Abstract Algebra I & II

David J. Hunter[1] < Margaret L. Morrow[2†]

[1]Westmont College
[2]SUNY Plattsburgh

[†]The relation "Hunter < Morrow" indicates that Chapters 1–5 of these notes were originally written by Margaret Morrow. David Hunter revised these chapters and added Chapters 6–13, and he takes full responsibility for this version of these notes.

Contents

To the Student **v**

Introductory Activity **1**

1 Introduction to Groups **5**

2 New Groups from Old **9**
2.1 Direct Products of Groups 9
2.2 Subgroups 10
2.3 Cyclic Subgroups 11

3 Homomorphisms and Isomorphisms **13**
3.1 Definitions 13
3.2 Preservation of Structure 14
3.3 Kernel and Image 15

4 Cosets: First Ideas and Applications **16**
4.1 Definition and Examples 16
4.2 Cosets and Partitions 17
4.3 Cosets and Group Order 17

5 Normal Subgroups and Quotient Groups **18**
5.1 Normal Subgroups 19
5.2 Quotient Groups 19
5.3 Isomorphism Theorems 20

6 Rings and Ideals **22**
6.1 Rings 22
6.2 Homomorphisms and Kernels 23
6.3 Ideals 24

7 Quotient Rings **26**
7.1 Cosets 26

7.2 Constructing Quotient Rings 26
7.3 Isomorphisms 27

8 Divisibility **28**
8.1 Integral Domains and Fields 28
8.2 The Division Algorithm 29
8.3 Greatest Common Divisor 30
8.4 The Euclidean Algorithm 32

9 Prime Ideals and Maximal Ideals **34**
9.1 Roots of Polynomials 34
9.2 Prime Ideals 35
9.3 Maximal Ideals 35
9.4 Field Extensions 36

10 Advanced Group Theory **38**
10.1 Some Important Facts 38
10.2 Group Actions 39
10.3 The Class Equation 40
10.4 The Normalizer 41
10.5 Sylow Theory 41
10.6 Finite Group Facts 42

11 Fields **43**
11.1 Field Extensions 43
11.2 Algebraic Extensions 44
11.3 Degree Multiplication 45
11.4 Properties of Algebraic Extensions 46

12 Isomorphisms of Fields **47**
12.1 Isomorphisms and Automorphisms 47
12.2 The Galois Group 48
12.3 Extensions of Isomorphisms 48
12.4 Separability 49

13 Galois Theory **51**
13.1 Towers and Galois Groups 51
13.2 The Fixed Field 51
13.3 The Galois Correspondence 52
13.4 Radical Extensions 54

13.5 Solvability by Radicals 55
13.6 Insolvability of the Quintic 55
13.7 The Fundamental Theorem of Algebra 56

To the Student

Have you ever wondered how modern mathematics came to be? To what extent are the definitions and theorems that we find in the canonical textbooks the result of choices made by historical figures? Is there something intrinsic to the subject that forces modern mathematical theory down the path that it takes? Put another way, would Earthling mathematicians recognize the work of a community of mathematicians from a distant galaxy?

We can glean some insight into these questions by proceeding axiomatically: make as few assumptions and definitions as possible, and see where logical deduction leads. The material in these notes represents the consequences of some very low-level mathematical foundations: logic, sets, and the integers. These consequences have applications throughout pure and applied mathematics, and are part of the *lingua franca* of the discipline.

Historically, much of this subject was motivated by the search for solutions to polynomial equations. There is a well-known formula for solving any quadratic polynomial equation, but are there analogs to this formula for polynomials of degree greater than 2? It is easy to believe that our hypothetical space-alien mathematical colleagues would also be interested in such formulas, but mathematical theory required to answer this question turns out to be surprisingly deep.

Throughout this semester and the next (should you persevere), you will be guided through a series of deductive discoveries along the path that modern mathematicians have blazed. Whether this path is the only reasonable one will be yours to judge once you have completed the journey.

These notes (along with the sequel) give a comprehensive coverage of two semesters of advanced undergraduate or beginning graduate algebra. However, these notes contain mostly questions, and you must supply the answers. Your written accounts of your inquiry and our class discussions will produce a complete abstract algebra textbook of your own construction.

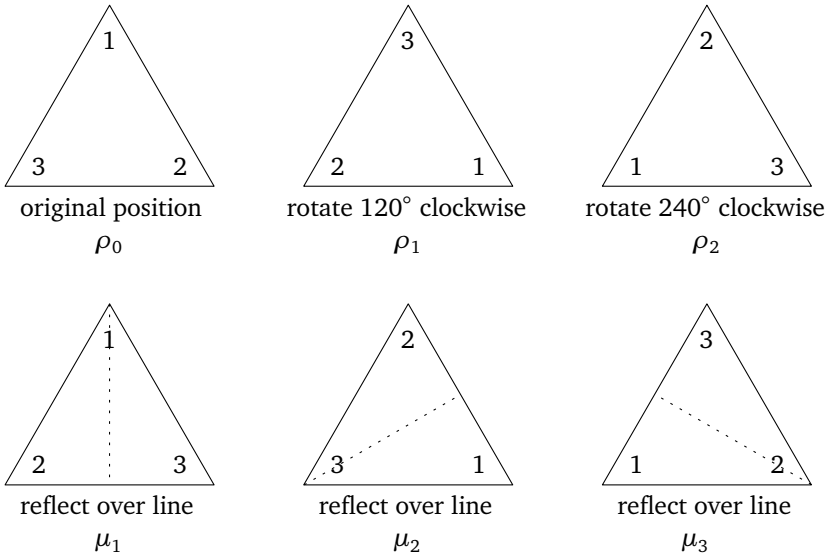
Introductory Activity: Some Useful Examples

Example I: Symmetries.

We can think of a **symmetry** of a plane figure as a rigid motion of the figure that results in the figure simply being repositioned on top of its original outline.

It is the final position of the figure that is important, not the motion as such. For example, if we rotate the triangle below through 120° or 480°, the triangle ends up in the same final position, so we do not think of these as distinct symmetries.

1. Consider the symmetries of an equilateral triangle, as illustrated below. Each sketch shows the resulting position when the specified motion is applied to the triangle starting in the original position.



Cut an equilateral triangle out of a sheet of paper, and number the vertices 1, 2, and 3 as shown in the original position. Put the number of each vertex on the back of the triangle as well.

We can apply one of the rigid motions, and then, *continuing from the new position of the triangle,* apply another of the rigid motions. We can then record the overall effect as one of six symmetries listed above.

For example if we first apply μ_1, then (continuing from the resulting position) apply ρ_1 (a 120° clockwise rotation) we end up with μ_2. Using our usual function composition notation, we can write $\rho_1 \circ \mu_1 = \mu_2$.

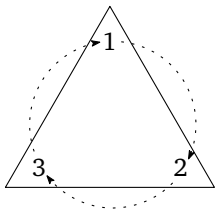
It is useful to write the results of all such combinations in table form, as shown below. We show the result of $\rho_1 \circ \mu_1$ in the row labeled ρ_1 and the column labeled μ_1.

Important: The convention is that we enter the result of $\rho_1 \circ \mu_1$ into the row corresponding to ρ_1 and the column corresponding to μ_1, even though when we do these motions we first do the reflection μ_1 and then the rotation ρ_1.

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0						
ρ_1						
ρ_2						
μ_1						
μ_2						
μ_3						

Use the cut-out triangle to determine the result of all the compositions and complete the table. We will denote this collection of symmetries, together with composition, by D_3.

2. You may have noticed that you can determine which symmetry was performed by looking at the labels of each vertex. Instead of representing rotations and reflections using Greek letters, it is often convenient to represent them using **cycle notation.** For example, starting with the original position, the rotation ρ_1 moves vertex 1 to vertex 2, vertex 2 to vertex 3, and vertex 3 to vertex 1.



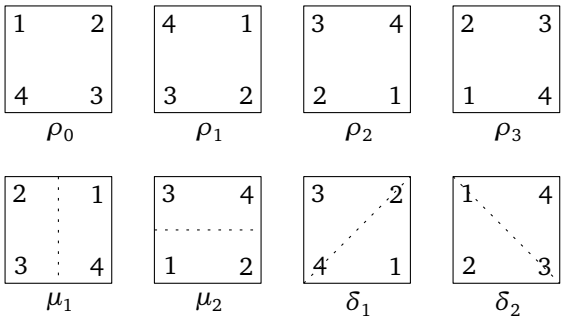
$\rho_1 = (1\ 2\ 3)$

We can denote this rotation with the cycle (1 2 3), which we read as "1 goes to 2, 2 goes to 3, 3 goes to 1". In cycle notation, each vertex moves to the one after it, and the last one wraps around to the first.

Complete the table below, giving the cycle that corresponds to each symmetry.

ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
(1)	(1 2 3)		(2 3)		

3. Develop similar tables for the symmetries of a square. We will use the notation D_4 for the symmetries of a square together with composition. Use the symbols indicated in the diagram below to denote the eight symmetries.



Using a cut-out square (or any other method), compute the compositions and fill out the following table.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0								
ρ_1								
ρ_2								
ρ_3								
μ_1								
μ_2								
δ_1								
δ_2								

In addition, write each symmetry in cycle notation. (Notice that ρ_2, μ_1, and μ_2 need to be written as products of two disjoint cycles.)

ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
(1)	(1 2 3 4)			(1 2)(3 4)			

Example II: Clock arithmetic. Consider the numbers on a clock, and imagine 0 in place of 12. (We will denote this set by $\mathbb{Z}_{12}$). So $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$.

We define "addition modulo 12" on this set as follows: for a and b in this set, $a+b \pmod{12}$ is the hour on the clock-face that is b hours after a. For example, $9+5=2 \pmod{12}$, since 0 is 3 hours after 9, and we need an additional 2 hours after that.)

We can also define "multiplication mod 12" on $\mathbb{Z}_{12}$ by thinking of multiplication as repeated addition modulo 12. So for a and b in $\mathbb{Z}_{12}$, we think of $a \cdot b \pmod{12}$ as the result of adding b to itself a times, modulo 12. For example $3 \cdot 7 = 9 \pmod{12}$.

There is nothing special about 12 here; we can just as easily define addition and multiplication mod n on the set $\{0,1,2,...,n-1\}$ for any fixed positive integer n. Simply imagine a clock-face with the numbers $\{0,1,2,...,n-1\}$ in place of $\{0,1,2,3,4,5,6,7,8,9,10,11\}$, and for a and b in this set, define $a+b \pmod{2}$ to be the hour on this clock-face that is b hours after a. Define $a \cdot b \pmod{n}$ to be the result of adding b to itself a times, modulo n.

We can draw up tables for these operations, just as we did for symmetries.

1. Consider $\mathbb{Z}_5 = \{0,1,2,3,4\}$ Draw up a table for addition mod 5, and a separate table for multiplication mod 5.

+	0	1	2	3	4
0					
1					
2					
3					
4					

·	0	1	2	3	4
0					
1					
2					
3					
4					

2. Consider $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ Draw up a table for addition mod 6, and a separate table for multiplication mod 6.

+	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

·	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Chapter 1

Introduction to Groups

In this course, we stipulate the meanings of the terms and symbols using **definitions**. When faced with a new definition, try to understand it by thinking of examples that satisfy the conditions of the definition. It also helps to try to come up with "non-examples," meaning entities closely related to the defined concept, but that do not conform precisely to the definition.

Definition 1.1. A **binary operation** $*$ on a set A is a function $A \times A \to A$, where $(a,b) \mapsto a*b$. In other words, a binary operation inputs two elements a, b of the set A, and outputs a well-defined element $a*b$ of the set A.

Problem 1. Which of the following are binary operations on the specified set? If not, explain why not.

(a) Addition on $\mathbb{Z}$, the set of integers.

(b) Subtraction on $\mathbb{Z}$, the set of integers.

(c) Subtraction on $\mathbb{N}$, the set $\{1,2,3,\ldots\}$ of natural numbers.

(d) Division on $\mathbb{R}$, the set of real numbers.

(e) Division on $\mathbb{Z} \setminus \{0\}$.

(f) Composition on D_4, the symmetries of the square.

(g) Composition on the set of rotations in D_4.

(h) Multiplication modulo 6 on $\mathbb{Z}_6$.

Definition 1.2. A binary operation is **associative** if $(a*b)*c = a*(b*c)$ for all $a,b,c \in A$. An element e is said to be an **identity** for $*$ if $a*e = e*a = a$ for all $a \in A$. An element b is an **inverse** of the element a if $a*b = b*a = e$.

Problem 2. Refer back to those operations in Problem 1 that were binary operations. Do the following for each of these binary operations.

(a) Determine whether the operation is associative, and if not, prove that the operation is not associative.

(b) State whether there is an identity for the operation, and if so, identify it.

(c) If there is an identity for the operation, determine which elements (if any) have inverses.

Definition 1.3. A binary operation is **commutative** if $a * b = b * a$ for all $a, b \in A$.

Problem 3. Determine which of the binary operations in Problem 1 are commutative, and if not, provide proof that the operation is not commutative.

Problem 4. Prove that if a binary operation $*$ on a set A has an identity element, then that identity element is unique.

Definition 1.4. A **group** is a set G together with a binary operation $*$ on G satisfying the following:

1. The operation $*$ is associative.
2. There is an element in G which is an identity for $*$.
3. Every element in G has an inverse with respect to $*$ in G.

We denote the group by $\langle G, * \rangle$. We refer to the set G as the **underlying set** of the group $\langle G, * \rangle$. (However if the specific operation is clear from the context, or is not important in the context, we sometimes simply write G instead of $\langle G, * \rangle$ for the group, and speak of "the group G.")

Problem 5. Which of the following are groups? If not, explain why not.

(a) $\langle \mathbb{Z}, + \rangle$

(b) $\langle \mathbb{Z}, - \rangle$

(c) $\langle \mathbb{Z}, \times \rangle$

(d) $\langle \mathbb{Z}, \div \rangle$

(e) $\langle \mathbb{R}^+, \times \rangle$ ($\mathbb{R}^+$ denotes the set of positive real numbers.)

(f) The set of symmetries of a regular pentagon with operation composition.

(g) $\mathbb{Z}_6$ with operation addition mod 6.

(h) $\mathbb{Z}_6$ with operation multiplication mod 6.

(i) $\mathbb{Z}_6 \setminus \{0\}$ with operation multiplication mod 6.

(j) $\mathbb{Z}_5 \setminus \{0\}$ with operation multiplication mod 5.

Problem 6. Prove that the following is, or is not a group, as appropriate. The set $S = \mathbb{R} \setminus \{1\}$ with operation defined by $a * b = a + b - ab$ for all a and b in S. (On the right side of the equation, the operations are the usual addition and multiplication in $\mathbb{R}$.)

Problem 7. Prove that the following is, or is not a group, as appropriate: The set $M_2(\mathbb{R})$ of all 2 by 2 matrices, with real numbers as entries, and operation matrix multiplication.

Definition 1.5.

- A group $\langle G, * \rangle$ is said to be **abelian** if $*$ is commutative.
- We say a group is **finite** if the underlying set contains finitely many elements. We say a group is **infinite** if the underlying set contains infinitely many elements.
- For a finite group G, the **order** of G is the number of elements in G. We also say that an infinite group has **infinite order**.

Problem 8. Provide at least two examples of abelian groups.

Problem 9. Refer back to Problem 5. Identify the finite groups in that question, and for each of these state the order of the group.

Problem 10. Provide at least two examples of non-abelian groups. For one of these, prove that the group is non-abelian.

Problem 11. Suppose $\langle G, * \rangle$ is a group, with s, t and u in G. Prove or disprove as appropriate: If $s * t = u * s$, then $t = u$.

Remark: Using equations. Let a, b, c be elements of a group G. Since the binary operation in a group is well defined, we are allowed to multiply both sides of an equation by the same element. In other words, $a = b$ implies that $c * a = c * b$ and $a * c = b * c$.

Problem 12. Let G be a group, and let $a \in G$. Prove that a has a unique inverse.

Problem 13. Suppose G is a group, with a and b in G. Prove that if $a * b = e$, then $b * a = e$. Use this to prove that if G is a group, with a and b in G and $ab = e$, then a is the inverse of b.

Notation: For convenience, instead of using "$*$" to denote the group operation, we often use multiplicative notation as follows:

- In place of $a * b$ write ab.
- Denote the inverse of a (the uniqueness of which is ensured by Problem 12), by a^{-1}.
- Let a^1 denote a, and for $n \in \mathbb{N}$, with $n > 1$, define a^n to be aa^{n-1}.

It is important to note that we have simply introduced some notation; the operation "multiplication" in a group is *not* in general familiar old multiplication. Take care when working in an arbitrary group not to take for granted properties of exponents that are familiar from working with the real numbers. So for example, in the next two problems you may not assume that $a^m a^n = a^{m+n}$, nor that $(a^m)^n = a^{mn}$.

Problem 14. In a group G, if $a \in G$ and $n \in \mathbb{N}$, then both $(a^n)^{-1}$ and $(a^{-1})^n$ have unambiguous interpretations in terms of the definitions above. Prove that these two are in fact equal.

Problem 15. Prove that if G is a group, with $a \in G$, then $(a^{-1})^{-1} = a$.

You have shown in Problem 14 that $(a^n)^{-1}$ and $(a^{-1})^n$ have unambiguous meanings, and are in fact equal. The symbol a^{-n}, on the other hand, is not automatically defined by the definitions already given. It is convenient to define a^{-n} as simply another notation for $(a^n)^{-1}$ and $(a^{-1})^n$:

Definition 1.6. In a group G with $a \in G$, we define a^{-n} to be $(a^n)^{-1}$. Also, we define a^0 to be the identity, e.

As we've said, we cannot simply assume that exponents will have the same properties in an arbitrary group as they do when working with real numbers. Some familiar properties of exponents for real numbers are in fact false in certain groups. The next problem establishes two basic principles that *do* apply in an arbitrary group.

Problem 16. Suppose G is a group, with $a \in G$. Using notation like

$$a^n = \underbrace{a * a * \cdots * a}_{n},$$

give an informal argument that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{N}$. (It is tedious, but not hard, to show that these statements hold for $m, n \in \mathbb{Z}$ as well. A formal proof requires induction.)

Problem 17. Suppose G is a group, with a, b, and x in G. If $x = a^{-1}b$, can we conclude that $xa = b$? Either prove this conclusion true, or provide a counterexample.

Problem 18. Prove or disprove, as appropriate: Suppose G is a group, with a, b and c in G. If $ac = bc$, then $a = b$.

Problem 19. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^2 = a^2b^2$.

Problem 20. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^{-1} = a^{-1}b^{-1}$.

Problem 21. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^{-1} = b^{-1}a^{-1}$.

Historically, the central focus of abstract algebra was the solution of equations. The following problem gives an indication of the connection:

Problem 22. Suppose G is group, with a and b in G. Consider the equation $ax = b$.

(a) Prove that $a^{-1}b \in G$.

(b) Prove by substituting that $x = a^{-1}b$ is a solution for the equation.

(c) Prove that $x = a^{-1}b$ is the *only* solution for the equation $ax = b$; that is, this solution is *unique.*

You have thus shown that if G is a group, then for all a and b in G, there is a unique solution in G for the equation $ax = b$. Similarly there is a unique solution in G for $xa = b$.

Chapter 2

New Groups from Old

Some notational conventions:

- From now on, the phrase "the group $\mathbb{Z}_n$" will be taken to mean the set $\{0,1,2,\ldots,n-1\}$ with operation addition modulo n.
- For groups such as $\mathbb{Z}_n$, where it is natural to use **additive notation**, we replace our multiplicative expressions by the additive analogues, as follows:
  - for n an integer, in place of a^n write na
  - in place of a^{-1} write $-a$
  - write "0" for the identity.

Problem 23. Translate each of the following into additive notation:

(a) $a^n = e$

(b) "There exists an element x such that $ax = b^{-1}$."

(c) $a^{-1}ba = e$

(d) $(a^{-1})^n = (a^n)^{-1}$

(e) $(a^{-1})^{-1} = a$

(f) $a^n a^m = a^{n+m}$

(g) $(a^n)^m = a^{nm}$

Yet another notational convention: Let $\mathbb{Z}_n^*$ denote the set $\{1,2,3,\ldots,n-1\}$ (notice the 0 is omitted).

Problem 24. Is multiplication modulo 7 a binary operation on $\mathbb{Z}_7^*$? If so, write out the operation table for multiplication modulo 7 on $\mathbb{Z}_7^*$. Is $\mathbb{Z}_7^*$ with a group under this operation? If not, explain why not.

2.1 Direct Products of Groups

Definition 2.1. Recall that the **Cartesian product** of two sets X and Y is the set of all ordered pairs (x,y) where $x \in X$ and $y \in Y$. Suppose that $\langle G, *_G \rangle$ and $\langle H, *_H \rangle$ are groups. Define an operation $*$ on $G \times H$ as follows: for all (g_1,h_1) and (g_2,h_2) in $G \times H$, define $(g_1,h_1)*(g_2,h_2)$ to be $(g_1 *_G g_2, h_1 *_H h_2)$.

In practice, we will often use multiplicative notation for all three of these operations, writing $(g_1,h_1)(g_2,h_2) = (g_1g_2,h_1h_2)$, where the operation in the first coordinate is the operation in G, and the operation in the second coordinate is the operation in H. (We often express this idea by saying that the operation on $G \times H$ is defined "component-wise.")

Problem 25. Complete the operation table for $\mathbb{Z}_2 \times \mathbb{Z}_3$, where the operation is defined component-wise. (Use additive notation, since both operations are based on addition.)

$+,+$	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$(0,0)$						
$(0,1)$						
$(0,2)$						
$(1,0)$						
$(1,1)$						
$(1,2)$						

Problem 26. Prove that if G and H are groups, then $G \times H$, with operation defined component-wise, is a group. (Use multiplicative notation, since there is nothing to indicate that additive notation is appropriate).

Another convention: Suppose G and H are groups. When we refer to "the group $G \times H$," the operation is assumed to be the component-wise operation we defined above.

It is interesting and important to consider the question of what properties a direct product of groups inherits from the original groups. Here is one example of this question:

Problem 27. Prove or disprove: if G and H are abelian groups, then $G \times H$ is abelian.

Problem 28. Consider the group $\mathbb{Z}_5^* \times \mathbb{Z}_2$. (The operation in the group on the left is multiplication modulo 5, and the operation in the group on the right is addition modulo 2.) Draw up the operation table for this group.

2.2 Subgroups

Suppose G is a group, and H a subset of G. If a and b are elements of H, then ab denotes that element of G defined by the group operation of G.

Definition 2.2.

- We say that H is **closed** under the operation $*$ if for all a and b in H, $a * b$ is in H. (Sometimes one says "the operation $*$ is closed on H.")
- We say that "H is closed under taking inverses" if for all a in H, the inverse of a is in H.

Definition 2.3. Suppose that G is a group. A subset H of G is called a **subgroup** of G if

1. H contains the identity of G,
2. H is closed under the operation of G, and
3. H is closed under taking inverses.

(If H is subgroup of G we sometimes say that H "inherits" the operation from G.) It follows immediately from this definition that a subgroup of a group is a group, under the inherited operation, with the same identity element.

Problem 29.

(a) Identify all the subgroups of $\langle \mathbb{Z}, + \rangle$.

(b) Identify all the subgroups of $\langle \mathbb{Z}_6, + \rangle$.

(c) Identify all the subgroups of $\langle \mathbb{Z}_5^*, \times \rangle$.

Definition 2.4. The **permutation group** S_4 consists of the following 24 elements: (1), (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 2 4), (1 3 2), (1 3 4), (1 4 2), (1 4 3), (2 3 4), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2). These elements represent the 4! permutations of the symbols 1,2,3,4, given in **cycle notation**. In a cycle $(a_1\ a_2\ a_3\ \cdots\ a_k)$, the corresponding permutation moves a_1 to a_2, a_2 to a_3, and so on, with the last element a_k moving to a_1. Cycles (and therefore permutations) are multiplied by performing their actions from right to left, as with function composition. For example:

$$(1\,2\,4)(2\,4\,3) = (1\,2)(3\,4).$$

Similar definitions yield the groups S_n for $n \in \mathbb{N}$.

Problem 30. Find five different subgroups of S_4, all of different orders.

Problem 31. In the introductory activity, we saw that the elements of the group D_4 can be written in cycle notation, and that composition of permutations corresponds to composition of symmetries. Use cycle notation and permutation composition to do this problem.

(a) Identify all the subgroups of D_4.

(b) Based on the results of this problem and the previous two problems, formulate a conjecture about the order of a subgroup compared to the order of the group.

Problem 32. Prove that if H and K are subgroups of a group G, then their intersection $H \cap K$ is a subgroup of G.

Problem 33. Suppose G and H are groups, with S a subgroup of G, and T a subgroup of H. Prove or disprove as appropriate: $S \times T$ is a subgroup of $G \times H$.

Problem 34. Let H be a subgroup of a group G, and let $x \in G$ be some element. The **conjugate** of H by x is the set $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Prove that xHx^{-1} is also a subgroup of G.

2.3 Cyclic Subgroups

Problem 35. Let G be a group, and let g be a fixed element of G. Define $H = \{g^n \mid n \in \mathbb{Z}\}$. Prove that H is a subgroup of G.

Definition 2.5. The subgroup considered in Problem 35 is called the "**cyclic subgroup** generated by a" and is denoted $\langle a \rangle$.

Problem 36. Show that all of the subgroups considered in Problem 29 are cyclic, and write each subgroup in the form $\langle a \rangle$, for a suitably chosen generator a in the parent group.

Definition 2.6. If G is a group and $G = \langle a \rangle$ for some $a \in G$, then G is called a **cyclic** group. In particular, cyclic subgroups are cyclic.

Problem 37.

(a) Prove that every cyclic group is abelian.

(b) State the contrapositive of the statement in part 1, and use it to find an example of a group that isn't cyclic.

(c) Give a counterexample to show that the converse of the statement in part 1 is false.

Problem 38. Let G and H be groups. Prove that if $G \times H$ is a cyclic group, then G and H are both cyclic groups.

Definition 2.7. The set $U(n)$ is the subset of $\mathbb{Z}_n$ consisting of elements that have multiplicative inverses, modulo n. That is,

$$U(n) = \{a \in \mathbb{Z}_n \mid ab = 1 \text{ for some } b \in \mathbb{Z}_n\}.$$

The elements of $U(n)$ are called the **units** of $\mathbb{Z}_n$.

Problem 39.

(a) Prove that $U(n)$ is a group under multiplication modulo n.

(b) A group of the form $U(n)$ is called a "U-group." Are all U-groups cyclic? Prove or disprove.

Chapter 3

Homomorphisms and Isomorphisms

Most fields of mathematics have "structure-preserving" mappings. For example, in linear algebra, linear transformations "preserve" the vector space structure (scalar multiplication and vector addition). In geometry, isometries preserve the distances between points. In abstract algebra, the structure-preserving maps are homomorphisms and isomorphisms.

3.1 Definitions

Definition 3.1. Suppose that $\langle G, *_G \rangle$ and $\langle H, *_H \rangle$ are groups. We say that a function $\phi : G \longrightarrow H$ is a **homomorphism** if for all $a, b \in G$, $\phi(a *_G b) = \phi(a) *_H \phi(b)$.

A homomorphism that is one-to-one and onto is called an **isomorphism**.

We say that groups G and H are **isomorphic** if there exists an isomorphism $\phi : G \longrightarrow H$ between them. In this case we can write $\phi : G \xrightarrow{\sim} H$ to denote the isomorphism and $G \simeq H$ to denote that the groups are isomorphic.

Intuitively, two groups are "isomorphic" to each other if the operation table for one of them can be obtained from the operation table of the other, by simply reordering and renaming elements in the group, and renaming the operation. We express this by saying that the isomorphism *preserves algebraic structure*. Try the following exercise to get a feel for this:

Problem 40. Draw up an operation table for each of the following groups. Then decide which pairs of these are isomorphic, in the sense of the intuitive "reordering and renaming" description given above; if reordering is necessary, show the reordering; also specify the renaming.

(a) $\langle \mathbb{Z}_4, + \rangle$

(b) $U(8)$

(c) $\mathbb{Z}_2 \times \mathbb{Z}_2$, with operation addition modulo 2 on each component.

(d) $G = \{1, -1, i, -i\}$, with operation multiplication in the complex numbers. Recall that $i^2 = -1$.

Problem 41. Suppose that G is an abelian group. Prove that the function defined by $\phi(g) = g^2$ is a homomorphism from G to G.

Recall (Definition 1.5) that the order of a group is the size of the group. The next definition allows us to talk about the order of an element.

Definition 3.2. The **order** of an element $a \in G$ is the order of the cyclic subgroup $\langle a \rangle$.

Problem 42. Let $G = \langle a \rangle$, where a has order n. Define a map $\phi : \langle \mathbb{Z}, + \rangle \longrightarrow \langle G, \cdot \rangle$ by $\phi(i) = a^i$. Prove that ϕ is a homomorphism, but it isn't one-to-one.

Problem 43. Let $G = \langle a \rangle$, where a has infinite order. Define a map $\phi : \langle \mathbb{Z}, + \rangle \longrightarrow \langle G, \cdot \rangle$ by $\phi(i) = a^i$. Prove that ϕ is an isomorphism.

The previous problem shows that, up to isomorphism, there is only one infinite cyclic group: the integers $\mathbb{Z}$ under addition.

Problem 44. Let G and H be groups, with identities e_G and e_H, respectively. Let $\phi : G \longrightarrow H$ be a homomorphism. Prove that $\phi(e_G) = e_H$. (Hint: Consider $\phi(e_G e_G)$.)

3.2 Preservation of Structure

The last problem shows that homomorphisms map the identity to the identity. In the next few problems, we will show that homomorphisms preserve other algebraic structures in a group. Furthermore, we will show that isomorphic groups share many group-theoretic properties. In fact, one could say that "group-theoretic properties" are precisely those properties that are preserved by isomorphisms.

Problem 45. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. Prove that, for all $a \in G$, $\phi(a^{-1}) = (\phi(a))^{-1}$.

Problem 46. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is an isomorphism. Prove that if G is abelian, then H is abelian. Would this statement still be true if ϕ were just a homomorphism and not an isomorphism?

Problem 47. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is an isomorphism. Prove that if G has an element of order n, then H has an element of order n. Would this statement still be true if ϕ were just a homomorphism and not an isomorphism?

To prove that two given groups, G and H say, are isomorphic, you must show that *there exists* an isomorphism from G to H. So, logically, to prove that two given groups, G and H, are *not* isomorphic, you have to show that no function $\phi : G \longrightarrow H$ is an isomorphism. But this direct approach is too hard! Instead one usually tries to demonstrate that no isomorphism could exist using one of the following approaches:

- Show that the two groups have different order.
- Show that one group has some algebraic property that the other does not. For example,
  - G might be abelian, and H non-abelian,
  - G might have an element of some specified order, while H does not,
  - G might be cyclic, and H not,

– every equation of some particular form (such as $x^2 = a$) might have a solution in G, while some equation of that form in H does not have a solution.

Problem 48. In each of the following, prove that the two groups specified are not isomorphic.

(a) S_4 and $\mathbb{Z}_6 \times \mathbb{Z}_4$

(b) $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_8$

(c) $U(10)$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$

(d) $\langle \mathbb{Q}^*, \cdot \rangle$ and $\langle \mathbb{Z}, + \rangle$, where $\mathbb{Q}^*$ denotes the nonzero rational numbers.

(e) $\langle \mathbb{R}^*, \cdot \rangle$ and $\langle \mathbb{R}, + \rangle$

3.3 Kernel and Image

Definition 3.3. If $\phi : A \longrightarrow B$ is a function from a set A to a set B, and $C \subseteq A$, then the **image** of C under ϕ, denoted $\phi(C)$, is defined to be the set $\{b \in B \mid \text{there is some } c \in C \text{ with } \phi(c) = b\}$.

Definition 3.4. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. The **kernel** of ϕ, denoted by $\text{Ker}(\phi)$, is defined to be the set $\{g \in G \mid \phi(g) = e\}$, where e is the identity of H.

Problem 49. Let $\phi : U(10) \longrightarrow U(10)$ be defined by $\phi(a) = a^2$ for all $a \in U(10)$. (You already proved in Problem 40 that ϕ is a homomorphism.) Determine $\phi(U(10))$ and $\text{Ker}(\phi)$.

Problem 50. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. Prove that $\text{Ker}(\phi)$ is a subgroup of G.

Problem 51. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. Let K be a subgroup of G. Prove that $\phi(K)$ is a subgroup of H.

Problem 52. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. Prove that $\text{Ker}(\phi) = \{e\}$ if and only if ϕ is one-to-one.

Problem 53. Suppose that G and H are groups, and that $\phi : G \longrightarrow H$ is a homomorphism. Prove that $\phi(G)$ is abelian if and only if, for all $x, y \in G$, $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$.

Chapter 4

Cosets: First Ideas and Applications

Sometimes in mathematics there is a way of looking at things that at first seems rather useless, but which turns out to be really powerful. Cosets are like that. At first it might seem that this construction is strangely irrelevant. Persevere; you will soon find how much can be derived from the idea.

4.1 Definition and Examples

Definition 4.1. Suppose G is a group, with H a subgroup of G, and $a \in G$. Then aH denotes the set $\{ah \mid h \in H\}$, and is called a **left coset** of H in G (or, if necessary, the left coset of H determined by a). (In additive notation, the left coset of H determined by a is denoted $a+H$.)

To help you interpret this definition, note that it means that $x \in aH$ if and only if there exists some $h \in H$ with $x = ah$. The following exercises should help you to understand this definition.

Problem 54. Consider the group D_4, and the subgroup $H = \langle \delta_1 \rangle = \{\rho_0, \delta_1\}$ of D_4. List the distinct left cosets of the form aH for $a \in D_4$, and list the elements of each of these. How many distinct (not equal) left cosets are there for H?

Problem 55. Consider the group S_3, and the subgroup $K = \langle (1\,2\,3) \rangle = \{(1), (1\,2\,3), (1\,3\,2)\}$ of S_3. List the distinct left cosets of K in S_3, and list the elements of each of these. How many distinct left cosets are there for K?

Problem 56. Consider the group $\mathbb{Z}$, and its subgroup $H = \langle 5 \rangle = 5\mathbb{Z}$. List the distinct left cosets of the form $n+H$ for $n \in \mathbb{Z}$, and list the elements of each of these. How many distinct left cosets are there for H?

The following three problems develop some properties of cosets that are very useful in later proofs.

Problem 57. Prove or disprove as appropriate: Suppose G is a group, H a subgroup of G, and a and b elements of G. If $aH = bH$, then $a = b$.

Problem 58. Suppose G is a group, H a subgroup of G, and $a \in G$. Prove or disprove as appropriate: If $aH = H$, then $a \in H$.

Problem 59. Prove or disprove as appropriate: Suppose G is a group, H a subgroup of G, and a and b elements of G. If $a \in bH$, then $b \in aH$.

4.2 Cosets and Partitions

Problem 60. Prove that if $a \in H$, then $aH = H$. (This is the converse of the statement in Problem 58.)

Problem 61. Suppose that H is a subgroup of a group G. Prove that for all $a, b \in G$, either $aH = bH$ or $aH \cap bH$ is empty.

Notation and terminology: If X is a finite set, the number of elements in X is denoted by $|X|$. (For an infinite set X, $|X|$ denotes its cardinality.) Recall that if G is a group, then the size $|G|$ is called its **order**.

Problem 62. Suppose G is a group, H subgroup of G, and a an element of G. Consider the function $f : H \longrightarrow aH$ defined by $f(h) = ah$ for all $h \in H$. (Note: this is a map of *sets*, not of groups, so it can't be a homomorphism.) Prove that f is one-to-one and onto. Explain why this implies that, for all $x, y \in G$, $|xH| = |yH|$.

Problem 63. Consider the subgroup $H = \langle (1\,2\,3\,4) \rangle$ of S_5.

(a) What is $|S_5|$?

(b) What is $|H|$?

(c) How big are the cosets of H in S_5? (Use Problem 62.)

(d) How many distinct cosets of H in S_5 are there? (Use Problem 61.)

(e) Do you think that S_5 has a subgroup of order 7? Why or why not?

4.3 Cosets and Group Order

Problem 64. Suppose that G is a finite group and H is a subgroup of G. Prove that $|H|$ divides $|G|$. (That is, the number of elements of G is an integer multiple of the number of elements of H.) Explain why it follows that the order of any element of G also divides $|G|$.

Problem 65. Prove that every group of prime order is cyclic.

Problem 66. Show that any homomorphism of groups $\phi : G \longrightarrow H$ where $|G|$ is prime must either be the trivial homomorphism or a one-to-one map.

Problem 67. Explain why there are no nontrivial homomorphisms $\phi : \mathbb{Z}_7 \longrightarrow S_6$.

Problem 68. Let $\phi : G \longrightarrow H$ be a homomorphism and let $K = \text{Ker}(\phi)$. Let a be a fixed element of G. Prove that $aK = \{x \in G \mid \phi(x) = \phi(a)\}$.

Chapter 5

Normal Subgroups and Quotient Groups

This chapter explores an important and elegant abstraction: under certain conditions, the cosets of a group can be multiplied, making the set of cosets into a new group. The following computational example will help motivate this idea.

Problem 69. The group A_4 is a subgroup of S_4 with the following multiplication table.

$\circ$	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(134)	(243)	(142)	(124)	(143)	(132)	(234)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)	(123)	(134)	(243)	(142)	(124)	(143)	(132)	(234)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)	(243)	(142)	(123)	(134)	(234)	(132)	(143)	(124)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)	(142)	(243)	(134)	(123)	(143)	(124)	(234)	(132)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)	(134)	(123)	(142)	(243)	(132)	(234)	(124)	(143)
(123)	(123)	(134)	(243)	(142)	(132)	(234)	(124)	(143)	(13)(24)	(14)(23)	(1)	(12)(34)
(134)	(134)	(123)	(142)	(243)	(124)	(143)	(132)	(234)	(12)(34)	(1)	(14)(23)	(13)(24)
(243)	(243)	(142)	(123)	(134)	(143)	(124)	(234)	(132)	(14)(23)	(13)(42)	(12)(34)	(1)
(142)	(142)	(243)	(134)	(123)	(234)	(132)	(143)	(124)	(1)	(12)(34)	(13)(42)	(14)(23)
(124)	(124)	(143)	(132)	(234)	(14)(23)	(13)(24)	(12)(34)	(1)	(142)	(243)	(134)	(123)
(143)	(143)	(124)	(234)	(132)	(12)(34)	(1)	(14)(23)	(13)(24)	(123)	(134)	(243)	(142)
(132)	(132)	(234)	(124)	(143)	(1)	(12)(34)	(13)(24)	(14)(23)	(243)	(142)	(123)	(134)
(234)	(234)	(132)	(143)	(124)	(13)(24)	(14)(23)	(1)	(12)(34)	(134)	(123)	(142)	(243)

(a) The set $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ is a subgroup of A_4. Explain how this fact can easily be verified using the above table.

(b) Write out the cosets of V in A_4. (How big are they? How many of them are there?)

(c) Print out the above table, or make a screenshot and edit it in a drawing program. Assign a different color to each coset, and color each element in the table according to which coset it belongs to. What do you notice?

(d) Name the cosets X, Y, and Z. Is there an obvious multiplication that makes the set $\{X, Y, Z\}$ into a group? Draw a multiplication table.

(e) According to the "obvious" multiplication, if αV and βV are cosets, what coset is their product $(\alpha V)(\beta V)$?

Definition 5.1. Suppose that H is a subgroup of a group G and that a is some element of G. Then Ha denotes the set $\{ha \mid h \in H\}$, and is called a **right coset** of H in G.

Problem 70. Show, by giving an example of a group G, a subgroup H, and an element $a \in G$, that Ha can be different from aH. Is the statement, "If $x \in aH$ and $y \in bH$, then $xy \in (ab)H$" true, for all $a, b \in G$ in your example?

Problem 71. Let $\phi : G \longrightarrow H$ be a homomorphism of groups, and let K be the kernel of ϕ. Prove that $aK = Ka$ for any $a \in G$.

Problem 72. Let H be a subgroup of a group G with the property that $gH = Hg$ for all $g \in G$. Let $a, b \in G$. Prove that if $x \in aH$ and $y \in bH$, then $xy \in (ab)H$.

5.1 Normal Subgroups

Definition 5.2. If H is a subgroup of a group G, we say that H is a **normal subgroup** if it satisfies the condition that $gH = Hg$ for all $g \in G$. In this case, we write $H \lhd G$ and say "H is normal in G."

For example, Problem 69 establishes that $V \lhd A_4$. Problem 71 shows that kernels are normal subgroups. Of course, any subgroup of an abelian group is normal.

Problem 73. Let H be a subgroup of a group G. Prove that $H \lhd G$ if and only if the following condition holds: for all $h \in H$ and for all $g \in G$, ghg^{-1} is in H.

Definition 5.3. Suppose X and Y are subsets of a group G. The set $XY = \{xy \mid x \in X \text{ and } y \in Y\}$ is the **product** of the sets X and Y. This product is also called "set multiplication."

Problem 74. Suppose that H is a normal subgroup of a group G. Let $a, b \in G$ and define $X = aH$ and $Y = bH$. Prove that $XY = (ab)H$. (In other words, prove that the product of two cosets of a normal subgroup is another coset, and the representative of the product is the product of the representatives.)

Problem 75. Give an example to show that the hypothesis that $H \lhd G$ is needed in Problem 74. That is, find an example of a group and a subgroup where the product of two cosets fails to be a coset.

Notation: Let H be a subgroup of a group G. The set of all left cosets of H in G is denoted by G/H. In other words, $G/H = \{gH \mid g \in G\}$.

Problem 76. Let H be a normal subgroup of a group G. Prove that the set G/H is a group under coset multiplication.

Problem 77. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_6$, and let H be the cyclic subgroup generated by $(2,2)$. That is, $H = \langle (2,2) \rangle$. Notice that $H \lhd G$ since G is abelian. Give the group table for G/H. What well-known group is G/H isomorphic to?

5.2 Quotient Groups

Definition 5.4. The group G/H is called the **quotient group** of G by H, often pronounced "G mod H."

Problem 78. Let G be a group with $H \lhd G$. Prove or disprove: If G is cyclic, then G/H is cyclic.

Problem 79. Let G be a group with $H \lhd G$. Prove or disprove: If G is abelian, then G/H is abelian.

Problem 80. Let G be a group with $H \lhd G$. Prove or disprove: If G/H is abelian, then G is abelian.

Problem 81. In Problem 71, you proved that all kernels are normal subgroups. Prove that all normal subgroups are kernels. That is, given a group G with a normal subgroup $N \lhd G$, give a definition for a homomorphism $\phi : G \longrightarrow G/N$ such that $\text{Ker}(\phi) = N$, and show that the ϕ you define really is a homomorphism with this kernel.

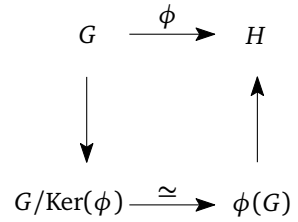
5.3 Isomorphism Theorems

Problem 82. Let $\phi : G \longrightarrow H$ be a homomorphism of groups, and let $K = \text{Ker}(\phi)$. In Problem 71, you proved that $K \lhd G$. Define a map $\psi : G/K \longrightarrow H$ by the formula $\psi(aK) = \phi(a)$. Prove that this map is **well defined**. That is, prove that it doesn't depend on the choice of representative for the coset aK: Show that if $aK = bK$, then $\psi(aK) = \psi(bK)$.

Problem 83. Prove that the map ψ defined in Problem 82 is a homomorphism.

Problem 84. Prove that the map ψ defined in Problem 82 is one-to-one. Conclude that if $\phi : G \longrightarrow H$ is a homomorphism of groups, then $G/\text{Ker}(\phi) \simeq \phi(G)$.

The result of Problem 84 is extremely important: henceforth, we shall refer to it as the **First Isomorphism Theorem.** Informally, it says that if you mod out by the kernel, you get a group that is isomorphic to the image. As a commutative diagram, the First Isomorphism Theorem is represented as follows.



The downward map is the projection $a \mapsto aK$, and the upward map is the inclusion $a \mapsto a$. The map labeled as an isomorphism is the map considered in Problem 84.

Problem 85. Let $G = \langle a \rangle$, where a has order n. Use the result of Problem 84 and the homomorphism of Problem 42 to prove that $\mathbb{Z}/\langle n \rangle \simeq G$.

Problem 85 establishes that there is only one finite cyclic group of every order, up to isomorphism.

Problem 86. Prove that if H and K are subgroups of a group G, and $K \lhd G$, then HK is a subgroup of G and $K \lhd HK$.

Problem 87. Let H and K be normal subgroups of a group G such that $H \cap K = \{e\}$. Prove that $hk = kh$ for all $k \in K$ and $h \in H$, and then show that the map $\phi : H \times K \longrightarrow HK$ defined by $\phi(h,k) = hk$ is an isomorphism.

Problem 88. Let H and K be subgroups of a group G with $K \lhd G$. Consider the map

$$\phi : H \longrightarrow (HK)/K$$

defined by $\phi(a) = aK$. Use this map and the First Isomorphism Theorem to prove that $(HK)/K \simeq H/(H \cap K)$.

Problem 89. Let H and K be normal subgroups of a group G with $K \leq H$. Prove that H/K is a subgroup of G/K, and furthermore, that $H/K \lhd G/K$.

Problem 90. Let H and K be normal subgroups of a group G with $K \leq H$. Consider the map

$$\phi : G \longrightarrow (G/K)/(H/K)$$

defined by $\phi(g) = (gK)(H/K)$. Use this map and the First Isomorphism Theorem to prove that $G/H \simeq (G/K)/(H/K)$.

Chapter 6

Rings and Ideals

To this point in the course, groups have been our main object of study, and we have established several key results about groups and learned some important techniques. Groups were defined with a somewhat minimal list of properties: associativity, identity, inverses. Given so few properties, it isn't surprising that most of the theorems we have been able to prove about groups have been fairly abstract.

Fortified with our newfound algebraic skills, we now move on to consider sets with additional properties, namely **rings** and **fields**. While the additional properties make these sets more complicated, the resulting theorems we will be able to prove will seem more like familiar facts about numbers. Historically, the ultimate goal of this study was to understand solutions of polynomial equations. While this remains our one of our goals (for this semester and the next), the resulting theory has been widely applied in other areas of mathematics.

6.1 Rings

Definition 6.1. A **ring** is a set R together with and addition operation $+$ and a multiplication operation $\cdot$ such that the following conditions hold.

1. $\langle R, + \rangle$ is an abelian group with identity $0 \in R$.
2. Multiplication is associative.
3. Multiplication distributes over addition: For all $a, b, c \in R$, $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$.

We say that a ring is **commutative** if $ab = ba$ for all $a, b \in R$. We call a ring a **ring with unity** if there is an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. In a ring with unity, the elements of a ring need not have multiplicative inverses. Elements that do have multiplicative inverses are called **units**.

Problem 91. Each set below is an example of a ring. For each example, determine whether it is commutative, whether it is a ring with unity, and if so, what the units are.

(a) $\mathbb{Z}$, the integers under addition and multiplication.

(b) $\mathbb{Z}_n$, the integers modulo n under addition and multiplication.

(c) $M_2(\mathbb{R})$, the set of 2×2 matrices with entries in $\mathbb{R}$. Addition is componentwise (add the corresponding entries), while multiplication is matrix multiplication.

(d) $\mathbb{Q}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \{0,1,2,\ldots\} \text{ and } a_i \in \mathbb{Q}\}$, the set of polynomials in the variable x with rational coefficients. Add and multiply polynomials like you do in high school algebra: "combine like terms" and "FOIL."

The next four problems establish some basic properties of rings that we will use routinely subsequent work. The proofs use only the above properties in the definition of a ring, but at the same time they can be slightly tricky.

Problem 92. Let R be a ring, and let $r \in R$. Prove that $0 \cdot r = 0 = r \cdot 0$.

Problem 93. Let R be a ring with unity, and let $r \in R$. Let -1 denote the additive inverse of 1. Prove that $-1 \cdot r = -r$. (That is, show that $-1 \cdot r$ is the additive inverse of r.)

Problem 94. Let R be a ring with unity, and let -1 denote the additive inverse of 1. Prove that $-1 \cdot -1 = 1$.

Problem 95. Let R be a ring with unity. Prove that if $1 = 0$, then $R = \{0\}$. (This ring is called the "zero ring.")

Just as groups have subgroups and group homomorphisms, rings have **subrings** and **ring homomorphisms**.

Problem 96. Without consulting any textbooks, the internet, or anyone else, make a guess at a definition of a **subring**. Find a nontrivial example of a subring that fits your definition.

Problem 97. Without consulting any textbooks, the internet, or anyone else, make a guess at a definition of a **ring homomorphism**. Find a nontrivial example of a ring homomorphism that fits your definition.

6.2 Homomorphisms and Kernels

As problems 94 and 95 illustrate, many of the definitions and examples associated with rings are natural extensions of those for groups. We won't necessarily restate them all, but here's one:

Definition 6.2. Suppose that R and S are rings, and that $\phi : R \longrightarrow S$ is a ring homomorphism. The **kernel** of ϕ, denoted by $\text{Ker}(\phi)$, is defined to be the set $\{r \in R \mid \phi(r) = 0\}$, where 0 is the additive identity of S.

Problem 98. Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients. Fix $a \in \mathbb{Z}$. It is easy to check that the map $\epsilon_a : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ defined by $\epsilon_a(p(x)) = p(a)$ is a ring homomorphism. Take this as given. The map ϵ_a is called the **evaluation homomorphism**.

(a) Compute the kernel of ϵ_0.

(b) Compute the kernel of ϵ_3.

Problem 99. Define $\phi : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$ by $\phi(n) = n^5$.

(a) Show that ϕ is a homomorphism of rings.

(b) Compute $\text{Ker}(\phi)$.

(c) Based on part (b), what do you conclude about ϕ?

Don't forget: If R is a ring, then $\langle R, + \rangle$ is an abelian group. So any theorems you know about groups apply to R as an abelian group under addition. Beware, however, that theorems about groups do not apply to the multiplication in a ring. You can appeal to group theory to prove facts about the addition in a ring, but you still may have some work to do to prove corresponding facts about the ring's multiplication.

Problem 100. Prove that the image of a ring homomorphism is a subring of the codomain. That is, if $\phi : R \longrightarrow S$ is a ring homomorphism, and $\phi(R) = \{\phi(r) \mid r \in R\}$, then $\phi(R)$ is a subring of S.

Problem 101. Let $\phi : R \longrightarrow S$ be a ring homomorphism, and let $K = \text{Ker}(\phi)$.

(a) Explain why $\langle K, + \rangle$ is a subgroup of $\langle R, + \rangle$.

(b) Prove that, if $k \in K$ and $r \in R$, then $kr \in K$ and $rk \in K$.

Explain how the result you just proved shows that K is a subring of R, and in fact is a stronger condition.

6.3 Ideals

In our study of groups, we found that the kernel K of a group homomorphism was a subgroup with an additional property: $gK = Kg$ for all group elements g. We defined a subgroup with this property to be a "normal" subgroup, and we saw how to use normal subgroups to construct quotient groups. In the same way, Problem 101 shows that the kernel of a ring homomorphism is a subring with some additional desirable properties; a set with these properties is called an **ideal**.

Definition 6.3. Let R be a ring. A subset $I \subseteq R$ is called an **ideal** of R if it satisfies the following properties.

- $\langle I, + \rangle$ is a subgroup of $\langle R, + \rangle$.
- For all $r \in R$ and $a \in I$, $ra \in I$ and $ar \in I$.

This definition defines a "two-sided ideal." It is possible to consider "left ideals" and "right ideals" which only satisfy one of the conditions $ra \in I$ and $ar \in I$, respectively. We will use the term "ideal" to refer to a two-sided ideal by default. Of course, in a commutative ring, you only have to check one of these conditions, since all ideals are two sided.

Problem 102. Let $\mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients.

(a) Let I be the subset of $\mathbb{Z}[x]$ consisting of polynomials with no constant term; that is, $I = \{a_1x + a_2x^2 + a_3x^3 + \cdots \mid a_i \in \mathbb{Z}\}$. Is I an ideal of $\mathbb{Z}[x]$? Prove or disprove.

(b) Let J be the subset of $\mathbb{Z}[x]$ consisting of polynomials with only even degree terms; that is, $J = \{a_0 + a_2x^2 + a_4x^4 + \cdots \mid a_i \in \mathbb{Z}\}$. Is J an ideal of $\mathbb{Z}[x]$? Prove or disprove.

Problem 103. Let R be the set of all real-valued functions on $\mathbb{R}$. That is, $R = \{f \mid f : \mathbb{R} \longrightarrow \mathbb{R}\}$. Such functions can be added and multiplied *pointwise:* If f and g are functions, then $f+g$ and $f \cdot g$ are functions defined by the formulas $(f+g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$. With these operations, R is a commutative ring.

(a) Prove that the set $I = \{f \in R \mid f(3) = 0\}$ is an ideal of R.

(b) Prove that the set $J = \{f \in R \mid f(3) = 1\}$ is not an ideal of R.

Problem 104. Let I be the subset of $M_2(\mathbb{R})$ consisting of matrices whose second column is zero. That is,

$$I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

Prove that I is a left ideal but it isn't a right ideal.

Problem 105. Let R be a commutative ring. Fix an element $a \in R$. Define the set $I \subseteq R$ by $I = \{ra \mid r \in R\}$. Prove that I is an ideal of R.

Definition: If R is a commutative ring and $a \in R$, then the set $\{ra \mid r \in R\}$ is called the **principal ideal** generated by a. This ideal is denoted by (a).

Problem 106. Find all (distinct) principal ideals of the ring $\mathbb{Z}_{12}$. Make a conjecture that generalizes this problem to $\mathbb{Z}_n$.

Chapter 7

Quotient Rings

Problem 107. Let I be an ideal of a ring R with unity. Prove that if $1 \in I$, then $I = R$. (In other words, prove that no proper ideal can contain the multiplicative identity.)

7.1 Cosets

Let I be an ideal of a ring R. For any $r \in R$, the set $r + I = \{r + i \mid i \in I\}$ is called a **coset** of I in R. The set of all cosets of I in R is denoted by R/I. If X and Y are subsets of a ring, we define "set addition" by letting the **sum** $X + Y$ be the set $\{x + y \mid x \in X \text{ and } y \in Y\}$. These definitions are identical to the corresponding definitions for a group; the only difference is that we are using additive notation instead of multiplicative notation.

Problem 108. Let I be an ideal of a ring R. Explain why $\langle I, + \rangle$ is a normal subgroup of $\langle R, + \rangle$. Which problems (that we have already proved) establish the following facts?

(a) The cosets of I in R partition R.

(b) The cosets of I in R all have the same size (or cardinality).

(c) If R is finite, then $|I|$ divides $|R|$.

(d) For all $r, s \in R$, $(r + I) + (s + I) = (r + s) + I$.

(e) The set R/I is a group under coset addition.

Problem 109. If X and Y are subsets of a ring, we could define "set multiplication" by letting the product XY be the set $\{xy \mid x \in X \text{ and } y \in Y\}$, as we did with groups. Unfortunately, this notion of multiplication fails on the cosets of a ring; give an example to show that it fails. In other words, find an example of a ring R, an ideal I, and cosets $a + I$ and $b + I$ such that the set $\{xy \mid x \in a + I \text{ and } y \in b + I\}$ is not a coset of I in R.

7.2 Constructing Quotient Rings

We now know that the set R/I is an abelian group; we would like to make it into a ring. However, in light of Problem 109, we need a different notion of what it means to multiply the cosets of a ring.

Definition 7.1. Let I be an ideal of a ring R, and let $a, b \in R$. The **coset product** of $a+I$ and $b+I$ is the coset $ab+I$. That is, $(a+I)(b+I) = ab+I$.

The next problem has you check that the coset product is well defined.

Problem 110. Let I be an ideal of a ring R, and let $a, b \in R$. Prove that the coset product does not depend on the choice of coset representatives. That is, prove that if $a+I = x+I$ and $b+I = y+I$, then $ab+I = xy+I$.

Problem 111. Prove that the set R/I is a ring under coset addition and coset multiplication.

7.3 Isomorphisms

Problem 112. The ring $\mathbb{Z}_2[x]/(x^2)$ has four elements. List them, and make an addition and multiplication table. Is this ring isomorphic to any other rings that you have seen before?

Problem 113. Review your solution to Problem 84 and the discussion at the beginning of Section 5.3. Then state and prove the First Isomorphism Theorem for rings.

Problem 114. Let R be a ring. Prove that the set $\{0\}$ is an ideal of R, and that $R/\{0\} \simeq R$.

Problem 115. Let R be a ring with unity. Prove that R has a subring that is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/(n)$ for some n.

Problem 116. Let $\mathbb{R}$ denote the ring of real numbers, let $\mathbb{R}[x]$ be the ring of polynomials with real coefficients, let (x^2+1) be the principal ideal generated by x^2+1, and let $\mathbb{C}$ denote the ring of complex numbers. Prove that $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$.

Chapter 8

Divisibility

In a ring, you can add, subtract, and multiply, but you can't divide, in general. However, there are certain abstract properties that approach the idea of division in a ring, and the extent to which a ring has these properties characterizes different types of rings. For simplicity in what follows, we will mainly consider the case of commutative rings with unity, though some of these ideas can be stated in more generality.

Definition 8.1. We say that a commutative ring R has the **cancellation property** if, for all $a, b, r \in R$ with $r \neq 0$, $ar = br$ implies $a = b$.

Definition 8.2. A nonzero element a in a commutative ring R is called a **divisor of zero** (or "zero divisor") if there exists some nonzero $r \in R$ such that $ar = 0$.

Problem 117. Let R be a commutative ring. Prove that, if R has the cancellation property, then R has no divisors of zero.

Problem 118. Let R be a commutative ring. Prove that, if R has no divisors of zero, then R has the cancellation property.

8.1 Integral Domains and Fields

Definition 8.3. A commutative ring with unity is called an **integral domain** if it satisfies the cancellation property (or equivalently, if it has no divisors of zero).

For example, $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_6$ isn't, because 2 is a zero divisor in $\mathbb{Z}_6$.

Definition 8.4. A commutative ring with unity is called a **field** if every nonzero element has a multiplicative inverse.

For example, $\mathbb{Q}$ is a field.

Problem 119. Prove that every field is an integral domain.

Problem 120. Prove that a field has no nontrivial proper ideals. Use this fact to explain why any nontrivial homomorphism $\phi : F \longrightarrow E$ of fields must be one-to-one.

Definition 8.5. Let $p(x) \in R[x]$ be the polynomial $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. The **degree** of $p(x)$ is the greatest integer k such that $a_k \neq 0$. Notation: $\deg(p) = k$.

Every polynomial has a degree, except for the zero polynomial. If $\deg(p) = 0$, then $p(x) = c$ for some nonzero constant $c \in R$.

Problem 121. Let R be an integral domain, and let $p(x), q(x) \in R[x]$ be nonzero polynomials. Prove that $\deg(pq) = \deg(p) + \deg(q)$. Use this fact to explain why $R[x]$ must also be an integral domain.

8.2 The Division Algorithm

When you learned the algorithm for long division in grade school, your teacher probably didn't mention the issues of *existence* and *uniqueness*. The process always terminated in a result, and every question only had one answer. These issues become more murky as we consider division of polynomials in a more abstract setting.

Theorem 8.6 (The Division Algorithm)**.** Let R be a commutative ring with unity, and let $f(x), g(x) \in R[x]$. Furthermore, suppose that

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

such that b_n is a unit in R. Then there are polynomials $q(x)$ and $r(x)$ in $R[x]$ (called the "quotient" and "remainder") such that

$$f(x) = q(x)g(x) + r(x)$$

and either $r(x) = 0$ or $\deg(r) < \deg(g)$.

Problem 122. Find polynomials $q(x)$ and $r(x)$ guaranteed by the division algorithm in $\mathbb{Z}[x]$ when $f(x) = 4x^3 + 3x^2 + 2x + 1$ and $g(x) = x^2 - x - 1$. Is the answer uniquely determined?

Problems 123–125 will lead you through a proof of the division algorithm. Let f, g, and R be as in the hypotheses of the theorem.

Problem 123. Let $X = \{f(x) - g(x)p(x) \mid p(x) \in R[x]\}$. Suppose that $0 \in X$. Show that the conclusion of the division algorithm (i.e., the last sentence) follows in this case.

Problem 124. Let X be as in Problem 123, and suppose that $0 \notin X$. Then every element of X has a degree. Let $r(x)$ be an element of minimal degree in X, and let $l = \deg(r)$. Then $f(x) = q(x)g(x) + r(x)$ for some $q(x) \in R[x]$, so we just need to show that $\deg(r) < \deg(g)$. Suppose to the contrary that $r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_lx^l$ with $c_l \neq 0$ and $l \geq n$. Show that the degree of the polynomial $r(x) - b_n^{-1}c_lx^{l-n}g(x)$ is less than l.

Problem 125. Let r and X be as in Problem 124, so $r(x) = f(x) - q(x)g(x)$. Substitute the formula $f(x) - q(x)g(x)$ for $r(x)$ to show that the polynomial $r(x) - b_n^{-1}c_lx^{l-n}g(x)$ is in X. Explain why this conclusion results in a contradiction.

Problem 126. Suppose, in addition to the hypotheses of the division algorithm, that R is an integral domain. Prove that the polynomials $q(x)$ and $r(x)$ are uniquely determined.

Problem 127. Show that if R is not an integral domain, then the uniqueness property of Problem 126 can fail. In particular, show that in $\mathbb{Z}_4[x]$, there are polynomials $q_1(x)$, $q_2(x)$, $r_1(x)$, $r_2(x)$, and $g(x)$ with $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$ and such that $q_1(x) \neq q_2(x)$ and $r_1(x) \neq r_2(x)$, but such that $q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$.

Problem 128. Let F be a field. Use the division algorithm to prove that every ideal of $F[x]$ is a principal ideal. That is, prove that if I is an ideal of $F[x]$, then there is some generating polynomial $p(x) \in F[x]$ such that $I = (p(x))$.

Terminology: The highest-degree term of a polynomial is called its **leading term**. A polynomial is **monic** if its leading term has coefficient 1.

Problem 129. Let F be a field, and let $(p(x))$ be an ideal of $F[x]$. Prove that $(p(x)) = (m(x))$ for some monic polynomial $m(x)$.

Problem 130. Suppose that R is a commutative ring with unity, and that the only ideals of R are R and $\{0\}$. Prove that R is a field. (This is the converse of Problem 120.)

Problem 131. Let F be a field. Prove that the only units of $F[x]$ are the nonzero constants. (More generally, if R is an integral domain, then any unit of $R[x]$ must have degree zero.)

Notation and Terminology: The set of all **multiples** of a in a ring R is denoted by $(a) = \{ra \mid r \in R\}$ and is called the **principal ideal generated by** a. Similarly, let $a_1, a_2, \ldots, a_n \in R$, a commutative ring. The set of all **linear combinations** of the a_i's is denoted by $(a_1, a_2, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$. The next problem will show that this set is also an ideal, called the ideal **generated** by $a_1, a_2, \ldots, a_n$.

Problem 132. Let $a_1, a_2, \ldots, a_n \in R$, a commutative ring. Prove that $(a_1, a_2, \ldots, a_n)$ is an ideal of R.

Problem 133. In $\mathbb{Z}[x]$, prove that $(x, 2) \neq (x + 2)$, $(x, 2) \neq (x)$, and $(x, 2) \neq (2)$.

8.3 Greatest Common Divisor

Definition 8.7. Let $a, b \in R$, a commutative ring. We say that a **divides** b, written $a \mid b$, if $ar = b$ for some $r \in R$. Alternatively, we also say that b is a **multiple** of a.

Problem 134. Let $a, b, c \in R$, a commutative ring. Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$. (This shows that the "|" relation is **transitive**.)

Problem 135. Let $a, b \in R$, an integral domain. Suppose that $a \mid b$ and $b \mid a$. Show that $a = ub$, where u is a unit in R.

Definition 8.8. Let R be an integral domain, and let $f(x), g(x) \in R[x]$. The **greatest common divisor** of $f(x)$ and $g(x)$ is a polynomial $d(x)$ that satisfies the following three properties.

1. $d(x) \mid f(x)$ and $d(x) \mid g(x)$.
2. If $c(x) \in R[x]$ is a polynomial such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$, then $c(x) \mid d(x)$.
3. $d(x)$ is monic.

In this case we write $d(x) = \gcd(f(x), g(x))$.

Warning: Some books omit condition 3 when giving this definition. We include it for convenience, because our focus later will be on polynomial rings over fields. You may notice some discrepancies when dealing with polynomial rings over rings that aren't fields. For example, according to our definition, in $\mathbb{Z}[x]$, $\gcd(3x+1, 6x+2) = 1$, while other definitions would allow $3x+1$ as the common divisor.

The use of the definite article "the" in this definition suggests that the greatest common divisor of two polynomials, if it exists, is uniquely determined. We still need to prove this assertion.

Problem 136. Let R be an integral domain, and let $f(x), g(x) \in R[x]$. Suppose that $f(x)$ and $g(x)$ have a greatest common divisor. Prove that it is unique.

Problem 137. Find the greatest common divisor of $x^2 - x - 6$ and $x^3 + x^2 - 3x - 2$ in $\mathbb{Q}[x]$.

Problem 138. Let $a(x), b(x), f(x), g(x) \in R[x]$, where R is an integral domain. Suppose that $a(x)f(x) + b(x)g(x) = 1$. Prove that $\gcd(f(x), g(x)) = 1$. (We say that such polynomials $f(x)$ and $g(x)$ are **relatively prime**.)

Theorem 8.9. Let F be a field, and let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$. Then there exist polynomials $a(x)$ and $b(x)$ in $F[x]$ such that

$$d(x) = a(x)f(x) + b(x)g(x)$$

is the greatest common divisor of $f(x)$ and $g(x)$.

Problem 139. The following statements establish a proof of the above theorem. Give a reason for each statement (cite previous problems, or give a brief justification).

(a) The set I of all linear combinations of $f(x)$ and $g(x)$ is an ideal of $F[x]$.

(b) The ideal I can be written as $I = (d(x))$ for some monic polynomial $d(x)$.

(c) There exist polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $d(x) = a(x)f(x) + b(x)g(x)$.

(d) The polynomial $d(x)$ is a common divisor of $f(x)$ and $g(x)$.

(e) If $c(x) \in F[x]$ is a polynomial such that $c(x) \mid f(x)$ and $c(x) \mid g(x)$, then $c(x) \mid d(x)$.

Problem 140. Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$, where F is a field. Let $I = (f(x))$. Suppose that $g(x) + I$ is a unit in the quotient ring $F[x]/I$. Prove that $f(x)$ and $g(x)$ are relatively prime.

Problem 141. Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$, where F is a field. Let $I=(f(x))$. Suppose that $f(x)$ and $g(x)$ are relatively prime. Prove that $g(x)+I$ is a unit in the ring $F[x]/I$.

Problem 142. Let $I=(x^2+x+1)$ in $\mathbb{Q}[x]$. Find the multiplicative inverse of $x+1+I$ in $\mathbb{Q}[x]/I$, or explain why no such inverse exists.

8.4 The Euclidean Algorithm

Euclid's Elements (300 BC) describe a procedure for computing the greatest common divisor of two numbers. Remarkably, this procedure works in polynomial rings over fields. In the next eight problems we will prove that it produces the greatest common divisor, and also that it gives the polynomials $a(x)$ and $b(x)$ to express $\gcd(f(x),g(x))$ as a linear combination $a(x)f(x)+b(x)g(x)$.

The idea is to repeat the division algorithm: Given polynomials $f(x)$ and $g(x)$ in $F[x]$, make the following sequence of calculations, continuing until the remainder of the division problem is zero.

$$\begin{aligned}
f(x) &= q_1(x)g(x)+r_1(x) && \text{where } \deg(r_1)<\deg(g)\\
g(x) &= q_2(x)r_1(x)+r_2(x) && \text{where } \deg(r_2)<\deg(r_1)\\
r_1(x) &= q_3(x)r_2(x)+r_3(x) && \text{where } \deg(r_3)<\deg(r_2)\\
r_2(x) &= q_4(x)r_3(x)+r_4(x) && \text{where } \deg(r_4)<\deg(r_3)\\
&\text{etc.}\ldots\\
r_{k-2}(x) &= q_k(x)r_{k-1}(x)+r_k(x) && \text{where } \deg(r_k)<\deg(r_{k-1})\\
r_{k-1}(x) &= q_{k+1}(x)r_k(x) && \text{where } r_{k+1}(x)=0
\end{aligned}$$

Problem 143. Apply the Euclidean algorithm to the polynomials $f(x)=x^4+x^3+x^2+x+1$ and $g(x)=x^2+1$ in $\mathbb{Q}[x]$. Why must this procedure always terminate?

Problem 144. Suppose that you carry out the Euclidean algorithm on some polynomials $f(x)$ and $g(x)$ in $F[x]$, a polynomial ring over a field, and that after three steps you find that $r_3(x)=u$, a constant polynomial in $F[x]$. Find polynomials $a(x)$ and $b(x)$ (in terms of u, the q_i's and the r_i's) such that $a(x)f(x)+b(x)g(x)=1$.

Problem 145. It is easy to check that the ring $\mathbb{Z}_3$ is a field. Carry out the Euclidean algorithm using the polynomials $f(x)=x^4+2x^3+2x+1$ and $g(x)=x^3+2x^2+x+2$ in $\mathbb{Z}_3[x]$.

Problems 146–149 will lead you through a proof that the Euclidean algorithm computes the greatest common divisor.

Problem 146. Let $I=(f(x),g(x))$ be the ideal of $F[x]$ consisting of all linear combinations of $f(x)$ and $g(x)$. Prove that, in the Euclidean algorithm, the remainders

$$r_1(x), r_2(x), r_3(x), \ldots, r_k(x)$$

are all elements of I.

Problem 147. Let $f(x)$ and $g(x)$ in $F[x]$, a polynomial ring over a field, and suppose that $c(x)$ is a common divisor of $f(x)$ and $g(x)$. Prove that $c(x)$ divides all of the remainders $r_1(x), r_2(x), r_3(x), \ldots, r_k(x)$ produced by the Euclidean algorithm.

Problem 148. Let $f(x)$ and $g(x)$ in $F[x]$, a polynomial ring over a field, and suppose that $r_1(x), r_2(x), r_3(x), \ldots, r_k(x)$ are the remainders produced by the Euclidean algorithm. Prove that $r_k(x)$ divides all of the other remainders.

Problem 149. Let $f(x)$ and $g(x)$ in $F[x]$, a polynomial ring over a field, and suppose that $r_k(x)$ is the last nonzero remainder produced by the Euclidean algorithm. Prove that $r_k(x) = ud(x)$, where $u \in F$ and $d(x) = \gcd(f(x), g(x))$.

Problem 150. Revisit Problem 145. Write the greatest common divisor of $f(x) = x^4 + 2x^3 + 2x + 1$ and $g(x) = x^3 + 2x^2 + x + 2$ in $\mathbb{Z}_3[x]$ as a linear combination of $f(x)$ and $g(x)$. Is $g(x) + (f(x))$ a unit in $\mathbb{Z}_3[x]/(f(x))$?

Chapter 9

Prime Ideals and Maximal Ideals

Historically, the development of modern abstract algebra was motivated by the study of the solutions to polynomial equations with integer coefficients. Solutions to quadratic equations were largely understood by Hindu mathematicians in the 7th century and Arab mathematicians in the 9th century, and special cases were known to the ancient Greeks and Babylonians. However, the general situation for higher-degree polynomials was not understood until the 19th century, and the important theorems rely on modern group theory as well as ring and field theory.

9.1 Roots of Polynomials

Definition 9.1. Let $p(x) \in R[x]$, where R is a commutative ring. An element $a \in R$ is called a **root** of $p(x)$ if $p(a) = 0$.

Problem 151. Let $f(x) \in F[x]$, where F is a field. Let $a \in F$, and let $r(x)$ be the remainder of the division algorithm applied to $f(x)$ and $g(x) = x - a$. Show that $r(x) = f(a)$.

Problem 152. Let $f(x) \in F[x]$, where F is a field, and let $a \in F$. Prove that a is a root of $f(x)$ if and only if $(x-a) \mid f(x)$.

Problem 153. Explain why a polynomial of degree n over a field F can have at most n distinct roots in F.

Problem 154. Find an example of a commutative ring in which the polynomial $x^2 - 1$ has more than two distinct roots.

Definition 9.2. Let F be a field. A non-constant polynomial $f(x) \in F[x]$ is called **reducible** over F if it can be factored into two polynomials of lower degree. That is, if there exist $p(x)$ and $q(x)$ with $\deg(p) < \deg(f)$ and $\deg(q) < \deg(f)$ and $f(x) = p(x)q(x)$. A non-constant polynomial is called **irreducible** over F if it is not reducible over F.

For example, $x^2 + 1$ is irreducible over $\mathbb{Q}$, but this polynomial is reducible over $\mathbb{C}$ since $x^2 + 1 = (x - i)(x + i)$. The polynomial $3x + 6$ is irreducible over $\mathbb{Q}$ (and over $\mathbb{C}$) because its only factorization is $3x + 6 = (3)(x + 2)$, but these factors are not both of lower degree.

Problem 155. Let F be a field, and let $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Prove that $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.

Problem 156. Give a counterexample to show that the conclusion of Problem 155 does not hold for polynomials of degree 4 (or higher), in general.

9.2 Prime Ideals

Proposition 30 of Book VII of Euclid's Elements says, "If two numbers, multiplied by one another make some number, and any prime number measures the product, then it also measures one of the original numbers." This basic number-theoretical property, known as *Euclid's Lemma,* can be stated in modern language as follows: If a prime number p divides a product ab, then $p \mid a$ or $p \mid b$. The next definition is an abstraction of this basic fact.

Definition 9.3. Let I be an ideal of a commutative ring R. Then I is a **prime ideal** if it is a proper ideal and, for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Problem 157. In the ring $\mathbb{Z}$, show that (7) is a prime ideal, but (6) is not a prime ideal.

Problem 158. Prove that if I is a prime ideal of a commutative ring R with unity, then R/I is an integral domain.

Problem 159. Let I be an ideal of a commutative ring R. Prove that if R/I is an integral domain, then I is a prime ideal.

Problem 160. Let F be a field, and suppose that $p(x) \in F[x]$ is a reducible polynomial. Show that $(p(x))$ is not a prime ideal of $F[x]$.

Problem 161. Prove *Euclid's lemma* for polynomials: Let F be a field, and suppose that $p(x) \in F[x]$ is irreducible. Prove that if $p(x) \mid a(x)b(x)$ for some $a(x), b(x) \in F[x]$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$. Hint: If $p(x) \nmid a(x)$, then $p(x)$ and $a(x)$ are relatively prime, since $p(x)$ is irreducible.

Problem 162. Let F be a field, and suppose that $p(x) \in F[x]$ is an irreducible polynomial. Show that $(p(x))$ is a prime ideal of $F[x]$.

9.3 Maximal Ideals

Problem 163. Let I be an ideal of a commutative ring R with unity, and suppose that X is an ideal of R/I. Let $J = \{r \in R \mid r + I \in X\}$. Prove that J is an ideal, that $I \subseteq J$, and that $X = J/I$. (In other words, prove that every ideal of a quotient of a ring R is a quotient of an ideal of R.)

Definition 9.4. If M is a proper ideal of a ring R with the property that there are no other ideals I such that $M \subsetneq I \subsetneq R$, then M is called a **maximal** ideal of R.

Problem 164. Let M be a ideal of a commutative ring R with unity. Prove that M is maximal if and only if R/M has no proper nontrivial ideals. (Use Problem 163.)

Problem 165. Let M be a ideal of a commutative ring R with unity. The following two facts are immediate corollaries of results we have already established. Prove each result, citing the appropriate problem(s) that establish each.

(a) M is maximal if and only if R/M is a field.

(b) If M is maximal, then M is prime.

9.4 Field Extensions

Finally, we are ready for our main goal: a method for constructing a field in which a given polynomial has a root, as well as a method for constructing finite fields.

Definition 9.5. A **principal ideal domain** (PID) is an integral domain in which every ideal is a principal ideal.

Recall that Problem 128 established that $F[x]$ is a principal ideal domain when F is a field.

Problem 166. Let R be a PID, and suppose that I and J are ideals with $I \subseteq J$, and that I is a nonzero prime ideal. Justify each step of the following argument.

(a) $I = (a)$ and $J = (b)$ for some nonzero $a, b \in R$.

(b) $a = rb$ for some $r \in R$.

(c) Either $r \in I$ or $b \in I$.

(d) If $b \in I$, then $I = J$.

(e) If $r \in I$, then $J = R$.

Problem 167. Explain why the previous problem establishes the following fact: In a PID, every nonzero prime ideal is maximal.

Problem 168. Prove that if F is a field and $p(x) \in F[x]$ is an irreducible polynomial, then $F[x]/(p(x))$ is a field.

Problem 169. Let $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

(a) Explain why $p(x)$ is irreducible.

(b) Explain why $\mathbb{Z}_2[x]/(p(x))$ is a field.

(c) Explain why every nonzero element of $\mathbb{Z}_2[x]/(p(x))$ can be written as $f(x)+(p(x))$, where $f(x)$ has degree at most 2.

(d) List the eight distinct elements of $\mathbb{Z}_2[x]/(p(x))$.

Problem 170. Find an element of $\mathbb{Q}[x]/(x^2-2)$ whose square is twice the multiplicative identity of $\mathbb{Q}[x]/(x^2-2)$.

Problem 170 illustrates the following result, which is an application of Problem 168. This problem uses the term **extension field**, which simply means a field of which a given field is a subset (up to isomorphism).

Problem 171. Given a field F and a non-constant polynomial $f(x) \in F[x]$, prove that there is an extension field E that contains a copy of F and a root of $f(x)$.

We therefore have an algebraic construction for a field E that extends a field F to contain a root α of any polynomial. If α is the root that E contains, we often write $E = F(\alpha)$ (pronounced "F adjoin α"), to remind ourselves of the above theorem.

Consider the case $F = \mathbb{Q}$. Using algebraic tools that we have developed, we can construct a huge family of irrational numbers: those that are solutions to polynomial equations with integer coefficients. These numbers are called the **algebraic** numbers. Irrational numbers that aren't algebraic are called **transcendental**. Examples include e and π. The existence of such numbers requires additional axioms beyond those of algebra.

In high school, you learned that the solutions of a quadratic equation could be written using square roots. It turns out that the solutions to cubic and quartic equations can be written using cube roots and fourth roots, but the formulas are very messy, compared to the quadratic formula. A natural question is whether the solutions to all polynomial equations can be written as formulas involving rational numbers, $+, -, \times, \div$ and nth roots, or **radicals**. In other words, can all algebraic numbers be expressed in terms of rational numbers and symbols like $\sqrt[n]{\ }$, possibly nested in complicated ways? The answer is "no," and the proof of this fact is one of the great achievements of modern mathematics, and is what inspired most of what we have studied this semester. The remaining chapters explore this theory, which ties together groups, fields, and symmetry in surprising and beautiful ways.

Chapter 10

Advanced Group Theory

While the techniques of modern algebra permeate almost every area of advanced mathematics, most of these ideas were originally motivated by questions arising from the study of polynomial equations. In the previous chapter, we developed the algebraic construction of a field in which a given polynomial has a root. In earlier chapters, we studied some of the basics of group theory. This semester, we will see how these two topics are connected; we will use group theory to study fields containing roots of polynomials. These notes will provide a path for you to discover what is now known as *Galois Theory*, named in honor of the French mathematician Évariste Galois (1811-1832).

10.1 Some Important Facts

We begin by reviewing some results that we have developed earlier in these notes.

Theorem 10.1 (Cyclic groups)**.**

1. Every subgroup of a cyclic group is cyclic.
2. If G is a group and $g \in G$ with $|g| = n < \infty$, then $|\langle g \rangle| = n$.
3. If G is a group and $g \in G$ with $|g| = n < \infty$, then $g^m = 1$ if and only if $n \mid m$.
4. If $G = \langle g \rangle$ with $|g| = n < \infty$, then $\langle g^k \rangle = G$ if and only if $(n,k) = 1$.

Theorem 10.2 (Lagrange)**.** The order of a subgroup of a finite group divides the order of the group.

Definition 10.3. A subgroup H of a group G is **normal** (written $H \lhd G$) if $gH = Hg$ for all $g \in G$.

Theorem 10.4 (Quotient Groups)**.** The set of left cosets of a subgroup H is a group G is denoted by G/H. Its size $|G/H|$ is denoted by $[G : H]$ and is called the **index** of H in G. If $H \lhd G$, then G/H is a group under the operation $(aH)(bH) = abH$.

Theorem 10.5 (First Isomorphism Theorem)**.** Let $\phi : G \longrightarrow G'$ be a group homomorphism. Then $G/\mathrm{Ker}(\phi) \simeq \phi(G)$ under the correspondence $a\,\mathrm{Ker}(\phi) \longleftrightarrow \phi(a)$. In particular, ϕ is one-to-one if and only if $\mathrm{Ker}(\phi) = \{e\}$.

Problem 172. Let H be a subgroup of a group G, and suppose that $[G:H]=2$. Prove that $H \lhd G$.

Problem 173. Let $\phi : \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_3$ be the homomorphism determined by $\phi(1)=2$. Illustrate the correspondence between cosets and group elements given by the First Isomorphism Theorem when it is applied to ϕ.

Problem 174. In the Introductory Activity at the beginning of these notes, you constructed a table of permutations corresponding to the elements of the group D_4. Show, by multiplying permutations, that all eight of these can be obtained by taking products of $(12)(34)$ and (13). That is, show that $D_4 \simeq \langle (12)(34), (13) \rangle$.

Problem 175. Use the group in Problem 174 to find groups K, H, and G such that $K \lhd H \lhd G$ but $K \not\lhd G$. (This shows that the normality relation is not transitive.)

Problem 176. A regular tetrahedron is a polyhedron with four faces, each of which is an equilateral triangle. Its symmetry group contains reflections and rotations. If the vertices of a regular tetrahedron are labeled 1, 2, 3, 4, show that this symmetry group is isomorphic to S_4. Find a small generating set, and do enough calculations to show that your generating set does in fact generate this group.

10.2 Group Actions

In the last few problems, we imagined each element of a symmetry group as performing an isometry of a geometric object. More algebraically, we represented these groups elements as permutations of the vertices of the object, and thought of the elements as bijective functions on a set of symbols. A **group action** is an abstraction of this technique.

Definition 10.6. A **group action** of a group G on a set X is a way of assigning a function $\phi_g : X \longrightarrow X$ to every group element $g \in G$, such that function composition of the ϕ_g's is compatible with group multiplication, i.e.,

$$\phi_e(x) = x \text{ and } \phi_{gh}(x) = \phi_g(\phi_h(x))$$

for all $g, h \in G$ and all $x \in X$, where e is the identity of G.

Since every element of a group is invertible, every ϕ_g is a bijective function.

Definition 10.7. If G acts on X, the set X_G of **fixed points** is the subset of points in X that are fixed by the action of G. In symbols,

$$X_G = \{x \in X \mid \phi_g(x) = x \text{ for all } g \in G\}.$$

Problem 177. Let G be a group and let $X = \{H \mid H \leq G\}$ be the set of all subgroups of G. For any $g \in G$, define $\phi_g(H) = gHg^{-1}$. Show that this definition describes a group action. Characterize the elements of X_G.

Problem 178. Let S be a set, and let $X = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_i \in S\}$ be the set of all n-tuples of elements of S. Show that the group $\mathbb{Z}_n$ acts on X by shifting: $\phi_k(x_0, x_1, \ldots, x_{n-1}) = (x_{0+k}, x_{1+k}, \ldots, x_{n-1+k})$, where the subscripts are taken modulo n.

Problem 179. Let H be a subgroup of a group G (not necessarily a normal subgroup). Let $X = \{gH \mid g \in G\}$ be the set of left cosets of H in G (not necessarily a group). Then H acts on X by left multiplication: $\phi_h(gH) = hgH$. Prove that $kH \in X_H$ if and only if $k^{-1}Hk = H$.

Definition 10.8. If a group G acts on a set X, the **orbit** Gx of an element $x \in X$ is the set of all elements that x can be sent to under the action. That is, $Gx = \{\phi_g(x) \mid g \in G\}$. (It is easy to see that the orbits form a partition of X.)

Definition 10.9. If a group G acts on a set X, the **isotropy subgroup** G_x is the subgroup of G consisting of all group elements whose action on x is trivial. For this reason, the isotropy subgroup is often called the **stabilizer** of x, and is denoted stab(x). In symbols,

$$G_x = \text{stab}(x) = \{g \in G \mid \phi_g(x) = x\}.$$

Theorem 10.10 (Orbit-Stabilizer)**.** If G acts on a set X, then the stabilizer stab(x) is a subgroup of G. Furthermore, $[G : \text{stab}(x)] = |Gx|$. (For finite groups, the size of the orbit times the size of the stabilizer equals the size of the group.)

Problem 180. For the symmetry group of the regular tetrahedron (Problem 176), compute the orbit and stabilizer of the vertex labeled 1. Check that the Orbit-Stabilizer theorem holds.

Problem 181. Let G be the group of rotational symmetries of a polyhedron, and suppose $|G| = p$ is prime. Apply the orbit-stabilizer theorem to infer something about the geometric structure of the polyhedron. Give examples.

10.3 The Class Equation

Problem 182. If G is a group that acts on a finite set X, explain why **class equation**

$$|X| = |X_G| + \sum |Gx_i|$$

holds, where the sum is taken over a set $\{x_i\}$ of representatives of orbits of size greater than 1. If in addition, $|G| = p^n$ for some prime p, explain why $|X| \equiv |X_G| \mod p$.

Problem 183. Consider the group $G = \langle (12)(34), (13) \rangle$ from Problem 174. Let $H = \langle (13) \rangle$. List all the left cosets of H in G. For the action, given in Problem 179, of H on $X = \{gH \mid g \in G\}$, compute the fixed point set X_H and all the orbits Hx_i, and show that the class equation holds.

Problem 184. Let G be a group of order np, where p is prime and $n \in \mathbb{N}$. Let

$$X = \{(g_0, g_1, g_2, \ldots, g_{p-1}) \mid g_i \in G \text{ and } g_0 g_1 g_2 \cdots g_{p-1} = e\}$$

be the set of all p-tuples of elements of G whose product is the identity. Compute $|X|$. By Problem 178, the group $\mathbb{Z}_p$ acts on X by shifting: $\phi_k(g_0, g_1, \ldots, g_{p-1}) = (g_{0+k}, g_{1+k}, \ldots, g_{p-1+k})$, where the subscripts are taken modulo p. Show that this action has a fixed point, then use the class equation to show that it must have more than one fixed point.

Problem 185. Use the result of the previous problem to prove that if p is a prime that divides $|G|$, then G has an element of order p.

Problem 186. Let H be a subgroup of G. Prove that the set $K = \{k \in G \mid kHk^{-1} = H\}$ is a subgroup of G, and that $H \lhd K$.

10.4 The Normalizer

Problem 187. The group K of Problem 186 is called the **normalizer** of H in G, written $N[H]$. Explain why $N[H]$ is the biggest subgroup of G that H is normal in.

Problem 188. Suppose that G is a finite group. Consider the action of a subgroup H on the set X of left cosets of H in G, given in Problem 179.

(a) Explain why $[G:H] = |X|$.

(b) Explain why $[N[H]:H] = |X_H|$.

Problem 189. Apply the mod-p class equation of Problem 182 to prove that if $|H| = p^i$ for some prime p, then $[G:H] \equiv [N[H]:H] \mod p$.

Problem 190. Suppose that H is a subgroup of a finite group G, with $|G| = p^m n$ for some m, n, and prime p. Suppose also that $|H| = p^i$. Prove that if $i < m$, then H is properly contained in its normalizer (i.e., $H \subsetneq N[H]$).

Problem 191. Investigate the above results for $G = S_4$ and $p = 2$. In particular, determine all the subgroups of S_4 that have order 2^i for some i. For each of these subgroups, determine its normalizer.

10.5 Sylow Theory

Theorem 10.11 (The Sylow Theorems)**.** Let G be a group of order $p^n m$, where p is prime and p does not divide m.

1. G has a subgroup of order p^n. (Such a subgroup is called a **Sylow p-subgroup**.)
2. Any two Sylow p-subgroups of G are conjugate.
3. The number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.

Proof of Part 1 (sketch). By Cauchy's Theorem, G has a subgroup H of order p. If $n = 1$, we are done. Otherwise, $H \subsetneq N[H]$ by Problem 190. Consider the usual projection map $\pi : N[H] \longrightarrow N[H]/H$. By Problem 189, $[N[H]:H] \equiv 0 \mod p$, and since $H \neq N[H]$, p must divide $|N[H]/H|$. So by Cauchy's Theorem, $N[H]/H$ has a subgroup K of order p. The preimage of K, $\pi^{-1}(K)$, is a subgroup of order p^2. Keep repeating this construction (inductively replacing H with $\pi^{-1}(K)$) to obtain a subgroup of order p^n. □

Problem 192. Prove Part 2 of Theorem 10.11 as follows: Let H and K be Sylow p-subgroups of G, and consider the action of H on the cosets of K in G: $\phi_h(gK) = hgK$. Apply Problem 182 to show that this action has a fixed point. Then show that if xK is this fixed point, then $x^{-1}Hx = K$.

Problem 193. Prove Part 3a of Theorem 10.11 (that the number of Sylow p-subgroups of G is congruent to 1 modulo p) as follows: Let K be a Sylow p-subgroup of G, and let X be the set of all Sylow p-subgroups of G. By Part 2, K acts on X by conjugation: $\phi_k(H) = kHk^{-1}$. Show that this action has only one fixed point, then apply Problem 182.

Problem 194. Prove Part 3b of Theorem 10.11 (that the number of Sylow p-subgroups of G divides $|G|$) as follows: By Part 2, G acts on the set X of Sylow subgroups by conjugation: $\phi_g(H) = gHg^{-1}$. Compute the number of orbits, and apply the Orbit-Stabilizer theorem.

Problem 195. Prove that every group of order 45 has a normal subgroup of order 9. Give a general condition for determining when a Sylow p-subgroup is a normal subgroup.

Definition 10.12. A group is called **simple** if it has no nontrivial proper normal subgroups.

Problem 196. Prove that there are no simple groups of order 56.

10.6 Finite Group Facts

The following lemma was proved as Problem 87.

Lemma 10.13. Let H and K be normal subgroups of a group G such that $H \cap K = \{e\}$. Then $hk = kh$ for all $k \in K$ and $h \in H$, and $HK \simeq H \times K$.

Problem 197. Let $|G| = pq$, p, q prime, $p < q$.

(a) Show that if $p \nmid (q-1)$, there are only two proper nontrivial subgroups of G. In this case, what can be said about the group G?

(b) Show that if $p \mid (q-1)$, the above is not necessarily true. (i.e., Find a counterexample with more than two proper nontrivial subgroups).

Definition 10.14. The **center** $Z(G)$ of a group G is the set of all elements of G that commute with all elements of the group. That is, $Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}$.

Problem 198. Prove that $Z(G)$ is a subgroup of G, and that $Z(G) \lhd G$.

Problem 199. Show, by giving nontrivial examples, that the center of a group can be the whole group, a proper nontrivial subgroup, or a trivial subgroup.

Problem 200. Consider the action of G on itself by congugation: $\phi_g(x) = gxg^{-1}$.

(a) Show that the fixed point set G_G of this action is the center $Z(G)$.

(b) Let p be prime and $n \in \mathbb{N}$. Use the class equation to show that every group of order p^n has nontrivial center.

Problem 201. Prove that every group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Chapter 11

Fields

A **field** is a set F together with operations $+$ and $\cdot$ that obey the commutative, associative, and distributive properties in the usual way. Every field contains the elements 0 and 1. Every element of a field has an additive inverse, and every element except 0 has a multiplicative inverse, so you can regard a field as having subtraction and division as well. Examples of fields include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the finite field $\mathbb{F}_p = \mathbb{Z}_p$ of order p, where p is prime.

11.1 Field Extensions

At the end of Chapter 9, we proved the following.

Theorem 11.1. Given a field F and a non-constant polynomial $f(x) \in F[x]$, there is an extension field E that contains a copy of F and a root of $f(x)$.

Proof (sketch). Let $p(x)$ be an irreducible factor of $f(x)$, and let $E = F[x]/(p(x))$. Then $\alpha = x + (p(x))$ is the root. □

We denote this extension field as $F(\alpha)$, pronounced "F adjoin α," and instead of doing computations with cosets, we simply use the symbols of F along with α, using the fact that α is a root of $p(x)$ when we simplify expressions. We can also adjoin more roots by repeating this construction, in which case we denote $(F(\alpha))(\beta)$ as $F(\alpha, \beta)$, and so on.

Our choice of notation suggests that $F(\alpha)$ is the smallest field containing both F and α, and indeed it is: Suppose that K is a field containing a field F and an element α such that $p(\alpha) = 0$, where $p(x)$ is an irreducible polynomial in $F[x]$. Define $\phi : F[x] \longrightarrow K$ by $\phi(f(x)) = f(\alpha)$. It is straightforward to check that ϕ a homomorphism with kernel $(p(x))$, so the First Isomorphism Theorem implies that K has a subfield isomorphic to $F[x]/(p(x))$, which we denote as $F(\alpha)$.

For example, if $F = \mathbb{R}$, $f(x) = p(x) = x^2 + 1$, and we use the symbol i for α, then the field E guaranteed by Theorem 11.1 is denoted as $\mathbb{R}(i)$, better known as the complex numbers $\mathbb{C}$.

Problem 202. Find an irreducible polynomial with rational coefficients that has $\sqrt{2+i}$ as a root. (Start with the equation $x = \sqrt{2+i}$, and manipulate it algebraically to obtain an equation with only rational coefficients.)

Problem 203. Find a quadratic polynomial with coefficients in $\mathbb{Q}(i)$ that has $\sqrt{2+i}$ as a root. Show that this polynomial is irreducible over $\mathbb{Q}(i)$ by showing that it has no roots in $\mathbb{Q}(i)$.

Problem 204. Compute the extension field $F(\alpha)$ guaranteed by Theorem 11.1 when $F=\mathbb{F}_2$ and α is a root of $f(x)=x^2+x+1$. List all the elements of the extension field $F(\alpha)$, and make addition and multiplication tables.

$+$	0	1	?	?
0				
1				
?				
?				

$\cdot$	0	1	?	?
0				
1				
?				
?				

Problem 205. Find some problems and/or theorems from last semester to explain why $\mathbb{Q}[x]/(x^4-9)$ is not a field. Find an element of this ring (written as a coset) that violates one of the defining properties of a field.

Problem 206. Suppose that $a_0, a_1, b_0, b_1 \in \mathbb{Q}$, and that $a_0 + b_0\sqrt{2} = a_1 + b_1\sqrt{2}$. Prove that $a_0 = a_1$ and $b_0 = b_1$.

Problem 207. Suppose that $m = a_0 + b_0\sqrt{2}$ and $n = a_1 + b_1\sqrt{2}$ for some $a_0, a_1, b_0, b_1 \in \mathbb{Q}$. Show that $m+n$, mn, and m/n can all be written in the form $a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.

11.2 Algebraic Extensions

Problem 208. Review your linear algebra notes (or look on the internet), and give brief, informal, definitions of the following terms, in your own words: *vector space*, *basis*, *linear independence*, *spanning set*, *dimension*. Use the terms of linear algebra to describe the results of Problems 206 and 207.

Definition 11.2. If E is an extension of a field F, then an element $\alpha \in E$ is called **algebraic** over F if it is the root of some polynomial in F. If every element of E is algebraic over F, then E is called an **algebraic extension** of F.

For example, $\sqrt{2}$ is algebraic over $\mathbb{Q}$, since it is a root of the polynomial x^2-2. If a number is not algebraic over $\mathbb{Q}$, it is called **transcendental**; π is an example. The next theorem recasts some results from Chapter 9 using the terms we have just introduced.

Theorem 11.3 (Algebraic Extension Theorem)**.** If α is algebraic over F, there is a unique irreducible monic polynomial $p(x) = \mathrm{Irr}(\alpha, F)$ in $F[x]$ such that $p(\alpha) = 0$. Furthermore, $F(\alpha)$ is a vector space over F with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, where $n = \deg(p)$.

Proof (sketch). The set of polynomials having α as a root is an ideal of $F[x]$, which is a PID, so $p(x)$ generates this ideal. The independence of the α^i's follows from the minimality of $p(x)$, since a dependence relation would yield a polynomial $q(x)$ such that $q(\alpha) = 0$ and $\deg(q) < \deg(p)$. Since the elements of $F[x]/(p(x))$ can be written as $f(x)+(p(x))$ with $\deg(f) < n$, the fact that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ spans $F(\alpha)$ follows from our identification of α with $x+(p(x))$. □

The polynomial $\text{Irr}(\alpha, F)$ is called the **minimal polynomial** for α over F. For example, $\text{Irr}(i, \mathbb{Q}) = x^2 + 1$.

Problem 209. Let $F(\alpha)$ be an algebraic extension of F, where $\text{Irr}(\alpha, F)$ has degree $n \geq 1$. Suppose that $\beta \in F(\alpha)$. Regard $F(\alpha)$ as a vector space over F. Find a result from linear algebra to explain why the set $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is a dependent set.

Problem 210. Let $\beta \in F(\alpha)$ as in the previous problem. Use that fact that $\{1, \beta, \beta^2, \ldots, \beta^n\}$ is a dependent set to explain why β must be algebraic over F. (Use Definition 11.2 in your explanation.) Find a relationship between the dimension of $F(\beta)$ as a vector space over F and the dimension of $F(\alpha)$ as a vector space over F.

Problem 211. Use the Algebraic Extension Theorem to give a quick proof of Problem 206.

11.3 Degree Multiplication

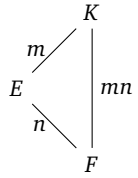
The Algebraic Extension Theorem tells us that the extension $F(\alpha)$ of a field F is a vector space over F. If E is an algebraic extension that is also a finite-dimensional vector space over F, we write $[E : F]$ to denote the dimension of E as a vector space over F.

A sequence of extensions $F \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_j$ is called a **tower** of extensions. We use this term because it is convenient to write towers of extensions as Hasse diagrams, with the bigger fields at the top. For example, the tower $F \subseteq E \subseteq K$ can be written as follows.

The following theorem extends the Algebraic Extension Theorem to tell us how to find dimensions and bases in towers of extensions.

Theorem 11.4 (Degree Multiplication Theorem)**.** Given a tower of algebraic extensions $F \subseteq E \subseteq K$, $[K : F] = [K : E][E : F]$. Furthermore, if $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis for E over F and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is a basis for K over E, then $\{\alpha_i \beta_j \mid i = 1, \ldots n, j = 1, \ldots, m\}$ is a basis for K over F.

If we write the degrees of each extension next to the corresponding lines in the Hasse diagram, Theorem 11.4 can be illustrated as follows.



Proof of Theorem 11.4 (sketch). The proof that the set $\{\alpha_i\beta_j\}$ spans K follows from the distributive property. The proof that this set is independent follows from the independence of $\{\alpha_i\}$ and $\{\beta_j\}$, using the factorization $\sum_{i,j} c_{ij}\alpha_i\beta_j = \sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j$. □

Problem 212. Check that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. It follows that $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. Use the Degree Multiplication Theorem to find a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$. Justify your answer.

Problem 213. Show that $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ by showing that $\sqrt{2}$ and $\sqrt{3}$ are in the first set and that $\sqrt{2}+\sqrt{3}$ is in the second.

Problem 214. Use Theorem 11.4 to find a basis for $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$ as a vector space over $\mathbb{Q}$. Justify your answer. Use this basis to find an element α such that $\mathbb{Q}(\alpha) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\right)$.

An extension E of a field F is called **simple** if $E = F(\alpha)$ for some element $\alpha \in E$. An extension E over F is called **finite** if E is a finite-dimensional vector space over F, that is, if $[E : F] < \infty$. It follows from Problems 209 and 210 that *all finite extensions are algebraic,* since any $\beta \in E$ will form a dependent set $\{1, \beta, \beta^2, \ldots, \beta^n\}$ for sufficiently large n.

Problem 215. Suppose that $[E : F] = p$, a prime number. Prove that E is a simple extension of F.

Problem 216. Let E be a finite extension of a field F, and let $p(x) \in F[x]$ be irreducible over F and have degree that is not a divisor of $[E : F]$. Show that $p(x)$ has no zeros in E.

11.4 Properties of Algebraic Extensions

Problem 217. Let E be an extension field of F. Let $\alpha \in E$ be algebraic of odd degree over F. Show that α^2 is algebraic of odd degree over F, and $F(\alpha) = F(\alpha^2)$.

Problem 218. Show that if F, E, and K are fields with $F \subseteq E \subseteq K$, then K is algebraic over F if and only if E is algebraic over F and K is algebraic over E.

Problem 219. Find all roots (in $\mathbb{C}$), of the polynomial $x^3 - 2$. Write these roots in the form $re^{i\theta}$ and also in the form $a + bi$.

Problem 220. Let α, β, and γ be the roots of $x^3 - 2$. Show that the fields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$, and $\mathbb{Q}(\gamma)$ are all different.

Problem 221. Recall that a map of vector spaces is determined by where it maps a basis. Furthermore, a map of vector spaces is an isomorphism of vector spaces if it maps a basis to a basis. For example, using the notation of Problem 220, the vector space map $\psi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\beta)$ defined by $\psi(1) = 1$, $\psi(\alpha) = \beta^2$, and $\psi(\alpha^2) = \beta$ is an isomorphism of vector spaces. Show that ψ is *not* an isomorphism of fields. (Hint: ψ respects addition. What doesn't it respect?)

Chapter 12

Isomorphisms of Fields

So far we have seen how roots of polynomials give rise to algebraic extensions of fields. We have also observed that groups can describe the symmetries of polyhedra by describing the possible permutations of their vertices. Analogously, we can understand the structure of field extensions by studying how certain groups permute the roots of associated polynomials.

12.1 Isomorphisms and Automorphisms

Problem 222. Let $\phi : F_1 \longrightarrow F_2$ be a homomorphism of fields. Show that $\phi(1) = 1$. Furthermore, show that if F_1 and F_2 both contain $\mathbb{Q}$, then $\phi(x) = x$ for all $x \in \mathbb{Q}$. (In other words, ϕ **fixes** $\mathbb{Q}$.)

Problem 223. Show that a homomorphism of fields must be injective if it isn't trivial.

Problem 224. Show (without using the upcoming theorem) that there are no nontrivial field homomorphisms $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$.

The preceding four problems illustrate that homomorphisms between fields are scarce. Isomorphisms are even rarer. The following theorem completely characterizes isomorphisms between simple extensions. The statement of the theorem is lengthy, but the proof is not deep. Rather, it simply makes official the observation that preservation of field operations severely restricts the number of possible isomorphisms.

Theorem 12.1. If α and β are roots of the same irreducible polynomial in $F[x]$, then the vector space map $F(\alpha) \longrightarrow F(\beta)$ defined by mapping the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ to the basis $\{1, \beta, \ldots, \beta^{n-1}\}$ is an isomorphism of fields. Conversely, this map can only be an isomorphism of fields if α and β are roots of the same irreducible polynomial. Furthermore, for any field E containing F, any map $F(\alpha) \longrightarrow E$ that fixes F must map α to a root of $\mathrm{Irr}(\alpha, F)$, and such a map is determined by the image of α.

Idea of proof. If α and β satisfy the same irreducible polynomial, then they satisfy the same relations under the field operations, so $\alpha \mapsto \beta$ will be homomorphic. Conversely, since homomorphisms preserve field operations, α and β must satisfy the same relations if $\alpha \mapsto \beta$. □

Problem 225. An isomorphism from a field F to itself is called an **automorphism** of F. Find three different automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, besides the identity. (Consider that $\mathbb{Q}(\sqrt{2},\sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{2})$, and apply Theorem 12.1.)

Problem 226. How many different automorphisms of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ are there? List them.

12.2 The Galois Group

Definition 12.2. Suppose that E is an extension of a field F. The **Galois group** of E over F, denoted $\mathrm{Gal}(E/F)$, is the set of all automorphisms of E that fix the elements of F.

Problem 227. Explain why $\mathrm{Gal}(E/F)$ is a group. If $F \subseteq E \subseteq K$ is a tower of fields, explain why $\mathrm{Gal}(K/E)$ is a subgroup of $\mathrm{Gal}(K/F)$.

Problem 228. Compute $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2}))$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. What familiar groups are these groups isomorphic to?

Problem 229. Assign convenient labels to the elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$ and make a group table. What familiar group is this group isomorphic to?

Problem 230. Let p be prime. It is a fact that the polynomial $x^{p-1}+x^{p-2}+\cdots+x+1$ is irreducible over $\mathbb{Q}$, and that its roots are $\omega, \omega^2, \ldots, \omega^{p-1}$, where $\omega = e^{2\pi i/p}$. Use these facts to determine the group $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$.

Problem 231. Suppose that $p(x) \in F[x]$ is a polynomial of degree n, and that its roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all distinct. Explain why $\mathrm{Gal}(F(\alpha_1,\alpha_2,\ldots,\alpha_n)/F)$ is isomorphic to a subgroup of S_n.

12.3 Extensions of Isomorphisms

Definition 12.3. Suppose that $\phi : F \longrightarrow F'$ is an isomorphism of fields, that E is an extension field of F, and that E' is an extension field of F'. An **extension** of the map ϕ is an isomorphism $\tilde{\phi} : E \longrightarrow E'$ such that $\tilde{\phi}(a) = \phi(a)$ for all $a \in F$. In other words, the following diagram commutes.

$$\begin{array}{ccc} E & \xrightarrow[\simeq]{\tilde{\phi}} & E' \\ \subseteq\uparrow & & \uparrow\subseteq \\ F & \xrightarrow[\simeq]{\phi} & F' \end{array}$$

Problem 232. Let α, β, γ be the roots of x^3-2, and let $E = \mathbb{Q}(\alpha,\beta,\gamma)$. Let $\omega = e^{2\pi i/3}$ and let $F = \mathbb{Q}(\omega)$, and notice that $F \subseteq E$. By Theorem 3.1, an automorphism $\phi : F \longrightarrow F$ is determined by setting $\phi(\omega) = \omega^2$. Find three different extensions of ϕ to automorphisms $E \longrightarrow E$. Are there any elements of $\mathrm{Gal}(E/\mathbb{Q})$ that are *not* extensions of ϕ?

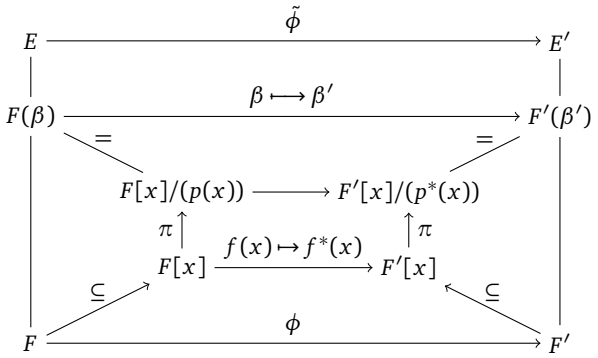
Definition 12.4. A **splitting field** of a polynomial $f(x) \in F[x]$ is an extension field E of F in which $f(x)$ factors into linear factors, and such that $f(x)$ does not factor into linear factors in any proper subfield of E.

Problem 233. Find a splitting field E of $x^4 - 5$ over $\mathbb{Q}$, and compute $[E : \mathbb{Q}]$.

Problem 234. Let $F = \mathbb{Q}(\sqrt{5})$ and let $E = \mathbb{Q}(i\sqrt[4]{5})$, and notice that $F \subseteq E$. By Theorem 3.1, an automorphism $\phi : F \longrightarrow F$ is determined by setting $\phi(\sqrt{5}) = -\sqrt{5}$. Show that ϕ cannot be extended to an automorphism $E \longrightarrow E$.

Theorem 12.5. Let $\phi : F \longrightarrow F'$ be an isomorphism of fields, and let $f(x) \in F[x]$. Suppose that $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. Let $f^*(x) \in F'[x]$ be the polynomial given by $f^*(x) = \phi(a_0) + \phi(a_1)x + \phi(a_2)x^2 + \cdots + \phi(a_n)x^n$. If E is a splitting field of $f(x)$ and E' is a splitting field of $f^*(x)$, then there is an isomorphism $\tilde{\phi} : E \longrightarrow E'$ extending ϕ.

Proof (sketch). The following commutative diagram illustrates how the extension $\tilde{\phi}$ is built by induction on $[E : F]$. The towers on the left and right exist because E and E' are splitting fields.



If $[E : F] = 1$, there is nothing to extend. Suppose as inductive hypotheses that an extension $\tilde{\phi}$ exists for field extensions of degree less than $[E : F]$. For the inductive step, let β be a root of an irreducible factor $p(x)$ of $f(x)$, and let π be the usual projection. The map $\phi : F \longrightarrow F'$ extends to a map $F(\beta) \longrightarrow F'(\beta')$ by applying Theorem 11.1. We then apply the inductive hypotheses to extend this map to $\tilde{\phi} : E \longrightarrow E'$. □

Problem 235. Explain why the result of Problem 234 does not contradict Theorem 12.5. What does Problem 232 tell you about the uniqueness of the extension guaranteed by Theorem 12.5?

Problem 236. Suppose that E and E' are two splitting fields of the same polynomial $f(x) \in F[x]$. Prove that there is an isomorphism $E \longrightarrow E'$ that fixes F.

12.4 Separability

Definition 12.6. An irreducible polynomial is called **separable** if all its roots have multiplicity one. A polynomial is **separable** if all of its irreducible factors are.

Theorem 12.7. Let ϕ, $f(x)$, F, F', E, and E' be as in Theorem 12.5. If $f(x)$ is separable, then there are exactly $[E : F]$ extensions of ϕ to isomorphisms $E \longrightarrow E'$.

Proof (sketch). The idea is to piggyback onto the inductive argument in the proof of Theorem 12.5. By Theorem 11.3, $\deg(p) = [F(\beta) : F] = n$. Since $f(x)$ is separable, so is $p(x)$, so there are n distinct choices for β in the inductive step. Thus, at each stage, there are $[F(\beta) : F]$ different ways to extend ϕ to a map $F(\beta) \longrightarrow F(\beta')$. Inductively, the total number of extensions is $[E : F(\beta)][F(\beta) : F] = [E : F]$, by Theorem 11.4. □

Problem 237. Suppose that E is the splitting field of $f(x) \in F[x]$, and that $f(x)$ is separable. Explain why $|G(E/F)| = [E : F]$.

Problem 238. Let E be the splitting field of $x^3 - 1$ and let K be the splitting field of $x^3 - 2$. Compute $\mathrm{Gal}(E/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$, up to isomorphism. (Instead of computing all of the automorphisms, use Problem 237 and Problem 231 and your knowledge of groups.)

Definition 12.8. If $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ is a polynomial over a field F, the **formal derivative** is the polynomial $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$.

This definition is algebraic, not analytical; the field F need only satisfy the algebraic field axioms, not the axioms of the real or complex numbers. It is easy to prove, using only algebra, that the formal derivative has many of the familiar properties of the calculus derivative, including linearity, the product rule, and the chain rule.

Problem 239. Let $f(x) \in F[x]$, let E be a splitting field of F, and suppose that $\alpha \in E$ is a repeated root of $f(x)$, so we can write $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in E[x]$. Use the product and chain rules to show that $f'(\alpha) = 0$.

Problem 240. Let $f(x) \in F[x]$ be irreducible, and suppose that $f'(x) \neq 0$. Explain why there must exist $g(x), h(x) \in F[x]$ such that $f(x)g(x) + f'(x)h(x) = 1$.

Problem 241. Explain why an irreducible polynomial must be separable if its derivative is nonzero. Conclude that, in particular, all polynomials over $\mathbb{Q}$ (and over extensions of $\mathbb{Q}$) are separable.

Chapter 13

Galois Theory

13.1 Towers and Galois Groups

Definition 13.1. Suppose that $\phi : K \longrightarrow K'$ is a homomorphism of fields, and that E is a subfield of K. The **restriction** $\phi|_E$ of ϕ to the domain E is the map $\phi|_E : E \longrightarrow K'$ defined by $\phi|_E(a) = \phi(a)$ for all $a \in E$.

For Problems 242–245, let $F \subseteq E \subseteq K$ be a tower of fields, where K and E are splitting fields of polynomials $g(x)$ and $f(x)$, respectively, over F, and consider the following map Φ:

$$\begin{aligned} \mathrm{Gal}(K/F) &\xrightarrow{\Phi} \mathrm{Gal}(E/F) \\ \sigma &\longmapsto \sigma|_E \end{aligned}$$

where $\sigma|_E$ is the restriction of σ to the domain E.

Problem 242. Show that Φ really does take values in $\mathrm{Gal}(E/F)$. (Does the restriction of σ really map into E?) Does your explanation use the hypotheses that E and K are splitting fields?

Problem 243. Check that Φ is a homomorphism of groups, and compute its kernel. Does your explanation use the hypotheses that E and K are splitting fields?

Problem 244. Show that Φ is onto. Does your explanation use the hypotheses that E and K are splitting fields?

Problem 245. Apply the First Isomorphism Theorem to Φ and state a theorem about the Galois groups of the tower $F \subseteq E \subseteq K$.

Problem 246. Let K be the splitting field of $x^4 - x^2 - 2$ over $F = \mathbb{Q}$, and let E be the splitting field of $x^2 - 2$ over $\mathbb{Q}$. Compute the groups $\mathrm{Gal}(K/F)$, $\mathrm{Gal}(E/F)$, and $\mathrm{Gal}(K/E)$, and illustrate the theorem from Problem 245.

13.2 The Fixed Field

The Galois group is a particular group of automorphisms of a field; namely, it is the group of automorphisms of the field that fix some subfield. Given a field extension, you can, in principle,

compute its Galois group. In this section, we consider the reverse: under certain circumstances, given a group, you can find an extension whose Galois group is the given group.

More precisely, let $\mathrm{Aut}(K)$ be the group of all automorphisms of some field K. Suppose that H is a subgroup of $\mathrm{Aut}(K)$. Consider the following set:

$$K_H = \{a \in K \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

Problem 247. Prove that K_H is a subfield of K. This field is called the **fixed field** of H.

Problem 248. Refer to Problems 219, 220, and 234. Let $K = \mathbb{Q}(\alpha, \beta, \gamma)$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. If we identify the symbols $1, 2, 3$ with the roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, respectively, then $\mathrm{Gal}(K/\mathbb{Q}) = S_3$. For each subgroup H of S_3, compute the fixed field K_H. (There are 6 subgroups of S_3: one of order 3, three of order 2, S_3 itself, and the trivial subgroup. Compute all six fixed fields.)

Problem 249. Let K be the splitting field of $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$. Problem 230 says that $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic of order 4. Therefore there is a unique subgroup $H \leq \mathrm{Gal}(K/\mathbb{Q})$ of order 2. Compute K_H.

Problem 250. Consider all the subgroups and fixed fields you found in Problems 248 and 249. Is it always true that $\mathrm{Gal}(K/K_H) = H$? Check to see if this equation holds for your examples. Make a conjecture.

Problem 251. Consider all the subgroups and fixed fields you found in Problems 248 and 249. Is it always true that $K_{\mathrm{Gal}(K/E)} = E$? Check to see if this equation holds for your examples. Make a conjecture.

13.3 The Galois Correspondence

We now have all the pieces in place to state the Fundamental Theorem of Galois Theory. In fact, we have proved many of the key parts of this theorem already. First, we make a definition, which contains several important facts.

Definition 13.2. An extension K over F is called a **Galois extension** (or a **normal extension**) if it satisfies any of the following (equivalent) properties:

1. $K_{\mathrm{Gal}(K/F)} = F$.
2. Every irreducible $p(x) \in F[x]$ that has a root in K is separable and splits in K.
3. K is a splitting field of a separable polynomial $f(x) \in F[x]$.

Theorem 13.3. Let K/F be a Galois extension, and let $G = \mathrm{Gal}(K/F)$. Then there is a one-to-one correspondence of intermediate fields between K and F and subgroups of G that preserves analogous structure. This map of sets is called the **Galois correspondence.** More precisely, let $\mathfrak{S}$ be the set of all subgroups of G and let $\mathfrak{F}$ be the set of all intermediate fields between K and F.

1. The Galois correspondence is the following bijection Γ of sets:

$$\begin{aligned} \mathfrak{S} &\xrightarrow{\Gamma} \mathfrak{F} \\ H &\longmapsto K_H \end{aligned}$$

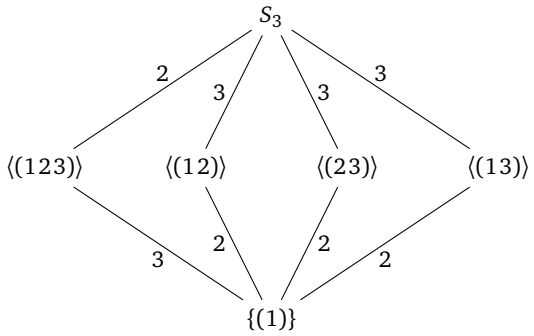
2. The inverse Γ^{-1} of the above map is:

$$\begin{aligned} \mathfrak{F} &\xrightarrow{\Gamma^{-1}} \mathfrak{S} \\ E &\longmapsto \mathrm{Gal}(K/E) \end{aligned}$$

3. Under the correspondence Γ, the lattice of subgroups is the reverse of the lattice of subfields.
4. The index of each subgroup equals the degree of the corresponding extension. In other words,
$$[G : \mathrm{Gal}(K/E)] = [E : F] \text{ and } [G : H] = [K_H : F]$$
5. An extension E over F is Galois if and only if $\mathrm{Gal}(K/E) \lhd G$.

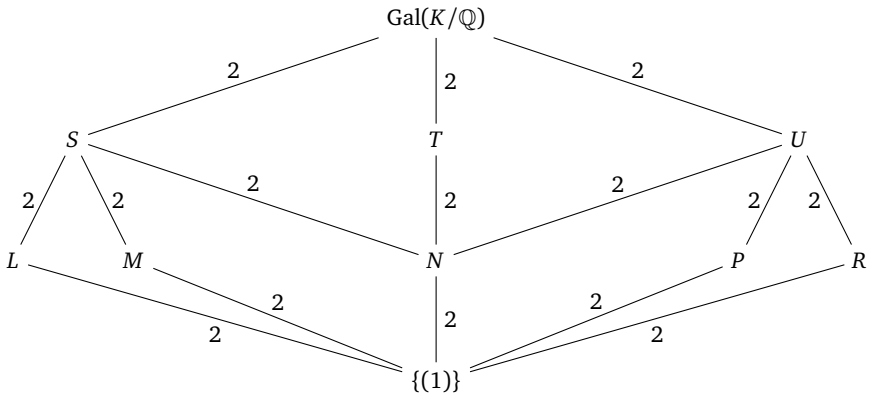
The Galois Correspondence gives a technique for finding all possible intermediate fields between a field F and a splitting field over F. Typically, one calculates $\mathrm{Gal}(K/F)$, uses known facts from group theory to construct the lattice of subgroups of $\mathrm{Gal}(K/F)$, and then uses the correspondence to find the lattice of subfields. The lattice of subfields will have the same shape as the lattice of subgroups, only upside down.

Problem 252. Let K be the splitting field of x^3-2 over $\mathbb{Q}$. In Problem 248, we found that $\mathrm{Gal}(K/\mathbb{Q}) = S_3$, where the letters $1,2,3$ are identified with the roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, respectively. The lattice of subgroups of S_3 is given by the following diagram. Compute the corresponding lattice of subfields.



Problem 253. Let K be the splitting field of x^4-2 over $\mathbb{Q}$. Compute $\mathrm{Gal}(K/\mathbb{Q})$ and represent it as a subgroup of S_4.

Problem 254. Let K be as in Problem 253. The lattice of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ is shown below. Identify each subgroup.



Problem 255. Let K be as in Problem 253. Draw its lattice of subfields.

Problem 256. Let K be the splitting field of x^5-1 (see Problem 249). Compute the lattice of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and the lattice of subfields of K.

13.4 Radical Extensions

The Galois correspondence is a truly elegant theorem on its own, but its development was a means to understand the solutions to polynomial equations. At issue is the question of whether the roots of all polynomial equations can be written in terms of field operations and radicals ($\sqrt{}$, $\sqrt[3]{}$, etc). By the time of Galois, mathematicians already had equations for solving general cubic and quartic equations (and of course, quadratic equations), in terms of radicals. The quintic case, and beyond, was one of the largest open problems of the day.

To frame this problem in the language of modern algebra, we define a **radical extension** as one whose elements can all be written in terms of radicals.

Definition 13.4. A **radical extension** of a field F is an extension $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ such that there exist natural numbers $k_1,k_2,\ldots,k_n$ such that $\alpha_i^{k_i}\in F(\alpha_1,\alpha_2,\ldots,\alpha_{i-1})$ for $i=2,\ldots n$, and $\alpha_1^{k_1}\in F$. A polynomial in $F[x]$ is **solvable by radicals** if its splitting field over F is contained in some radical extension of F.

Problem 257. Show that the splitting field of x^n-1 over $\mathbb{Q}$ is a radical extension (and therefore that this polynomial is solvable by radicals), for any $n\in\mathbb{N}$.

Problem 258. Show that the splitting field of x^6+4x^3-6 over $\mathbb{Q}$ is a radical extension.

Problem 259. Let K be the splitting field of x^n-a over $\mathbb{Q}$. Suppose that $F\subseteq K$ is an extension of $\mathbb{Q}$ that contains $\omega=e^{2\pi i/n}$, a primitive nth root of unity. Show that $\mathrm{Gal}(K/F)$ is abelian.

Problem 260. Let F be an extension of $\mathbb{Q}$ that does not contain $\omega=e^{2\pi i/n}$. Show that $\mathrm{Gal}(F(\omega)/F)$ is abelian.

Problem 261. Let F be an extension of $\mathbb{Q}$ that does not contain $\omega = e^{2\pi i/n}$. Let K be the splitting field of $x^n - a$ over F. Show that $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/F(\omega))$ is abelian. Give an example to show that $\mathrm{Gal}(K/F)$ need not be abelian.

13.5 Solvability by Radicals

Definition 13.5. A group G is **solvable** if there exists a sequence of groups

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

such that H_{i+1}/H_i is abelian, for $i = 0, 1, \ldots, n-1$.

Problem 262. Show that S_3 and D_4 are solvable.

Problem 263. Show that S_4 is solvable.

Problem 264. Let F be an extension of $\mathbb{Q}$, and let K be the splitting field of $x^n - a$ over F. Use the results of Problems 259–261 to show that $\mathrm{Gal}(K/F)$ is solvable.

Problem 264, along with an induction argument, proves the "only if" direction of the following great theorem of Galois.

Theorem 13.6 (Galois)**.** Let F be an extension of $\mathbb{Q}$, let $f(x) \in F[x]$, and let K be the splitting field of $f(x)$ over F. Then $f(x)$ is solvable by radicals if and only if $\mathrm{Gal}(K/F)$ is a solvable group.

Problem 265. Use Theorem 13.6 and your above examples of solvable groups to prove that every polynomial of degree 2, 3, or 4 over $\mathbb{Q}$ is solvable by radicals.

Problem 266. There are lots of ways to prove that A_5 is a simple group (i.e., that it has no proper, nontrivial normal subgroups). Search the internet for a proof that A_5 is simple, and give a "bullet-point" summary of the argument in your own words.

13.6 Insolvability of the Quintic

There are formulas, involving only field operations and radicals, that give general solutions to polynomial equations of degree 2, 3 and 4 over $\mathbb{Q}$. In degree 2, we have the familiar quadratic formula for solving the equation $ax^2 + bx + c = 0$.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

There are also radical formulas for solving equations of the form $ax^3 + bx^2 + cx + d = 0$ and $ax^4 + bx^3 + cx^2 + dx + e = 0$, but they are extremely long and complicated.

The following problems give an example of a quintic polynomial with rational coefficients that is not solvable by radicals. Note that the existence of such a polynomial proves that there can be no general radical formula for solving quintic polynomials.

Problem 267. By Problem 172, we know that $A_5 \lhd S_5$. Suppose that H is any other proper, nontrivial, normal subgroup of S_5. Use Lemma 10.13 to show that $|H| = 2$. Then show that no such H can exist. Conclude that S_5 is not a solvable group.

Problem 268. Suppose that $f(x) \in \mathbb{Q}[x]$ is has degree 5 and is irreducible. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Explain why $\text{Gal}(K/\mathbb{Q})$ must contain a 5-cycle.

Problem 269. By graphing, check that $x^5 - 4x + 2$ has exactly three real roots. Explain why it must therefore have two complex roots, $a + bi$ and $a - bi$. Use these observations to conclude that if K is the splitting field of $x^5 - 4x + 2$ over $\mathbb{Q}$, then $\text{Gal}(K/\mathbb{Q})$ must contain a 2-cycle.

Problem 270. Prove that no proper subgroup of S_5 can contain both a 5-cycle and a 2-cycle.

Problem 271. The polynomial $x^5 - 4x + 2$ is irreducible over $\mathbb{Q}$. Explain why $x^5 - 4x + 2$ is not solvable by radicals.

13.7 The Fundamental Theorem of Algebra

The next ten problems will develop an algebraic proof of the following theorem.

Theorem 13.7 (Fundamental Theorem of Algebra)**.** The field $\mathbb{C}$ of complex numbers contains all the roots of any polynomial in $\mathbb{R}[x]$.

Since, for any $f(x) \in \mathbb{C}[x]$, the real polynomial $f(x)\overline{f(x)}$ has a root whenever $f(x)$ does, Theorem 13.7 is equivalent to statement that $\mathbb{C}$ is an algebraically closed field. There is an easy proof of this theorem using Liouville's Theorem from complex analysis, but we are going to construct an algebraic proof using the Galois correspondence (Theorem 3.11). Of course, we can't even define the real numbers without assuming additional axioms. For our proof, the following axiom (a weak form of the intermediate value theorem) will suffice.

Axiom 13.8. Let $p(x) \in \mathbb{R}[x]$ be a polynomial with real coefficients. If there are real numbers $a, b \in \mathbb{R}$ such that $p(a) > 0$ and $p(b) < 0$, then $p(x)$ has a root in $\mathbb{R}$.

Problem 272. Use Axiom 13.8 to prove that every positive real number $r > 0$ has a real square root. (Consider $p(x) = x^2 - r$.)

Problem 273. Explain why $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$. Use this fact and the quadratic formula to prove that, for any $a, b \in \mathbb{R}$, the equation $(x + iy)^2 = a + bi$ has a solution where both x and y are real numbers. (Hence every complex number has a square root in $\mathbb{C}$.)

Problem 274. Use Problem 273 to prove that there are no extension fields E of $\mathbb{C}$ such that $[E : \mathbb{C}] = 2$.

Problem 275. Let $p(x) \in \mathbb{R}[x]$ be a polynomial of odd degree. Use Axiom 13.8 to prove that $p(x)$ has a real root.

Problem 276. Use Problem 275 to prove that there are no extension fields E of $\mathbb{R}$ such that $[E:\mathbb{R}]$ is odd.

Problem 277. Let E be a splitting field over $\mathbb{R}$ such that $[E:\mathbb{R}] = 2^n m$, where m is odd. Use Problem 237, Sylow Theorem I, and Problem 276 to prove that $m = 1$.

Problem 278. Let $p(x) \in \mathbb{R}[x]$, and let E be the splitting field of $(x^2+1)p(x)$ over $\mathbb{R}$. Notice that E contains $\mathbb{C}$. Use Problem 277 to prove that $|\mathrm{Gal}(E/\mathbb{C})| = 2^k$ for some $k \geq 0$.

Problem 279. Let G be a group of order 2^k, for some $k \geq 1$. Recall (Problem 200) that its center $Z(G)$ is nontrivial. Use an induction argument similar to the one used in the proof of Sylow I (Section 10.5) to show that G has a subgroup of index 2.

Problem 280. Let $p(x)$, E, and k be as in Problem 278. Use Theorem 13.3, Problem 279 and Problem 274 to prove that $k = 0$.

Problem 281. Explain how the preceding problems constitute a proof of Theorem 13.7.