Introductory Abstract Algebra

Margaret L. Morrow

SUNY Plattsburgh
# Contents

Acknowledgements iii

To the Instructor iv

0.1 The context. iv
0.2 Prerequisite for this course. v
0.3 Class organization and assessment. vi
0.4 Dealing with different backgrounds and inclinations. vi
0.5 The problems. vii

Introductory worksheet: some useful examples 1

1 Introduction to groups 4

2 New groups from old 9
  2.1 Direct products of groups: 10
  2.2 Subgroups 10
  2.3 Some more examples of groups 11
  2.4 Some very special subgroups of an arbitrary group 12

3 More on cyclic groups. 15

4 Homomorphisms and Isomorphisms 19

5 Cosets: first ideas and applications 23

6 Normal subgroups and quotient groups 26

Notes to the Instructor 29
Acknowledgements

I am indebted to the Educational Advancement Foundation for providing me with the opportunity to explore Inquiry Based Learning, first at a Summer Workshop, and then at several summer IBL conferences. I am deeply grateful to Ed Parker and Stan Yoshinobu for their guidance and wise advice, both at the Summer workshop, and over the intervening years. I am also indebted to the students in my IBL abstract algebra classes, who have with patience, persistence, and good humor taken the leap into independent learning. Finally, sincere thanks to the referee of this paper, and to the editor, for their many very helpful suggestions.
To the Instructor

0.1 The context.

These notes were developed for teaching a one-semester Introduction to Abstract Algebra course using an Inquiry Based Learning (IBL) approach. I began developing the notes during a summer 2007 IBL workshop.

Our Introduction to Abstract Algebra course, MAT 301, is a core course in our Mathematics Major. All mathematics major students are required to take it. The prerequisite is a course called Sets, Functions and Relations, which is essentially an introduction to proof course. Instructors in later courses in the Mathematics Major sequence expect students to have familiarity with basic notions from Group Theory, up to and including the first isomorphism theorem. A small proportion of the students take a second course in Abstract Algebra; this second course deals with rings, fields, and Galois theory.

The MAT 301 class typically contains students with a wide range of backgrounds and inclinations. Usually about half the students are secondary education majors. Typically there are a few outstanding students in the class, and a few who really battle with the ideas.

I taught Introduction to Abstract Algebra for almost a decade prior to trying an IBL approach. I tried several different texts, and with most of these found that a large majority of my students did not engage the ideas. They were passive, and increasingly daunted as the level of abstraction of the ideas increased. An exception to the inadequacy of texts in engaging students was the text A book of Abstract Algebra, by Charles C. Pinter (now available in Dover). The problem based approach of this text supported active participation by my students. This text undoubtedly influenced my approach in these notes. Teaching MAT 301 using an IBL approach was the logical culmination of my exploration of different teaching approaches for Introductory Abstract Algebra.

There is a previously published set of IBL notes for Abstract Algebra designed for a two-semester sequence for an audience comparable to mine (Group Theory, David M. Clark, JIBLM, number 3, April 2007). The coverage in Clark’s notes is comparable to the coverage in a traditional one-
semester introductory abstract algebra class. The fact that two semesters are needed to reach topics that are standard in an introductory abstract algebra course presents a difficulty for me, given the context of the abstract algebra course within our course sequence. In particular instructors in subsequent courses in our program require that certain fundamental ideas be discussed in the one-semester *Introduction to Abstract Algebra* class.

The notes that I present here may be of use to instructors with similar constraints to mine, who are keen to try an IBL approach in a one-semester Abstract Algebra class. The notes present a viable route to establishing the main ideas of elementary group theory, through the first isomorphism theorem, using an IBL approach with students of modest background, in a one-semester course. Of course this involves sacrifice of content, and the user will notice in these notes the omission of some standard material from the course. Notably, the theory of permutation groups is not developed. (Two of the three times I taught using these notes, I have given my students a short reading assignment on permutation groups, together with some exercises related to the more computational aspects of the theory.)

I have taught the course using these notes three times, and the notes have been honed over these three iterations. In each of the three years I had between 17 and 20 students in the class.

The instructional approach in most of the mathematics classes at our school is a traditional lecture approach. In this context I have found it essential to constantly explain to the student the benefits of an IBL approach, and to provide constant encouragement. The responses I have had from the students are, I believe, typical of IBL classes. Some students feel transformed by the approach (as evidenced in comments both during the course and several years later). A few students do not buy into the approach throughout the semester. The majority of students surprise themselves with how much they can accomplish in this course and, I know from experience, end up with a much deeper understanding of elementary abstract algebra than they would with a one-semester traditional lecture-based class.

### 0.2 Prerequisite for this course.

At our school the prerequisite is a course called *Sets, Functions and Relations*. This is essentially an introduction to proofs course. In *Sets, Functions and Relations*, students should have encountered the following, and these notes do assume that students have seen these before (though not that the students are expert at them):

- Basic logic, including quantifiers.
To the Instructor

• Elementary definitions related to divisors and prime numbers in the integers.
• Definitions related to Sets.
• Proofs involving one-to-one and onto functions.
• Proofs involving equivalence relations and partitions.

0.3 Class organization and assessment.

Most of the time in class is taken up with students presenting their solutions to the class, and class discussion of these solutions. The students use a document projector to display their solutions. Class presentations and participation in class discussion constitute a large part of the student’s grade (about 25%).

Students are required to write up all proofs, and to include these in a portfolio for the class. The portfolio is reviewed a few times during the semester, but is assigned a grade only at the end. Students turn in specified proofs for grading on a weekly basis; sometimes this a proof that has already been presented in class, sometimes not. Students are also required to complete a short “online journal” each week. Content questions in these focus on key issues that have arisen during class discussion; these assignments also always include some kind of journaling, in which students are asked to reflect on their progress and reactions in the course. Besides anything else these “online journals” help keep me in touch with how the students are feeling about the course. The portfolio, writing assignments and “online journal” contribute roughly 40% of the grade. The remainder of the grade is based on a midterm, a final, and one or two long quizzes.

Students are told that they may not use any resource outside the class for developing presentations or write-ups of proofs.

0.4 Dealing with different backgrounds and inclinations.

Each time I have taught the course, the group as a whole has progressed at a different rate through the course material. It is easy to adjust to the different groups, supplementing or omitting material as appropriate. Students within the classes also have very different levels of difficulty with the material.

There are many simpler problems for students who find the material more difficult. Students who find the material easier, will be challenged by the harder problems in the basic sequence. Also I sometimes assign optional
“challenge problems” when it seems appropriate. I have included a few of
these challenge problems in the notes for instructors.

Only once during the three years in which I have used these notes, have I
felt it appropriate to invite a student to simply move through the notes at his
own pace, and present his solutions to me in my office; the student in ques-
tion completed the problems several weeks before the end of the semester,
and then worked on additional material.

0.5 The problems.

I do not recommend giving the problems to the students as a complete pack-
age. I usually hand out half a page or less at a time. When we have made
significant progress on those, I give out the next half page. This also allows
for inserting additional problems if and when the direction of class discus-
sions makes this appropriate.

About 45 of the questions in the notes are labelled “ex”, for “exercise”. These questions typically require the students to practice applying defini-
tions and theorems to specific examples. These have a different status from
the other problems in that when I assign them, students know that I expect
them to come to class with these pretty much completed. Sometimes stu-
dents start working on these toward the end of class after encountering a
new definition. I encourage students to help each other out with exercises
(though not with the other problems) if necessary. I often have students just
compare their answers to these questions in groups, rather than having them
put up on the board. Sometimes students will ask to have someone put up
the solution to an exercise on the board, and in that case we do it that way,
but it usually does not count as a “presentation”.

The main goal throughout the problems is effective communication with
my students. Rigor and formality is occasionally relaxed in the interests of
communication.

In some exercises I ask students to explain something, (as distinct from
proving that thing). Students might need guidance on the distinction be-
tween these two. My intention is that for a proof, all details need to be
presented, and the style should be fairly formal, whereas when I ask for an
"explanation” details could be omitted and the style could be more informal.
For example, one might “explain” that $\mathbb{Z}_5$ is cyclic by simply saying that the
element 1 is a generator, whereas a proof that $\mathbb{Z}_5$ is cyclic would perhaps
require a more formal argument that $\mathbb{Z}_5$ is equal to the cyclic subgroup gen-
erated by 1.

I have included in the instructor’s version of these notes some comments
related to the problem sequence, and to specific problems. These are referenced at the relevant place in the notes, and may be found in the *Notes to the Instructor* at the end of the problem sequence. The student version of the notes does not display the references or comments.
Introductory worksheet: some useful examples

1. **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. (We can extend this idea to symmetries of figures in three dimensions.)

   *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.

   (a) 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).

   ![Diagram of equilateral triangle with labeled vertices and indicated motions](image)

   Draw an equilateral triangle on a sheet of paper, and number the vertices 1, 2, and 3 as shown in the sketch. Now cut the triangle out, leaving the hole intact. This cut-out triangle will be helpful as you work through what follows.

   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 $\mu_1$, then (continuing from the resulting position) apply $\rho_1$ (a 120° clockwise rotation) we end up with
\[ \mu_2. \] Using our usual function composition notation, we can think of this as \( \rho_1 \circ \mu_1 \). In fact we 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 labelled \( \rho_1 \) and the column labelled \( \mu_1 \).

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

<table>
<thead>
<tr>
<th></th>
<th>( \rho_0 )</th>
<th>( \rho_1 )</th>
<th>( \rho_2 )</th>
<th>( \mu_1 )</th>
<th>( \mu_2 )</th>
<th>( \mu_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \rho_0 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \rho_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \rho_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \mu_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \mu_2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( \mu_3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use the cut-out triangle to determine the compositions and use this to complete the table.

We will denote this collection of symmetries, together with composition, by \( D_3 \).

(b) Develop a similar table for the symmetries of a square. We will use the notation \( D_4 \) for the symmetries of a square together with composition.

So that we are all using the same notation, call the original position \( \rho_0 \), denote clockwise rotations through 90°, 180°, and 270° by \( \rho_1 \), \( \rho_2 \) and \( \rho_3 \) respectively, and label the reflections as indicated in the sketch.

(Start by sketching and naming all eight symmetries of the square for reference, and as for the triangle, use a cut-out square to calculate the compositions.)

2. 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 this as repeated addition modulo 12. So for \( a \) and \( b \) in the \( \mathbb{Z}_{12} \), we think of \( ab \pmod{12} \) as the result of adding \( b \) to itself \( a \) times, modulo 12.

For example \((3)(7) = 9 \pmod{12}\).

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

(a) 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.

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

Introduction to groups

Notational conventions:

\( \mathbb{N} \): The set of natural numbers: \{1, 2, 3 \ldots \}  \\
\( \mathbb{Z} \): The set of integers: \{ \ldots, -2, -1, 0, 1, 2 \ldots \}  \\
\( \mathbb{Q} \): The set of rational numbers: \{ \frac{n}{m} | n, m \in \mathbb{Z}, m \neq 0 \}  \\
\( \mathbb{R} \): The set of real numbers.  \\
\( \mathbb{C} \): The set of complex numbers: \{a + bi | a, b \in \mathbb{R}\} where i = \sqrt{-1}.

Definition: A binary operation \( \ast \) on a set \( A \) is a function which sends \( A \times A \) to \( A \). We denote the image of \( (x, y) \) under this function by \( x \ast y \).

(Always, when faced with a new definition, try to understand it by thinking of examples, and of non-examples, meaning entities closely related to the defined concept, but that do not conform precisely to the definition.)

1. (ex) Which of the following are binary operations on the specified set? If not, explain why not.
   (a) Addition on \( \mathbb{Z} \).
   (b) Subtraction on \( \mathbb{N} \).
   (c) Division on \( \mathbb{R} \).
   (d) Division on \( \mathbb{Z}\setminus\{0\} \).
   (e) Composition on \( D_4 \).
   (f) Composition on the set of rotations in \( D_4 \).
   (g) Multiplication mod 6 on \( \mathbb{Z}_6 \).
Definitions:

- A binary operation \( * \) on a set \( A \) is said to be associative if 
  \[(a * b) * c = a * (b * c)\] for all \( a, b \) and \( c \) in \( A \).
- A binary operation \( * \) on \( A \) is said to be commutative if \( a * b = b * a \) for all \( a \) and \( b \) in \( A \).
- Suppose \( * \) is a binary operation on \( A \). An element \( e \) of \( A \) is said to be an identity for \( * \) if \( a * e = e * a = a \) for all \( a \in A \).
- Suppose \( * \) is a binary operation on \( A \), with identity element \( e \). Let \( a \in A \). An element \( b \) of \( A \) is said to be an inverse of \( a \) with respect to \( * \) if 
  \[a * b = b * a = e.\]

(Reminder: test your understanding of each definition by finding examples of operations that do have the property, and examples of operations that do not have the property.)

2. (ex) Refer back to those operations in question 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.

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

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

Definition: A group is a set \( G \) together with a binary operation \( * \) on \( G \) satisfying the following:

   (a) The operation \( * \) is associative.
   
   (b) There is an element in \( G \) which is an identity for \( * \).
   
   (c) 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 \( G \)”.)
Note that we assume all the familiar properties of the operations on \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} \) and \( \mathbb{C} \), and you may use these freely in all that follows.

5. (ex) 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.

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 \( \mathbb{R} \).)

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.

Definitions:
• 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 \( G \).

8. (ex) Provide at least two examples of abelian groups.

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

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

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 \( t = u \).
More 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 an inverse of \( a \) (the existence of which is ensured by the group axioms), 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 \( (a^m)^n = a^{mn} \).

12. 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 already given. Prove that these two are in fact equal.

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

You have shown in problem 12 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:** 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 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 two problems establish two basic principles that do apply in an arbitrary group.  

14. Suppose \( G \) is a group, with \( a \in G \). Prove that \( a^m a^n = a^{m+n} \) for all integers \( m \) and \( n \).

15. Suppose \( G \) is a group, with \( a \in G \). Prove that \( (a^m)^n = a^{mn} \) for all integers \( m \) and \( n \).

16. 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.
17. Suppose \( G \) is a group, with \( a \) and \( b \) in \( G \). Prove that if \( ab = e \), then \( ba = e \). 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 \( b \).

18. Prove or disprove, as appropriate: In a group, inverses are unique.
   (More precisely: if \( G \) is a group, and if \( a \in G \), then there is a unique inverse for \( a \) in \( G \)).

19. Prove or disprove, as appropriate: Suppose \( G \) is a group, with \( a, b \) and \( c \) in \( G \). If \( ac = bc \), then \( a = b \). ³

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

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

22. 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:

23. 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. ⁴

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 mod \( n \).

- 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.

24. (ex) Translate each of the following into additive notation:

(a) \( a^n = e \)
(b) “There exists an element \( t \) such that \( at = b^{-1} \)"
(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.)

25. (ex) Is multiplication modulo 7 a binary operation on \( \mathbb{Z}_7^* \)? If so, write out the operation table for multiplication (mod 7) on \( \mathbb{Z}_7^* \). Is \( \mathbb{Z}_7^* \) with multiplication (mod 7) a group? If not, explain why not.
2.1 Direct products of groups:

**Definition:** Suppose that $G$ and $H$ 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 $(g_1g_2, h_1h_2)$, 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 is defined “component-wise”.)

26. (ex) Determine the operation table for $\mathbb{Z}_2 \times \mathbb{Z}_3$, where the operation is defined component-wise. (Use additive notation, since the operation is based on addition.)

27. 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 think about what properties a direct product of groups inherits from the original groups. Here is one example of this:

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

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

2.2 Subgroups

As you might guess, subgroups are important in group theory.

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 $G$.

**Definitions:**

- We say that $H$ is “closed” under the operation if for all $a$ and $b$ in $H$, $ab$ 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 $H$. 

Margaret L. Morrow  
www.jiblm.org
\textbf{Definition:} Suppose that $G$ is a group. A subset $H$ of $G$ is called a \textit{subgroup of} $G$ if

1. $H$ is non-empty
2. $H$ is closed under the operation of $G$
3. $H$ is closed under taking inverses.

(If $H$ is subgroup of $G$ we sometimes say that $H$ \textit{inherits} the operation from $G$.)

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

31. (ex) Identify all the subgroups of
   (a) $\langle \mathbb{Z}_4, + \rangle$
   (b) $\langle \mathbb{Z}_6, + \rangle$

32. (ex) Identify all the subgroups of $D_4$.

33. Prove that if $H$ is a subgroup of $G$, then $H$ is a group under the operation inherited from $G$.

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

35. 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 $G \times H$.

36. Prove that if $G$ is an abelian group, then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of $G$.

### 2.3 Some more examples of groups

The next problem gives us many more examples of groups.

First, note that when we remove 0 from the underlying set of $\mathbb{Z}_5$ to obtain $\mathbb{Z}_5^*$, all the remaining elements have multiplicative inverses under the multiplication (mod 5), and with this operation $\mathbb{Z}_5^*$ is a group. A similar situation arises from removing 0 from the underlying set of $\mathbb{Z}_7$, In the following we generalize the idea of forming a group based on those elements of the underlying set of $\mathbb{Z}_n$ that have multiplicative inverses under multiplication (mod $n$):

\textbf{Definition:} Let $n$ be any positive integer. An element $m$ of $\mathbb{Z}_n$ is called a \textit{unit} in $\mathbb{Z}_n$ if it has an inverse under multiplication (mod $n$), in $\mathbb{Z}_n$.

\textbf{Definition:} For every positive integer $n$, let $U(n)$ denote the set of all units in $\mathbb{Z}_n$, together with the operation multiplication mod $n$. 

Margaret L. Morrow  
www.jiblm.org
37. (ex)

(a) List the units in each of the following:
   i) $\mathbb{Z}_7$
   ii) $\mathbb{Z}_6$
   iii) $\mathbb{Z}_8$
(b) Draw up the table for multiplication (mod 8) in $U(8)$. Is this a group? Explain why or why not. Determine the inverse of 3 in $U(8)$.
(c) Draw up the table for multiplication (mod 10) in $U(10)$. Is this a group? If not explain why not.
(d) Is there any positive integer $n$ for which $U(n)$ with multiplication (mod n) will fail to be a group? Either provide an $n$ for which $U(n)$ is not a group, or explain why $U(n)$ is a group for all positive integers $n$.
(e) Make a conjecture: what condition on $n$ ensures that the underlying set for $U(n)$ is precisely $\mathbb{Z}_n^*$?
(f) Make a conjecture: for a given positive integer $n$, how can one identify the units in $\mathbb{Z}_n$, without writing out the whole table for multiplication mod n on $\mathbb{Z}_n$?

2.4 Some very special subgroups of an arbitrary group

Suppose $\langle G, \cdot \rangle$ is a group, and $a \in G$. Consider the set \{a^n | n \in \mathbb{Z}\}. Note that this set is closed under the operation of G. (Why?)

Definition: Suppose $G$ is a group with $a \in G$. We let $\langle a \rangle$ denote the set \{a^n | n \in \mathbb{Z}\} together with the operation inherited from $G$.

38. (ex) List each of following, where the calculations take place in the specified group:
   (a) In $U(10)$, list $\langle 3 \rangle$ and $\langle 9 \rangle$.
   (b) In $U(8)$, list $\langle 3 \rangle$ and $\langle 1 \rangle$.
   (c) In $U(5)$, list $\langle 2 \rangle$, $\langle 3 \rangle$ and $\langle 4 \rangle$.
   (d) Let $\mathbb{R}^*$ denote $\mathbb{R} \setminus \{0\}$. In $\langle \mathbb{R}^*, \cdot \rangle$, list $\langle 2 \rangle$, $\langle \frac{1}{2} \rangle$ and $\langle 4 \rangle$.

39. (ex) List each of following, where the calculations take place in the specified group:
   (a) In $\langle \mathbb{Z}, + \rangle$, list $\langle 2 \rangle$, $\langle 3 \rangle$ and $\langle -3 \rangle$
   (b) In $\langle \mathbb{Z}_6, + \rangle$, list $\langle 2 \rangle$, $\langle 0 \rangle$, $\langle 1 \rangle$, and $\langle 4 \rangle$.
   (c) In $\langle \mathbb{Z}_{12}, + \rangle$, list $\langle 3 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$ and $\langle 10 \rangle$

40. Let $G$ be a group, with $a \in G$. Prove that $\langle a \rangle$ is a subgroup of $G$. 

Margaret L. Morrow  www.jiblm.org
Two extremely important definitions:

**Definition:** Let $G$ be a group with $a \in G$. The subgroup $\langle a \rangle$ is called the *cyclic subgroup generated by $a$.*

(Note that we could not have defined $\langle a \rangle$ as a cyclic subgroup until we had actually proved that this would always be a subgroup. But now you can go back and look at all the cyclic subgroups you generated in the last few questions.)

**Definition:** The *order of an element $a$ in a group $G$* is the smallest positive integer $m$ such that $a^m = e$, provided such an integer exists. If such an integer exists, we say that the order of $a$ is *finite*, and we will denote “the order of $a$” by $|a|$. If no such integer exists, we say that $a$ has *infinite order*.

*Take care:* the word “order” is used in many different ways in mathematics. Contrast the definition above with our previous definition of the *order of a group*, which is simply the number of elements in the group. The idea of the order of an element in a group turns out to be really useful.

41. (ex) Determine the order of the specified elements in the specified group.
   
   (a) 3 and 1 in $U(8)$
   
   (b) 3 and 7 in $U(10)$
   
   (c) 1, -1 , 2 and $\frac{1}{2}$ in the group $\langle \mathbb{R}^*, \cdot \rangle$

42. (ex) Suppose $\langle G, \cdot \rangle$ is a group, and that $G = \langle a \rangle$, where $a$ is an element in $G$ having order 10, with $G = \langle a \rangle = \{a^0, e, a^1, a^2, \ldots, a^9\}$. Determine the order of each of the elements of $G$.

43. (ex) Determine the order of the specified elements in the specified group.
   
   (a) 0, 1, 2, 3, 4 and 5 in $\langle \mathbb{Z}_6, + \rangle$
   
   (b) 0, 1, 2, and -1 in $\langle \mathbb{Z}, + \rangle$
   
   (c) 0, 1, 2, 3, 4, 5, 6, 8, 9, 10 and 11 in $\langle \mathbb{Z}_{12}, + \rangle$

**Definition:** We say that a group $G$ is *cyclic* if there exists some element $a$ in $G$ such that $G$ is the cyclic subgroup generated by $a$. In this case we also say that $G$ is *generated by $a$*, and that $a$ is a *generator* of $G$. (Suggestion: translate the definition into logic symbols.)

44. (ex) Which of the following are cyclic groups? Explain why or why not in each case.
New groups from old

(a) $U(10)$
(b) $U(8)$
(c) $U(5)$
(d) $D_4$

**Notational convention:** From now, for $n$ a positive integer, if no operation is specified, then $\mathbb{Z}_n$ will denote the group $\mathbb{Z}_n$ with operation addition mod $n$.

45. (ex) Which of the following are cyclic groups? Explain why or why not in each case.
   (a) $\langle \mathbb{Z}, + \rangle$
   (b) $\mathbb{Z}_8$
   (c) $\mathbb{Z}_3 \times \mathbb{Z}_5$
   (d) $\mathbb{Z}_2 \times \mathbb{Z}_4$

46. Prove that every cyclic group is abelian.

47. Prove that if $G \times H$ is a cyclic group, then $G$ and $H$ are cyclic groups.

48. Prove or disprove, as appropriate: If $G$ and $H$ are cyclic groups, then $G \times H$ is a cyclic group.

49. (ex) Suppose $\langle G, \cdot \rangle$ is a group, and that $G = \langle a \rangle$, where $a$ is an element in $G$ having order 10, with $G = \langle a \rangle = \{a^0 = e, a^1, a^2, \ldots, a^9\}$. List all generators of $G$. (Exercise 42 should help.)

50. (ex) List all generators of $\mathbb{Z}_{12}$. (Exercise 43(c) should help.)
Chapter 3

More on cyclic groups.

Our next goal is to deeply understand the structure of all cyclic groups. First we need some results from elementary number theory.

Recall the following definitions. Here \( n \) and \( m \) are integers and \( m \neq 0 \):

- We say \( n \) is divisible by \( m \) if there exists an integer \( k \) with \( n = mk \). (We also in this case say \( m \) is a divisor of \( n \).)

- We say that a positive integer \( p \) is prime if \( p \) has exactly two divisors, \( p \) and 1. (Note: this implies that 1 is not considered to be a prime.)

- Let \( m \) and \( n \) be integers, not both zero. A positive integer \( d \) is said to be the greatest common divisor of \( m \) and \( n \) if
  - \( d \) is a divisor of both \( n \) and \( m \), and
  - if \( s \) is a positive integer that is a divisor of both \( m \) and \( n \), then \( s \) is a divisor of \( d \)

  (Notation: gcd\((m, n)\))

- We say that two integers \( m \) and \( n \) are relatively prime if the greatest common divisor of \( m \) and \( n \) is 1.

Now a theorem of elementary number theory, which we will use without proof:

- **The division algorithm**
  
  Suppose \( n \) and \( m \) are integers, with \( m > 0 \). Then there exist unique integers \( q \) and \( r \) with \( n = mq + r \), and \( 0 \leq r < m \).

51. (ex) Find the values for \( q \) and \( r \) as specified in the division algorithm for each of the following:
   a) \( n = 47, m = 7 \) 
   b) \( n = 42, m = 6 \) 
   c) \( n = -26, m = 5 \).
   d) \( n = -3, m = 5 \).
52. Suppose that $G$ is a group, and $a \in G$. Prove that if the order of $a$ is $m$, then for all integers $q$ and $r$, $a^{mq+r} = a^r$.

53. Suppose that $a$ is an element of a group $G$ and that the order of $a$ is $m$. Prove that if $n$ is an integer with $a^n = e$, then $m$ is a divisor of $n$.

54. (ex) Suppose that $G$ is a group with $a \in G$, and suppose that $a^{-5} = e$. Find a positive integer $m$ with $a^m = e$. (Prove that $a^m = e$ for your choice of $m$.)

55. Suppose that $a$ is an element of a group $G$. Prove that if there is some integer $n$, $n \neq 0$, with $a^n = e$, then there exists a positive integer $m$ with $a^m = e$.

56. Let $G$ be a group, and let $a \in G$. Prove that if the order of $a$ is infinite, then all integer powers of $a$ are distinct; that is if $i$ and $j$ are integers, with $i \neq j$, then $a^i \neq a^j$.

57. Let $G$ be a group, and let $a \in G$. Prove that if $a$ has finite order $m$, then for every integer $n$, there is some integer $s$ with $0 \leq s < m$ such that $a^n = a^s$.

58. Let $G$ be a group, and let $a \in G$. Prove that if $a$ has finite order $m$, then $a^0, a^1, a^2, \ldots, a^{m-1}$ are distinct elements of $G$. 
Note that the previous three problems basically tell us about the structure of every cyclic group, as follows: \(^{14}\)

59. **Theorem**: (Already proved in the previous problems.) Suppose \(G\) is a cyclic group with generator \(a\) (so \(G = \langle a \rangle \)).

(a) If the order of \(a\) is infinite, then \(G = \{ \ldots a^{-2}, a^{-1}, e, a^1, a^2 \ldots \}\), where the elements listed are all distinct from each other.

(b) If the order of \(a\) is finite, order \(m\) say, then \(G\) contains exactly \(m\) elements, namely \(G = \{ e, a^1, a^2 \ldots a^{m-1} \}\).\(^{15}\)

60. Suppose \(H\) is a subgroup of a group \(G\) with \(a \in G\). Suppose \(n, m, q\) and \(r\) are integers with \(n = mq + r\). Prove that if \(a^n\) and \(a^m\) are both in \(H\), then so is \(a^r\).

The following is standardly taken as an axiom when working with non-negative integers, and we will do the same:

**Well-ordering principle**: Every non-empty set of positive integers contains a least element.

The following somewhat amazing theorem tells us something about every subgroup of every cyclic group.\(^{16}\)

61. Suppose that \(G\) is a cyclic group, with generator \(a\). Prove that if \(H\) is a subgroup of \(G\) then \(H\) is cyclic.\(^{17}\)

62. Suppose \(n\) and \(m\) are integers. Let \(H = \{ sm + tn \mid s \in \mathbb{Z} \text{ and } t \in \mathbb{Z} \}\). Prove that \(H\) is a cyclic subgroup of \(\mathbb{Z}\).

63. Suppose \(n\) and \(m\) are integers. In the previous problem we showed that \(H = \{ sm + tn \mid s \in \mathbb{Z} \text{ and } t \in \mathbb{Z} \}\) is a cyclic subgroup of \(\mathbb{Z}\). Prove that if \(d\) is a generator of \(H\), then \(d = \gcd(m, n)\).

64. **A rather nice theorem in number theory**: Prove the following:

(a) Suppose \(n\) and \(m\) are integers, with \(d = \gcd(m, n)\). Then there exist integers \(s\) and \(t\) with \(sm + tn = d\).

(b) Suppose \(n\) and \(m\) are relatively prime integers. Then there exist integers \(s\) and \(t\) with \(sm + tn = 1\).

65. (ex) Find (by trial and error) at least two pairs of values for \(s\) and \(t\) that illustrate the “rather nice theorem” above for each of the following values for \(n\) and \(m\):

   a) Take \(n = 6\), and \(m = 8\).  
   b) Take \(n = 4\), and \(m = 9\).
More on cyclic groups.

66. Suppose that \( G \) is a cyclic group, with generator \( a \), where the order of \( a \) is \( m \). Prove that if \( k \) is an integer relatively prime to \( m \), then \( a^k \) is also a generator of \( G \).

67. (ex) For each of the specified cyclic groups, list all distinct subgroups.
   a) \( \mathbb{Z}_{12} \)  
   b) \( \mathbb{Z}_{18} \).

68. (ex) Suppose that \( G \) is a cyclic group, with \( G = \langle a \rangle \), for some \( a \in G \), where the order of \( a \) is 12. Determine all distinct subgroups of \( G \).\(^{18}\)

69. (ex) Suppose that \( G \) is a cyclic group, with \( G = \langle a \rangle \), for some \( a \in G \), where the order of \( a \) is 18. Determine all generators of \( G \).

70. (ex)
   (a) Write the statement of the theorem in problem 66 using additive notation.
   (b) Determine all generators of each of the following cyclic groups:
      a) \( \mathbb{Z}_{12} \)  
      b) \( \mathbb{Z}_7 \)  
      c) \( \mathbb{Z}_{24} \).

71. Prove that the units in \( \mathbb{Z}_n \) (where \( n \) is a positive integer) are precisely the elements of \( \mathbb{Z}_n \) that are relatively prime to \( n \).\(^{19}\)
Chapter 4

Homomorphisms and Isomorphisms

These are the “structure preserving” mappings in abstract algebra. Most fields of math have “structure preserving” mappings; for example, in linear algebra, linear transformations “preserve” the vector space structure (scalar multiplication and vector addition).

More formally, we have the following extremely important definitions:

Definitions:

- Suppose that \langle G, \ast \rangle and \langle H, \odot \rangle are groups. We say that a function \( \phi : G \to H \) is a homomorphism if for all \( a, b \in G \), \( \phi(a \ast b) = \phi(a) \odot \phi(b) \).

- We say that a function \( \phi : G \to H \) is an isomorphism if \( \phi \) is a homomorphism, and as well \( \phi \) is one-to-one and onto.

(Recall the definitions: A function \( f : A \to B \) is said to be one-to-one if for every \( x, y \in A \), whenever \( f(x) = f(y) \) then \( x = y \). A function \( f : A \to B \) is said to be onto if for every \( b \in B \), there exists some \( a \in A \) with \( f(a) = b \).)

Definition: We say that groups are isomorphic if there exists an isomorphism between them.

Intuitively, two groups are “isomorphic” 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:

72. (ex) Draw up an operation table for each of the following groups. Then decide which 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) \( G = \langle a \rangle \), where the order of \( a \) is 4
(c) \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).
(d) \( H = \{1, -1, i, -i\} \) with operation multiplication in the complex numbers. (Recall: \( i = \sqrt{-1} \), and \( i^2 = -1 \).)

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

74. Let \( G \) be an infinite cyclic group, with \( G = \langle a \rangle \). Define \( \phi : G \to \langle \mathbb{Z}, + \rangle \) by \( \phi(a^n) = n \) for every \( n \in \mathbb{Z} \). Prove that \( \phi \) is an isomorphism.

75. Let \( G \) be a finite cyclic group, with generator \( a \), and suppose that the order of \( a \) is \( m \). Define \( \phi : G \to \mathbb{Z}_m \) by \( \phi(a^n) = n \) for every \( n \) with \( 0 \leq n < m \). Prove that \( \phi \) is an isomorphism.

76. Let \( \mathbb{R}^+ \) denote the set of positive real numbers; let \( e \) denote the Euler number (a real number, base of the natural logarithm function; not an identity). Consider the function \( \phi : \langle \mathbb{R}, + \rangle \to \langle \mathbb{R}^+, \cdot \rangle \) defined by \( \phi(a) = e^a \) for all real numbers \( a \).

(a) Prove that \( \phi \) is a group homomorphism.
(b) Prove that the function \( \phi \) defined in part (a) is an isomorphism.

We have said that an isomorphism preserves algebraic structure. In particular, an isomorphism maps the identity to the identity, maps “inverses to inverses”, and maps elements to elements having the same order. Further, if two groups are isomorphic, they share algebraic properties, such as if one of them is abelian, then so is the other; if one is cyclic, so is the other, and so on! (We will provide proofs of these facts in the ensuing problems.)

Homomorphisms also preserve algebraic structure, but not nearly as strongly as isomorphisms. We explore this in the following problems. Of course every theorem about homomorphisms also applies to isomorphisms, since an isomorphism is just a special kind of homomorphism.

77. Suppose that \( G \) and \( H \) are groups, and that \( \phi : G \to H \) is a homomorphism.

(a) Prove that if \( e_G \) is the identity of \( G \), then \( \phi(e_G) \) is the identity of \( H \).
(b) Prove: For all \( a \in G \), \( \phi(a^{-1}) = (\phi(a))^{-1} \).

78. Suppose that \( G \) and \( H \) are groups, and that \( \phi : G \to H \) is an isomorphism. Prove that if \( G \) is abelian, then \( H \) is abelian.

79. Suppose that \( G \) and \( H \) are groups, and that \( \phi : G \to H \) is an isomorphism. Prove that if \( G \) has an element of order \( n \), then \( H \) has an element of order \( n \).
Note carefully: 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 \( \phi : G \rightarrow H \) 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 (or different cardinality)
- 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 (as a special case, 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.

80. (ex) In each of the following, prove that the two groups specified are not isomorphic.
   (a) \( D_4 \) and \( \mathbb{Z}_2 \times \mathbb{Z}_4 \).
   (b) \( \mathbb{Z}_2 \times \mathbb{Z}_4 \) and \( G = \langle a \rangle \), where the order of a is 8.
   (c) \( \mathbb{Z}_3 \times \mathbb{Z}_3 \) and \( \mathbb{Z}_9 \).
   (d) \( U(10) \) and \( \mathbb{Z}_2 \times \mathbb{Z}_3 \).

Definition: If \( \phi : A \rightarrow B \) is a function from a set A to a set B, and \( C \subseteq A \), then \( \phi(C) \) is defined to be the set \( \{ b \in B \mid \text{there is some } c \in C \text{ with } \phi(c) = b \} \).

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

81. (ex) Let \( \phi : U(10) \rightarrow U(10) \) be defined by \( \phi(a) = a^2 \) for all \( a \in U(10) \). (You already proved in problem 73 that \( \phi \) is a homomorphism.) Determine \( \phi(U(10)) \) and \( \text{Ker}(\phi) \).

82. Suppose that G and H are groups, and that \( \phi : G \rightarrow H \) is a homomorphism. Prove that if G is abelian, then so is \( \phi(G) \).

83. Provide an example of groups G and H, with a homomorphism from G to H, where G is abelian, and H is not abelian. (If not possible, explain why not.)
84. Suppose that $G$ and $H$ are groups, and that $\phi : G \to H$ is a homomorphism. Prove that $\text{Ker}(\phi)$ is a subgroup of $G$.

85. Suppose that $G$ and $H$ are groups, and that $\phi : G \to H$ is a homomorphism. Suppose too that $K$ is a subgroup of $G$. Prove that $\phi(K)$ is a subgroup of $H$.

86. Suppose $\phi : G \to H$ is a group homomorphism, and that $a$ is an element of order $m$ in $G$ (where $m$ is a positive integer). Make and prove a conjecture about the order of $\phi(a)$.

87. Suppose $\phi : G \to H$ is a group homomorphism. Prove or disprove as appropriate: If $G$ is cyclic, then so is $H$. 
Chapter 5

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 is a strangely irrelevant idea to spend time on. Bear with this; you will soon find how much can be derived from the idea.

Definition: Suppose \( \langle G, * \rangle \) is a group, with \( H \) a subgroup of \( G \), and \( a \in G \). Then \( a * H \) denotes the set \( \{ a * h | h \in H \} \), and is called a left coset of \( H \) in \( G \) (or, if necessary, the left coset of \( H \) determined by \( a \)).

(If the intended operation is clear, we usually denote \( a * H \) by \( aH \), or even \( a + H \) if appropriate.)

(To help you interpret this definition, note that it means that \( x \in a * H \) iff there exists some \( h \in H \) with \( x = a * h \).)

The following exercises should help you to understand this definition.

88. (ex) Consider the group \( D_4 \), and the subgroup \( H = \{ \rho_0, \delta_1 \} \) of \( D_4 \). List the distinct left cosets of \( H \) in \( D_4 \), and list the elements of each of these. How many distinct (not equal) left cosets are there for \( H \)?

89. (ex) Consider the group \( D_4 \), and the subgroup \( K = \{ \rho_0, \rho_1, \rho_2, \rho_3 \} \) of \( D_4 \). List the distinct left cosets of \( K \) in \( D_4 \), and list the elements of each of these. How many distinct left cosets are there for \( K \)?

90. (ex) Consider the group \( \langle \mathbb{Z}, + \rangle \), and its subgroup \( H = \{ n \in \mathbb{Z} | n = 5m \text{ for some } m \in \mathbb{Z} \} \) (which we denote by \( 5\mathbb{Z} \)). List the distinct left cosets of \( H \) in \( \langle \mathbb{Z}, + \rangle \), 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.
91. Is the following true or false? 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 $a = b$.

92. Is the following true or false? 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 for all $h \in H$, $ah = bh$.

93. Is the following true or false? 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 $b \in aH$.

Now some really important ideas:

94. Suppose $G$ is a group and $H$ a subgroup of $G$. Define a relation on $G$ as follows: for all $a, b \in G$ $a \sim b$ iff $a \in bH$. Prove that $\sim$ is an equivalence relation.
   (Remark: recall that an equivalence relation on a set always gives rise to a partition of the set.)

95. Suppose $G$ is a group and $H$ a subgroup of $G$. Prove that the collection of distinct left cosets of $H$ in $G$ form a partition of $G$.

96. Suppose $G$ is a group, $H$ subgroup of $G$, and $a$ an element of $G$. Consider the function $f : H \rightarrow aH$ defined by $f(h) = ah$ for all $h \in H$.
   (a) Prove that $f$ is one-to-one.
      If $G$ is a finite group, what does this imply about the relation between the number of elements in $H$ and the number of elements in $aH$?
   (b) Prove that $f$ is onto.
      If $G$ is a finite group, what does this imply about the relation between the number of elements in $H$ and the number of elements in $aH$?
   (c) Suppose $G$ is a finite group and $H$ subgroup of $G$. Prove that for all $a \in G$, the number of elements in $H$ is equal to the number of elements in $aH$.
   (d) Suppose $G$ is a group and $H$ subgroup of $G$. Prove that for all elements $a$ and $b$ in $G$, the number of elements in $aH$ is equal to the number of elements in $bH$.

97. (ex)$^{28}$ Consider a group $G$ of order 120, with a subgroup $H$ of order 4.
   How many elements are there in each left coset of $H$ in $G$? How many distinct left cosets has $H$ in $G$? Explain how your reached your answer.
   Could $G$ have a subgroup of order 7? Explain why or why not.
98. Prove: Suppose $G$ is a finite group and $H$ a subgroup of $G$. Then the number of elements in $H$ is a divisor of the number of elements in $G$.

99. (ex) Consider the group $\langle \mathbb{Z}_{18}, + \rangle$. What are the possible sizes for a subgroup of $\langle \mathbb{Z}_{18}, + \rangle$? For each of these possible sizes, provide at least one subgroup of $\langle \mathbb{Z}_{18}, + \rangle$ that has that size.

(Do not however assume that if $G$ is a group of order $n$, then $G$ has a subgroup of order $m$ for every divisor $m$ of $n$; this is not in general true.)

100. Prove that if $G$ is a finite group and $a$ is an element of $G$, then the order of $a$ is a divisor of the order of $G$.

101. Prove that if $G$ is a group with prime order, then $G$ is cyclic.

(Isn’t that beautiful? You have just figured out something about every finite group with prime order in the whole universe :-))
Chapter 6

Normal subgroups and quotient groups

We have been studying cosets, and we found that they were very useful in proving that the order of a subgroup is a divisor of the order of a group. Another way in which they are a powerful way of thinking is in forming new groups called “quotient groups”. These are a crucial concept in Abstract Algebra. Before we can talk about these we need to consider a special kind of subgroup, called a normal subgroup.

If \( H \) is a subgroup of a group \( G \), we previously defined left cosets of \( H \) in \( G \). In an analogous way, we can define right cosets of \( H \) in \( G \):

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

102. (ex) Refer to questions 88, 89, and 90. In each case, determine all right cosets of the given subgroup in the specified group.
Is it true or false that if \( H \) is a subgroup of a group \( G \), then for all \( a \in G \), we have \( aH = Ha \)?

**Definition:** A subgroup \( H \) of a group \( G \) is said to be a normal subgroup of \( G \) if for all \( a \in G \), \( aH = Ha \).

103. (ex) Refer to questions 88, 89, and 90. In each case, say whether the given subgroup is a normal subgroup of the specified group.

104. Suppose \( G \) is a group, and \( H \) a subgroup of \( G \). Prove that \( H \) is normal if and only if the following condition holds: for all \( h \in H \), and for all \( x \in G \), \( xhx^{-1} \) is in \( H \).

Notice that the previous problem provides an equivalent way of defining normal subgroups.
105. Prove or disprove as appropriate: If \( G \) is an abelian group, then every subgroup of \( G \) is normal.

106. Let \( G \) be a group, and \( H \) a normal subgroup of \( G \). Consider the collection of all left cosets of \( G \). (So we are considering the set \( \{ aH | a \in G \} \) with elements that are sets.) Suppose that \( a_1, a_2, b_1 \) and \( b_2 \) are elements of \( G \) with \( a_1H = a_2H \), and \( b_1H = b_2H \). Prove that \( (a_1b_1)H = (a_2b_2)H \).

107. Let \( G \) be a group, and \( H \) a normal subgroup of \( G \). Let \( G/H \) denote \( \{ aH | a \in G \} \). Define an operation on \( G/H \) as follows: for \( aH \) and \( bH \) in \( G/H \), define \( (aH)(bH) \) to be \( (ab)H \). Prove that this operation is well defined. (The issue is that a coset \( aH \) may have different names. If we use different names for the cosets we are multiplying, we want to be sure that we still get the same coset as an answer.) (Note: \( G/H \) is often read as “\( G \) mod \( H \)”.)

By the way, notice that normal subgroups were defined the way they were precisely so that the operation on cosets would be well defined.

108. Suppose \( G \) is a group, and \( H \) a normal subgroup of \( G \). Prove that the set of cosets \( G/H \) with operation defined as in problem 107 is a group.

**Definition:** Suppose \( G \) is a group, and \( H \) a normal subgroup of \( G \). The group consisting of the set \( G/H \) with operation defined by \( (aH)(bH) = (ab)H \) is called the quotient group of \( G \) by \( H \). (Sometime the term “factor group” is used in place of “quotient group”.)

Notice that we have developed a new way of constructing new groups from existing groups. We will show in problems that follow that there is a deep relation between factor groups and homomorphisms.

109. (ex) Consider the group \( G = \mathbb{Z}_{20} \) and the normal subgroup \( H = \langle 5 \rangle \) of this group.
   
   (a) List \( H \).
   
   (b) List the distinct left cosets of \( H \) in \( G \).
   
   (c) Draw up an operation table for the group \( G/H \).

110. (ex) Consider the group \( G = D_4 \) (symmetries of a square) and the normal subgroup \( H = \{ \rho_0, \rho_1, \rho_2, \rho_3 \} \) of this group.
   
   (a) List the distinct left cosets of \( H \) in \( G \).

   (b) Draw up an operation table for the group \( G/H \).
(c) By inspection, identify at least one familiar group that is isomorphic to $G/H$.

111. Suppose $G$ is a group, and $H$ is a normal subgroup of $G$. Prove or disprove as appropriate: If $G$ is abelian, then $G/H$ is abelian.\(^{30}\)

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

113. Suppose $G$ and $H$ are groups, and that $\phi : G \to H$ is a homomorphism. Let $K$ denote $\text{Ker}(\phi)$.

(a) Prove that if $a_1K = a_2K$ for some $a_1, a_2 \in K$, then $\phi(a_1) = \phi(a_2)$.

(b) The fact you proved in part (a) allows us to define a new mapping $\psi : G/K \to H$ by $\psi(aK) = \phi(a)$ for all $aK \in G/K$. Prove that $\psi$ is a homomorphism from $G/K$ to $H$.

114. Suppose that $G$ and $H$ are groups, and that $\phi : G \to H$ is a homomorphism. Prove that $G/\text{Ker}(\phi) \cong \phi(G)$. (The notation $\cong$ is shorthand for “is isomorphic to”.)

In abstract algebra, one of the most common ways of showing that two groups are isomorphic is by defining an appropriate homomorphism $\phi$ and then deriving an isomorphism via $G/\text{Ker}(\phi) \cong \phi(G)$. Use this idea to do the next problem:

115. Prove that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$. (The notation $6\mathbb{Z}$ denotes \{ $n \in \mathbb{Z} | n = 6m$ for some $m \in \mathbb{Z}$ \}.) (Hint: consider the function $\phi : \mathbb{Z} \to \mathbb{Z}_6$ defined by $\phi(n) = n \mod 6$ for all $n \in \mathbb{Z}$.)

116. Suppose $G$ is a group, and $H$ is a normal subgroup of $G$. Prove or disprove as appropriate: If $G/H$ is abelian, then $G$ is abelian.

117. Suppose $G$ is a group, and $H$ is a normal subgroup of $G$. Prove or disprove as appropriate: If $G$ is cyclic, then $G/H$ is cyclic.
Notes to the Instructor

1. I have the students do this in-class on the first day of class, after a brief introduction to symmetry. The material in this worksheet is used later in the problem sequence. Toward the end of the class I give them the first few problems from the next chapter to prepare for the subsequent class meeting.

2. For time considerations the instructor might tell students to skip the following two problems.

3. Once students have completed this problem, I introduce the term “right cancellation”, and comment that “left cancellation” is also valid.

4. I used to include this question in the form “If \( G \) is a group, then for all \( a \) and \( b \) in \( G \), there is a unique solution in \( G \) for the equation \( ax = b \).” However I have found it effective to get to the subtleties more quickly by asking it as in this problem.

5. From experience I find this to be the most transparent definition of subgroups to give to my students. To maintain momentum in the course, I do not develop equivalent definitions for a subgroup. In applying this definition, some students have (perhaps surprising) difficulty showing that the subset \( H \) is non-empty; this usually sorts itself out, with someone pointing out that in many cases, it is easiest just to point out that the identity element is in \( H \).

6. I usually have students write up and turn in at least one of the following, before they are presented in class.

7. My goal in the above is simply to have some more groups to work with, so if the students do not come up with a conjecture for (f) I just let it slide, and tell them what elements to use for \( U(n) \), for any specific \( n \) when the need arises.

8. Of course the difficulty that some students will have is in realizing that \( \{a^n|n \in \mathbb{Z}\} \) need not be an infinite set.

9. My students have significant difficulty with translating the definition for \( \langle a \rangle \) into additive notation. You might want to ask your students to write the definition using additive notation before trying this exercise.

10. The goal of this exercise is to help students to internalize the definition of the order of an element. Some students do not quickly notice a connection between the order of an element, and the order of the cyclic subgroup generated by that element. It is worth highlighting a conjecture about this, if it arises in class discussion. The related theorems are proved in chapter 3.
My students have significant difficulty with translating the definition for order of an element into additive notation. You might want to ask your students to write the definition using additive notation before trying this exercise.

My students would have encountered these definitions in the course Sets, Functions and Relations, which is prerequisite for this course.

The following sequence of theorems culminates in the characterization of all cyclic groups.

I do not give the students the next statement until they have thought carefully about the previous three problems.

What follows is preparation for proving that every subgroup of a cyclic group is cyclic.

The students of course find the proofs of the following two theorems challenging. I usually move on, leaving them out there as a challenge. Discussion about promising candidates for a generator for \( H \) usually leads to at least one student producing a proof at some stage.

As pointed out by the editor, the following three problems provide a nice application of the theorem in the previous problem. The theorem in the third problem is needed in some of the subsequent problems in these notes. If time is an issue, proofs for these three problems could be omitted.

I do not formally include the sufficient condition for two elements of a cyclic subgroup to generate the same subgroup. Sometimes students notice some patterns related to this based on examples, and formulate a conjecture.

This problem may be regarded as a challenge problem. It can be omitted without breaking the flow of the problem sequence.

My students would have written proofs related to one-to-one and onto functions in the course Sets, Functions and Relations, which is a prerequisite for this course.

As suggested by the editor of this paper, this is an ideal place to address the issue of well-defined mappings. Students will likely initially simply write \( \phi(a^na^k) = \phi(a^{n+k}) = n+k = \phi(a^n) + \phi(a^k) \). Discussing the error could lead to a productive discussion of what it means for a function to be "well-defined". This will be helpful later when discussing what it means for multiplication of cosets to be well-defined.

This problem may be regarded as a challenge problem. It can be omitted without breaking the flow of the problem sequence.

This is the only instance in this course in which I sometimes provide a model proof, requesting students to supply reasons, as shown below. If I do not do this, students usually spend quite a lot of time trying to just show directly that \( \phi(e_G)b = b\phi(e_G)b = b \) for all \( b \in H \), which is a dead-end in the case where \( \phi \) is not necessarily onto; while they no doubt learn a lot by going through this, for time considerations one might consider providing a model proof.

Part a): Complete this proof, by supplying reasons where indicated.

Suppose that \( \phi : G \to H \) is a homomorphism, and that \( e_G \) is the identity of G. Denote the
identity of $H$ by $e_H$.
Now $\phi(e_G) = \phi(e_G e_G)$ (Why?)
$= \phi(e_G) \phi(e_G)$ (Why?)
But also $\phi(e_G) = e_H \phi(e_G)$ (Why?)
Thus $\phi(e_G) \phi(e_G) = e_H \phi(e_G)$.
But then it follows by right cancellation in a group that $\phi(e_G) = e_H$, as required.

24The following could be included in this question as challenge problems.

1. $\langle \mathbb{Q}^*, \cdot \rangle$ and $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{R}^*, \cdot \rangle$ and $\langle \mathbb{R}, + \rangle$

25My students have usually seen the first of these definitions in the already completed Sets, Functions and Relations class, and they usually notice that the second is closely related to the definition of the null set in their Linear Algebra class.

26If pressed for time, some of the remaining problems in this section can be omitted without breaking the continuity of the notes, with the important exception of proving that $\text{Ker}(\phi)$ is a subgroup of the domain of $\phi$. This fact is needed later in these notes.

27My students would have encountered equivalence relations and partitions in the Sets, Functions and Relations course which is a prerequisite for this course.
For students who are not confident with these ideas, the following two problems may be included in place of the previous problem. I in fact include these in addition to the previous problem; I find that those students who do not see the connection to the previous problem and approach them from scratch deepen their understanding of partitions. I try to select someone who has developed the proofs in this way to present them. Once the proofs have been presented from scratch someone usually points out that they are in fact a direct consequence of the equivalence relation established in the previous problem.

1. Suppose $G$ is a group and $H$ a subgroup of $G$. Prove that for all $a, b \in G$, either $aH = bH$ or $aH \cap bH$ is empty.
2. Suppose $G$ is a group and $H$ a subgroup of $G$. Prove that $\bigcup_{a \in G} aH = G$
   (Recall: $\bigcup_{a \in G} aH$ denotes the union of $aH$ taken over all $a \in G$; that is $\bigcup_{a \in G} aH = \{g \in G | g \in aH$ for some $a \in G\}$.)

Of course the following problem should be very easy by this stage. In my experience it is nevertheless worth including as a problem, rather than simply as a remark.

28The following computational problem is intended to give students who need it a foothold for the proof of Lagrange’s theorem, which follows it. Lagrange’s theorem is deliberately not named at this point in the notes to avoid the temptation to look for a reference elsewhere.

29At this point I usually illustrate this by color coding elements on a group table. Arrange the elements so that elements in the same coset are adjacent, and then color elements in the same coset the same color.
If time runs out, this is a reasonable place to stop - or just end by stating and discussing briefly the first isomorphism theorem, which is proved in the following sequence of problems.