tau^{i-1}\sigma_1\tau^{1-i}$.

A.4 HW4

1. Let $\langle 12\rangle$ be the subgroup of $(\mathbb{Z}, +)$ consisting of all integers divisible by 12. Let G be the quotient group $\mathbb{Z}/\langle 12\rangle$. Find all the normal subgroups of G and count the number of elements of the corresponding quotient groups.

2. Let G be a group, N a normal subgroup, $p : G \to G/N$ a quotient map. Let S be the set of subgroups of G that contains N, S' be the set of subgroups of G/N.

   (a) Show that the map $F : S \to S'$ defined by $F(H) = p(H)$ is a bijection. (Hint: show that the map $H' \mapsto p^{-1}(H')$ is its inverse)

   (b) Show that $H \in S$ is a normal subgroup of G iff $p(H)$ is a normal subgroup of G/N.

   (c) If $H \in S$ and $H \trianglelefteq G$, show that there is an isomorphism from G/H to $(G/N)/p(H)$ defined as $aH \mapsto (aN)p(H)$ (Need to first show that it is well defined.)

   (This is usually called the Third Isomorphism Theorem.)

3. Let G be a group, $H \leq G$ a subgroup. Show that H is a normal subgroup of G if and only if the sets $\{gh : h \in H\}$ and $\{hg : h \in H\}$ are equal for all $g \in G$. (The set $\{hg : h \in H\}$ is often denoted as Hg and called a "right coset".)

4. Let G be a group, N a normal subgroup, H a subgroup.

   (a) Show that the set $NH = \{nh : n \in N, h \in H\}$ is a subgroup of G.

   (b) Show that N is a normal subgroup of NH.

   (c) Show that $N \cap H$ is a normal subgroup of H.

   (d) Show that the map $f : (NH)/N \to H/(N \cap H)$ defined as $(nh)N \mapsto h(N \cap H)$ is a group isomorphism. (Need to first show that it is well defined.)

   (This is called the Second Isomorphism Theorem.)

Answer:

1. Because the group itself is abelian all subgroups are normal subgroups. To find the possible normal subgroups, start with $\{0 + \langle 12\rangle$, add elements to it till it becomes G itself, and list all the groups one obtained via this process. Below are all the possibilities and the corresponding cardinality of the quotient groups:

$\{0 + \langle 12\rangle\}$	12
G	1
$\langle 2 + \langle 12\rangle\rangle$	2
$\langle 3 + \langle 12\rangle\rangle$	3
$\langle 4 + \langle 12\rangle\rangle$	4
$\langle 6 + \langle 12\rangle\rangle$	6

2. (a) Let $F' : S' \to S$ be $F'(H') = p^{-1}(H')$. $F'(H') = p^{-1}(H') \supseteq p^{-1}(\{e_{G'}\}) = N$ so it is well defined. We will now show that F and F' are inverses of one another.

   i. For every $H \in S$, $F'(F(H)) = \{g \in G : p(g) = p(g') \text{ for some } g' \in H\} = \{g \in G : g = g'n \text{ for some } n \in H, g' \in H\}$. Because $N \leq H$, this set is just H.

   ii. For every $H' \in S'$, $F(F'(H')) = \{p(g) : p(g) \in H'\} = H' \cap p(G) = H'$.

   (b) If $H \in S$ is normal, then for every $g \in G$, $H = gHg^{-1}$. Apply p to elements on both sides, we get $p(H) = p(g)H(p(g))^{-1}$. Because p is a surjection, $p(H)$ is normal. On the other hand, if $H \in S$ is not normal, there is some $g \in G$ such that $gHg^{-1} \neq H$. However $N = gNg^{-1} \leq gHg^{-1}$, hence $gHg^{-1} \in S$. Now apply p to both the elements of H and of gHg^{-1}, from (a) we know that the resulting subgroups under p are also different, hence $p(H)$ is not normal in G/N.

   (c) Denote this map as ϕ.

   i. To show ϕ is well defined, if $aH = a'H$, then $a' = ah$ for some $h \in H$, hence $a'N = (aN)(hN)$. Because $hN \in p(H)$, we have $(a'N)p(H) = (aN)p(H)$.

   ii. To show that it is a group homomorphism, let $aH, bH \in G/H$, $\phi(aH)\phi(bH) = ((aN)p(H))((bN)p(H)) = ((aN)(bN))p(H) = ((ab)N)p(H) = \phi((ab)H) = \phi((aH)(bH))$.

   iii. ϕ is a surjection because every element of $(G/N)/p(H)$ can be written as $(aN)p(H)$ for some $a \in G$, hence equals $\phi(aH)$.

   iv. Now we show ϕ is an injection, which we can do by showing that the kernel is trivial. If $\phi(aH) = (eN)p(H)$, $aN \in (eN)p(H) = p(H)$, in other words $p(a) \in p(H)$. However by (a) above, $p^{-1}(p(H)) = H$, hence $a \in H$, $aH = eH$.

3. If H is normal, then any element of the form gh where $h \in H$ can be written as $(ghg^{-1})g$, so $gH \subseteq Hg$; any element of the form hg where $h \in H$ can be written as $g(g^{-1})h(g^{-1})^{-1}$ which is in gH, so $Hg \subseteq gH$. If H is not normal, by HW3 Problem 3 there is some $g \in G$, $h \in H$ such that $ghg^{-1} \notin H$, hence $gh \in gH$ but $gh \notin Hg$.

4. (a) $e = ee \in NH$. For any $nh, n'h' \in NH$, $(nh)(n'h') = (n(hn'h^{-1}))(hh') \in NH$, $(nh)^{-1} = (h^{-1}n^{-1}h)h^{-1}$.

   (b) It is easy to see that N is a subgroup of NH. N being normal in G implies that $gNg^{-1} = N$ for all $g \in G$. Because $NH \leq G$, $gNg^{-1} = N$ for all $g \in NH$, which implies that N is a normal subgroup of NH.

   (c) For any $g \in H$, $n \in H \cap N$, $gng^{-1} \in H$ because $H \leq G$, $gng^{-1} \in N$ because N is normal, hence $gng^{-1} \in H \cap N$. Now apply HW3 Problem 3.

(d) i. First we show that it is well defined. If $(nh)N = (n'h')N$, there is some $n'' \in N$ such that $n'h' = nhn''$, hence $h' = h(h^{-1}(n'^{-1}n)h)n''$. Here $(h^{-1}(n'^{-1}n)h)n''$ is in N because N is normal, and it is in H because it equals $h^{-1}h'$.

ii. Next we show that it is a group homomorphism. For $(nh)N, (n'h')N \in NH/N$, $f(((nh)N)((n'h')N)) = f((nhn'h')N) = f(((n(hn'h^{-1}))(hh'))N) = (hh')(N \cap H) = (h(N \cap H))(h'(N \cap H)) = f((nh)N)f((n'h')N)$

iii. Surjectivity is because $h(N \cap H) = f(hN)$.

iv. To show injectivity, we only need to show the kernel is trivial. If $nh \in NH$, $n \in N$, $h \in H$ is sent to identity by f, then $h \in H \cap N$, hence $nh \in N$, $(nh)N = eN$.

A.5 HW5

1. Show that the map $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined as $(t, x) \mapsto xe^t$ is a left $(\mathbb{R}, +)$ action on $\mathbb{R}$. Write down the corresponding permutation representation. Is the action effective? Is the action transitive? Is the action free?

2. Let G be a group, X and Y be two left G sets.

   (a) Show that $\cdot : G \times (X \times Y) \to X \times Y$ defined as $(g, (x, y)) = (gx, gy)$ is a left G action on $X \times Y$.

   (b) If $f : X \to Y$ is a map, show that f is G equivariant if and only if $\{(x, f(x)) : x \in X\}$ is a G invariant subset of the left G set $(X \times Y, \cdot)$.

3. Let G be a group with more than one elements, X be a non empty left G set. Show that $\cdot : G \times P(X) \to P(X)$ defined as $(g, A) \mapsto \{ga : a \in A\}$ is a left G action on $P(A)$. Can this action be free? Can this action be transitive?

4. Any non empty set X is a left S_X set via the action $\cdot : S_X \times X \to X$, $(\sigma, x) \mapsto \sigma(x)$. Show that if X has 3 or more elements then the only S_X equivariant map from X to X is the identity.

5. Write down a group G, two left G sets X and Y, such that there are no G equivariant map from X to Y.

Answer:

1. $t \mapsto (x \mapsto xe^t)$. The kernel is $\{0\}$ so it is effective. The stablizer of 0 is $\mathbb{R}$ so it is not free. There are no real number t such that $e^t \times 1 = 0$ so it is not transitive.

2. (a) $e \cdot (x, y) = (ex, ey) = (x, y)$, $a \cdot (b \cdot (x, y)) = a \cdot (bx, by) = (abx, aby) = (ab) \cdot (x, y)$.

(b) If f is G-equivariant, for any $(x, f(x))$, $g \cdot (x, f(x)) = (gx, gf(x)) = (gx, f(gx))$, so the set $\{(x, f(x) : x \in X\}$ is G-invariant. If the set $\{(x, f(x)) : x \in X\}$ is G invariant, for any $g \in G$, $x \in X$, $g \cdot (x, f(x)) = (gx, gf(x)) \in \{(x, f(x)) : x \in X\}$, hence $gf(x) = f(gx)$, which implies that f is G equivariant.

3. $e \cdot A = \{ea : a \in A\} = A$. $g \cdot (h \cdot A) = g \cdot \{ha : a \in A\} = \{gha : a \in A\} = (gh) \cdot A$. The action is neither free nor transitive, because the stablizer of $X \in P(X)$ is G, and no $g \in G$ has $g \cdot \emptyset = X$.

4. If there is such a S_X equivariant map f, let $x \in X$, we must have $(S_X)_x \subseteq (S_X)_{f(x)}$. We will now show that $f(x) = x$. Suppose not, let $a \in X$ be an element which is neither x nor $f(x)$, let $g \in S_X$ be the element that switches $f(x)$ and a while fixing every other element, then $g \in (S_X)_x \backslash (S_X)_{f(x)}$, a contradiction.

5. Let G be a group with more than one elements, X be a set with a single element x and the group action is trivial, Y be G with left action. Then if f is such an equivariant map, let $g \neq e$, then $f(x) = f(gx) = gf(x) \neq f(x)$, a contradiction.

A.6 HW7

1. Find the elements of the automorphism group of $\mathbb{Z}/\langle p \rangle$, where p is a prime number.

2. Let G be a group, N a normal subgroup, $p : G \to G/N$ the quotient map and $s : G/N \to G$ a group homomorphism such that $p \circ s = id_{G/N}$. Let H be the image of s, the permutation representation $\psi : H \to Aut(N)$ defined as $(\psi(h))(n) = hnh^{-1}$.

   (a) Show that if ψ sends every element to identity then H is a normal subgroup of G (which, from the lecture, implies that $G \cong N \times H$).

   (b) Let $Inn(N)$ be a subset of $Aut(N)$ consisiting of elements of the form $x \mapsto nxn^{-1}$ for $n \in N$. Show that $Inn(N) \trianglelefteq Aut(N)$.

   (c) Show that there is an $s' \in Hom(G/N, G)$ such that $p \circ s' = id_{G/N}$ and the image of s' is a normal subgroup of G.

   (d) Show that all groups of 15 elements are abelian.

3. Show that the set of rational numbers of the form $2^n a$ where $n \in \mathbb{Z}$, $a \in \mathbb{Z}$, is a subring of $(\mathbb{Q}, +, \times)$.

4. Let K be a field. Show that the map $r \mapsto (x \mapsto r \times x)$ is an injective homomorphism from the group $(K \backslash \{0\}, \times)$ to the automorphism group of abelian group $(K, +)$.

Answers

1. An automorphism must send $1 + \langle p \rangle$ to some $a + \langle p \rangle \in \mathbb{Z}/\langle p \rangle$, hence it must send $n + \langle p \rangle$ to $na + \langle p \rangle$. It is easy to see that this is a bijection iff $a \notin \langle p \rangle$.

2. (a) For any $h \in H$, any $g \in G$, $s(p(g))^{-1}g \in N$, hence $s(p(g))^{-1}g = h^{-1}s(p(g))^{-1}gh$, so $ghg^{-1} \in H$.

   (b) i. Let $c_n(x) = nxn^{-1}$, then $c_n(ab) = nabn^{-1} = nan^{-1}nbn^{-1} = c_n(a)c_n(b)$, so $Inn(N)$ is a subset of $Aut(N)$.

   ii. $c_e = id_N$, so $Inn(N)$ contains the identity element.

   iii. $c_a \circ c_b = c_{ab}$, $(c_a)^{-1} = c_{a^{-1}}$, so $Inn(N) \leq Aut(N)$.

   iv. For any $f \in Aut(N)$, $c_a \in Inn(N)$, $fc_af^{-1}(x) = f(af^{-1}(x)a^{-1}) = f(a)xf(a)^{-1} = c_{f(a)} \in Inn(N)$, so it is a normal subgroup.

   (c) Sorry, I missed a condition here, we need to have a homomorphism $\psi' : H \to N$ such that $\psi(h) = c_{\psi'(h)}$.

   (d) This follows from (a) and the fact that the only map from $\mathbb{Z}/3$ to $Aut(\mathbb{Z}/5) \cong \mathbb{Z}/4$ is the one sending everything to identity.

3. $2^0 0 = 0$, $-(2^n a) = 2^n(-a)$, $2^n a + 2^m b = 2^{\min(m,n)}(2^{n-\min(m,n)}a + 2^{m-\min(m,n)}b)$.

4. Let m_r be $x \mapsto rx$.

   (a) Firstly we show that it is well defined:

   $$m_r(a + b) = r(a + b) = ra + rb = m_r(a) + m_r(b)$$

   $$m_r \circ m_{r^{-1}} = m_{r^{-1}} \circ m_r = id_K$$

   (b) Now show that it is an injection: if $r \neq r'$, $m_r(1) = r \neq r' = m_{r'}(1)$.

   (c) Now show that this is a group homomorphism: $m_{rr'}(x) = rr'x = r(r'x) = m_r(m_{r'}(x))$, so $m_{rr'} = m_r \circ m_{r'}$.

A.7 HW8

1. (a) Show that the set of real valued continuous functions on $\mathbb{R}$, denoted as $C(\mathbb{R})$, with the usual function addition and multiplication, forms a commutative ring. Does this ring has multiplicative identity? Is it an integral domain?

   (b) Show that the map $f : C(\mathbb{R}) \to \mathbb{R}$ defined as $f(a) = a(1)$ is a ring homomorphism.

2. Let R be an integral domain. Let $Q = (R \times (R\backslash\{0\}))/\sim$, where $(a, b) \sim (c, d)$ iff $ad = bc$, and define $+ : Q \times Q \to Q$ as $([(a, b)], [(c, d)]) \mapsto [(ad + bc, bd)]$, $\times : Q \times Q \to Q$ as $([(a, b)], [(c, d)]) \mapsto [(ac, bd)]$.

   (a) Show that $\sim$ is an equivalence relation.

(b) Show that the maps + and $\times$ are both well defined.

(c) Show that $i : R \to Q$ defined as $i(r) = [(r, 1)]$ is an injective ring homomorphism, and that it is a bijection if and only if R is a field.

3. Show that if ring R is an integral domain, so is the ring of polynomials $R[t]$.

4. Let A be an abelian group, which we see as an $End(A)$ module by $f \cdot a = f(a)$.

   (a) Show that there is a ring homomorphism $i : \mathbb{Z} \to End(A)$, such that $i(1) = id_A$.

   (b) View A as a $\mathbb{Z}$ module via the ring homomorphism i above. Show that $Hom_{\mathbb{Z}}(A, A)$ consists of all group homomorphisms from A to itself.

   (c) Write down an A with finitely many elements such that $Hom_{End(A)}(A, A)$ has fewer elements than $Hom_{\mathbb{Z}}(A, A)$.

Answer:

1. (a) One can show that this is a subring of commutative ring $\prod_{\alpha\in\mathbb{R}} \mathbb{R}$. The fact that it is a subring is because constant 0 function is continuous, and continuity of functions is preserved under addition, negation and multiplication. The multiplicative identity element is the constant function $x \mapsto 1$. The ring is not an integral domain, because $\max(0, x)$ and $\max(0, -x)$ both belongs to it and their product is 0.

   (b) $f(a + b) = (a + b)(1) = a(1) + b(1) = f(a) + f(b)$, $f(ab) = (ab)(1) = a(1)b(1) = f(a)f(b)$

2. (a)
   - $ab = ab$ hence $(a, b) \sim (a, b)$.
   - $(a, b) \sim (c, d) \implies ad = bc \implies cb = da \implies (c, d) \sim (a, b)$.
   - $(a, b) \sim (c, d), (c, d) \sim (f, g) \implies ad = bc, cg = df \implies adcg = bcdf \implies ag = bf \implies (a, b) \sim (f, g)$.

   (b) If $(a, b) \sim (a', b')$, $(c, d) \sim (c', d')$, then $ab' = a'b$, $cd' = c'd$, hence $(ad + bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd$, so +is well defined; $acb'd' = a'c'bd$, so $\times$ is well defined.

   (c) One can further check that Q is a ring. $i(r + r') = [(r + r', 1)] = [(r, 1)] + [(r', 1)] = i(r) + i(r')$, $i(rr') = [(rr', 1)] = [(r, 1)][(r', 1)] = i(r)i(r')$, $\ker(i) = \{r \in R : (r, 1) \sim (0, 1)\} = \{0\}$. i is a surjection iff for any $b \neq 0$, there is some $r \in R$ such that $(r, 1) \sim (a, b)$, which means $a = br$. This is equivalent to $(R\backslash\{0\}, \times)$ being a field.

3. It is easy to see that $R[t]$ is commutative with multiplicative identity 1. If $f, g \in R[t]$ are both non zero, their leading coefficient, i.e. coefficient of the term with the highest degree, are both non-zero. So the leading coefficent of fg is the product of the leading coefficient of f and the leading coefficient of g, which because R is an integral domain, must be non-zero. Hence $R[t]$ is an integral domain.

4. (a) Let $i(0)$ be $a \mapsto 0$. When $n > 0$, let $i(n)$ be the map sending $a \in A$ to the sum of n copies of a, $i(-n)$ be $a \mapsto -((i(n))(a))$. Then one can verify that i is well defined and is a ring homomorphism.

   (b) Let f be a group homomorphism from A to itself. Then for any positive integer n, $f(na) = f(a+\cdots+a) = f(a)+\cdots+f(a) = nf(a)$. When $n = 0$ or $n < 0$ it is analogous, hence $f \in Hom_{\mathbb{Z}}(A, A)$.

   (c) Let $A = \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. Then the map $\sigma : (a, b) \mapsto (b, 0)$ is a group homomorphism hence an element of $Hom_{\mathbb{Z}}(A, A)$, but $\tau : (a, b) \mapsto (0, b) \in End(A)$ and $\sigma(\tau(a, b)) = (b, 0)$, $\tau(\sigma((a, b))) = \tau(b, 0) = (0, 0)$, so $\sigma \notin Hom_{End(A)}(A)$.

A.8 HW9

1. Let $\mathbb{Z}$ be the rings of integers, $(6) = \{6n : n \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Let R be the quotient ring $\mathbb{Z}/(6)$. Write down all the subrings of R. Which of them are ideals of R?

2. Let R be a commutative ring with identity. An element $p \in R$ is called a **prime element**, if

   (a) There are no $q \in R$ such that $pq = 1$.

   (b) For any $a, b, c \in R$ such that $ap = bc$, either there is $m \in R$ such that $b = mp$, or there is $n \in R$ such that $c = np$.

   Show that

   (a) If $a \in R$, the set $(a) = \{ra : r \in R\}$ is an ideal of R.

   (b) If $p \in R$ is a prime element then (p) is a prime ideal of R.

3. Let R be the ring of 2×2 real matrices, with multiplication being matrix multiplication.

   (a) Write down a subring S which is not an ideal.

   (b) Write down all ideals of R.

4. Let R be a ring with multiplicative identity 1. An element $u \in R$ is called a **unit**, if there is $v \in R$ such that $uv = vu = 1$. Show that the set of units of a ring R form a group under ring multiplication. We call it the **group of units** of R.

5. Let R and S be two rings. $R \times S$ is their direct product, which is a ring with addition and multiplication defined as $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \times (c, d) = (ac, bd)$.

   (a) Show that $I = \{(a, 0) : a \in R\}$ is an ideal of $R \times S$, and the quotient ring $(R \times S)/I$ is isomorphic to S as a ring.

   (b) Show that if both R and S have multiplicative identity, so does $R \times S$.

(c) If both R and S have multiplicative identity, show that the group of units of $R \times S$ is isomorphic to the direct product of the group of units of R and the group of units of S.

Answer

1. A subring is a subgroup under addition, and it is easy to verify that all 4 such subgroups are closed under multiplication hence are subrings. They are $\{0+(6)\}$, $\{0+(6), 3+(6)\}$, $\{0+(6), 2+(6), 4+(6)\}$ and R itself. All are ideals of R.

2. (a) $ra + r'a = (r + r')a$, $r(ta) = (rt)a$.

   (b) R is commutative hence so is $R/(p)$. By (a), $1 + (p) \neq 0 + (p)$, and is the multiplicative identity of $R/(p)$. If $(a+(p))(b+(p)) = 0+(p)$, then $ab \in (p)$, from (b) we see that $a \in (p)$ or $b \in (p)$, so $R/(p)$ is an integral domain.

3. (a) The subset consisting of upper triangular matrices is closed under addition, negation and matrix multiplication hence is a subring. It isbnot an ideal because identity matrix is upper triangular, but identity multiply with any non upper triangular matrix isn't.

   (b) R itself and $\{0\}$ are clearly ideals of R. We will show there are no others: let I be an ideal of R, which contains a non-zero element a. Let E_{ij} be the matrix with the (i, j)-th entry 1 and all other entries 0. Suppose the (k, l)th entry of a is $c \neq 0$, then $E_{kl} = \frac{1}{c} E_{kk} a E_{ll} \in I$, and the identity matrix $I_2 = \sum_i E_{ii} = \sum_i E_{ik} E_{kkl} E_{li} \in I$, so $I = R$.

4. If $uv = vu = 1$, $u'v' = v'u' = 1$, then $(uu')(v'v) = (v'v)(uu') = 1$, so the set of units is closed under multiplication. Associativity follows from the fact that R is a ring, and $1 \times 1 = 1$ so 1 is a unit. If u is a unit and $uv = vu = 1$, then v is also a unit, and is the inverse of u under multiplication. Hence the set of units form a group under multiplication.

5. (a) I is closed under addition and negation, and $(c, d)(a, 0) = (ca, 0)$, $(a, 0)(c, d) = (ac, 0)$. The isomorphism follows from applying isomorphism theorem to ring homomorphism $(a, b) \mapsto b$.

   (b) Let 1_R and 1_S be the multiplicative identities of R and S respectively, then $(1_R, 1_S)$ is the multiplicative identity of $R \times S$.

   (c) (a, b) is a unit, iff there are $c \in R, d \in S$ such that $(a, b)(c, d) = (c, d)(a, b) = (1_R, 1_S)$, which means $ac = ca = 1_R$, $bd = db = 1_S$. Hence, the group of units of $R \times S$ as a set equals the cartesian product of the group of units of R and the group of units of S. By definition of $R \times S$, the multiplication is the group operation under direct product.

A.9 HW10

1. Let (2) be the ideal of the integer ring $\mathbb{Z}$ consisting of even numbers, R be the quotient ring $\mathbb{Z}/(2)$. Can there be any scalar multiplication $\cdot : R \times \mathbb{Z} \to \mathbb{Z}$, such that $(1+(2)) \cdot 1 = 1$, and $(\mathbb{Z}, +, \cdot)$ is an R module? Write down one or show that such scalar multiplication can not exist.

2. Let R be a ring, I and J be two ideals.

   - Show that if $I \cup J$ is an ideal then either $I \subseteq J$ or $J \subseteq I$.
   - Show that $I + J$, defined as $\{a+b : a \in I, b \in J\}$ is an ideal of R.
   - If I' is an ideal containing $I \cup J$, show that $I + J \subseteq I'$.

3. (a) Show that the quotient ring $K = \mathbb{Z}/(2)$ is a field.

   (b) In polynomial ring $K[x]$, find the greatest common divisor of x^3+1 and x^5+x.

4. Let R be a PID, p a non zero element such that (p) is a prime ideal of R. Show that $R/(p)$ is a field. (Hint: look at the gcd of p and a.)

5. Let $R = \mathbb{Z}[x]$ be the polynomial ring with integer coefficients. Show that the ideal $(x, 2) = \{xf + 2g : f, g \in R\}$ is not a principal ideal.

Answer:

1. There can not be such a module structure. Because if there is, $0 = (0 + (2)) \cdot 1 = ((1+(2)) + (1+(2))) \cdot 1 = 1 + 1 = 2$

2. (a) If $I + J$ is an ideal then it is a subgroup of $(R, +)$, hence one is contained in the other. The other direction is obvious.

   (b) For any $a, a' \in I$, $b, b' \in J$, $r \in R$, we have

      i. $0 = 0 + 0 \in I + J$

      ii. $(a+b) + (a'+b') = (a+a') + (b+b') \in I + J$

      iii. $-(a+b) = (-a) + (-b) \in I + J$

      iv. $r(a+b) = ra + rb \in I + J$

   (c) For any $a + b \in I + J$, where $a \in I$, $b \in J$, by assumption $a \in I'$, $b \in I'$, hence $a + b \in I'$.

3. (a) The only non zero element is $1 + (2)$, which forms the trivial group under multiplication.

   (b) Run Euclid's algorithm:

$$x^5 + x = x^2(x^3+1) + (x^2+x)$$

$$x^3 + 1 = (x+1)(x^2+x) + (x+1)$$

$$x^2 + x = x(x+1)$$

   So the gcd is $x + 1$.

4. We only need to show that any non zero element has multiplicative inverse. For any non-zero $a+(p) \in R/(p)$, $a \notin (p)$. Let $m = gcd(a,p)$, then there is some q such that $p = mq$, so either $m \in (p)$ or $q \in (p)$. The former case contradicts with $a \notin (p)$, so $q \in (p)$, there is some n such that $q = np$, which implies that $mn = 1$.

   Now because $m \in (a,p)$, there are s,t such that $m = sa + tp$, so $1 = nsa + ntp$, $(a+(p))(ns+(p)) = 1+(p)$.

5. Suppose this ideal is (m), then because 2 is a multiple of m, $m = \pm 1$ or ± 2. Because x is a multiple of m, $m = \pm 1$ hence $1 \in (m)$, but clearly $1 \notin (2,x)$, a contradiction.

A.10 HW11

1. Let D be an Euclidean domain. Recall that a non zero element $p \in D$ is called a **prime** if $D/(p)$ is an integral domain.

   (a) Let p,q be two non zero primes in D. Show that either p and q are coprime, or there is a unit u such that $q = up$.

   (b) If p is a non zero prime, show that $D/(p)$ is a field.

2. Let D be an integral domain. Suppose $a \in D$ such that

   (a) $D/(a)$ is a field.

   (b) Any element of D is either a unit or in the ideal (a).

   (c) $\bigcap_{n=1}^{\infty}(a^n) = \{0\}$

   Prove that D is an Euclidean domain.

3. A power series $\sum_{n=0}^{\infty} a_n x^n$, where $a_n \in \mathbb{R}$, is called **convergent** if it converges on some interval $(-\epsilon, \epsilon)$ for some $\epsilon > 0$. Let $\mathbb{R}\{x\}$ be the ring of convergent power series with real coefficients, with the usual power series addition and multiplication. Show that it is an Euclidean domain. (Hint: you can use problem 2.) Let a be the power series of $\sin(x)$, b be the power series of $e^x - 1$, find $gcd(a,b)$ in $\mathbb{R}\{x\}$.

Answer:

1. (a) Let $m = \gcd(p,q)$. Then there are $a,b \in D$ such that $p = ma$, $q = mb$. If m is a unit, then p and q are coprime. If not, then p is a prime factor of m, hence $m = up$ for some unit p, similarly $m = vq$ for some unit v, so $q = (v^{-1}u)p$.

   (b) Let $a+(p)$ be a non-zero element in $D/(p)$, we only need to show that it has multiplicative inverse. Let $m = gcd(a,p)$, then by the argument in (a), m is a unit or $m \in (p)$. The second case implies that $a \in (m) \subseteq (p)$, a contradiction. Hence $gcd(a,p) = 1$, there are $s,t \in D$ such that $sa + tp = 1$, which means that $(a+(p))(s+(p)) = (1+(p))$.

2. Define the Euclidean function v as $v(r) = \sup\{n : r \in (a^n)\}$. By (c) this is well defined, we just need to show that we have division with remainders: given $x, y \in D$, $y \neq 0$, if $x = 0$ then $x = 0y$, if $v(x) < v(y)$ then $x = 0y+x$, if $v(x) \geq v(y) = n$, then $x \in (a^n)$, there is some $q \in D$ such that $x = qa^n$. Similarly, there is some $u \in D$ such that $y = ua^n$. If $u \in (a)$ then $y \in (a^{n+1})$, a contradiction, hence by (b) u is a unit, $x = qa^n = qu^{-1}y+0$.

3. Use Problem 2, $a = x$. $gcd(\sin(x), e^x - 1) = x$.

B Honors HW

B.1 Honors HW1

1. Let S be a set. $S' = S \times \{-1, 1\}$. Let S^* be the set of finite sequences of elements of S' of the form $s_1 s_2 \dots s_n$. Here we allow $n = 0$, which corresponds to an empty sequence. Define $\sim$ as the smallest equivalence relation on S^* such that if $s_i = (s, d_i)$, $s_{i+1} = (s, -d_i)$ then $s_1 \dots s_i s_{i+1} \dots s_n \sim s_1 \dots s_{i-1} s_{i+2} \dots s_n$ (see HW1(b)). Let $F(S) = S^*/\sim$, define $* : F(S) \times F(S) \to F(S)$ as $([a], [b]) \mapsto [ab]$ where ab is the concatenation of a and b.

   (a) Show that $*$ is well defined, and $(F(S), *)$ is a group. (We call this **the free group generated by** S.)

   (b) Let G be a group, show that for every $f \in Map(S, G)$, there is a unique group homomorphism $F \in Hom(F(S), G)$, such that $F([(s, 1)]) = f(s)$ for every $s \in S$.

2. Let $\{G_i : i \in I\}$ be a family of groups, $G = \prod_{i \in I} G_i$ their direct product. For every $i \in I$, let $p_i : G \to G_i$ be $\alpha \mapsto \alpha(i)$.

   (a) Show that p_i are all group homomorphisms.

   (b) Let H be a group, for every $i \in I$, pick $f_i \in Hom(H, G_i)$. Show that there is a unique $f \in Hom(H, G)$ such that $f_i = p_i \circ f$ for all $i \in I$.

   (c) Can you find a group G', such that there are injective homomorphisms $j_i : G_i \to G'$ for all $i \in I$, and if for any group H, for every $i \in I$, one pick some arbitrary $g_i \in Hom(G_i, H)$, then there is a unique $g \in Hom(G', H)$ such that $g_i = g \circ j_i$ for all $i \in I$? (Hint: use a construction similar to Problem 1 above. This is called the **free product**.)

Answer:

1. (a) i. To show that the map is well defined, if $a \sim a'$, $b \sim b'$, then one can go from a to a' via a finite sequence of insertion or deletion of pairs of the form $(s, 1)(s, -1)$ or $(s, -1)(s, 1)$, and similarly from b to b'. Now do the corresponding insertions and deletions starting from ab, one gets $a'b'$.

   ii. Associativity is from the associativity of sequence concatenation. Identity element is equivalence class represented by the empty sequence, and the inverse of an element $[(s_1, d_1) \dots (s_n, d_n)]$ is $[(s_n, -d_n) \dots (s_1, -d_1)]$.

   (b) To show uniqueness, $F(S)$ is generated by $\{[(s, d)] : s \in S, d = \pm 1\}$. So a homomorphism from $F(S)$ to G is determined by its value on $\{[(s, d)]\}$. The homomorphism F sends $[(s, 1)]$ to $f(s)$ and $[(s, -1)]$ to $f(s)^{-1}$, so if it exists it is unique. To show existence, define $F' : S^* \to G$ as $F'((s_1, d_1)\dots(s_n, d_n)) = f(s_1)^{d_1}\dots f(s_n)^{d_n}$. For any $a \in S^*$, if a' is a with a pair $(s, d)(s, -d)$ added or deleted, $F'(a) = F'(a')$, hence F' is constant on each equivalence class of $\sim$, hence it induces a map $F : F(S) \to G$. It is a group homomorphism because $F([ab]) = F'(ab) = F'(a)F'(b) = F([a])F([b])$.

2. (a) $p_i(\alpha\beta) = (\alpha\beta)(i) = \alpha(i)\beta(i) = p_i(\alpha)p_i(\beta)$.

   (b) $f \in Hom(H, G)$ can be defined as $f(h) = (i \mapsto f_i(h))$. It is easy to see that this is a group homomorphism. If there is f' satisfying $f_i = p_i \circ f'$, then for any $h \in H$, $i \in I$, $f_i(h) = (f'(h))(i)$, hence $f' = f$.

   (c) Let Γ be the set of finite sequences of elements of the form (c, i) where $i \in I$, $c \in G_i$. Let $\sim$ be an equivalence relation on Γ, such that $a \sim a'$ if one can go from a to a' by adding or deleting (e, i), or replacing $(c, i)(c', i)$ with (cc', i). By similar argument as in Problem 1(a), this is a group under group operation $([a], [b]) \mapsto [ab]$. Now define j_i as $j_i(c) = [(c, i)]$. The group homomorphism g would be defined as $g([(c_1, i_1)(c_2, i_2)\dots(c_n, i_n)]) = g_{i_1}(c_1)g_{i_2}(c_2)\dots g_{i_n}(c_n)$. By the same argument as in Problem 1(b), this is a well defined group homomorphism, and is also the unique one such that $g_i = g \circ j_i$ for all $i \in I$.

B.2 Honors HW2

1. Find all automorphisms from $\mathbb{Z} \times \mathbb{Z}$ to itself.

2. Write down a finite abelian group whose automorphism group is non abelian.

3. Let A and G be two groups, $\psi : G \to Aut(A)$ a homomorphism, $E = A \rtimes_\psi G$. Let $p : E \to G$ be the quotient map, $i : A \to \ker(p)$ an isomorphism. Let $C^1(G, A)$ be $\{s \in Hom(G, E) : p \circ s = id_G\}$.

   (a) Show that if $s \in C^1(G, A)$, then $s' : G \to E$ defined as $s'(g) = i(a)s(g)i(a)^{-1}$ is another element in $C^1(G, A)$.

   (b) Let
   $$\begin{gathered}\sim = \{(s, s') \in C^1(G, A) \times C^1(G, A) : \\ \text{there is } a \in A, \text{ for all } g \in G, s'(g) = i(a)s(g)i(a)^{-1}\}\end{gathered}$$
   Show that $\sim$ is an equivalence relation. The **first group cohomology** $H^1(G, A)$ is defined as $C^1(G, A)/\sim$.

   (c) Show that when A is abelian, one can give a group structure on $C^1(G, A)$ and a group structure on $H^1(G, A)$, such that the quotient map from $C^1(G, A)$ to $H^1(G, A)$ is a group homomorphism.

Answer:

1. $(m,n) \mapsto (am+bn, cm+dn)$, where $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1$.

2. $\mathbb{Z}/2 \times \mathbb{Z}/2$. The two automorphisms $(a,b) \mapsto (b,a)$ and $(a,b) \mapsto (a+b,b)$ do not commute.

3. (a) $s'(gg') = i(a)s(gg')i(a)^{-1} = i(a)s(g)i(a)^{-1}i(a)s(g')i(a)^{-1} = s'(g)s'(g')$, $p(s'(g)) = p(s(g)) = g$.

   (b) $s(g) = i(e)s(g)i(e)^{-1}$. If $s'(g) = i(a)s(g)i(a)^{-1}$ then $s(g) = i(a^{-1})s'(g)i(a^{-1})^{-1}$. If $s'(g) = i(a)s(g)i(a)^{-1}$, $s''(g) = i(a')s'(g)i(a')^{-1}$, then $s''(g) = i(a'a)s(g)i(a'a)^{-1}$.

   (c) Pick $s_0 \in C^1(G,A)$. Then any $s \in C^1(G,A)$ can be written as $s(g) = s_0(g)i(\alpha(g))$, where $\alpha : G \to A$ satisfies

   $$\alpha(gg') = (\rho(g'^{-1}))(\alpha(g))\alpha(g')$$

   where $\rho : G \to Aut(A)$ is defined as $(\rho(g))(a) = i^{-1}(s_0(g)i(a)s_0(g)^{-1})$. It is easy to see that such αs form an abelian group under group operation $(\alpha\alpha')(g) = \alpha(g)\alpha'(g)$. Functions of the form

   $$g \mapsto i^{-1}(s_0(g)^{-1}i(a)s_0(g)i(a)^{-1})$$

   form a subgroup and H^1 is the quotient.

B.3 Honors HW3

Let G be a finite group, $\mathbb{C}[G]$ be the group ring. Recall that an element $a \in \mathbb{C}[G]$ is a function from G to $\mathbb{C}$. We denote it as $a = \sum_{g \in G} a_g g$ where $a_g = a(g) \in \mathbb{C}$. Let $1e \in \mathbb{C}[G]$ be the multiplicative identity of $\mathbb{C}[G]$. Let M be a $\mathbb{C}[G]$-module that satisfies $1e \cdot x = x$ for all $x \in M$.

1. Show that the ring homomorphism $i : \mathbb{C} \to \mathbb{C}[G]$ defined as $z \mapsto ze$ induces a $\mathbb{C}$-vector space structure on M.

2. For any $g \in G$, show that $x \mapsto gx$ is a bijective $\mathbb{C}$-linear map from M to M.

3. Let $(\cdot,\cdot)$ be a Hermitian form on the $\mathbb{C}$-vector space M. Show that $(\cdot,\cdot)_G$ defined as
$$(x,y)_G = \sum_{g \in G} (gx, gy)$$
is a Hermitian form on M.

4. Suppose N is a $\mathbb{C}[G]$-submodule of M. Show that the orthogonal complement of N under $(\cdot,\cdot)_G$ defined above is also a $\mathbb{C}[G]$-submodule.

5. If $M \neq 0$, and the only $\mathbb{C}[G]$-submodule of M is 0 or M itself, we call M an **irreducible module**. Let G be the group with 2 elements, find all irreducible modules over $\mathbb{C}[G]$.

Answer:

1. This is because $i(1) \times f = f$ for any $f \in \mathbb{C}[G]$.

2. Linearlity is due to distribution law and the fact that ze commutes with any element in $\mathbb{C}[G]$. The map $x \mapsto g^{-1}x$ is its inverse, so it is a bijection.

3. This is because any $\mathbb{C}$ linear map sends Hermitian forms to Hermitian forms, and sums of Hermitian forms are also Hermition.

4. Suppose $v \in N^{\perp}$, then for any $x \in N$, any $\sum_g a_g g \in \mathbb{C}[G]$, $(\sum_g a_g g \times v, x)_G = \sum_g a_g(gv, g(g^{-1}x))_G = 0$. $N^{\perp}$ closed under addition and negation is obvious, and $0 \in N^{\perp}$.

5. Let g be the non identity element in G, then $x \mapsto gx$ is a $\mathbb{C}$ linear map T_g such that $T_g^2 = id_M$. So T_g has eigenvalue 1 or -1, and the eigenspace is a submodule. Hence if M is irreducible it must be isomorphic to $\mathbb{C}$ with the action being $gx = x$ or $gx = -x$.

C Midterm Review

1. Write down all the elements of the subgroup of S_4 generated by $(1,2)(3,4)$ and $(1,3)(2,4)$, and write down all its subgroups. There is no need for justification. Is this group abelian?

2. Let $G = S_3$. Consider the map $\cdot : G \times Map(G,G) \to Map(G,G)$ defined as $(g,f) \mapsto (x \mapsto gf(g^{-1}x))$.

   (a) Show that $\cdot$ is a left G action.

   (b) In the left G-set $(Map(G,G),\cdot)$, is there a G-orbit with 3 elements? Write down one or prove that such a G-orbit does not exist.

3. Let G be a group, H a normal subgroup. Recall that for a group G, a conjugacy class is an orbit of the action $(g,x) \mapsto gxg^{-1}$.

   (a) Show that each conjugacy class of H is contained in a unique conjugacy class of G.

   (b) If G is a finite group, show that all the conjugacy classes of H that lies in the same conjugacy class of G have the same number of elements.

4. Let G be a group, consider the map $G \times Map(G,\mathbb{R}) \to Map(G,\mathbb{R})$ defined as $(g,f) \mapsto (x \mapsto f(gx))$.

   (a) Show that this map is a left G-action if and only if G is abelian.

   (b) When G is abelian, show that any subgroup H of G is the stablizer of some $f_H \in Map(G,\mathbb{R})$.

Answer:

1. The subgroup is $\{e,(1,3)(2,4),(1,2)(3,4),(1,4)(2,3)\}$. It is abelian. Its subgroups are $\{e\}$, itself, $\{e,(1,3)(2,4)\}$, $\{e,(1,2)(3,4)\}$ and $\{e,(1,4)(2,3)\}$.

2. (a) $(e\cdot f)(x)ef(e^{-1}x) = f(x)$, $(a\cdot(b\cdot f))(x) = a(bf(b^{-1}(a^{-1}x))) = (ab)f((ab)^{-1}x)$.

   (b) We only need find an element f whose stablizer is a subgroup of S_3 with 3 elements. Pick such a subgroup $H = \langle(1,2)\rangle$, then we can pick f as, for example,

   $$f(x) = \begin{cases} x & x \notin H \\ xa & x \in H \end{cases}$$

   where $a \in G \backslash H$.

3. (a) Two elements x and y are in the same conjugate class of H iff $y = hxh^{-1}$ for some $h \in H$, which implies that they are in the same conjugacy class of G.

(b) Suppose $x, y \in H$ are in the same conjugacy class of G but not the same conjugacy class of H, then there is some $g \in G \backslash H$ such that $y = gxg^{-1}$. By orbit stablizer theorem we only need to show that the conjugacy action by H has the isomorphic stablizer. The isomorphism and its inverse are just conjugation by g and g^{-1}.

4. (a) The "if" part is similar to Problem 2(a) above. To show the "only if" part, consider f_1 as the function that sends e to 1 and every other element to 0. Let $a, b \in G$, $(ab)f$ sends $(ab)^{-1}$ to 1 and all else to 0, while $a(bf)$ sends $(ba)^{-1}$ to 1 and all else to 0. Hence $ab = ba$ and the group is abelian.

   (b) We can pick the function as $f_H(x) = 1$ if $x \in H$ and 0 if otherwise. Then, the stablizer equals

$$\{g \in G : gx \in H \text{ iff } x \in H\} = H$$

D Midterm

1. Let S_4 be the permutation group of $\{1,2,3,4\}$. $\sigma = (1,2,3,4) \in S_4$ (σ sends 1 to 2, 2 to 3, 3 to 4 and 4 to 1). Let H be the smallest subgroup of S_4 containing σ, $\cdot : H \times \{1,2,3,4\} \to \{1,2,3,4\}$ a left H action defined as $h \cdot a = h(a)$.

   (a) Write down all the elements of H. (20 points)

   (b) Is the action $\cdot$ free? Is it transitive? Is it effective? (15 points)

2. Let G be a group, X a non empty set, $\cdot : G \times X \to X$ a left G action on X, and $\rho : G \to S_X$ defined as $\rho(g) = (x \mapsto g \cdot x)$ is the corresponding permutation representation. Let $\cdot' : G \times X \to X$ be defined as $g \cdot' x = g \cdot (g \cdot x)$, $m : G \to G$ be defined as $m(g) = g^2$.

   (a) Show that if G is abelian, then m is a group homomorphism. (15 point)

   (b) Show that if G is abelian, then $\cdot'$ is a left G action on X. (15 points)

   (c) Show that $\cdot'$ is a left G action if and only if the image of ρ is abelian. (10 points)

3. Let G be a group, N a normal subgroup of G, $p : G \to G/N$ the quotient map to the quotient group G/N. Let $G \times G$ be the direct product of G with itself (group operation on $G \times G$ is defined as $(a,b)(c,d) = (ac, bd)$), $H = \{(a,b) \in G \times G : p(a) = p(b)\}$.

   (a) Show that H is a subgroup of $G \times G$. (20 points)

   (b) Show that the set $(G \times G)/H$ has a bijection to G/N. (5 points)

Answer:

1. (a) $e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)$

   (b) It is free, transitive and effective.

2. (a) $m(a)m(b) = a^2b^2 = abab = m(ab)$.

   (b) $(ab) \cdot' x = (ab) \cdot ((ab) \cdot x) = (abab) \cdot x = (aabb) \cdot x = (aa) \cdot ((bb) \cdot x) = a \cdot' (b \cdot' x)$, $e \cdot' x = e \cdot (e \cdot x) = x$.

   (c) For any $g \in G$, $x \in X$, $g \cdot' x = g \cdot (g \cdot x) = (\rho(g) \circ \rho(g))(x)$.

   Suppose $\rho(g)$ is abelian. $e \cdot' x = e \cdot (e \cdot x) = x$, $a \cdot' (b \cdot' x) = (\rho(a) \circ \rho(a) \circ \rho(b) \circ \rho(b))(x) = (\rho(ab) \circ \rho(ab))(x) = (ab) \cdot' x$. So $\cdot'$ is a left G action.

   Suppose $\cdot'$ is a left G action, then for any $x \in X$, any $a, b \in G$, $(\rho(a) \circ \rho(a) \circ \rho(b) \circ \rho(b))(x) = a \cdot' (b \cdot' x) = (ab) \cdot' x = (\rho(a) \circ \rho(b) \circ \rho(a) \circ \rho(b))(x)$. Hence $\rho(a) \circ \rho(a) \circ \rho(b) \circ \rho(b) = \rho(a) \circ \rho(b) \circ \rho(a) \circ \rho(b)$. Apply cancellation law in the group S_X, we see that $\rho(a) \circ \rho(b) = \rho(b) \circ \rho(a)$, hence $\rho(G)$ is abelian.

3. (a) $p(e) = p(e)$ hence $(e, e) \in H$. If $(a, b), (a', b') \in H$, then their product in $G \times G$, which is (aa', bb'), is also in H, because $p(aa') = p(a)p(a') = p(b)p(b') = p(bb')$, and the inverse of (a, b) in $G \times G$, which equals (a^{-1}, b^{-1}), is also in H because $p(a^{-1}) = (p(a))^{-1} = (p(b))^{-1} = p(b^{-1})$. These show that H is a subgroup of G.

   (b) The bijection can be defined as $F : (g, h)H \mapsto p(g)p(h)^{-1}$. To show that it is well defined, if $(g', h') = (g, h)(a, b)$ for $(a, b) \in H$, then $p(g')p(h')^{-1} = p(g)p(a)p(b)^{-1}p(h)^{-1} = p(g)p(h)^{-1}$. To show that it is an injection, if $p(g)p(h)^{-1} = p(g')p(h')^{-1}$, then $p(g^{-1}g') = p(h^{-1}h')$, so $(g', h')H = (g, h)H$. To show that it is a surjection, for every $q \in G/N$, let $a \in G$ such that $p(a) = q$, then $q = F((a, e)H)$.

E Final Review

1. Let $\mathbb{Z}$ be the ring of integers, (4) the ideal generated by 4, and S_3 the permutation group of $\{1, 2, 3\}$. Let $R = \mathbb{Z}/(4)$ be the quotient ring.
   (a) Find all ring homomorphisms from R to R.
   (b) Find all ideals of the group ring $R[S_3]$.
2. Let R be a ring, $a \in R$. Consider the $(R, +)$ action on R defined as $(r, x) \mapsto x + ar$.
   (a) Write down the permutation representation.
   (b) Can you write down examples of R and a such that this action is transitive, free, and effective but not free?
3. (a) Show that any integral domain with finitely many elements is a field.
   (b) Let R be a commutative ring with identity, I a prime ideal of R such that R/I is a finite set. Show that any ideal J containing I is either R or I itself.
4. Let R be an Euclidean domain, p, q, r three distinct primes. Find $gcd(pq, qr)$.

Answer:

1. (a) Such a homomorphism f must send 1 to some element $f(1)$ such that $f(1)^2 = f(1)$. So $f(1) = 0$ or 1, f is either identity or the constant 0 map.
   (b) By definition, I only need to satisfy (1) I is a subgroup of $(R[S_3], +)$; (2) It is invariant under left and right multiplication by $g \in R[S_3]$ where $g \in S_3$. By looking the left and right action of S_3 to S_3, we have the following cases:
      i. $\{0\}$
      ii. $(\sum_{g\in S_3} 2g)$
      iii. $\{\sum_{g\in S_3} 2a_g g\}$, $(\sum_{g\in S_3} 2g, \sum_{g\in S_3\setminus A_3} 2g)$, $(\sum_{g\in S_3} 2a_g g : \sum_{g\in A_3} 2a_g = \sum_{g\in S_3\setminus A_3} 2a_g = 0\}$, $\{\sum_{g\in S_3} 2a_g g : \sum_g a_g \in (2)\}$.
      iv. $(\sum_g g)$.
      v. $(\sum_{g\in A_3} g - \sum_{g\in S_3\setminus A_3} g)$.
      vi. $\{\sum_g a_g g : a_g + a_{g'} \in (2)\}$, $(\sum_g g, \sum_{g\in A_3} g - \sum_{g\in S_3\setminus A_3} g)$, $\{\sum_g a_g g : a_g + a_{g'} \in (2), \sum_g a_g = 0\}$.
      vii. $R[S_4]$, $(\sum_{g\in A_3} g, \sum_{g\in S_3\setminus A_3} g)$, $(\sum_g a_g g : a_g + a_{g'} \in (2),\ \text{if } g, g' \in A_3$ or $g, g' \notin A_3\}$, $\{\sum_g a_g g : \sum_{g\in A_3} a_g = \sum_{g\in S_3\setminus A_3} a_g = 0\}$, $\{\sum_g a_g g : \sum_{g\in A_3} a_g \in (2), \sum_{g\in S_3\setminus A_3} a_g \in (2)\}$, $\{\sum_g a_g g : \sum_g a_g \in (2)\}$, $\{\sum_g a_g g : \sum_g a_g = 0\}$.

   (There would not be anything this complicated in the exam!)

2. (a) $r \mapsto (x \mapsto x + ar)$.

   (b) If $R = \mathbb{Z}$, the action is transitive if $a = 1$, free if $a = 1$. If the action is not free, there is some $x \in R$, $r \in R$, $r \neq 0$, such that $ar + x = x$, so $ar + y = y$ for all y, which means that r is in the kernel of the permutation representation. So it is not possible to be effective but not free.

3. (a) We just need to show that any non-zero element has multiplicative inverse. Let $c \in D$ be a non-zero element, consider the map $r \mapsto cr$, if 1 is in the image then c has multiplicative inverse, if 1 is not in the image, then it is not surjective hence not injective. Because this is a group homomorphism from $(D, +)$ to itself, it would have non-trivial kernel, which contradicts with the assumption that D is integral domain.

   (b) By (a) above, R/I is a field, hence the image of J under the quotient map $\pi : R \to R/I$ is either R/I itself or the 0 ideal. Hence $J = R$ or $J = I$.

4. Let $m = gcd(p, r)$. If p and r are coprime, m can be chosen as 1, so there are s, t such that $1 = sp + tr$, hence $q = spq + tqr$, which implies that $q = gcd(pq, qr)$. If p and r are not coprime, they must be off by multiplying a unit, hence $pq = uqr$ for some unit u, their gcd is pq.

F Final

1. In the quotient set $\mathbb{Z}/6$, define

$$+ : \mathbb{Z}/6 \times \mathbb{Z}/6 \to \mathbb{Z}/6$$

and

$$\times_k : \mathbb{Z}/6 \times \mathbb{Z}/6 \to \mathbb{Z}/6$$

as

$$[a] + [b] = [a + b], [a] \times_k [b] = [kab]$$

Here k is an integer.

   (a) Show $+$ and $\times_k$ are both well defined, and for any integer k, $(\mathbb{Z}/6, +, \times_k)$ is a ring. (15 points)

   (b) Find out all k such that $(\mathbb{Z}/6, +, \times_k)$ is a ring with multiplicative identity. Can $(\mathbb{Z}/6, +, \times_k)$ be an integral domain? If so, when? (15 points)

   (c) Write down all left $(\mathbb{Z}, +)$ actions on the set $\mathbb{Z}/6$ that satisfy the following condition: for any $n \in \mathbb{Z}$, the map $x \mapsto n \cdot x$ is a group homomorphism from $(\mathbb{Z}/6, +)$ to itself. (10 points)

2. Let $(R, +, \times)$ be a ring with multiplicative identity 1, $(M, +, \cdot)$ a left R module. Let N be the set of group homomorphisms from $(R, +)$ to $(M, +)$. For any $r \in R$, $f, f' \in N$, define $f +' f'$ and $r \cdot' f$ as

$$(f +' f')(x) = f(x) + f'(x)$$

$$(r \cdot' f)(x) = r \cdot f(x)$$

   (a) Show that $(N, +', \cdot')$ is a left R module. (15 points)

   (b) Let $Aut(M)$ be the group of R-module automorphisms of M. Show that the map $(\sigma, f) \mapsto \sigma \circ f$ is a left $Aut(M)$ action on N. Is this action always effective? (15 points)

   (c) Show that $K = \{r \mapsto r \cdot m : m \in M\}$ is a submodule of N which is isomorphic to M if R is commutative; and R is commutative if for all R-module M the set $K = \{r \mapsto r \cdot m : m \in M\}$ is a submodule of N isomorphic to M. (10 points)

   (d) Suppose R is commutative, let K be defined as above, write down an R-module homomorphism f from N to itself, such that $f \circ f = f$ and $f(N) = K$. (5 points)

3. Let R be a principal ideal domain, $a, b \in R$, $m = gcd(a, b)$, $(a) = \{ra : r \in R\}$, $(b) = \{rb : r \in R\}$.

   (a) Show that there is some $y \in (a) \cap (b)$, such that $ab = my$. (10 points)

   (b) Show that $(a) \cap (b) = (y)$. (5 points)

Answer:

1. (a)
   - $+$ is defined as group operation of the quotient group $\mathbb{Z}/\langle 6\rangle$, so it is well defined and $(\mathbb{Z}/6,+)$ is an abelian group.
   - To show that $\times_k$ is well defined, if $[a]=[a']$, $[b]=[b']$, then both $a'-a$ and $b'-b$ are multiples of 6, hence

     $$ka'b'-kab=ka'(b'-b)+kb(a'-a)$$

     which is a multiple of 6, hence $[ka'b']=[kab]$.
   - For any $[a]$, $[b]$, $[c]$ in $\mathbb{Z}/6$,

     $$([a]\times_k[b])\times_k[c]=[k^2abc]=[a]\times_k([b]\times_k[c])$$

     $$([a]+[b])\times_k[c]=[kac+kbc]=[kac]+[kbc]=[a]\times_k[c]+[b]\times_k[c]$$

     $$[a]\times_k([b]+[c])=[kab+kac]=[kab]+[kac]=[a]\times_k[c]+[b]\times_k[c]$$

   (b) There is a multiplicative identity iff there is some $a\in\mathbb{Z}$ such that $[kac]=[c]$ for all $c\in\mathbb{Z}$. Hence this is equivalent to $k\in[1]$, and the multiplicative identity is $[1]$, or $k\in[5]$, and the multiplicative identity is $[5]$. It can never be an integral domain because $[2]\times_k[3]=[0]$.

   (c) Because 1 is the generator of $(\mathbb{Z},+)$, the action must be $(n,x)\mapsto\psi^n(x)$ where ψ is an automorphism from $(\mathbb{Z}/6,+)$ to itself. There are two such automorphisms: identity and $x\mapsto -x$.

2. (a)
   - Firstly we show that $+'$ is well defined. For any $a,b\in N$, $a+'b$ is the map $r\mapsto a(r)+b(r)$. For any $r,r'\in R$,

     $$(a+'b)(r+r')=a(r+r')+b(r+r')=(a(r)+b(r))+(a(r')+b(r'))=(a+'b)(r)+(a+'b)(r')$$

     so $a+'b\in N$, and $+'$ is well defined.
   - For any $a\in N$, $c\in R$, $r,r'\in R$,

     $$(c\cdot'a)(r+r')=c\cdot a(r+r')=c\cdot a(r)+c\cdot a(r')=(c\cdot'a)(r)+(c\cdot'a)(r')$$

     So $c\cdot'a\in N$, $\cdot'$ is well defined.
   - The associativity of $(N,+')$ is due to the associativity of $(M,+)$, the identity element is $0_N\in N$ defined as $r\mapsto 0$, the negation of $a\in N$ is defined as $-a:r\mapsto -a(r)$. One can verify that 0_N and $-a$ are both elements of N.
   - For any $a,b\in R$, $l,n\in N$, we have

     $$(a+b)\cdot'n=(r\mapsto(a+b)\cdot n(r))=(r\mapsto a\cdot n(r)+b\cdot n(r))=(a\cdot'n)+'(b\cdot'n)$$

     $$a\cdot'(l+'n)=(r\mapsto a\cdot(l(r)+n(r))=(r\mapsto a\cdot l(r)+a\cdot n(r))=(a\cdot'l)+'(a\cdot'n)$$

     $$a\cdot'(b\cdot'n)=(r\mapsto a\cdot b\cdot n(r))=(r\mapsto ab\cdot n(r))=(ab)\cdot'n$$

(b) The map is well defined because composition of group homomorphisms are group of homomorphisms. The fact that this is a left group action is due to associativity of function compositions, and any map composing with identity equals itself. The action is always effective, because if it sends all elements of N of the form $x \mapsto x \cdot m$ for some $m \in M$ to itself then $\sigma(m) = m$ for all m which implies that $\sigma = id_M$.

(c) By construction, K is a subgroup of $(N, +')$.

- If R is commutative, for any $a = (r \mapsto r \cdot m) \in K$, $c \in R$,

$$c \cdot' a = (r \mapsto c \cdot (r \cdot m)) = (r \mapsto cr \cdot m) = (r \mapsto r \cdot (c \cdot m)) \in K$$

  so K is closed under scalar multiplication hence an R-submodule, and $f \mapsto f(1)$ is an isomorphism from K to M.

- Let $M = R$, then $(r \mapsto r) \in K$, then a times this element is in K iff $ar = ra$ for all r iff R is commutative.

(d) Let $f(\alpha) = (r \mapsto r\alpha(1))$. One can check that it satisfies all the requirements.

3. (a) $a = qm$, $b = pm$, then $ab = (pqm)m$.

(b) We only need to show that any element x in $(a) \cap (b)$ is a multiple of $y = pqm$. Because $x \in (a) \cap (b)$, there are $f, g \in R$ such that $x = af = bg$. Let $m = sa + tb$, then $sq + tp = 1$, hence

$$x = (sq + tp)x = sqbg + tpaf = (sq + tf)y$$