Modern Algebra and Geometry

Sriaditya Vedantam

Modern Algebra and Geometry

Sriaditya Vedantam
svedantam@zyphensvc.com

It has definitely been an eventful two semesters with a lot of ups and downs with a disastrous ending, but I enjoyed each step of the way. I love those who stood by me and supported me wholeheartedly. I also love those who gave me advice and basically gave me reality checks throughout the semester, because god knows I needed it. I've struggled a lot with faith and my identity, but I now understand a lot about who I am and what I want to become.

Definitely not an attack helicopter though.

This course has been my favorite this year, and I am glad to be sharing with you my love for algebra. Trust me, given ages ago, I would have never believed to be saying that, not even ages, right before the year started.

Lastly, I would like to give a personal thanks to Dr. Leonard Chastkofsky for just being a gosh darn great professor.

He pushed me to think about problems outside of the class in algebraic circumstances and solutions. Also just being human.

Contents

Preface

What I understood from this course is that abstract algebra is an introductory course in nature, briefly touching many different topics here and there. It is not a well-defined body of knowledge, it has a standard list of topics to learn, but it is very optional to how one may want to approach them.

This textbook is a collection of notes from an undergraduate course in Abstract Algebra. This is not meant to replace a textbook in any manner. Take what I have in this textbook with a pound of salt, as it has weight to it but is not impossible to throw over. It is filled with explanations in a way that I try to explain to others as if I were talking to you. I have dealt with a novelesque textbook this semester, and trust me it will not be like me talking to you without having to decipher the theorems and proofs in the text. I use exercises that I found were fun to solve while also grasping the content material and being able to solve them.

As most of you will want and expect, there is a solutions page at the end of the textbook and it is very much my own solutions. Some of them may not be the best or most efficient way to solve them. I may have also lost points in class for some of the problems, however, this is definitely going to be community-based help if you would like me to correct a solution and I will be happy to credit you in the next revision of the textbook. Feel free to contact me through email.

Now a common objection to the course here at the University of Georgia is that we learn rings before groups, and from what I know, I definitely do agree with this objection. However, I will leave the text as is in the sequence of topics that I learned.

I included an extra section that I did not go over but was definitely something that is important to remember and learn about. This being, the first chapter: Introduction to Algebra. If you have not taken a proofs-based course or had a rough start, I highly heed you look at this section.

I am really into open courseware, which means this will always be open for everyone to use and distribute as long as you have the page that includes my credits, which is Pages 1 and 2.

Looking into this textbook, we definitely see a drop off in quality coming around midway through Chapter 3, "Congruence Classes in $\mathbb{Z}$". I prioritized getting definitions and theorems across more than the explanations for each one, but it does actively reflect how the class is modeled. I believe perhaps looking back there was a heavy explanation-based class which dropped off as the course progressed into more and more theory rather than practicality (theory in secret). This picked back up here and there for example with rings and polynomials, but went back to straight claims.

The audience I did write this for was content with my half-done work, but I will be updating this as I go down the line, especially since this only considers one term of the course.

Coming into term two of the course, I started to study a little different. Instead of only containing my class notes, I wanted to include a lot more comments into the coursework and this improvement started to allow me to do better on the tests and homework without having to rely on others to understand homework problems and so forth. I have started doing Anki decks of the theorems, doing the ungraded practice problems, and also the practice exams and quizzes that Dr. C provides. These are an effective way of learning. For retaking notes on content, I find a similar video on Youtube and take notes from that content.

Semester Two Preface coming soon!

Chapter 1

Introduction to Algebra

The content in this chapter is things to know by heart. We will not be going back and explaining the content discussed in this chapter.

1.1 Logic

For those coming from a pure symbolic proofs-based class, this text will definitely be a bit striking as I don't like using symbols every time they can be used. It's easier to convey thoughts by just using words and to depict very slight meanings that may not be robotic. It is definitely not impossible to do the mental conversion into symbolic language, however, the way I learned proofs was to use more words than symbols.

As a matter of fact, some classes may even deduct points for the overuse of symbols, and I have heard this tale through and through from many people. So take what you will, but I hope this will create some change. If there is one thing to take away from this section is that there is nothing ever wrong with using words over symbols, while there is the vice versa.

Let P and Q be statements. It should have been discussed in a proof class the difference between statements, questions, and commands.
"P and Q": This is true if and only if P and Q are both true. This is denoted by $\wedge$.
"P or Q": This is true for all cases of P or Q being true, or false if they are both false. This is denoted by $\vee$.
"P implies Q": We use implications to show that if P has some true or false factor, then we result in Q being true or false. For example, we usually write this in our English language as: "If P, then Q". This means that if P is true, then Q will also happen. This is true for 3/4 possible outcomes, which means this is true when P and Q are both true and false, and also true with P is false but Q is true. This is only false if P is true and Q is false. A false premise is always a true implication to mind you. Implications are denoted by $\implies$.
"P if and only if Q": This is called a biconditional, or an equivalence statement. This is short for saying "P implies Q and Q implies P". This is denoted by $\iff$.
"It is not the case that P": This is true if and only if P is false, also called negation.

1.2 Sets and Classes

Set Theory is very much its own field so we will not be getting into the specifics and the nitty-gritty of each topic, but it will be a brief overview.
Elements are either a part of a set or not part of a set. There are infinitely many elements and they have a choice of being a member of a set. When an element, x, is a member of set A we denote this by

$$x \in A.$$

Otherwise we say

$$x \notin A.$$

. We can also write this out in words as "x is (not) an element of A". These are some of the few things most people use symbols for regardless of their preferences for symbolic language.

The following are predicates.
1. "For all" is denoted by $\forall$.
2. "There exists" is denoted by $\exists$.
The **axiom of extensionality** states given sets A and B. For all elements, x, if $x \in A$ and $x \in B$, then $A = B$.
For all elements, $x \in A$, if $x \in B$, then A is a **subset** of B, denoted by $A \subseteq B$.
The **empty set** is a set with no elements, denoted by $\varnothing$.
A **class of sets** is a set that contains other sets and only sets. The **power axiom** states that for every set A, the power class $P(A)$ contains all subsets of A within a set. This is denoted by 2^A and has $2^{|A|}$ elements.
A **union of sets** considers all of the elements in both sets, denoted by $A \bigcup B$
An **intersection of sets** considers only the common elements in both set, denoted by $A \bigcap B$.
A **disjoint set** is when given when $A \bigcap B = \varnothing$. A **family of sets** is a class of sets where each element, mind you a set, is indexed. Generally denoted by $\bigcup_{i \in I} A_i := \{x : x \in A_i \text{ for some } i \in I\}$. Similarly with $\bigcap_{i \in I} A_i$.
The **complement** of A is related to the negation of A, where we use DeMorgan's Laws.

1.3 Functions

Given sets A and B, a **function** will map f from A to B, denoted as $f : A \mapsto B$. This means that will assign one element in $a \in A$ to exactly one $b \in B$. The $a = b$ written as $f(a)$. **Images** mean the range of the function. The **domain** of f is written as dom f, while B is the **co-domain** also known as range. Two functions are equal if they have the same domain, range, and values for each element in the domain.

Suppose $S \subseteq A$, then the function from S to B is $g : S \mapsto B \iff g : a \mapsto f(a)$ for $a \in S$. This is more known as the **restriction** of the domain.

Let $f : A \mapsto B$ and $g : B \mapsto C$, Then a composite function of $h : a \mapsto g(f(a))$ is equivalent to $h : A \mapsto C$. This is called a **composite** of f and g.

Functions are **injective**, or one-to-one, if for all $a, b \in A$, $a \neq b$ implies $f(a) \neq f(b)$. This means all values in the domain are only mapped to one value in the co-domain.A **surjective** function, or onto, is given for all $b \in B$, $b = f(a)$ for some $a \in A$. This means all values in the co-domain are mapped to at least one value in the domain. A function is **bijective**, or one-to-one correspondence, if it is injective and surjective. Given the previous mappings of f and g, then if f and g are injective, we should check that gf is injective. If gf is injective, then check that f is injective. If f and g are surjective then we should check that gf is surjective. If gf is surjective, then we should check that g is surjective.

1.4 Relations

A **cartesian product** of sets A and B gives us

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

Note that $A \times \varnothing = \varnothing = \varnothing \times B$.

An equivalence relation, denoted by $\sim$ from A to B is

- **reflexive:** $a \sim a$ for all $a \in A$;
- **symmetric:** $a \sim b$, then $b \sim a$ for $a \in A$ and $b \in B$;
- **transitive:** $a \sim b$, $b \sim c$, then $a \sim c$ for $a, b, c \in A, B, C$

1.5 Well Ordering and Induction

Definition 1.5.1: Well-Ordering

Every nonempty subset of $\mathbb{Z}^{\geqslant 0}$ contains a smallest element.

This takes into account that there is an order relation (¡) on all integers of Z. The direct consequence of this definition is Mathematical Induction. Mathematical Induction is a proof technique that uses recursive techniques to prove that a statement is true for all elements past its base case.

Theorem 1.5.1 Principle of Mathematical Induction

Assume that $n \in \mathbb{Z}^{\geqslant 0}$ and P(n) is given.

1. P(0) is a true statement.
2. When P(k) is true, then P(k + 1) is also true.

Then P(n) is true for all $n \in \mathbb{Z}^{\geqslant 0}$.

A remark on this theorem is that P(k) does not have to be true, but we assume so. This is called the induction hypothesis. In proofwriting, if we are given an "If... Then..." statement, we generally assume that the statement before the "Then" is true, and attempt to prove the rest. This is the same thing we have proved through Induction. It can be seen as a result of continued direct proofs compiled together and generalized to become the induction we know today. The following example is how we use Induction in today's world, and it's important to note how we use it compared to how one may have done it for a proofs course. In other words, a practical application of how a researcher would use induction.

Example 1.5.1

A set of n elements has 2^n subsets
$P(0) : 2^0 = 1$ subsets.
$P(1) : 2^1 = 2$ subsets.
$P(3) : 2^3 = 8$ subsets.
Assume P(k) is a set with k elements and has 2^k subsets. Now prove $P(k+1) = 2^{k+1}$ subsets.
In a more standardized proofwriting, we can define a set

$$S := \{n \in \mathbb{Z}^{\geqslant 0} : \ P(n) \ is \ true\},$$

and show that $S = \mathbb{Z}^{\geqslant 0}$. Let our induction hypothesis be "P(n) is true". Since we have shown that our base case : P(0) is true, then we assume P(k) is true and attempt to prove P(k+1). Let's suppose that since P(n) is true, then $\#S = k$, which is the cardinal of set S. If we are to add a new element to set S and attempt to prove $k+1$, every subset has the option to choose between including $k+1$ or not including $k+1$. Therefore set S has $2 * 2^k = 2^{k+1}$ subsets. Thus proving $k+1 \in S$, therefore $S = \mathbb{Z}^{\geqslant 0}$. ■

1.6 A variation on Induction

Now with mathematical induction, also just referenced as induction, we can also show another type called Strong or Complete Induction.

Theorem 1.6.1 Principle of Complete Induction

Assume that $n \in \mathbb{Z}^{\geqslant 0}$, P(n) is given. If

1. P(0) is true, and
2. P(j) is true for all j such that $0 \leqslant j \leqslant t$, then P(t) is also true.

Proof: Let's prove this through induction. Let our induction hypothesis be if "P(j) is true for all j such that $0 \leqslant j \leqslant t$, then P(t) is also true" Suppose there is a set S, such that

$$S := \{n \in \mathbb{Z}^{\geqslant 0} : \ P(j) \ is \ true \ for \ all \ j \ such \ that \ 0 \leqslant j \leqslant n\}$$

For our base case, let's set n = 0, and suppose that $0 \in S$, thus P(0) is true.
Now assume P(k) is true, therefore P(k+1) is also true due to our induction hypothesis. Therefore $k \in S$ and $k + 1 \in S$ is true. Therefore by induction, $S = \mathbb{Z}^{\geqslant 0}$, and we have proved Complete Induction. ■

Similar to how we used weak or regular induction to prove complete induction, we can do the same in reverse. In fact, we can prove all of these theorems and definitions using one another. We can use the well-ordering axiom to prove mathematical induction and use mathematical induction to prove complete induction. To complete the loop, prove well ordering through complete induction. On a harder note, we can prove regular induction through complete induction, but it is possible.

$Well - Ordering \implies Induction$

Proof: Let us define the set S as

$$S := \{n \in \mathbb{Z}^{\geqslant 0} : \ P(n) \ is \ false\} \subseteq \mathbb{Z}^{\geqslant 0}.$$

Our goal in this proof is to show that the set $S = \phi$.
Assume $S \neq \phi$. Then let $d \in S$ be the smallest element. Let P(0) be true, but this means that $d \neq 0$. So that means $d \geqslant 1$. So if $d - 1 \geqslant 1$, then $d - 1 \in \mathbb{Z}^{\geqslant 0}$. Since $d - 1 < d, \ then \ d - 1 \in S$, so P(d-1) is true. By assumption $P(d-1) \implies P(d)$ so P(d) is true, so $d \notin S$. So $S = \phi$, therefore P(k) is true for all $k \in \mathbb{Z}^{\geqslant 0}$. ■

Now that we have jump-started the proofwriting structure in our heads, let's go ahead and start this course with our next topic: Fundamentals of Arithmetic and Divisibility.

Example 1.6.1 (Exercise 1)
$0a = 0$ for any integer a, given $0 + 0 = 0$.

Chapter 2

Fundamentals of Arithmetic and Divisibility

2.1 Axioms

Axioms are trivial definitions used in everyday life — or even mathematics — that we take for granted. They are definitions that are inarguable and are the core of math today. I never quite understood the hierarchy of math statements, but this is a way to look at it: Axioms are a specific type of definition that is just taken as a fact or true. Definitions are similar to axioms in which they build the premise of future statements, these may or may not include proofs to explain why this may be true. Lemmas are true statements that are not important in the long run, but are trivial to understand to understand future statements, generally are associated with proof. Propositions are important statements that must be associated with proof and are vital research building blocks. Theorems are big conclusion that wraps each concept mentioned in a paper into one central idea and are even more important than propositions, these also require proofs to be stated alongside the statement. Now the following axioms or properties are what we accept without another thought, but they are important to mention to understand future content when they are brought up again.

Definition 2.1.1: Additive Properties

1. Addition is well-defined. Given $a, b \in \mathbb{Z}$, $a + b$ is a uniquely defined integer.
2. Substitution Law: Since addition is well-defined, if $a = b$, and $c = d$, then $a + c = b + d$.
3. Commutative Law: For all $a, b \in \mathbb{Z}$, $a + b = b + a$.
4. Associative Law: For all $a, b, c \in \mathbb{Z}, (a + b) + c = a + (b + c)$.
5. There exists a zero element $0 \in \mathbb{Z}$, called the additive identity, satisfying $0 + a = a$ for any $a \in \mathbb{Z}$.
6. For all $a \in \mathbb{Z}$, there exists a unique additive inverse, $-a \in \mathbb{Z}$, satisfying $a + (-a) = 0$

Definition 2.1.2: Multiplicative Properties

Multiplication is well-defined. Given $a, b \in \mathbb{Z}$, $a \cdot b$ is a uniquely defined integer.

Substitution Law: If $a = b$ and $c = d$, then $ac = bd$.

Z is closed under multiplication, for all $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$.

Commutative Law: For all $a, b \in \mathbb{Z}$, $ab = ba$.

Associative Law: For all $a, b, c \in \mathbb{Z}, (ab)c = a(bc)$

$1 \in \mathbb{Z}$ is the multiplicative identity, satisfying $1a$

Definition 2.1.3: Distributive Property

For all $a, b, c \in \mathbb{Z}, a(b+c) = ab + ac$.

Definition 2.1.4: Trichotomy Principle

Z can be split into three distinct sets.

$$\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$$

Definition 2.1.5: Positivity Axiom

The sum or product of positive integers is positive.

Definition 2.1.6: Discrete Property

We have learned these already but they are the Well-Ordering Principle of N, and the Principle of Induction.

2.2 Division

Now that we have learned the axioms of arithmetic, let us learn about the division algorithm.
We have all (hopefully) learned how to divide in grade school. As a revision, you can divide a number evenly by some other number and whatever is left over will result as the remainder. This can be written more formally as:

$$dividend = (divisor)(quotient) + (remainder)$$

Now there is an important understanding I wanted to show to the audience. Every basic arithmetic operation can be written in terms of addition and multiplication. We will later see with rings that we make our lives easier by doing subtraction which shows both an inverse and additive property. But for now, that's all mumbo jumbo.

Theorem 2.2.1 Division Algorithm

Suppose $a, b \in \mathbb{Z}, b > 0, a = qb + r$ such that $\exists q, r \in \mathbb{Z}$, with $0 \leqslant r < b$.

Proof: Let there be set S such that

$$S := \{a - xb : a - xb \geqslant 0, x \in \mathbb{Z}\}$$

Check $S \neq \phi$

Given a and b, find x, such that $a - xb$. If $a \geqslant 0$, let $x = 0$, then $a - xb \implies a \geqslant 0$.
If $a < 0$ and let $x = a$, then $a - ab = a(1 - b)$, and since $b > 0, b \geqslant 1$, therefore $1 - b \leqslant 0$.
Since $S \neq \phi$ then S is well-ordered. $\exists r \in S$, such that r is the smallest element of S.

Claim: $r \geqslant 0$ and $r < b$. Since $r \in S, \exists q \in \mathbb{Z}$ such that $r \geqslant 0$ and $r = a - qb$. Prove that $r < b$.
Suppose $r \geqslant b$, then we can let

$$\begin{aligned} d &= a - (q+1)b \\ &= a - qb - b \\ &= r - b \\ r - b &\geqslant 0 \end{aligned}$$

So $0 \leqslant b < r, d = a - (q+1)b$, therefore $d \in S$, but $d < r$. Therefore we have a contradiction that r is the smallest element of S, therefore $r < b$. ■

There is a lot to dissect here. I want to dedicate special focus to this theorem. This will lay the foundation so glance your eyes on this beauty and take it in its glory. But in all seriousness, this is a really important topic to take in so let's explain it thoroughly. Similar to what we have in Figure 2.1 with the dividend equation, we just broke it down and generalized it using proof notation. So given that "a" is some dividend, we have divisor "b", and quotient "q" that are multiplied then added with remainder "r". There is also a reason why the division algorithm requires that r be less than b but at minimum 0. This may be trivial, but if r is greater than b, we can subtract r-b, and get the new remainder. It has the most optimized equation. Now that we understand what we are doing in more understandable terms, let us look at our proof itself and implement it as a core memory as how a child may remember their guardian.

Example 2.2.1

Let S be a set of remainders. We can do this through example. If

$$a = 81$$

$$b = 8$$

x is a variable

$$r = a - bx$$

If we let x = 1 for example, then r = 73.
If we let x = 4 for example, then r = 49.
If we let x = 10 for example, then r = 1.
If we let x = 11 for example, then r = -7.
However, r can only be at minimum 0, therefore r cannot be -7.
Therefore our most optimized r is when x = 10.
Of course, x can go in the opposite direction, since we did not bound Z only to non-negative integers.

Thus we have shown an example of the division algorithm. Now that we understand the values that set S can contain, even though we have provided proof, we must still prove this through math and generalize it. And that's exactly what we spend the rest of the proof doing. We answer questions in this proof such as, what if a is greater than 0 or less than 0? And what happens if r is greater than b, which we show that r is not the smallest integer which means we can technically have a solution of

Example 2.2.2

$$a = 81$$

$$b = 8$$

$$xisavariable$$

$$r = a - bx$$

If we let x = 1 for example, then r = 73.
If we let x = 4 for example, then r = 49.
If we let x = 10 for example, then r = 1.
If we let x = 11 for example, then r = -7.
However, r can only be at minimum 0, therefore r cannot be -7.
Therefore our most optimized r is when x = 10.
Of course, x can go in the opposite direction since we did not bound Z only to non-negative integers.

Thus we have shown an example of the division algorithm. Now that we understand the values that set S can contain, even though we have provided proof, we must still prove this through math and generalize it. And that's exactly what we spend the rest of the proof doing. We answer questions in this proof such as, what if a is greater than 0 or less than 0? And what happens if r is greater than b, which we show that r is not the smallest

integer which means we can technically have a solution of

$$a = 200$$
$$b = 2$$
$$x = 10$$
$$r = 180,$$

and this is a valid solution by the division algorithm if we did allow r to not be the smallest, even though we know it's not exactly true.

Proposition 2.2.1 Uniqueness in the Division Algorithm

The integers $q, r \in \mathbb{Z}$, in the division algorithm are unique.

Proof: Given $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^{\geqslant 0}$, Suppose $a = q_1 b + r_1$, such that $q_1, r_1 \in \mathbb{Z}$ and $0 \leqslant r_1 < b$. Also suppose that $a = q_2 b + r_2$, such that $q_2, r_2 \in \mathbb{Z}$ and $0 \leqslant r_2 < b$.
Claim: $q_1 = q_2$ and $r_1 = r_2$.

$$\begin{aligned} a &= q_1 b + r_1 \\ -a &= q_2 b + r_2 \\ 0 &= (q_1 - q_2)b + r_1 - r_2 \\ r_2 - r_1 &= (q_1 - q_2)b. \end{aligned}$$

Thus, $-b < r_2 - r_1 < b$. Therefore $-b < (q_1 - q_2)b < b$, then $-1 < q_1 - q_2 < 1$. Since $q_1, q_2 \in \mathbb{Z}$, and the only integer that is greater than -1 and less than 1 is 0, then $q_1 - q_2 = 0$. Therefore $q_1 = q_2$. Then

$$\begin{aligned} 0 &= (q_1 - q_2)b + r_1 - r_2 \\ 0 &= (0)b + r_1 - r_2 \\ 0 &= r_1 - r_2. \end{aligned}$$

Thus $r_1 = r_2$. ■

This proposition demonstrates that q and r are unique, and this is really important to show in math when we are proving an algorithm. Regardless of what q and r are, if they exist, then they are unique, sounding trivial but as we see the proof is rather... less trivial. This one is a bit more straightforward therefore there won't be a conceptualizing analysis on this proof. This is also just further building the proof techniques we have at our arsenal and allowing one to understand the algorithm through and through.

Definition 2.2.1: Logical Divide

Suppose $a, b \in \mathbb{Z}$. Let us define the logical divide of b divides a as $b \mid a$.
If $\exists q \in \mathbb{Z}$ in this logic, then $a = bq$. If $b = 0, a \neq 0$, then $b \nmid a$, because $0q = 0$, and $a \neq 0$.

There isn't a strict name for this definition as far as I know, therefore I created a name for it. Logical Divide. It is the logical notation for the phrase "x divides y", and it is trivial to Abstract Algebra. It is slightly different than say previous computationally algebraic courses, where one just computes some division and may even end up with a completed or incomplete (rational or not) answer. Note that up to now we are only sticking with the integers, and this is a really important fact to keep in mind. Therefore when we say that 2—4, then we really mean that 4 is evenly divisible by 2, but 3 does not divide 4, even if we can write it in terms of a decimal. Another way we can explain this topic is through the division algorithm. If it doesn't look similar, we can write b divides a as, a = bq + r, where r = 0. Now does this mean that if a = 0, does 0—0? Honestly, it's a debated topic in algebra and number theory, some may state yes, others may state no. But what's important, is that the majority say no, the same reason why your calculator cannot divide 0 from 0.
Now if a = 0 and b—a, there is an integer q in Z, such that a = bq and q is unique. This is proof we will not get into it for the sake of saving time and space, but it is a nice practice exercise.
One proof we will be looking at is:

Lemma 2.2.1

Assume $b \mid a, b \neq 0$, so $a = bq$ for $q \in \mathbb{Z}$, then $-b \mid a$.

Proof: $a = (-b)(-q)$, so $-b \mid a$, for $q \in \mathbb{Z}$. Similarly $b \mid -a$. ■

This is just a fun fact to rationalize that these four results are possible: b—a, b—-a, -b—a, -b—-a. Now on a larger note, we must prove transitivity through logical divides.

Lemma 2.2.2

Suppose $a, b, c \in \mathbb{Z}$. If $c \mid b$ and $b \mid a$¡ then $c \mid a$.

Proof: $\exists q_1, q_2 \in \mathbb{Z}$, such that $a = bq_1$ and $b = cq_2$. So $a = (cq_2)q_1 = c(q_2q_1)$. So $c \mid a$. ■

One thing to note is that divisibility is anti-reflexive, which means if b—a and a do not equal b or -b, then a does not divide b. There is a statement that could be said about linear combinations of a and b. If there is an integer c that divides both a and b, then there exists integers x and y, such that c—xa+yb. Therefore, c divides any linear combination of a and b. The proof of this is similar to the previous proof before. The idea is if you can write a and b in terms of c, then the linear combination could also be written in terms of c. Thus showing divisibility. Try to implement this on your own. If it hasn't been noticeable, there is nothing more to learning a course outside of learning the definitions and theorems.

Definition 2.2.2: Greatest Common Divisor

The GCD of a and b, written as $gcd(a, b) = d$, and $d > 0$ such that $d \mid a$ and $d \mid b$ and if $c \mid a$ and $c \mid b$, then $c \mid d$, and $c \leqslant d$.

The greatest common divisor is a concept that we have learned in grade school. If we recall, we can write the gcd(4,6) = 2, since 2—4 and 2—6.

Theorem 2.2.2 Linear Combinations of GCD

Let $a, b \in \mathbb{Z}$, not both 0. Let there be set S such that

$$S := \{xa + yb : x, y \in \mathbb{Z}, xa + yb > 0$$

Then $S \neq \phi$ and $S \subseteq \mathbb{Z}^{\geqslant 0}$, then by the well-ordering principle, S has the smallest element called d. Then $d = gcd(a, b)$.
The key statement is if $d = gcd(a, b)$, then $\exists x, y \in \mathbb{Z}$ such that $d = xa + yb$.

Proof: Let $S \neq \phi$. $\exists d \in S$ such that $\forall t \in S, d \leqslant t$ since $d \in S$. Then $\exists x, y \in \mathbb{Z}$ such that $d = xa + yb$. Now our goal is to prove that $d \mid a$.
If $d \in S$, then $d > 0$, so $\exists q, r \in \mathbb{Z}$ and $a = qd + r$ when $0 \leqslant r \leqslant d$.
Suppose $r > 0$, then

$$\begin{aligned} r &= a - qd \\ &= a - q(xa + yb) \\ &= a - qxa - qyb \\ &= (1 - qx)a - (qy)b. \end{aligned}$$

So r is a linear combination of a and b. Since $r > 0$ and $r < d$, then $r \in S$, contradicting the assumption that d is the smallest element of S.
If $r = 0$, then $a = qd$, therefore $d \mid a$.
Similarly we can show $d \mid b$.
Now suppose $c \mid a$ and $c \mid b$, then $c \mid xa + yb$, which is a linear combination of a and b, which equals d. Therefore d is unique.
Suppose $t > 0$ has the property that if $c \mid a$, $c \mid b$, then $c \mid t$, and $t \mid a$, $t \mid b$, then $t \mid d$ and $d \mid t$.
Therefore $d = t$. ■

If the gcd of any two integers ever equals 1, then we say that a and b are relatively prime. If they are relatively prime, then by the previous theorem, the linear combination will also equal 1.

Theorem 2.2.3

Suppose $gcd(a,b) = 1$ and $c \in \mathbb{Z}$ such that $a \mid bc$, then $a \mid c$.

Proof: Since the $gcd(a,b) = 1$, then $\exists x, y \in \mathbb{Z}$ such that $xa + yb = 1$. Therefore,

$$\begin{aligned} xa + yb &= 1 \\ cxa + cyb &= c \\ (cx)a + y(bc) &= c, \end{aligned}$$

then $a \mid a$ and $a \mid bc$, therefore $a \mid c$. ■

The last thing we will be looking at in this section is the extended gcd algorithm. The idea behind this is to use the gcd algorithm and then reverse the process in order to find the factors of the linear combination. This is more of a computational math. The GCD algorithm can be written in terms of the Division Algorithm and continuing to find the terms that make up the two factors. An idea of this is using the gcd(109, 26).

$$109 = 26(4) + 5$$

Because 109 can be split up by 26 and have a remainder of 5, this is no different than having a gcd of (26,5).

$$26 = 5(5) + 1$$

Now because we are left with a remainder of one, and one can go into any number, then 1 is our final answer for the gcd of (109, 26). This is a way to do the gcd algorithm through division. But what if we are to set this the other way around?

$$1 = 26–5(5)$$

Similar to what we did before, we are shifting all elements in the equation to create the one above.

$$1 = 26–5(109–26(4))$$

$$1 = (-5)(109) + (21)(26)$$

Thus we have found the linear combination factors of the equation.

2.3 Primes

In the realm of mathematics, prime numbers are the true VIPs. The Fundamental Theorem of Arithmetic serves as a bouncer taking off the cheap costumes that all the composites wear making sure only primes get through. In this post, we will look at how the FTA classifies numbers and how the primes are the real deal when it comes to these costumes. I'm excited about this topic because it practically is my field of interest!

Definition 2.3.1: Prime Integer

Let $p \in \mathbb{Z}$. p is prime if the only divisors of p are $-1, 1, -p, p$ and $p \neq -1, 0, 1$.

This definition has two criteria, 1) the divisors of p are restricted; 2) p is not equal to restricted values. We use the term restricted to denote more so a finite set of values, but this sounds like a stronger claim.
(1) By the only divisors of p, we mean that if you are to divide p by any other integer, using the division algorithm, we will get a remainder. Using the previous content learned, we will learn that the GCD of p and any relatively prime, or co-prime, is 1.
(2) When we have p not equal to a select few values, then this ensures that the prime number does not contradict the first criterion. This definition helps identify and distinguish prime numbers from other integers.

Theorem 2.3.1 Euclid's Lemma

Suppose p is prime, and $b, c \in \mathbb{Z}$ with $p|bc$, then $p|b$ or $p|c$. Proof. Suppose $p \nmid b$. We claim that the $gcd(p, b) = 1$.'

Proof: Suppose $d = gcd(p, b)$. Then $d > 0, d|p, d|b$, and since p is prime, then $d = 1$ or $d = p$. But $d \neq p$ since $p \nmid b$, so $d = 1$. Let's assume that p is prime. Then p would have some divisors $d, t \in \mathbb{Z}$, such that $p = dt$. Then according to our assumption, if p is prime, then the only divisors are $-1, 1 and - p, p$. Therefore, when $p|d$, then $d = -p, p$ and $t = -1, 1$. Or when $p|t$, then $t = -p, p$, and $d = -1, 1$. Thus p is prime. ■

This "lemma" is something Euclid used to prove something bigger. The name stuck as "Euclid's Lemma", however, it is the foundation for fields such as Number Theory. Its more appropriate name is the Fundamental Property of Prime Numbers. It sounds like a really basic lemma, but it does undermine its true essence. It shows that prime numbers are the building blocks of all integers and that a number divisible by a prime must be divisible by that prime individually or by another prime factor.

Theorem 2.3.2 Fundamental Theorem of Arithmetic (FTA)

If $n \in \mathbb{Z}$ and $n \neq -1, 0, 1$, then n can be written uniquely as a product of primes up to order and sign.

In other words, the theorem tells us that every composite number can be broken down into a unique set of prime factors. These prime factors are the building blocks of all positive integers. The uniqueness of the factorization means that no matter how you break down a composite number into its prime factors, the set of primes you obtain will always be the same, even if the order and sign of the primes might differ.

Lemma 2.3.1

Suppose p is prime. $a_1, a_2, a_3, \ldots, a_n \in \mathbb{Z}$ such that $p|a_1 a_2 \ldots a_n$. Then $p|a_1$ for some $i \in \mathbb{N}$.

Proof of Lemma: By induction on i, let $n = 1$. If $p|a_1$, then $p|a_1$ is true. Let $n = 2$. If $p|a_1 a_2$, then $p|a_1$ or $p|a_2$ is true. Suppose it's true for given $n = k$. Now let $n = k + 1$. If $p|a_1 a_2 \ldots a_k a_{k+1} = p|(a_1 a_2 \ldots a_k)a_{k+1}$, then $p|(a_1 a_2 \ldots a_k)$ or $p|a_{k+1}$. By induction, $p|a_i$ for some $i, 1 \leqslant i \leqslant k$, or $p|a_{k+1}$. ■

Now note that we haven't quite proved the Fundamental Theorem of Arithmetic, but something we have shown is a corollary of Euclid's Lemma, which relates to FTA a little bit. So let's go ahead and link these two out.

Proof of FTA Theorem:
Claim 1. Existence of Factorization:
Suppose $n \in \mathbb{Z}$ and $n \neq -1, 0, 1$. Then there exists primes $p_1 \ldots p_k$ such that $n = p_1 \ldots p_k$. If $n \in \mathbb{Z}$ is a negative integer, then $n = -m$ is a positive integer. If $n = p_1 \ldots p_k$, p prime, then $n = (-p_1)p_2 p_3 \ldots p_k$ is also a product of primes. So $\in \mathbb{N}$ is true for all $\in \mathbb{Z}$.

Proof of Claim 1: Suppose n is not prime, then $\exists a > 1$. So $n = ab$, given $b \in \mathbb{Z}$ and $b > 1$. Now apply strong induction on a and b.
$a = p_1 \ldots p_r$, p_i prime
$b = q_1 \ldots q_s, q_i$ prime
$n = ab = p_1 q_1 \ldots p_r q_s$ as a product of primes, i.e. if $n = p_1 \ldots p_r = q_1 \ldots q_s$, then $r = s$ and after rearranging $r_i = -q_i, q_i$, for each i. ■

Claim 2. Uniqueness of Factorization:
From existence, we can show uniqueness. By induction on the $min\{r, s\}$. Let our base case be $k = 1$. We can assume $r = 1$, so $p_1 = \mathbb{Q}1 \ldots \mathbb{Q}k, p_1$ prime, all $\mathbb{Q}i$ prime. So $s = 1, p_1 = \mathbb{Q}1$.

Proof of Uniqueness: Assume uniqueness for k, prove for $k+1$. Suppose $n = p_1 \ldots p_r = \mathbb{Q}1 \ldots \mathbb{Q}s, min\{r, s\} = k + 1$, as we can assume that $r = k + 1$. Then $p_1 \ldots p_k p_{k+1} = \mathbb{Q}1 \ldots \mathbb{Q}s$. So $p_1 \mathbb{Q}1 \ldots \mathbb{Q}s$, assume $p_1 = \mathbb{Q}1$. So $p_1 = -\mathbb{Q}1, \mathbb{Q}1$. Then let's replace this singular prime, $p_1 \ldots p_{k+1} = (p_1)\mathbb{Q}2 \ldots \mathbb{Q}s$. Then $p_1(p_2 \ldots p_{k+1}) = p_1(\mathbb{Q}2 \ldots \mathbb{Q}s)$. By cancellation law, then we can cross out the p_1's. Then the minimum number of terms is k. By the induction

hypothesis, $s = k + 1$, and after rearranging $\mathbb{Q}i = p_i$ all $i > 1$. So uniqueness is trying for k + 1. So true for all $k \in \mathbb{N}$. ■

The uniqueness of the factorization means that no matter how you break down a composite number into its prime factors, the set of primes you obtain will always be the same, even if the order of the primes might differ. For example, consider the number 60. The Fundamental Theorem of Arithmetic tells us that 60 can be expressed as a product of prime factors uniquely:

$$60 = 2 * 2 * 3 * 5$$

This factorization is unique for the number 60. You can change the order of the factors, but the set of primes (2, 3, and 5) will remain the same.

The Fundamental Theorem of Arithmetic tells us that every positive integer greater than 1 can be expressed uniquely as a product of prime factors. This unique factorization into prime numbers underpins countless mathematical discoveries, making it a cornerstone of number theory and algebra.

2.4 Exercises

Example 2.4.1 (Exercise 1)

Let a be any integer and let b and c be positive integers. Suppose that when a is divided by b, the quotient is q and the remainder is r, so that if ac is divided by bc, show that the quotient is q and the remainder is rc.

Example 2.4.2 (Exercise 2)

Let a, b, c, q be as in the previous exercise. Suppose that when q is divided by c the quotient is k. Prove that when a is divided by bc, then the quotient is also k.

Example 2.4.3 (Exercise 3)

Let n be a positive integer. Prove that a and c leave the same remainder when divided by n if and only if $a - c = nk$ for some integer k.

Example 2.4.4 (Exercise 4)

Prove that $b|a$ if and only if $(-b)|a$.

Example 2.4.5 (Exercise 5)

If $a|b$ and $b|c$, prove then $a|c$.

Example 2.4.6 (Exercise 6)

If $a|b$ and $a|c$, prove that $a|(b + c)$.

Example 2.4.7 (Exercise 7)

If $a|b$ and $a|c$, prove that $a|(br + ct)$ for any $r, t \in \mathbb{Z}$

Example 2.4.8 (Exercise 8)

Given a, b are non-zero. Suppose $a|b$ and $b|a$, then prove that $a = \pm b$.

Example 2.4.9 (Exercise 9)
If $a|b$ and $c|d$, then $ac|bd$.

Example 2.4.10 (Exercise 10)
If $a < 0$, find $gcd(a, 0)$.

Example 2.4.11 (Exercise 11)
Prove that $gcd(n, n + 1) = 1$ for every integer n.

Example 2.4.12 (Exercise 12)
If $a|c$ and $b|c$, must $ab|c$?

Example 2.4.13 (Exercise 13)
Given $n \in Z$, what are the possible values of $gcd(n, n + 2)$.

Example 2.4.14 (Exercise 14)
If $gcd(a, b) = d$, prove that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Example 2.4.15 (Exercise 15)
Suppose $gcd(a, b) = 1$. If $a|c$ and $b|c$, then prove that $ab|c$.

Example 2.4.16 (Exercise 16)
If $gcd(a, c) = 1$ and $gcd(b, c) = 1$, prove that $gcd(ab, c) = 1$.

Example 2.4.17 (Exercise 17)
If $a|c$ and $b|c$ and $gcd(a, b) = d$, prove that $ab|cd$.

Example 2.4.18 (Exercise 18)
If $a > 0$ and $b > 0$, prove that $lcm[a, b] = \frac{ab}{gcd(a,b)}$.

Example 2.4.19 (Exercise 19)
Verify that $2^5 - 1$ and $2^7 - 1$ are prime.

Example 2.4.20 (Exercise 20)
If $p > 5$ is prime and p is divided by 10, show that the remainder is $1, 3, 7,$ or 9.

Example 2.4.21 (Exercise 21)
Let p be an integer other than $0, \pm 1$ Prove that p is prime if and only if for each $a \in \mathbb{Z}$ either $(a, p) = 1$ or $p|a$.

Example 2.4.22 (Exercise 22)

Let p be an integer other than $0, \pm 1$ with this property: Whenever b and c are integers such that $p \mid bc$, then $p \mid b$ or $p \mid c$. Prove that p is prime.

Example 2.4.23 (Exercise 23)

If $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_i}$ and $b = p_1^{s_1} p_2^{s_2} \dots p_k^{s_i}$, where $p_1, p_2, \dots, p_k$ are distinct positive primes and each $r_i, s_i \geqslant 0$, then prove that

$gcd(a,b) = p_1^{n_1} p_2^{n_2} \dots p_k^{n_i}$, where for each i, $n_i = min\{r_i, s_i\}$.

Example 2.4.24 (Exercise 24)

If $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_i}$ and $b = p_1^{s_1} p_2^{s_2} \dots p_k^{s_i}$, where $p_1, p_2, \dots, p_k$ are distinct positive primes and each $r_i, s_i \geqslant 0$, then prove that

$lcm[a,b] = p_1^{t_1} p_2^{t_2} p_3^{t_3} \dots p_k^{t_i}$, where t_i = maximum of r_i, s_i.

Example 2.4.25 (Exercise 25)

Prove that $a \mid b$ if and only if $a^2 \mid b^2$.

Example 2.4.26 (Exercise 26)

Let p be prime and $1 < k < p$. Prove that p divides the binomial coefficient $\binom{p}{k}$.

Chapter 3

Congruence Classes in $\mathbb{Z}$

3.1 Congruences

When we talk about congruence classes mod n, we're essentially grouping integers based on the remainder they leave when divided by n. This creates a classification system, where numbers that share the same remainder form a class. It's like organizing a grand masquerade ball, where every guest wears a mask that matches their remainder modulo n, allowing them to join a specific group similar to classes/grades in school.

Definition 3.1.1: Congruence

Suppose $n \in \mathbb{N}$. If $a, b \in \mathbb{Z}$, we define $a \equiv b \mod n$ as a congruence. We say "a is congruent to b modulo n" if and only if $n|(b-a)$.

Lemma 3.1.1

$a \equiv b \mod n$ then $n|a-b$ if and only if there exists $q \in \mathbb{Z}$ such that $b = qn + a$. Prove this exercise on your own.

Definition 3.1.2: Equivalence Relation

Given S is a set and $\sim$ is a relation on S. $\sim$ is an equivalence relation if for all $a, b, c \in S$

1. $a \sim a$ (reflexive);
2. If $a \sim b$, then $b \sim a$ (symmetric);
3. If $a \sim b$ and $b \sim c$, then $a \sim c$ (transitive).

We will learn and find uses for the equivalence relation, but to connect it to the topics at hand, $a \equiv b$ is an equivalence relation that envelopes congruences and what we will learn about congruence classes. Essentially, $a \equiv b$ is the same as $a \sim b$.

Lemma 3.1.2

Congruence mod n is an equivalence relation.

Proof: **Case 1.**
Let $a \in \mathbb{Z}, a \equiv a \mod n$, because $a - a = 0$ and $n|0$.
Case 2.
Suppose $a \equiv b \mod n$ then $n|a-b$ and due to properties of the logical divide, $n|b-a$. Thus $b \equiv a \mod n$. **Case 3.**
Suppose $a, b, c \in \mathbb{Z}$, $a \equiv b \mod n$ and $b \equiv c \mod n$, so $n|b-a$ and $n|c-b$, so $n|(a-b)+(b-c) = n|a-c$. Thus $a \equiv c \mod n$. ■

Definition 3.1.3: Equivalence Classes

Suppose $\sim$ is an equivalence relation on S if $a \in S$. The equivalence class of a is $[a] := \{b \in S : b \sim a$.

Let's consider an equivalence relation $\sim$ on the set of integers $\mathbb{Z}$, where $a \sim b$ if and only if $a \equiv b \mod 5$ (congruence modulo 5). In this case:

$$[2]_5 = \{\ldots, 8, 3, 2, 7, 12, \ldots\}$$

This is the equivalence class of 2, consisting of all integers that are congruent to 2 modulo 5. Equivalence classes provide a systematic way of grouping elements in a set based on their relationships under an equivalence relation.

Definition 3.1.4: Congruence Classes

For a congruence mod n, if $a \in \mathbb{Z}$, $[a] := \{b \in \mathbb{Z} : b \equiv a \mod n\}$.

Congruence classes provide a systematic way of grouping integers based on their remainders when divided by n under a congruence relation. They are essential in modular arithmetic, number theory, and algebraic structures, contributing to a deeper understanding of mathematical relationships and structures. Two equivalence classes are the same if they include each other, for example, if $[a] = [b]$, then $a \in [b]$ and $b \in [a]$. The set S is the distinct union of its distinct equivalence classes. I.e. every element of S is in some equivalence class.

Proposition 3.1.1

If $a, b \in S$, then either $[a] = [b]$ or $[a] \bigcap [b] = \phi$.

Proposition 3.1.2

$[a] = [b] \iff a \equiv b \mod n$.

Proof.: ($\implies$). $[a] := \{x : x \equiv a \mod n\}$. so $a \in [a]$ since $a \equiv a \mod n$. So $a \in [b], [b] := \{x \in \mathbb{Z} : x \equiv b \mod n\}$, so $a \equiv b \mod n$.
($\impliedby$). **Case 1.** $[a] \subseteq [b]$**.**
Let $c \in [a]$, then $c \equiv a \mod n$. By transitivity, $c \equiv b \mod n$ so $c \in [b]$ so $[a] \subseteq [b]$.
Similarly, we can show $[b] \subseteq [a]$. Thus $[a] = [b]$. ■

This relationship provides a clear connection between the equality of equivalence classes and the congruence of integers modulo n.

Proof of Proposition 3.0.1: We need to prove if $[a] \bigcap [b] \neq \phi$ then $[a] = [b]$. Let $c \in [a] \bigcap [b]$, then $c \equiv a \mod n, c \equiv b \mod n$. So by the previous proposition, $[c] = [a] = [b]$, so $[a] = [b]$. ■

Proposition 3.1.3

Fix $n \geqslant 2$. The distinct congruence classes modulo n are $[0], [1], \ldots, [n-1]$. In fact, if $a \in \mathbb{Z}$, then $[a] = [r]$ where r is the remainder when a is divided by r.

Proof: If $a = qn + r, 0 \leqslant r \leqslant n - 1$, then $a \equiv r \mod n$ so $[a] = [r]$. By the division algorithm, $[a]$ must be one of these classes. By uniqueness, these classes are unique. ■

3.2 Modular Arithmetic

Definition 3.2.1: Modular Arithmetic

Fix $n \in \mathbb{Z}^{\geqslant 2}$. Define addition and multiplication on congruence classes mod n.

$$[a] + [b] = [a + b]$$

$$[a] \cdot [b] = [ab]$$

Given this definition, it seems a little ambiguous if you really sit down and analyze it but we come to learn that this gives us properties to also allow this arithmetic to be well-defined. This definition shows that it is closed under addition but also multiplication and I will leave that up to the reader to figure out how to find such values.

Theorem 3.2.1

If $a, b, c, d \in \mathbb{Z}$, then $a + b \equiv c + d \mod n$ and $ab \equiv cd \mod n$.

Proof: Given $n|c - a$, $n|d - b$, then $n|(c - d) - (a + b)$, so $n|(c - a) + (d - b)$. Thus $n|c - a, n|d - b, n|d(c - a) + a(d - b), n|cd - ab + cd - ab$, therefore $n|cd - ab$. ■

Theorem 3.2.2 Well-Defined Modular Arithmetic

Modular arithmetic is well-defined.

Proof: Suppose $[a] = [c]$ and $[b] = [d]$. Then by the previous theorem, $[a + b] = [c + d]$ and $[ab] = [cd]$. ■

Definition 3.2.2: $\mathbb{Z}_n$

The set of congruence classes mod n with addition is defined by:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Commutative, associative, and distributive hold for $\mathbb{Z}_n$.
The additive identity is $[0] + [a] = [a]$.
The multiplicative identity is $[1a] = [a]$.

$\mathbb{Z}_n := \{[a] : a \in \mathbb{Z}\} = \{[0], [1], \ldots, [n - 1]\}$.

Axiom 3.2.1 Additive inverses in $\mathbb{Z}_n$

Every element in $\mathbb{Z}_n$ has an additive inverse.

$$[a] + [-a] = 0$$

3.3 Units and Divisors

Definition 3.3.1: Units in Congruence Classes

$[a]$ is a unit if $[a]$ has a multiplicative inverse.

Theorem 3.3.1

$[a]$ is a unit if and only if $gcd(a, n) = 1$.

Proposition 3.3.1

All classes in $\mathbb{Z}_p$ are units.

Proof of Proposition 3.2.1: Suppose $[a] \in \mathbb{Z}_p$ is a unit so $\exists x \in \mathbb{Z}$ such that $[xa] = 1$. Then

$$\begin{aligned} xa \equiv 1 \mod p &\iff xa = 1 + qp \\ &\iff xa - qp = 1 \\ &\iff gcd(a, p) = 1 \end{aligned}$$

■

Easy to show the opposite by showing a multiplicative inverse in the $\mathbb{Z}_p$. So $[a]$ has a multiplicative inverse. This proposition, using $n \neq p$ will show it is true for the **Theorem 3.2.3**.
To show that $[a]$ is a unit in $\mathbb{Z}_{32}$ and find $[a]^{-1}$ in $\mathbb{Z}_{32}$. Let $a = 4$ and find an $x \in \mathbb{Z}$ such that $x4 + q32 = 1$, and use the Extended Euclidean Algorithm to find this inverse. We find that $x = -7$, which means $[x] = [-7] = [25]$.

Definition 3.3.2: Zero-Divisors

$[a]$ is a zero-divisor in $\mathbb{Z}_n$ if $\exists [x] \neq [0]$, with $[ax] = [0]$.

Theorem 3.3.2

$[a]$ is a zero-divisor in $\mathbb{Z}_n$ if and only if the $gcd(a, n) \neq 1$.

Proof: Let's prove the contrapositive. Suppose $gcd(a, n) = 1$, then $[a]$ is not a zero-divisor. Assume $gcd(a, n) = 1$. Suppose $b \in \mathbb{Z}$ with $[ab] = [0]$. $[a]$ is not a zero-divisor if and only iff $[ab] = [0]$ implies $[b] = [0]$. By **Theorem 3.2.3**, $[a]$ is a unit in $\mathbb{Z}_n$, so there exists $x \in \mathbb{Z}$, such that $[xa] = 1$. So $[x]([ab]) = [x0] = [0]$ or $[xa][b] = [1][b] = [b] = [0]$. Conversely, suppose $gcd(a, n) = d > 1$. ■

For example, if we take $\mathbb{Z}_{12}$, then since $gcd(4, 12) = 4$, then $[4]$ is a zero-divisor.

3.4 Exercises

I will work on these soon, but the base content is stabilized now.

Chapter 4

Rings

Around this chapter is where most textbooks will start. Some of the concepts that we introduced in the previous chapters are more seen as prior knowledge, or seen in an introduction chapter similar to what we have with Chapter 1. So from here on out, consider everything you learned so far as a foundation for the rest of the content.

4.1 Rings

Definition 4.1.1: Ring

A set with $+, \times$, called R. Addition has the properties of being commutative and associative. Multiplication is at minimum associative, and together distributive. There is an additive identity, usually denoted by 0_R. But there is also a multiplicative identity, denoted by 1_R. There exists an additive inverse in R, b, such that $a + b = 0$, and are unique.

Definition 4.1.2: Subrings

S is a subring of R if for all $a, b \in S$, has closure under addition and multiplication. It must also have the additive identity and additive inverses per each element.

For example, in an introduction to proofs class we may have seen that

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

We learned them assets, but looking at properties of rings and subrings, consider them all rings and subrings of the order. However, if we wanted to look outside of these number systems, let's look at matrices:

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$$

Note that this is a subring of $Mat_2(\mathbb{R})$.

Definition 4.1.3: Field

A commutative ring, $\mathbb{F}$, $1 \in \mathbb{F}$. if $a \in \mathbb{F}$, such that a is a unit. $\mathbb{F}$ is called a field.

Definition 4.1.4: Subfield

If S is a subring of field $\mathbb{F}$, and also closed under multiplicative inverses, then it is also a subfield.

We have previously learned that

$$\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$$

is a subring of $Mat_2(\mathbb{R})$. But I also claim it is a field itself.

Proof of Claim: Suppose $Mat_2(0) \notin M = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, which means a and b not both 0.

$$\det M = a^2 + b^2$$

Let $M^{-1} = \frac{1}{a^2+b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Thus we have shown that the subring also is closed under multiplicative inverses. This is a field. ■

Lemma 4.1.1

For n composite, $\mathbb{Z}_n$ is not a field if it has zero-divisors.

From now on $\mathcal{R}, \mathcal{S}$ is a ring and $\mathbb{F}$ is a field.

Definition 4.1.5: Integral Domain

Suppose n is a commutative ring with $1 \in \mathcal{R}$. We say $\mathcal{R}$ is an integral domain if $a \neq 0$ and $a \in \mathcal{R}$ and a is not a zero-divisor.

We can think of these integral domain rings as being almost a field but the only thing discerning them from being a field is the fact the only zero-divisor is $0_{\mathcal{R}} \in \mathcal{R}$. Remember that if there is $0 \in \mathcal{R}$ then it is no way it can be a field, since all fields have $0 \notin \mathbb{F}$, since all elements must have an inverse a.k.a a unit.

Corollary 4.1.1

$\mathbb{F}$ is an integral domain.

Proof: Suppose $a, b \in \mathbb{F}$ with $ab = 0$. Suppose $a \neq 0$, then a is a unit with inverse a^{-1}. then

$$\begin{aligned} a^{-1}(ab) &= a^{-1} \cdot 0 = 0 \\ &= 0 \\ (a^{-1}a)b &= 1b = 0 \\ &= b = 0 \end{aligned}$$

■

Let's look into something called extensions.

Definition 4.1.6: Field Adjoins

We call something an adjoin given that suppose we have $\mathbb{F} = \mathbb{Q}$. Note this field is a subfield of $\mathbb{R}$. Then an extension of $\mathbb{Q}$ is taking an element of $\mathbb{R} \setminus \mathbb{Q}$, and adding it to $\mathbb{Q}$. An example of this is,

$$\mathbb{Q}[\sqrt{7}] := \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}$$

In fact an exercise to do is to show that $\mathbb{Q}[\sqrt{7}]$ is a subfield. Based on everything we have observed, we can say that $\mathbb{Z}_p$ is a field and $\mathbb{Z}_n$ is not even an integral domain.

Axiom 4.1.1 Pigeonhole Principle

If you have $n + 1$ objects in n slots, one slot will have more than 1 element.

Theorem 4.1.1

Finite integral domain is a field.

Proof: Let F be a finite integral domain. We need to show that if $0 \neq u \in F$, then u has a multiplicative inverse. Consider the set $\{u, u^2, u^3, \ldots\}$. Suppose F has n elements, then there must be repetition. So $u^k = u^m$ for $m > k$.

$$u^m - u^k = 0$$
$$u^k(u^{m-k} - 1) = 0$$

Since F is an integral domain, then $u^k = 0$ or $u^{m-k} - 1 = 0$. Since $u \neq 0$, the $u^k \neq 0$. Then

$$u^{m-k} - 1 = 0$$
$$u^{m-k} = 1$$
$$u(u^{m-k-1}) = 1$$
$$u^{-1} = u^{m-k-1}.$$

Thus F is a field. ■

4.2 Homomorphisms and Isomorphisms

Definition 4.2.1: Homomorphism

Let $\mathcal{R}$ and $\mathcal{S}$ be rings. Suppose a function $f : \mathcal{R} \mapsto si$, with given that $a, b \in \mathcal{R}$, $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Definition 4.2.2: Isomorphism

Suppose f is a bijective homomorphism, then f is an isomorphism.

If f is an isomorphism, then $\mathcal{R}$ and $\mathcal{S}$ are isomorphic to each other. Suppose $\mathcal{R} = \mathbb{Z}$ and $\mathcal{S} = 2\mathbb{Z}$ and let $f : \mathcal{R} \mapsto \mathcal{S}$ defined by $f(m) = 2m$. Is an isomorphism?

Disproof:

$$f(m + n) = 2(m + n) = 2n + 2m$$
$$f(mn) = 2mn \neq f(m)f(n)$$

Not isomorphic. ■

Definition 4.2.3: Endomorphism

A homomorphism that maps $\mathcal{R}$ to itself is called an endomorphism.

Definition 4.2.4: Automorphism

An isomorphic endomorphism is called an automorphism.

Proposition 4.2.1

A bijection exists if and only if it has an inverse.

Proof: Let $g : \mathcal{S} \mapsto \mathcal{R}$, thus $f \circ g$ is the identity of $\mathcal{S}$. And $g \circ f$ is the identity of $\mathcal{R}$. Define $g(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Let $f(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = a + bi$. This is closed under addition and multiplication. It also has an inverse due to the determinate law for inverses. ■

Axiom 4.2.1 Isomorphism Properties

We can check the properties of a homomorphism to check if it is isomorphic.

1. # of elements in $\mathcal{R} = \mathcal{S}$
2. # of units in $\mathcal{R} = \mathcal{S}$ (Check how many coprimes in both sets)
3. # of 0-divisors for both are the same.

For example, we can state that $\mathbb{Z} \ncong \mathbb{Q}$. The reason is that every element in $\mathbb{Q}$ is a unit as the only unit in $\mathbb{Z}$ is 1. Similarly, $\mathbb{Z}_4 \ncong \mathbb{Z}_6$, due to the number of elements.
Perhaps in previous courses, such as Calculus III, you have looked at $\mathbb{R}^3$, which means a 3-tuple ordered pair that represents (x,y,z) in a space. However, this is a generalized fact. What if I wanted to have two points from different sets, but still create an ordered pair or tuple?

Axiom 4.2.2 Cartesian Product

If $\mathcal{R}$and $\mathcal{S}$ are rings, then $\mathcal{R} \times \mathcal{S} := \{(r, s) : r \in \mathcal{R}, s \in \mathcal{S}\}$ is also a ring under addition and multiplication.

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

It will be a fun exercise to prove the following lemma or at least a couple of examples.

Lemma 4.2.1

If the $gcd(m, n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Note that in $\mathbb{Z} \times \mathbb{Z}$, the zero-divisors are $(0, 1), (1, 0)$.
Let $\mathcal{R} = \mathcal{S} = \mathbb{Z}$ in $\mathbb{Z} \times \mathbb{Z}$. Let $\pi : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$. Then we have that $\pi[(1, 0)] = 1$, which is a unit. So a homomorphism need not preserve zero-divisors.

4.3 Exercises

I will work on these soon, but the base content is stabilized now.

Chapter 5

Polynomials

5.1 Polynomials

Definition 5.1.1: Polynomial

A polynomial with coefficients in a $\mathcal{R}$ is denoted by $\mathcal{R}[x]$, which is an extension field of x expanding the set to include

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.$$

We can think of a_n as coefficients.

Proposition 5.1.1

We do addition and multiplication component-wise, which means given an i large enough, a will eventually be 0. To understand what I mean, let

$$f(x) = a_0 + \ldots + a_nx^n$$
$$g(x) = b_0 + \ldots + b_mx^m,$$

given that $m \geqslant n$. Therefore

$$f(x) + g(x)$$

This informal definition raises several questions: What is x? Is it an element of R? If not, what does it mean to multiply x by a ring element? To answer these questions, note that an expression of the form $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ makes sense, provided that the a_1 and x are all elements of some larger ring. An analogy might be helpful here. The number π is not in the ring of integers ($\mathbb{Z}$), but expressions such as $3 - 4\pi + 12\pi^2 + \pi^3$ and $8 - \pi^2 + 6\pi^5$ make sense in the real numbers ($\mathbb{R}$). Furthermore, it is not difficult to verify that the set of all numbers of the form $\sum_{i=0}^{n} a_i\pi^i$, with $n \geqslant 0$ and $a_1 \in \mathbb{Z}$, is a subring of $\mathbb{R}$ that contains both $\mathbb{Z}$ and π. For the present, we shall think of polynomials with coefficients in a ring R in much the same way, as elements of a larger ring that contains both R and a special element x that is not in R. This is analogous to the situation in the preceding paragraph with R in place of $\mathbb{Z}$ and x in place of π, except that here we don't know anything about the element x or even if such a larger ring exists.
Feel free to check if $R[x]$ is a ring, but we will be concentrating on $\mathbb{Z}[x], \mathbb{Q}[x]\mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_p[x]$, and have their elements denoted by $f(x)$ or $P(x)$.

Definition 5.1.2: Degree of a Polynomial

If $f(x) \in \mathcal{R}[x]$, the degree of $f(x)$, denoted by $\deg f(x)$, is the largest n for which the coefficient of x^n is not 0. a_n is also called the leading term.

Definition 5.1.3: Additive Identity of $\mathcal{R}[x]$

a_n is 0.

If the $\deg f(x) = 0$, then the degree is undefined, which means the leading term is undefined.

Proposition 5.1.2 Degree Arithmetic

Suppose $\deg f(x) = m, \deg g(x) = n$,

$$\deg f(x) + g(x) \leqslant \max\{\deg f(x), \deg g(x)\}$$

if $m \neq n$

$$\deg f(x) + \deg g(x) = \max\{m, n\}$$

if $m = n$

$$\deg f(x) + \deg g(x) \leqslant \max\{m, n\}$$

If $f(x)g(x) = a_0b_0 + \ldots + a_nb_mx^{n+m}$, so $\deg f(x)g(x) \leqslant \deg f(x) + \deg g(x)$.
However, if $\mathcal{R}$ is an integral domain, then

$$\deg f(x)g(x) = \deg f(x) + \deg g(x)$$

Let $f(x), g(x) \in \mathbb{Z}_4[x]$, $f(x) = 2x, g(x) = 2x^2$, then $f(x)g(x) = 4x^3 = 0$.

From now on $\mathcal{R}$ is an Integral Domain.

Given that $\mathcal{R}$ is an integral domain, one may naturally ask, what are the units of $\mathcal{R}$?

Lemma 5.1.1

Suppose $u(x)$ is a unit with a multiplicative inverse $v(x)$. Then

$$u(x)v(x) = 1 = 1 + 0x + 0x^2 + \ldots$$

5.2 Division

Theorem 5.2.1 Division Algorithm in Polynomial Fields

Suppose $\mathbb{F}$ is a field and $a(x), b(x) \in \mathbb{F}[x], b(x) \neq 0$. Then there exists a unique $r(x) \in \mathbb{F}[x]$ with

$$a(x) = q(x)b(x) + r(x)$$

with $\deg(r(x)) > \deg(b(x))$ or $r(x) = 0$.

Proof: **Case 1:** If $a(x) = 0$ or $\deg(a(x)) < \deg(b(x))$, then $q(x) = 0$ and $r(x) = a(x)$ because $a(x) = b(x)0 + a(x)$. **Case 2:** If $a(x) \neq 0$ and $\deg(a(x)) > \deg(b(x))$, and $a(x)/b(x) = h(x)$, then $\deg(h(x)) < \deg(a(x))$. If $\deg(a(x)) = 0$, then $a(x) = a$, a constant in $\mathbb{F}$. $\deg(b(x)) < \deg(a(x))$ implies $b(x)$ equals a constant.

$$\begin{aligned} a(x) &= b(x)(b(x)^{-1}a(x)) + 0 \\ q(x) &= b(x)^{-1}a(x) \\ r(x0 &= 0. \end{aligned}$$

Assume the division is using strong induction. For all polynomials of $\deg(a(x)) < \deg(b(x))$ assume $b(x), a(x)$. Then $a(x) = a_nx^{n-m}b(x) + h(x)$ such that $\deg(h(x)) < \deg(a(x))$. $h(x) = q_1(x)b(x) + r(x)$ such that $\deg(r(x)) <$

$\deg(b(x))$ or $r(x) = 0$.
Proof of Uniqueness: Suppose

$$\begin{aligned} a(x) &= q_1(x)b(x) + r_1(x) \\ &= q_2(x)b(x) + r_2(x) \end{aligned}$$

where $\deg(r_1(x)), \deg(r_2(x)) < \deg(b(x))$ or $r_1(x), r_2(x) = 0$. So

$$\begin{aligned} [q_1(x) - q_2(x)]b(x) + [r_1(x) - r_2(x)] &= 0 \\ [q_1(x) - q_2(x)]b(x) &= [r_2(x) - r_1(x)]. \end{aligned}$$

So either $r_2(x) = r_1(x) = 0$ or $\deg(r_2(x) - r_1(x)) \leqslant \deg(r_1(x)) \leqslant \deg(r_2(x))$.
In any case $\deg(r_2(x) - r_1(x)) < \deg(b(x))$ or $r_2(x) = r_1(x) = 0$. Let's state $a(x) \neq 0$. Then $a(x)b(x) = a_n b_m x^{n+m} + \ldots a_0 b_0$, and $a_n b_m \neq 0$.
Suppose $(q_1(x) - q_2(x))b(x) \neq 0$. Then $\deg((q_1(x) - q_2(x))b(x)) = deg(q_1(x)q_2(x)) + deg(b(x)) \geqslant deg(b(x))$.
Conclusion: $(q_1(x) - q_2(x))b(x) = 0$ thus $q_1(x) = q_2(x)$. And since $r_2(x) - r_1(x) = 0$, then $r_2(x) = r_1(x)$. ■

The Division Algorithm for polynomial fields is a fundamental concept that allows you to divide one polynomial by another, similar to the division algorithm with integers. This algorithm helps you express one polynomial as a quotient of another polynomial plus a remainder.

Definition 5.2.1: Logical Divide of Polynomial Fields

Let $a(x), b(x) \in \mathbb{F}$ and $b(x) \neq 0$. We say $b(x)|a(x)$ if there exists a $q(x) \in \mathbb{F}$ such that $a(x) = q(x)b(x)$.

Definition 5.2.2: GCD of Polynomial Fields

Suppose $a(x), b(x) \in \mathbb{F}[x]$ not both 0. $d(x) = gcd(a(x), b(x))$ means $d(x)a(x), d(x)b(x)$, and if there exists a $c(x) \in \mathbb{F}[x]$ with $c(x)a(x), c(x)b(x)$, then $c(x)d(x)$ so $deg(c(x)) \leqslant deg(d(x))$.

Suppose we are in $\mathbb{Q}[x]$. Let

$$a(x) = (x-1)^2$$

and

$$b(x) = (x-1)(x-2).$$

Then the $gcd(a(x), b(x)) = x - 1$. But wait, doesn't $2x - 2|a(x)$ and $b(x)$.
We have a problem on our hands... We have to figure out how to circumvent this solution and before we can do that, let's go ahead and introduce a new term.

Definition 5.2.3: Monic

If $d(x) \in \mathbb{F}[x]$ has a leading coefficient of 1, then $d(x)$ is monic.

In algebra, monic polynomials are commonly used in the context of irreducible polynomials (polynomials that cannot be factored further). Monic irreducible polynomials have a leading coefficient of 1, and this condition simplifies discussions of unique factorization.

Definition 5.2.4: Polynomial Associates

If $c(x), d(x) \in \mathbb{F}[x]$ and $c(x) = \beta d(x)$ and $\beta \in \mathbb{F}$ and $\beta \neq 0$, we say $c(x)$ and $d(x)$ are associates.

We can think of associates as polynomial constant multiples.

Theorem 5.2.2 GCD Theorem

Suppose $a(x), b(x) \in \mathbb{F}[x]$ not both 0. Let

$$S := \{u(x)a(x) + v(x)b(x) \neq 0 : u(x), v(x) \in \mathbb{F}[x]\}$$

, then there exists $u(x), v(x) \in \mathbb{F}[x]$, such that $d(x) = u(x)a(x) + v(x)b(x)$ and $d(x) = gcd(a(x), b(x))$. S has a unique monic polynomial of the smallest degree which is the $gcd(a(x), b(x))$.

This theorem also answers the question to our gcd question, which shows that we want to have a monic polynomial of smallest degree as our $gcd(a(x), b(x))$. The set of degrees is a subset of $\mathbb{Z}^+$, and let $d(x)$ be a monic polynomial of minimal degree in S, so the theorem exists. The GCD (Greatest Common Divisor) Theorem for Polynomial Fields is a fundamental result in abstract algebra that addresses the existence and uniqueness of the greatest common divisor of two polynomials in a polynomial ring over a field. The theorem establishes a clear and precise method for finding the GCD of polynomials and its properties.

Proof: Let $d(x)$ be a monic polynomial such that $d(x) \in S$. If $c(x)$ is any polynomial in S, then $\deg(d(x)) \leqslant \deg(c(x))$. We need to show that $d(x)|a(x)$.

Let's use the division algorithm. Suppose $d(x) \neq 0$. We write $a(x) = q(x)d(x) + r(x)$, so $r(x) = 0$. We show this by saying $r(x)$ is a non-zero and $r(x) \in S$ and $r(x) = a(x) - q(x)d(x)$ where $d(x) = a(x)u(x) + b(x)v(x)$ such that

$$\begin{aligned} r(x) &= a(x) - q(x)(a(x)u(x) + b(x)v(x)) \\ &= 1 - q(x)u(x)a(x) - q(x)v(x)b(x)S. \end{aligned}$$

Contradicting $d(x)$ as being a polynomial with the least degree. We conclude $r(x) = 0$, so $d(x)|a(x)$. Similarly $d(x)|b(x)$. Suppose $c(x)|a(x), c(x)b(x)$, then $c(x)|u(x)a(x) + v(x)b(x) = d(x)$. ■

Definition 5.2.5: Relatively Prime

$a(x), b(x) \in \mathbb{F}$, not both 0. a(x) and b(x) are relatively prime if $gcd(a(x), b(x)) = 1$.

Corollary 5.2.1 Consequence of GCD Theorem

Suppose $a(x), b(x) \in \mathbb{F}$ are relatively prime and $c(x) \in \mathbb{F}$. If $a(x)|b(x)c(x)$, then $a(x)|c(x)$.

Proof: By the gcd theorem, we have $1 = u(x)a(x) + v(x)b(x)$, so $c(x) = c(x)u(x)a(x) + c(x)v(x)b(x)$. Since $a(x)|c(x)u(x)a(x)$ and $a(x)|c(x)v(x)b(x)$, then $a(x)|c(x)$. ■

If we let $\mathcal{R} = \mathbb{F}[x]$, we notice that it has very similar properties to $\mathbb{Z}$, such that it has the division and gcd algorithm. In fact, it also will have relatively prime and an equivalence to primes but for polynomials. Let's look at this equivalence.

Definition 5.2.6: Irreducible

A polynomial $p(x) \in \mathbb{F}[x]$ is irreducible if $p(x) = a(x)b(x)$ for $a(x), b(x) \in \mathbb{F}[x]$ then $a(x)$ is an associate of $p(x)$ or $a(x)$ is a unit.

5.3 Irreducibility

Proposition 5.3.1 Polynomial Euclid's Lemma

Suppose $p(x) \in \mathbb{F}[x]$ which is irreducible and $b(x) \in \mathbb{F}[x]$ such that $p(x) \nmid b(x)$, then $gcd(p(x), b(x)) = 1$.

Proof: Let $d(x) = gcd(p(x), b(x))$. $d(x)|p(x), d(x)|b(x)$, and since $p(x)$ is irreducible, then $d(x)$ is monic, $d(x) = 1$, $d = cp(x)$ given that $c \in \mathbb{F}$.
If $d(x) = cp(x)$ and $d(x)|b(x)$, then $p(x)|b(x)$, a contradiction arose. Therefore $p(x)|b(x)$ or $p(x)|c(x)$. ■

Corollary 5.3.1

If $p(x)|a_1(x)\dots a_n(x)$, given $a_i(x) \in \mathbb{F}[x]$, $p(x)$ is irreducible, then $p(x)|a_i(x)$ for some i. Then show the

answer by induction on n.

Theorem 5.3.1

Suppose you have any polynomial $a(x) \in \mathbb{F}[x]$, then $a(x)$ has a factorization into irreducible polynomials. This factorization is unique up to order and associates.

Proof: Use strong induction on degree of $a(x)$.
Uniqueness. If

$$\begin{aligned} a(x) &= p_1(x) \dots p_r(x) \\ &= q_1(x) \dots q_s(x), \end{aligned}$$

where $p_i(x), q_i(x)$ are irreducible. Then let $r = s$ and after rearranging $q_i(x)$, $p_i(x)$ is an associate of $q_i(x)$ each.
Proof of Uniqueness. $p_1(x) | q_1(x) \dots q_s(x)$, $p_i(x) | q_i(x)$ for some i. Without loss of generality, since $q_1(x)$ is irreducible, then $p_1(x), q_1(x)$ are associates. Proceed to show this by induction on $\min\{r, s\}$. ■

Lemma 5.3.1 Irreducible degrees

Degree 1 polynomials are irreducible.
If a degree 2 polynomial is reducible, then it is made of linear polynomials.

Lemma 5.3.2 Freshman's Dream

In $\mathbb{Z}_2$, $(x+1)^2 = x^2 + 1$.

Proposition 5.3.2

If $f(x)$ is irreducible $\mathbb{F}[x]$, so are all associates $f(x)$

Take note of that for the equation $x^2 + ax + b$, there are 3 choices for each a, b which means 9 total choices for this polynomial. The number of monic polynomials of $\deg n$ in $\mathbb{Z}_p[x]$ is p^n. Total number of polynomials of $\deg n$ is $(p-1)p^n$.

Example 5.3.1

Prove that $x^2 + 2$ is irreducible in $\mathbb{Q}[x]$.

Proof:

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \in \mathbb{R}$$

This factorization is unique. Since factorization $\mathbb{Q}[x]$ is also unique if $x^2 - 2$ had a factorization by linear. It would have include $(x - \sqrt{2})(x + \sqrt{2})$, but $\sqrt{2} \notin \mathbb{Q}$. ■

Let $\mathbb{F}$ be a field. Take $f(x) \in \mathbb{F}[x]$, there is a corresponding polynomial function, $\mathbb{F} \mapsto \mathbb{F}$ denoted by $f(x)$.

Theorem 5.3.2 Factor Theorem

Let $f(x) \in \mathbb{F}[x]$ and $a \in \mathbb{F}$ if $f(a) = 0$, then $(x-a)$ is a factor of the polynomial $f(x)$. i.e. $f(x) = g(x)(x-a)$.

Example 5.3.2

(a). Show that $x^2 + 2$ is irreducible in $\mathbb{Z}_5[x]$.

Proof of Example 5.2.2: We will do a proof by contradiction. Suppose x^2+2 is not irreducible. Then x^2+2 is made up of linear polynomials such that $(x+a)(x+b) = x^2+2$. But note that $(x+a)(x+b) = x^2+xa+xb+ab$, and we don't have a degree 1 in our polynomial. Therefore, $a = -b$, thus $(x+a)(x-a)$ will result in x^2+a^2, but note that $a^2 = 2$ or $a^2 = 3$, and $a = \pm\sqrt{2}$ or $a = \pm\sqrt{3}$, but $\sqrt{2}, \sqrt{3} \notin \mathbb{Z}_5$. Therefore, this polynomial, x^2+2 is irreducible. ■ ■

(b). Factor x^4-4 as a product of irreducibles in $\mathbb{Z}_5[x]$.

$$(x^2+2)(x^2-2)$$

However, (x^2-2) is not further reducible, since we will deal with an irrational $\sqrt{2}$, which is not in $\mathbb{Z}_5$.

Theorem 5.3.3 Remainder Theorem

Let $f(x) \in \mathbb{F}[x], a \in \mathbb{F}[x]$. Then $f(x) = g(x)(x-a)+r(x)$, given there exists $g(x) \in \mathbb{F}[x]$. $r(x)$ is a constant.

Proof of Remainder Theorem: By division algorithm, $f(x) = g(x)(x-a)+r(x)$ where $r(x) = 0$ or $\deg(r(x)) < \deg(x-a)$ or $r(x) = 0$.
If $\deg(r(x)) < \deg(x-1)$, then $\deg(r(x)) < 1$ implying that $\deg(r(x)) = 0$. So $r(x)$ is some constant or 0. ■

Proof of Factor Theorem: We know by remainder theorem $f(x) = g(x)(x-a)+r(x)$ where $r(x)$ is a constant, indexed function and by the previous example we now have that

$$\begin{aligned} f(a) &= g(x)(a-a)+r(x) \\ &= r(x). \end{aligned}$$

So $f(x) = g(x)(x-a)$. ■

Definition 5.3.1: Roots

a is a root of $f(x)$ if $f(a) = 0$.

Corollary 5.3.2 of Factor Theorem

Suppose $f(x) \in \mathbb{F}[x]$ has $\deg f(x) = n$, then $f(x)$ has at most n different roots.

Proof: By induction on $\deg f(x)$; Suppose $\deg f(x) = 0$, f is a non-zero constant with no roots.
$\deg f(x) = 1$, then $f(x) = a_1x + a_2$, $a \neq 0$. Only one root at $x = \frac{-a_2}{a_1}$. Assume true for polynomials of $\deg f(x) = n-1$. If $b \neq a$, then b is a root of f(x). $0 = f(b) = (b-a)g(b)$, $b-a \neq 0 \implies g(b) = 0$. By the induction hypothesis, there exists at most $n-1$ such b. So the number of roots of $f(x)$ is at most $1+(n-1) = n$.
■

If $f(x) \in \mathbb{Q}[x]$, then the rational root test tells us if $f(x)$ has a linear factor.

Definition 5.3.2: Rational Root Test

If $r|a_0$ and $s|a_n$ and $gcd(r,s) = 1$ then $\frac{r}{s}$ is a possible root given that $f(\frac{r}{s}) = 0$. Since a_0 and a_n have finitely many factors, then there are only finitely many factors to check.

For example, $2x^3-x^2+1$ is irreducible due to the Rational Root Test, as we find the $r/s = 1/2, 1$ and their additive inverses. After checking all possibilities plugged into $f(x)$, we see none of them are 0.
Suppose $f(x) \in \mathbb{Z}[x]$ and $g(x), h(x) \in \mathbb{Q}[x]$ then $\exists \alpha, \beta \in \mathbb{Q}$ such that

$$f(x) = (\alpha g(x))(\beta h(x)) \in \mathbb{Z}[x].$$

Suppose also that if $f(x) \in \mathbb{Q}[x]$, $f(x)$ is only irreducible if and only if there is a $c \in \mathbb{Q}$ such that $cf(x)$ can let us assume that $cf(x) \in \mathbb{Z}[x]$. The rational root test tells us if they are linear which suffices to show there is irreducibility for degrees 2 and 3 but not higher. This builds the foundation for the following theorem.

Theorem 5.3.4 Gauss's Lemma of Irreducibility

Suppose $f(x) \in \mathbb{Z}[x]$, if $f(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

One may ask, is the converse possible given these assumptions? I claim not always.
It is possible when given that $g(x)h(x) \in \mathbb{Q}[x]$, and the $\deg g(x), h(x) < \deg f(x)$, therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$. But what if we considered that $f(x)$ cannot even be written as a product of integer coefficients? This is a more simplified version of Gauss's lemma, but the actual lemma looks into something called primitivity, which is not looked into in this course.

Definition 5.3.3: Primitivity

$p(x)$ has integer coefficients and is called primitive if and only if the gcd of all the coefficients is 1.

If this is also true, then and only then will it be a bi-conditional statement.
This was a whole block of assumptions to unfold before displaying the if-then statement of (our) Gauss's lemma of irreducibility. But let's look at an example of how to apply this. Let $f(x) \in \mathbb{Q}[x], f(x) = 6x^2 - 5x + 1$, therefore it can be reduced into $f(x) = (x - \frac{1}{2})(6x - 2)$, therefore $f(\frac{1}{2}) = 0$. Thus we have shown a root in $\mathbb{Q}[x]$ which demonstrates that it is reducible. But we can also write this in the form of integer factors, as $f(x) = (2x - 1)(3x - 1) \in \mathbb{Z}[x]$ and you can verify this.

Lemma 5.3.3 Introductory Lemma

Suppose $f(x), g(x), h(x) \in \mathbb{Z}[x]$ where $f(x) = g(x)h(x)$. Let p be prime such that p divides every coefficient of $f(x)$, then either p divides every coefficient of $g(x)$ or $h(x)$.

Sketch of Proof: Suppose $f(x), g(x), h(x) \in \mathbb{Z}[x]$ where $f(x) = g(x)h(x)$. Then $a_0 = b_0c_0$, therefore $p|a_0$ which implies $p|b_0c_0$, and due to Euclid's lemma, then $p|b_0$ or $p|c_0$. Suppose $gcd(p, c_0) = 1$, then and $p|a_1 = b_0c_1 + b_1c_0$, then we know $p \nmid c_0$ implying $p|b_1$. Let there exist α, β such that $\alpha g(x), \beta h(x) \in \mathbb{Z}[x]$, then $\alpha\beta f(x) = (\alpha g(x))(\beta h(x))$. By canceling primes, dividing $\alpha\beta$, and using the introductory Lemma we get $f(x)$ being a product of polynomials of integer coefficients. ■

Theorem 5.3.5 Eisenstein's Theorem of Irreducibility

Suppose $f(x) \in \mathbb{Z}[x]$. Let $\deg f(x) = n$. Suppose $p \nmid a_n$ $p|a_i$ for $i < n$, $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$, then $f(x)$ is reducible in $\mathbb{Z}[x]$ by Gauss's Lemma. So $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $\deg g(x), h(x) < \deg f(x) = n$. So $p|a_0 = b_0c_0$ and so forth following Introductory Lemma. ■

Lemma 5.3.4

Linear Polynomials are not reducible

Sketch of Proof: Following Eisenstein's proof, we find that if linear polynomials are reducible then this contradicts Eisenstein's. ■

Let $f(x) = 2x^4 + 15x^3 + 30x^2 + 60x - 21$. $3 \nmid 2, 3|15, 30, 60, 21$, but $9 \nmid 21$. So $f(x)$ is irreducible by Eisenstein.

Theorem 5.3.6 Reduction mod P

Let $f(x) \in \mathbb{Z}[x]$. Let $p \nmid a_n$. Consider $\overline{f(x)} = \overline{a_n}x^n + \ldots + \overline{a_0}$ where $\overline{a_i}$ Is congruence class $a_i \mod p$. If $\overline{f(x)}$ is irreducible in $\mathbb{Z}_p[x]$ then $\overline{f(x)}$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. The converse is not true.

Let $f(x) = x^4 + 3x^3 + 6x^2 + 1 \in \mathbb{Q}[x]$. Try $p = 2$, $\overline{f(x)} = x^4 + x^3 + 1$ has no factors and roots, so it is not linear and irreducible.

Proof: Suppose $f(x)$ is irreducible in $\mathbb{Q}[x]$, then $f(x) = g(x)h(x) \in \mathbb{Z}[x]$. $\deg g(x), h(x) < n$. Let $\overline{f(x)} = f(x) \mod p$, since $p \nmid a_n$, and $a_n \neq 0$, so $\deg \overline{f(x)} = n$ implying that $k, m < n$. $\overline{f(x)}$ is a product of polynomials of smaller degree which is a contradiction, so $f(x)$ must be irreducible in $\mathbb{Q}[x]$. ■

Theorem 5.3.7 Fundamental Theorem of Algebra

If $f(x) \in \mathbb{C}[x]$, then $f(x)$ is irreducible, if and only if $f(x)$ is linear, if and only if every non-constant of $f(x) \in \mathbb{C}[x]$ can be factored as a product of linear factors, if and only if every non-constant $f(x) \in \mathbb{C}[x]$ has a root.

For example $f(x) = x^2 + 1 \in \mathbb{C}[x]$ has complex roots $\pm i$. $f(X) = (x + i)(x - i)$. Let $\theta = \frac{2\pi}{3}, \frac{4\pi}{3}$.

$$\begin{aligned} e^{\theta i} &= \cos\theta + i\sin\theta \\ \left(e^{\theta i}\right)^3 &= \cos 3\theta + i\sin 3\theta \\ &= \cos 2\pi + i\sin 2\pi \\ &= \cos 4\pi + i\sin 4\pi \\ &= 1 \end{aligned}$$

Roots of $x^n - 1$ are $e^{\theta i}, e^{2\theta i}, e^{3\theta i}, \ldots, e^{(n-1)\theta i}$

Proposition 5.3.3

Suppose $f(x) \in \mathbb{R}[x]$, every irreducible $f(x)$ has degree 1 and 2.

Example 5.3.3

Suppose $f(x) \in \mathbb{R}[x]$ and has degree 3. By IVT, there exists a $c \in \mathbb{R}, f(c) = 0$, so by the factor theorem, $(x - c)$ is a factor of $f(x) \in \mathbb{R}[x]$.

Proof Part 1.: Consider $f(x) \in \mathbb{R}[x]$ as a polynomial of $\mathbb{C}[x]$. By FTA, $f(x)$ has a root in $\mathbb{C}$. If this root is real, then $f(x)$ has a linear factor. So we can assume that $\omega = a + bi$ is a root of $f(x)$.
■

Claim. So is $\overline{\omega} = a - bi$***:*** Suppose $f(x)$, $a_i \in \mathbb{R}$. We assume $f(\omega) = 0$. We can suppose ϕ is a homomorphism of $\mathbb{C}$, which leaves $\mathbb{R}$ fixed. i.e. if $a \in \mathbb{R}$, $\phi(a) = a$, then ω and $f(\omega) = 0$, then $f(\phi(\omega)) = 0$.
■

Lemma 5.3.5

Now let $\phi(a + bi) = a - bi$, therefore $\phi : \mathbb{C} \mapsto \mathbb{C}$, therefore ϕ is a isomorphism.

Proof. ctd: Since complex conjugation is an isomorphism $\mathbb{C} \mapsto \mathbb{C}$. Therefore $f(\overline{\omega}) = 0$ also. Now suppose $f(\omega) = 0$, $\omega \notin \mathbb{R}$ and $f(\overline{\omega}) = 0$, $(x-\omega), (x-\overline{\omega})$ are factors of $\mathbb{C}[x]$ of $f(x)$. But $(x-\omega), (x-\overline{\omega}) = x^2-(\omega+\overline{\omega})x+\omega\overline{\omega}$, which $(\omega + \overline{\omega}) \in \mathbb{R}$, $\omega\overline{\omega} \in \mathbb{R}$. Therefore all factors are in $\mathbb{R}[x]$ hence, degree 1 or 2. ■

5.4 Congruences

Theorem 5.4.1

Let $m(x) \in \mathbb{F}[x]$. If $a(x), b(x) \in \mathbb{F}[x]$. Let's define $a(x) \equiv b(x) \mod m(x)$

Definition 5.4.1: Congruences

Let $m(x) \in \mathbb{F}[x]$. If $a(x), b(x) \in \mathbb{F}[x]$. Let's define $a(x) \equiv b(x) \mod m(x)$ if $m(x)|a(x) - b(x)$ if and only if there exists $q(x) \in \mathbb{F}[x]$, $a(x) - b(x) = q(x)m(x)$. If and only if $a(x) = b(x) + q(x)m(x)$

Definition 5.4.2: Congruence Class

Congruence of $a(x) \in \mathbb{F}[x]$ is denoted by $[a(x)]$. It consists of

$$[a(x)] := \{b(x) \in \mathbb{F}[x] : b(x) \equiv a(x) \mod m(x)\}$$

Definition 5.4.3: Polynomial Division Algorithm

Suppose $g(x) \in \mathbb{F}[x]$. $g(x) = q(x)m(x) + r(x)$, $\deg r(x) < \deg m(x)$ or $r(x) = 0$. If $r(x) \equiv g(x) \mod m(x)$, so $g(x) \in [r(x)]$. So every $g(x)$ is in exactly one of these congruence classes.

Lemma 5.4.1

In $\mathbb{Z}_p[x]$ if $\deg m(x) = n$, there are exactly p^n different congruence classes.

Similar to congruence classes in the integers, we also have similar ideas for addition and multiplication for polynomial congruences.

Definition 5.4.4: Modular Operations

Addition:

$$[a(x)] + [b(x)] = [a(x) + b(x)]$$

Multiplication:

$$[a(x)][b(x)] = [a(x)b(x)]$$

We can use this to check if it is well-defined.

Lemma 5.4.2 Well-Defined

Suppose $[a(x)] = [c(x)], [b(x)] = [d(x)]$.

1. $[a(x) + b(x)] = [c(x) + d(x)]$
2. $[a(x)b(x)] = [c(x)d(x)]$

5.5 Exercises

I will work on these soon, but the base content is stabilized now.

Chapter 6

Ideals and Quotient Rings

6.1 Ideals and Quotient Rings

Definition 6.1.1: Quotient Rings

Congruence classes mod $f(x)$ are noted by $\mathbb{F}[x]/(f(x))$ which is a ring. The additive identity of this ring is $[0] = [f(x)]$. This together is called a quotient ring closed under addition.

Theorem 6.1.1 Class of g(x)

$[g(x) \in \mathbb{F}[x]$ is a unit if and only if $gcd(f(x), g(x)) = 1$, then $g(x), f(x)$ are relative prime.

Proof: ($\Longleftarrow$). Suppose $gcd(f(x), g(x)) = 1$, then there exists $w(x), v(x)$ such that $w(x)g(x) + v(x)f(x) = 1$, so $[w(x)g(X)] = [1]$ so $[w(x)] = [g(x)]^{-1}$.
($\Longrightarrow$). Suppose $w(x)g(x) \equiv 1 \mod f(x)$, so $f(x)|w(x)g(x) - 1$ therefore there exists a $v(x) \in \mathbb{F}[x]$.

$$w(x)g(x) - 1 = v(x)f(x)$$
$$w(x)g(x) - v(x)f(x) = 1,$$

Therefore, $gcd(f(x), g(x)) = 1$. ■

Corollary 6.1.1

If $f(x)$ is irreducible in $\mathbb{F}[x]$, then $\mathbb{F}[x]/(f(x))$ is a field.

Proof: If $g(x) \in \mathbb{F}[x]$, $[g(x)] \neq [0]$, $f(x) \nmid g(X)$, then $gcd(f(x), g(x)) = 1$, so $[g(x)]$ is a unit in $\mathbb{F}[x]/(f(x))$. ■

Let $\mathbb{E} = \mathbb{F}[x]/(f(x))$, such that we have an injection from $\mathbb{F} \mapsto \mathbb{E}$ where $a \mapsto [a]$. We can consider $\mathbb{F}$ now a subfield of $\mathbb{E}$.

Definition 6.1.2: Roots in Quotient Rings

Suppose $\mathbb{F} \subseteq \mathbb{E}$, let $\alpha = [x]$, such that $f(x) \in \mathbb{E}[x]$, then $f(\alpha) = [0]$.

Axiom 6.1.1

$\mathbb{F} \cong \mathbb{E}$.

Definition 6.1.3: Ideal

Let $\mathcal{R}$ be a commutative ring. Given that $I \subseteq \mathcal{R}$. We call I an ideal if an only if I is a subring of $\mathcal{R}$ and if $r \in \mathcal{R}$, $a \in I$, then $ra \in I$.

Definition 6.1.4: Congruence mod I

Suppose $r, s \in \mathcal{R}$, $r \equiv s \mod I$ if $r - s \in I$.

Theorem 6.1.2 Congruence mod I is an Equivalence Relation

Given $a, b, c \in \mathcal{R}$ we have the following properties.
Reflexive. $a \equiv a \mod I$ because $a - a = 0 \in I$.
Symmetric. $a \equiv b \mod I, b \equiv a \mod I$ because $b - a, a - b \in I$.
Transitive. If $a \equiv b \mod I, b \equiv c \mod I$, then $a \equiv c \mod I$ because $a - b, b - c, a - c \in I$.

Definition 6.1.5: Coset

Instead of $[a]$ for $a \mod I$, we have the notation $a + I := \{a + i : i \in I\}$ called a coset.

For example $\mathbb{Z}_m[a] = a + m\mathbb{Z}$

Definition 6.1.6: Quotient Ring

$\mathcal{R}/I$ is called a quotient ring.

Theorem 6.1.3 Addition on Ideals

$$(a + I) + (b + I) = a + b + I$$
$$(a + I)(b + I) = (ab) + I$$

Proof: Suppose $a + I = c + I$ and $b + I = d + I$. Since $c - a, d - b \in I$, then $(c - a) + (d - b) \in I$ implies $(c + d) - (a + b) \in I$ which implies $c + d + I = a + b + I$.
To prove multiplication, since $c-a, d-b \in I$, then $c(d-b), b(c-a) \in I$ due to absorption property. $c(d-b)+b(c-a) \in I \implies cd - cb + cb - ba \in I$. Then $ab + I = cd + I$. ∎

Quotient Rings are independently associated with homomorphism $\phi : \mathcal{R} \mapsto \mathcal{S}$.

Definition 6.1.7: Generators

If $\mathcal{R}$ is any commutative ring, let $a \in \mathcal{R}$, the ideal generated by a is $\{ra : r \in \mathcal{R}\} =: (a)$.

Lemma 6.1.1

(a) is an ideal of $\mathcal{R}$.

Proof: **Case 1.** if$r_1a, r_2a \in (a)$, then $r_1a + r_2a = (r_1 + r_2)a \in (a)$.
Case 2. if $ra \in (a), s \in \mathcal{R}$, then $s(ra) = (rs)a \in (a)$. ∎

These generators are called the principal ideal generated by a.

Theorem 6.1.4

If $p(x)$ is irreducible in $\mathbb{F}[x]$ if and only if $\mathbb{F}[x]/(p(x))$ is a field if and only if $\mathbb{F}[x]/(p(x))$ is an integral domain.

Let $\mathcal{R}$ be a commutative ring with $1 \in \mathcal{R}$. Let A be any subset of the ideal generated by A which is the set of all finite linear combinations of elements.

$$(A) := \{r_1a_2 + \ldots + r_na_n : r_i \in \mathcal{R}, a_i \in A\}$$

Then (A) is the intersection of all ideals in $a \in A$.
Suppose $\mathcal{R} \in \mathbb{Z}, a, b \in \mathbb{Z}$ ideal generated by $(a,b) := \{xa + by : y, x \in \mathbb{Z}\} = \{r \cdot gcd(a,b) : r \in \mathbb{Z}\}$.
$\mathbb{Z}$ and $\mathbb{F}[x]$ are called principle ideal domains while $\mathbb{Z}[x], \mathbb{Q}[x,y]$ are not principle ideal domains.
$\phi : \mathbb{Z} \mapsto \mathbb{Z}/10\mathbb{Z}$, therefore $\phi(a) = [a]_{10} = a + 10\mathbb{Z}$.

Definition 6.1.8: Kernel

Let $K := \{x \in \mathbb{Z} : \phi(x) = 0\}$ which we learn is called the kernel of ϕ, $\ker \phi$.

Theorem 6.1.5

K is an ideal in $\mathcal{R}$.

From the previous example, $\ker \phi = (10) = 10\mathbb{Z}$. What we learned prior is that $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}_{10}$.

Proof of Theorem: **(1).** Suppose $x, y \in \ker \phi$, then $\phi(x) = \phi(y) = 0, \phi(x+y) = \phi(x) + \phi(y) = 0$.
(2). Suppose $x, y \in \ker \phi, r \in \mathcal{R}$, then $(rx) = \phi(r)\phi(x) = \phi(r)0 = 0$.
So $\ker \phi$ is an ideal in $\mathcal{R}$. ■

Definition 6.1.9: Image

$$\phi := \{s \in S : \exists r \in \mathcal{R}, \phi(r) = S\}$$

Theorem 6.1.6 First Isomorphism Theorem

Suppose $\phi : \mathcal{R} \mapsto \mathcal{S}$ is a homomorphism. Let $K = \ker \phi$. We can define $\overline{\phi} : \mathcal{R}/K \mapsto \phi$ such that $\overline{\phi}(r + K) = \phi(r)$. Then $\overline{\phi}$ is an isomorphism from $\mathcal{R}/K$ to ϕ, so $\mathcal{R}/K \cong \phi$.

Proposition 6.1.1

Suppose $\phi : \mathcal{R} \mapsto \mathcal{S}$ is a ring homomorphism, then ϕ is injective if and only if $\ker \phi = \{0\}$.

Proof of Proposition: $(\implies)$. Suppose ϕ is injective. Let $r \in \ker \phi$, so $\phi(r) = 0$, but $\phi(0) = 0$, so ϕ is injective $r = 0$.
$(\impliedby)$. Suppose $\ker \phi = \{0\}$. Let $r, s \in \mathcal{R}$ with $\phi(r) = \phi(s)$.

$$\phi(r) - \phi(s) = 0$$
$$\phi(r - s) = 0.$$

So $r - s \in \ker \phi$, so $r - s = 0$, therefore $r = s$. Therefore ϕ is injective. ■

Proof of First Isomorphism Theorem: Assume ϕ is a homomorphism. Suppose $r, s \in \mathcal{R}$, $\overline{\phi}(r+s) = \overline{\phi}(r) + \overline{\phi}(s)$, $\overline{\phi}(rs) = \overline{\phi}(r)\overline{\phi}(s)$
$\overline{\phi}$ is surjective. Suppose $s \in \phi$, then $\exists r \in \mathcal{R}$ such that $\phi(r) = s$, so $\overline{\phi}(r) = s$. ■

Example 6.1.1

Prove $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

Proof: Define $\phi : \mathbb{Q}[x] \mapsto \mathbb{C}$ so $\phi(f(x)) = f(\sqrt{2})$. Let $\ker \phi := \{f(x) \in \mathbb{Q}[x] : f(\sqrt{2}) = 0\}$.

$$x^2 - 2 \in \ker \phi$$

Claim. $\ker \phi$ is the ideal generated by $x^2 - 2$.
By the first isomorphism theorem, we find that $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$ ■

6.2 Field Extensions

Definition 6.2.1: Vector Space

A vector space over $\mathbb{F}$ is an additive abelian (commutative) group V equipped with scalar multiplication such that $a, a_1, a_2 \in \mathbb{F}$ and $v, v_1, v_2 \in V$.

1. $a(v_1 + v_2) = av_1 + av_2$.
2. $(a_1 + a_2)v = a_1v + a_2v$.
3. $a_1(a_2v) = (a_1a_2)v$.
4. $1_{=}v$.

Definition 6.2.2: Span

If every element of a vector space $V/\mathbb{F}$ is in a linear combination, we say set $\{v_1, v_2, \ldots, v_n\}$ span $V/\mathbb{F}$.

Definition 6.2.3: Linearly Independent

A subset of a vector space $V/\mathbb{F}$ is linearly independent over $\mathbb{F}$ when there is a linear combination with $c_i \in \mathbb{F}$, then $c_i = 0_{\mathbb{F}}$ for all i. else is dependent.

Definition 6.2.4: Basis

The subset is linearly independent and spans $V/\mathbb{F}$.

Definition 6.2.5: Dimension

If $p(x) \in \mathbb{F}[x]$ is irreducible, then $\mathbb{E}$ is an extension field of $\mathbb{F}$. In fact this is called a vector space over $\mathbb{F}$. Denoted by $[\mathbb{E} : \mathbb{F}]$.

Theorem 6.2.1

Suppose K is an extension field of dimension $[K : \mathbb{E}]$, then

$$[K : \mathbb{F}] = [K : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

Proof: Suppose $[\mathbb{E} : \mathbb{F}] = n$. Suppose $v_1, \ldots, v_n \in \mathbb{E}$ which are basis for $\mathbb{E}/\mathbb{F}$. Suppose $[K : \mathbb{E}] = m$. Suppose $w_1, \ldots, w_m \in K$, basis for $K/\mathbb{E}$. Our claim is that $\{w_iv_j : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ is the basis for $K/\mathbb{F}$. Which can also be stated as $\{w_iv_j\}$ span K. Let $u \in K$, $\{w_i\}$ span $K/\mathbb{E}$. So $u = \sum \alpha_i w_i, \alpha_i \in \mathbb{E}$. Each $\alpha_i = \sum \beta_{ij}v_j, \beta_{ij} \in \mathbb{F}$, so $u = \sum \beta_{ij}w_iv_j$. So $\{w_iv_j\}$ span K.
Suppose $\sum \beta_{ij}v_jw_i = 0$, $\forall i, \sum \beta_{ij}v_j \in \mathbb{E}$ since $\{w_i\}$ are linearly independent $/\mathbb{E}$.
$\sum \beta_{ij}v_j = 0$ for each i.
Since $\{v_j\}$ are a basis for $\mathbb{E}/\mathbb{F}$, $\beta_{ij} = 0$ for each j, i. Suppose $\mathbb{E}$ is an extension field of $\mathbb{F}$ and $u \in \mathbb{E}$. ∎

Definition 6.2.6: Algebraic and Transcendental Functions

Let $\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{R}$, $u = \pi$. There is no polynomial $p(u) = 0$, $p(x) \in \mathbb{Q}$. If there is no such polynomial, we say u is transcendental $/\mathbb{F}$.
If there is such a polynomial, we say u is algebraic $/\mathbb{F}$.

To understand two versions of field extensions, let's look at when $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. We can use the first isomorphism theorem.

Lemma 6.2.1 $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$

$$\begin{aligned} \text{A function } \phi : \mathbb{Q}[x] \mapsto \mathbb{Q}[\alpha] \text{ is injective } &\iff \ker\phi = \{0\}; \\ &\iff \nexists f(x) \in \mathbb{Q}[x] : f(x) = 0; \\ &\iff \alpha \text{ is transcendental of } \mathbb{Q}. \end{aligned}$$

Proof Part One: Using the first isomorphism theorem, we can let ϕ be a homomorphism,

$$\phi = \{f(\alpha) : f(x) \in \mathbb{Q}[\alpha]\} = \mathbb{Q}[\alpha].$$

So it is a surjective function. In fact

$$\ker\phi = \{f(x) \in \mathbb{Q}[x] : f(x) = 0\},$$

This ϕ is injective. Suppose α is transcendental/$\mathbb{Q}$, then $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]$. Therefore $\mathbb{Q}[\alpha]$ is a ring, not a field. ■

Definition 6.2.7: Minimal Polynomial

Suppose $p(x)$ is a monic polynomial of the smallest degree, this is called the minimal polynomial of $\alpha/\mathbb{Q}$.

Lemma 6.2.2

$p(x)$ is irreducible.

Proof: Suppose

$$\begin{aligned} p(\alpha) &= q(x)g(x) \\ &= q(x)g(x) = 0. \end{aligned}$$

So either $q(x) = 0$ or $g(x) = 0$. Since $p(x)$ is the smallest degree, either $q(x)$ or $g(x)$ is a unit in $\mathbb{Q}[x]$. ■

Continuation of Proof Sketch of Lemma 7.0.1: Using the first isomorphism, suppose α is algebraic. Let $\mathbb{Q}[x] \mapsto \mathbb{Q}[\alpha]$ and this map has $\ker\phi = (p(x))$. $p(x)$ is an irreducible minimal polynomial of α. Therefore $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}[x]$. Since $p(x)$ is irreducible, then $\mathbb{Q}[x]/(p(x))$ so $\mathbb{Q}(x)$ is a field and $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. ■

We have previously learned that $\mathbb{Q}(r)$ is a vector space.

$\mathbb{Q}(r) = \mathbb{Q}[r]$

What is the $\dim[\mathbb{Q}[r] : \mathbb{Q}]$? We have to find the basis. So what is the basis of $\mathbb{Q}[r]/\mathbb{Q}$?

Lemma 6.2.3

A basis is $1, r, r^2, \ldots, r^{n-1}$ where $n = \deg f(x)$.

Proof: $\mathbb{Q}[r] = \{f(x) : f(x) \in \mathbb{Q}[x]\}$. $|f(r) = 0, \deg f(x) = n|$. ■

Lemma 6.2.4

Basis when we mod out $f(x)$, therefore $f(x)$ is the minimum polynomial or $r/\mathbb{Q}$.

Proof: Suppose $g(x) \in \mathbb{Q}[r]$. By the division algorithm, $g(x) = f(x)q(x) + s(x)$. Plug in r:

$$g(r) = f(r)q(r) + s(r),$$

so $g(r) = s(r)$ since $f(r) = 0$. Therefore $s(r) = 0$ or $\deg s(r) < \deg f(x)$ or $s(r)$ is some polynomial. So $g(r)$ is the linear combination of $1, r, \ldots, r^{n-1}$. So $1, r, r^2, \ldots, r^{n-1}$ span $\mathbb{Q}[r] = \mathbb{Q}(r)$. ■

Definition 6.2.8: Adjoin

We say that $\mathbb{F}(u)$ is a field made by adjoining u to $\mathbb{F}$.

Theorem 6.2.2

Let $\mathbb{K}/\mathbb{F}$ and $u \in \mathbb{K}$ an algebraic element over $\mathbb{F}$ with minimal polynomial $p(x)$ of degree n, then

1. $\mathbb{F}(u) \cong \mathbb{F}[x]/(p(x))$;
2. $\{1_{\mathbb{F}}, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $\mathbb{F}(u)$ over $\mathbb{F}$;
3. $[\mathbb{F}(u) : \mathbb{F}] = n$

Corollary 6.2.1

If we have u and v have the same minimal polynomial $p(x)$ in $\mathbb{F}[x]$, then $\mathbb{F}(u) \cong \mathbb{F}(v)$.

Definition 6.2.9: Algebraic Extension

An extension field $\mathbb{K}$ of field $\mathbb{F}$ is said to be an algebraic extension if every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$.

Theorem 6.2.3

If $\mathbb{K}$ is a finite dimensional extension field of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

6.3 Exercises

I will work on these soon, but the base content is stabilized now.

Chapter 7

Geometric Constructions

7.1 Constructible Shapes

Which regular n-gons can be constructed?

Definition 7.1.1: Construct

a is constructible if you can construct a line of length a.

Definition 7.1.2: Constructible Point

A point in $\mathbb{R}^2$ is constructible if its coordinates are constructible.

Definition 7.1.3: Constructible Line

A constructible line is made of constructible points.

Theorem 7.1.1

Constructible numbers are in the extension field $\mathbb{Q}$.

Proof: Suppose a, b are constructible, they are closed under subtraction. ■

Theorem 7.1.2

$\mathbb{F}$ is constructible so is $\sqrt{a}$.

Proof: Suppose a triangle is enclosed in a semicircle with triangle length 1 and radius $\frac{a+1}{2}$. The distance, x, is $\frac{a+1}{2}$.

$$\begin{aligned} x^2 &= \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 \\ &= a \end{aligned}$$

Which shows distance $x = \sqrt{a}$ ■

Suppose we have constructible points, how do we get new points intersecting lines, circles, and lines on circles?

Definition 7.1.4: New Constructible Points

$\mathbb{F}[\alpha]$ where $[\mathbb{F}[\alpha : \mathbb{F}] = 2$. Which means any constructible point lies in a field:

$$\mathbb{Q} \subseteq \mathbb{Q}[a_1] \subseteq \mathbb{Q}[a_1, a_2] \subseteq \ldots \subseteq \mathbb{F}$$

Therefore $\mathbb{F}_k = \mathbb{F}_{k-1}[a_k]$, thus $[\mathbb{F}_k : \mathbb{F}_{k-1}] = 2$.

Let α be the root of a quadratic polynomial. So no constructible numbers must lie in field $\mathbb{F}$ where the $[\mathbb{F} : \mathbb{Q}] = 2^n$ for some n. Therefore $\sqrt[3]{2}$ is not constructible.

Lemma 7.1.1 Constructible Points

Let $r \in \mathbb{R}$ be a constructible with a straightedge and compass $\iff$ r lies in a field extension, $\mathbb{E}$ with $[\mathbb{E} : \mathbb{Q}] = 2^n$ (power of 2).

π is not constructible and neither is it algebraic. Therefore constructible points are also only possible iff $[\mathbb{Q}(r) : \mathbb{Q}] = 2^k$ for some k. We will show that we cannot trisect 60° since we can construct 60°, implying that not every angle can be trisected.
Because $20° = \theta = \frac{\pi}{4}$ can be constructed the $\cos\theta$ can be constructed.

$$\begin{aligned} cos2\theta &= \cos^2\theta - \sin^2\theta \\ &= 2cos^2\theta - 1 \end{aligned}$$

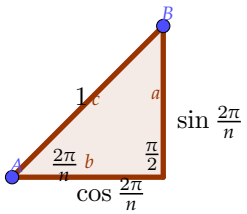
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

If $\theta = \frac{\pi}{4}$ then $\cos 3\theta = \frac{1}{2}$ and let $x = \cos 20$. Then

$$\begin{aligned} \frac{1}{2} &= 4x^3 - 3x \\ 0 &= 4x^3 - 3x\frac{1}{2} \\ 0 &= 8x^3 - 6x - 1 \end{aligned}$$

We claim that $8x^3 - 6x - 1$ is irreducible/$\mathbb{Q}$, which we can use the root test to check that it is indeed irreducible.

Question: Which regular n-gons can be constructed? i.e. for which n can angle $\frac{2\pi}{n}$ be constructed.
Such an angle can be constructed if and only iff $\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}$ can be constructed



if and only iff $(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$ is a constructable point if and only if $\rho = \cos\frac{2\pi}{n} + \sin\frac{2\pi}{n}$, $[\mathbb{Q}(\rho) : \mathbb{Q}]$ = power of two, $\rho^n = 1$, ρ is an n^{th} root of 1 satisfying $x^n - 1 = 0$. Suppose $n = 2^{a_1}p_2^{a_2}\ldots\rho_k^{a_k}$ is a factorization of regular n-gons is $p_1 = 2, p$ odd for $j \geqslant 2$ constructable if and only if $a_j = 1$ for $j \geqslant 2$ and each $p_i - gon$ is constructable.

Definition 7.1.5: Fermat Prime

If $2^{2^k} + 1 = p$ is prime, then p is a fermat prime.

Corollary 7.1.1

Let $\phi : \mathbb{Q}[x] \mapsto \mathbb{Q}[x] := \{f(x) : f(x) \in \mathbb{Q}[x]\}$. By $\phi(p(x)) = p(\alpha)$, this shows surjectivity.

Proof of Corollary: Suppose $\beta \in \mathbb{Q}[x]$, then $\exists f(x) \in \mathbb{Q}[x]$ such that $\beta = f(x)$, so $\phi(f(x)) = f(\alpha) = \beta$. ■

ϕ is injective if and only if $\ker \phi = \{0\}$. This is a consequence of the first isomorphism theorem.

Proposition 7.1.1 Proof

$\ker \phi = \{0\} \iff (f(x) = 0 \implies f(x) = 0) \iff \alpha/\mathbb{Q}$ is transendental

7.2 Exercises

I will work on these soon, but the base content is stabilized now.

Chapter 8

Groups

8.1 Definition of Groups

A group is a singular operation ring. Groups are basically bijections from a set to itself or permutations. Most of the course we will be looking at finite groups. Let X be a set. Assume $X \neq \phi$ Note S_X, called the symmetric group on X, be the permutations of set $X \equiv$ Bijections of $X \mapsto X$. The operations of composition properties have: Identity permutation e or i or 1. We also have associativity, $(a \circ b) \circ c = a \circ (b \circ c)$. We also have every element have a unique inverse, this is due to the group being a bijection of elements. If f is a permutation of X, then it's unique inverse is denoted f^{-1}.

An abstract group G is a nonempty set with the same axioms with the operation: $\cdot$, $*$, or juxtaposition. If there is an identity element say 1, so $1 * a = a * 1 = a$ for all $a \in G$. The group does not need to be commutative but the identity is commutative. Associative as for all $a, b, c \in G$, $(a * b) * c = a * (b * c) = a * b * c$. Every element $a \in G$ has an inverse a^{-1}.

Definition 8.1.1: Abelian Groups

G does not need to be commutative, but if it is we call it a commutative group or **abelian**.

S_X for X as any set. If G is a subset of S_X, which is closed under under composition and inverses, then G is a group. Cayley's Theorem has a representation of this. So every group is a subset of the symmetric group. Which we will prove later on.

Suppose $X := \{1, 2, \ldots, n\}$, then S_X is denoted by S_n, a symmetric group by n letters. For example, S_3 is the permutations of $\{1, 2, 3\}$. The notation for permutations is as follows: Suppose $\sigma \in S_3$, denote it

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}.$$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Suppose $\sigma_2 \circ \sigma_4$. Then we look at σ_2 and we see that $1 \to 3$, but then if we look at 3 in σ_4, then we see that $3 \to 3$, thus $1 \to 3$. And we do this so on to find $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Example 8.1.1

$$\sigma_4 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

If $(\mathcal{R}, +, \cdot)$ is a ring with operations addition and multiplication, then $(\mathcal{R}, +)$ is a group. The identity in an additive group is 0. It is associative, and every element, a, has an additive inverse, denoted by $-a$. In fact, these rings are abelian groups.

Let $\mathbb{F}$ be any field. Let $\mathbb{F}^* := \{a \in \mathbb{F} : a \neq 0\} := U(\mathbb{F})$ is a group under multiplication. This group has identity $1 \in \mathbb{F}$, it is also associative and has inverses. Operation $*$ on G means $* : G \times G \mapsto G$, therefore $*(g, h) = g * h$. More generally, if $\mathcal{R}$ is a ring, $\mathcal{R}^* := \{a \in \mathcal{R} : \text{a is a unit in } \mathcal{R}\} := U(\mathcal{R})$ is a group.

Example 8.1.2

$$\mathbb{Z}_6^* = \{1, 5\}.$$

8.2 Properties of Groups

Definition 8.2.1: Group under Multiplication

Suppose G is a group $(G, *)$. $(* : G \times G \mapsto G)$ $1 \in G$ $1 * a = a * 1$ $\forall a \in G$ $(a * b) * c = a * (b * c)$ $\forall a, b, c \in G$ $\forall a \in G, \exists a^{-1} \in G s.t. a^{-1} * a = 1$ $a^2 = a * a$ Inductively, $a^n = a * (a^{n-1}) = a * a * \cdots * a$

S_X = permutations on X under composition, non-commutative for $\#X \geqslant 3$. If $(\mathcal{R}, +, *)$ is a ring, then $(\mathcal{R}, +)$ is a group under addition which is commutative. Note that $(\mathcal{R}, +, *)$ is not the notation for group, but instead a ring. This means that $0 \in \mathcal{R}$ is possible even if it's closed under multiplication because it's not a group. $U(\mathcal{R}) = \mathcal{R}^*$ = set of units in $\mathcal{R} = \{u \in \mathcal{R} : \exists \in \mathcal{R}$ with $uv = vu = 1\}$ is a group.

Example 8.2.1

$\mathbb{Z}_n^*$ group of units in $\mathbb{Z}_m$.
$\mathbb{Z}_6^* = \{1, 5\}$
$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

If $\mathcal{R}$ is any ring, then $Mat_n(\mathcal{R})$ = ring of nxn matrices with entries in $\mathcal{R}$ $Mat_n(\mathcal{R})^*$ = group of invertible matrices entries in $\mathcal{R}$. If $n \geqslant 2$, $Mat_n(\mathcal{R})^*$ is non-abelian.

If $\mathbb{F}$ is a field, then matrices are transformations of vector spaces. $Mat_n(\mathbb{F})$ is the same as a linear transformation of an n-Dimensional vector space over $\mathbb{F}$. Suppose $A \in Mat_n(\mathbb{F})$, then v is an n-Dimensional vector space. We define $T(v) = Av$ as $T : V \mapsto V$ as a linear transformation. $T(\lambda v + \mu w) = \lambda T(v) + \mu T(w)$.

Definition 8.2.2: General Linear Group

This $Mat_n(\mathbb{F})^*$ = a group of invertible nxn matrices enteries in $\mathbb{F}$ under multiplication is denoted by $GL_n(\mathbb{F})$ (General Linear Group).

Example 8.2.2

$GL_2(\mathbb{F}_2)$.

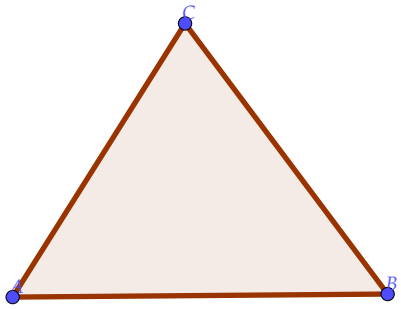
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \{0, 1\}$, is invertible if and only $ad - bc \neq 0$.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

So $\#GL_2(\mathbb{F}_2) = 6$, which is isomorphic to S_3.

Coming from geometry, they also have groups. If you take some solid and take the rigid motions of some $n-gon$ then it will also be a group. A rigid motion is when you take a figure and you lift it and put it back in the same place: rotations and reflections.



Example 8.2.3

Rigid motions of a regular 3-gon: Identity, rotation of $120° = \frac{2\pi}{3}$ counterclockwise call this r, or r^2 = rotation by $240° = \frac{4\pi}{3}$, or reflection in the vertical line call this s.

$$1 : 1 \to 1, 2 \to 2, 3 \to 3$$

$$r : 1 \to 2 \to 3 \to 1$$

$$r^2 : 1 \to 3 \to 2 \to 1$$

$$s : 1 \to 1, 2 \leftrightarrow 3$$

$$sr : 1 \leftrightarrow 3, 2 \to 2$$

$$rs : \text{reflection through 3.}$$

This group is denoted D_3 order 6 called the dihedral group. Some texts use D_6. D_n or D_{2n}

Example 8.2.4

Let H, K be groups. Group $H \times K$ has underlying set $H \times K$ with operation $(h_1, k_1) * (h_2, k_2) = (h_1 * h_2, k_1 * k_2)$. This makes $H \times K$ into a group - Identity is $(1, 1)$. - Associativity - Inverse $(h, k)^{-1} = (h^{-1}, k^{-1})$. - Closure under $*$.

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ has order 4 elements. $(\mathbb{Z}_4, +)$ also has 4 elements. $\mathbb{Z}_5^*, \mathbb{Z}_8^*$ also have 4 elements. Now... are they isomorphic? Let's look at the tables for these groups.

$(\mathbb{Z}_4, +)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$0 \longrightarrow 1$$
$$1 \longrightarrow 2$$
$$2 \longrightarrow 4$$
$$3 \longrightarrow 3$$

Theorem 8.2.1 Fundamental Theorem of Finite Abelian Groups

Every finite abelian group is a direct product of groups $(\mathbb{Z}_n, +)$ various n.

Definition 8.2.3: Other properties of Groups

Let G be a group. Some other properties which follow from the definition:

1. Cancelation law: Suppose $a, b, c \in G$.

$$ba = ca \implies b = c$$

Proof: $ab = ac$ implies the following:

$$a^{-1}(ab) = a^{-1}(ac) \tag{8.1}$$
$$a^{-1}a)b = (a^{-1}a)c \tag{8.2}$$
$$1b = 1c \tag{8.3}$$
$$b = c \tag{8.4}$$

■

2. Identity is unique. Suppose e, f identities with $ef = f = e$.
3. Inverses are unique: If $a \in G$, if $ba = ab = e$ and $ca = ac = e$, then $b = c$.

Proof: Suppose $ab = e = ac$ and $ba = e$, then $bac = ec = c$. Suppose $ac = e$, then $bac = b$, which implies $b = c$. ■

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

Proof:

$$(ab) * (b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

By uniqueness of inverse, $(ab)^{-1} = b^{-1}a^{-1}$ ■

5. $(a^{-1})^{-1} = a$. $a^{-1}a = aa^{-1} = e$ SO by uniqueness of inverse $(a^{-1})^{-1} = a$.

Definition 8.2.4: Order

Let G be a group. Let $a \in G$. The order of a is the smallest strictly positive integer n such that $a^n := a * a * \cdots * a = 1$. $a^n = a(a^{n-1})$
If there is no such n, a has infinite order.

Theorem 8.2.2

If $\#G$ is finite, every $a \in G$ has finite order.

Example 8.2.5

Dihedral groups have finite order for all elements.

Example 8.2.6 ($G_1 = (\mathbb{Z}_4, +)$)

Elements	Order
0	1
1	4
2	2
3	4

Example 8.2.7 ($G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$)

Elements	Order
(0,0)	1
(0,1)	2
(1,0)	2
(1,1)	2

Example 8.2.8 ($G_3 = \mathbb{Z}_5^*$)

Elements	Order
1	1
2	4
3	4
4	2

This is another way of showing G_1 and G_3, are isomorphic.

Corollary 8.2.1 Infinite Order

Suppose $a^n \neq e$ for all n. Then $|a| = \infty$.

Theorem 8.2.3

Suppose $a \in G, |a| = n$. If $k \in \mathbb{Z}$ such that $a^k = 1$ if and only if $n \mid k$.

Proof of Theorem 8.2.3: ($\implies$). Suppose $k \in \mathbb{Z}$ such that $a^k = 1$. Let $k = nq + r$, then:

$$\begin{aligned} a^k &= a^{nq+r} \\ &= a^{nq}a^r \\ &= (a^n)^q a^r \\ &= 1^q a^r \\ &= 1a^r. \end{aligned}$$

Since n is the smallest integer, then $r = 0$. Thus $n|k$.
($\impliedby$). Given $n|k$, then $k = nq$. Then:

$$\begin{aligned} a^{nq} &= (a^n)^q \\ &= 1^q \\ &= 1. \end{aligned}$$

Thus $a^k = 1$. ■

Corollary 8.2.2

$a^i = a^j$ if and only if $a^{i-j} = 1$. Thus $n|i - j$ or $i \equiv j \mod n$.

Proof of Corollary: ($\implies$). Given $a^i = a^j$, then:

$$a^i a^{-j} = a^j (a^j)^{-1}$$
$$a^{i-j} = 1.$$

Thus $a^{i-j} = 1$.
($\impliedby$). Given $a^{i-j} = 1$, then:

$$a^i a^{-j} = 1$$
$$a^i (a^j)^{-1} = 1$$
$$a^i (a^j)^{-1} a^j = a^j$$
$$a^i = a^j.$$

Thus $a^i = a^j$. ■

Theorem 8.2.4

Suppose $t|n$ then $|a^t| = \frac{n}{t}$.

Proof of Theorem 8.2.4: Let $|a^t| = k$. We know that $a^n = 1$, so $(a^t)^{\frac{n}{t}} = 1$, so $k \mid \frac{n}{t}$. Since $(a^t)^k = 1 = a^{kt}$. Thus $n \mid tk$, so $\frac{n}{t} \mid k, k = \frac{n}{t}$. ■

Suppose $|a| = 6$, then $|a^4| = 3$.
More generally, let $t \in \mathbb{Z}$, can assume $t \in \mathbb{Z}^{>0}$. Then the order is $\frac{lcm(t,n)}{t} = \frac{6}{gcd(4,6)}$. Then $|a| = \frac{n}{d}$ where $d = gcd(t,n)$.

Proof of Example: Let $|a^t| = k$ and we know $a^n = 1$, so $(a^t)^{n/d} = (a^{t/d})^n$ which $\frac{t}{d}$ is an integer, thus $(a^n)^{t/d} = 1^{t/d} = 1$. So $k \mid \frac{n}{d}$. Since $a^{tk} = 1$, then $n \mid kt, \frac{n}{d} \mid k \cdot \frac{t}{d}$ implies $\frac{n}{d} \mid k$. ■

8.3 Subgroups

Definition 8.3.1: Subgroup

Let G be a group $\varnothing \neq H \subseteq G$. H is a subgroup of G if it is a group under the operation of G. i.e. $\forall a, b \in H, ab \in H, 1 \in H$, if $a \in H$ then $a^{-1} \in H$, and associativity. Denoted by $H \leqslant G$.

Something to note that you may realize through a lot of practice problems is that $H \leqslant G$ if and only if $\forall a, b \in H, ab^{-1} \in H$. We could also have a subgroup $H \leqslant G$ and $\text{ord}(H) < \infty$, then $H \leqslant G$ if and only if $H \neq \varnothing$ and closed under operation of group.

Proof of Example: Let $a \in G$, $\exists n > 0, a^n = 1$, then $a^n = a(a^{n-1}), a^{n-1} \in H$. ■

$G = GL(n, \mathbb{F})$ = non-singular $n \times n$ matrices, entries in $\mathbb{F}$, determinant is non-zero, meaning General Linear Group. One of our exercises is $SL(n, \mathbb{F})$ = set of matrices in $GL(n, \mathbb{F})$ with the determinant always 1, meaning Special Linear Group.

$$\det(AB) = \det(A)\det(B)$$

If $\det(A) = \det(B) = 1$, then $\det(AB) = 1$. If $\det(A) \neq 0$, then $\det(A^{-1}) = \frac{1}{\det(A)} = 1$.

Let $\mathbb{C}^k$ be a set of non-zero complex numbers. Let $n \in \mathbb{Z}^{>0}$.

$$\left\{ \exp\left(\frac{2k\pi i}{n}\right) : k = 0, \ldots, n-1 \right\}$$

Which are the complex roots of i. $\exp\left(\frac{2k\pi i}{n}\right) = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$ since we can think of multiplication as cyclical.

Given any group, there are important examples you can get from any group. So we know that vector spaces are a constant multiple, or also algebraically stated as an ideal ring.

Definition 8.3.2: Cyclic Subgroup Generated by a

Let $a \in G$, $< a >$, which are a subgroup generated by a, is

$$\{a^n : n \in \mathbb{Z}\}$$

We need $n \in \mathbb{Z}$ since we want all multiplicative powers, positive and negative, since the order can be finite or infinite. Since its closed under multiplication and inverses, it is also a subgroup. We consider this as the smallest subgroup of G containing a.

We call this cyclic because we consider G to be a finite order. For an infinite subgroup, look at $(\mathbb{Z}, +)$, as a subgroup generated by 2 is $\ldots, -2, 0, 2, 4, \ldots$.

For example if $H \leqslant G$ and $a \in H$, then $< a > \leqslant H$.

Definition 8.3.3: Subgroup Generated by Subset

If $S \subseteq G$, the subgroup generated by S, $< S >$ is the smallest subgroup of G containing S. This is the same as $\bigcap_{H \leqslant G \text{ and } S \subseteq H} H$, which is the intersection of all subgroups of G containing.

For example, if we take two random elements of a symmetric group, they will contain the entire group.

Similar to ideals, we have trivial subgroups. For example, ponder about looking at a subgroup generated by an identity element.

Definition 8.3.4

If G is a group, and $G =< a >$ for some $a \in G$, then G is cyclic.

$(\mathbb{Z}_n, +)$ is cyclic as it is generated by 1, and also generated by any $m \in \mathbb{Z}_n$, with $\gcd(m, n) = 1$.
$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ is cyclic generated by 2,3.
$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, we find that $2^3 = 8 = 1$, which does not show that G is cyclic, since it does not contain the entire set. However, $3^2 = 2$ and $2^3 = 8 = 1$, so $3^6 = 1$, and since $\text{ord}(G) = 6$ and $\text{ord}(3) = 6$, then the group is cyclic.

Theorem 8.3.1

If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Proof of Theorem 8.3.1: This is a corollary of this **paper**. The work is extensive but we only need to know this Theorem. ■

8.4 Group Homomorphisms and Isomorphisms

Definition 8.4.1: Group Homomorphism

If we let $f : G \mapsto H$ a function with a multiplicative operator, then for all $a, b \in G$, $f(ab) = f(a)f(b)$.

Definition 8.4.2: Group Isomorphism

$f : G \mapsto H$ is an isomorphism if it is a bijective homomorphism.

Example 8.4.1

Let $G := \left\{\exp\left(\frac{2k\pi i}{n}\right) : n \in \mathbb{Z}; k = 0, \ldots, n-1\right\}$ under multiplication. Let $H : (\mathbb{Z}_n, +)$

Define $f : G \mapsto H$ by $f\left(\exp\left(\frac{2k\pi i}{n}\right)\right) = k \in \mathbb{Z}_n$. Prove G and H is an isomorphism.

Proof of Example 8.4.1: f is a homomorphism if $\exp\left(\frac{2k\pi i}{n}\right), \exp\left(\frac{2l\pi i}{n}\right) \in G$, then

$$f(\exp\left(\frac{2k\pi i}{n}\right)\exp\left(\frac{2l\pi i}{n}\right)) = f(\exp\left(\frac{2(k+l)\pi i}{n}\right)) = k + l = f(\exp\left(\frac{2k\pi i}{n}\right))f(\exp\left(\frac{2l\pi i}{n}\right))$$

So f is a homomorphism. f is a well-defined isomorphism. $\exp\left(\frac{2k\pi i}{n}\right) = \exp\left(\frac{2l\pi i}{n}\right)$ if and only if $\exp\left(\frac{2(k-l)\pi i}{n}\right) = 1$ if and only if $\frac{2(k-l)\pi}{n}$ is a multiple of 2π if and only if $n|k-l$ if and only if $k \equiv l \mod n$.

Thus $f : \exp\left(\frac{2k\pi i}{n}\right) \mapsto k$ (onto) or $\text{ord}(G) = \text{ord}(H) = n$.$G \cong H$ means that G and H are isomorphic. ■

Example 8.4.2

$f : (\mathbb{Z}, +) \mapsto (\mathbb{Z}_n, +)$ is defined by $f(k) = k = [k]$ is a homomorphism because $[k+l] = [k]+[l]$ but certainly not injective because $f(0) = f(n) = f(2n)$. But f is surjective if $k \in \mathbb{Z}_n, f(k) = k$.

Example 8.4.3

$f : (\mathbb{Z}, +) \mapsto G := \left\{\exp\left(\frac{2\pi ki}{n}\right)\right\}$, then $f(k+l) = f(k)f(l)$ is a homomorphism.

Proposition 8.4.1 Isomorphism of Infinite Cyclic Groups

Suppose G is an infinite cyclic group. Then $G \cong (\mathbb{Z}, +)$. Up to isomorphism, they can be different as sets, but there will always be an isomorphism between them due to their infinite nature. So there is only exactly one infinite cyclic group.

Proof of Proposition 8.4.1: Given G is an infinite cyclic group, operation under multiplication. There exists $a \in G$ such that $G := \{a^n : n \in \mathbb{Z}\}$. Define a map, $f : \mathbb{Z} \mapsto G$, by defining $n \mapsto a^n$. We can check f is a homomorphism, because $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$. If $f(m) = f(n)$ then $a^m = a^n$, then $a^{m-n} = 1$ if and only if $m - n = 0$ or $m = n$, showing injective. It is surjective because it is cyclic. ■

Proposition 8.4.2 Isomorphism of Finite Cyclic Groups

Suppose G is finite cyclic group under multiplication and $\text{ord}(G) = n$, then $G \cong (\mathbb{Z}_n, +)$.

Proof of Proposition 8.4.2: Given $\text{ord}(G) = n$ and G is a finite cyclic group under multiplication, let $f : (\mathbb{Z}_n, +) \to G$ be defined by $x \mapsto a^x$. Then:

$$\begin{aligned} f(a+b) &= c^{a+b} \\ &= c^a c^b \\ &= f(a)f(b). \end{aligned}$$

Thus f is a homomorphism. If $f(a) = f(b)$, then:

$$\begin{aligned} c^a &= c^b \\ c^{a-b} &= e \\ &\implies a \equiv b \mod n. \end{aligned}$$

Thus f is injective. Finally f is surjective since each element of $\mathbb{Z}_n \ni x \mapsto a^x$. Thus $(\mathbb{Z}_n, +) \cong G$. ■

Example 8.4.4

If p is prime, $(\mathbb{Z}_p^*, +) \cong (\mathbb{Z}_{p-1}, +)$

Proof of Example 8.4.4: Suppose p prime. Let $f : (\mathbb{Z}_p[x], +) \to (\mathbb{Z}_{p-1}, +)$ be defined by $x \mapsto x \mod p-1$. Then:

$$\begin{aligned} f(x+y) &= x+y \\ &= f(x)+f(y). \end{aligned}$$

Thus f is a homomorphism. If $f(x) = f(y)$ then:

$$\begin{aligned} x - y &\equiv 0 \mod p-1 \\ x &\equiv y \mod p-1. \end{aligned}$$

Thus f is injective. f is surjective since every element of $\mathbb{Z}_p[x]$ maps to some element in $\mathbb{Z}_p$. Thus $(\mathbb{Z}_p^*, +) \cong (\mathbb{Z}_{p-1}, +)$. ■

Definition 8.4.3: Automorphism

An isomorphism of $f : G \mapsto G$ is an automorphism.

Theorem 8.4.1 Properties of Homomorphisms

1. $f : G \to H$ is a homomorphism, then $f(1_G) = 1_H$.
2. If $a \in G$, $f(a^{-1}) = f(a)^{-1}$.
3. $\mathrm{Im}(f) = \{h \in H : \exists g \in G, f(g) = h\}$ is a subgroup of H.
4. If f is injective then $\overline{f} : G \to \mathrm{Im}f$ is defined by $\overline{f}(g) = f(g)$ is an isomorphism $G \xrightarrow{\sim} \mathrm{Im}(f)$.

Proof of Theorem 8.4.1: **1.** Given f is a homomorphism, then $f(1_G) = f(1_G \cdot 1_G) = f(1_G)f(1_G) = 1_H$.

2. $1 = aa^{-1}$. So $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1}) \implies f(a^{-1}) = f(a)^{-1}$.

3. Suppose $h_1, h_2 \in H$ and there exists $g_1, g_2 \in G$ such that

$$\begin{aligned} f(g_1) &= h_1 \\ f(g_2) &= h_2 \\ f(g_1g_2) &= f(g_1)f(g_2) = h_1h_2 \end{aligned}$$

So $h_1, h_2 \in \mathrm{Im}f$. Suppose $h \in H$ such that $\exists g \in G, f(g) = h$, by (2) $f(g^{-1}) = f(g)^{-1} = h^{-1}$ so $h^{-1} \in \mathrm{Im}f$. ■

Theorem 8.4.2 Cayley's Theorem

Every group G is isomorphic to a subgroup of a symmetric group, in fact a unique group of permutations of G as a set.

Proof of Theorem 8.4.2: Let G be a group. Define f_g as above, $f_g(x) = gx$ (we will dub this the Cayley representation to use from now on). We have so far shown that f_g is in $\mathrm{sym}(G)$ = permutations of G. $f : G \to \mathrm{sym}(G)$ is a homomorphism $g \mapsto f_g$.

We claim that $g \mapsto \mathrm{sym}(G)$ is injective. Let $g, h \in G$. Suppose $f_g = f_h$, then $gx = hx \implies g1 = h1 \implies g = h$ for all $x \in G$. By what we have done earlier, we know $G \cong \mathrm{Im}f$, and the $\mathrm{Im}f$ is a subgroup of $sym(G)$. ■

If G is finite $\text{ord}(G) = n$. Then $\text{sym}(G) \cong S_n$. Then G is isomorphic to a subgroup of S_n. Note that $\text{ord}(S_n) = n!$. This is called the Cayley representation.

We learned the sigma notation of permutations. Now learn the Cycle Notation.

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 3 & 6 & 4 \end{pmatrix}$$

However, its cycle representation can be just written as (1 2 5 6 4 3)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}$$

(1 3)(4 6 2)(5) or (1 3)(4 6 2). What about the product of cycles?

Example 8.4.5

$\sigma = (132)(465)$, $\tau = (23)(56)$. $\sigma\tau = (13)(2)(46)(5)$

Example 8.4.6

$\sigma = (1345)$ in S_5 $\sigma^2 = (14)(2)(35)$

Definition 8.4.4: Conjugate

Let $g, x \in G$, then gxg^{-1} is called the conjugate of x by g.

Example 8.4.7

S_3. $\sigma = (123), \tau = (12), \tau\sigma\tau^{-1} = \tau\sigma\tau = (132) = (213)$.

Example 8.4.8

$\sigma = (13546), \tau = (245), \tau^{-1} = (542) = (254), \tau\sigma\tau^{-1} = (13256)$

Conjugation preserves cycle structure. $\tau(a_1a_2 \dots a_k)\tau^{-1} = (\tau(a_1)\tau(a_2)\dots\tau(a_k))$. If for example $\tau(a_1)$ does not exist, then $\tau(a_1) = a_1$.

Definition 8.4.5: Faithful

If $g \mapsto f_g$ is a homomorphism and is injective, we call this faithful.

Definition 8.4.6: Group of Automorphisms of G

$\text{Aut}(G) := \{\phi : G \to G : \phi \text{ is an automorphism of } G\}$ under composition operation.

Example 8.4.9

Let's define $\phi : G \to \text{Aut}(G)$. $g \mapsto \phi_g$ by $\phi_g(x) = gxg^{-1}$ for $x \in G$.

Example 8.4.9: We claim $\phi_g \in \text{Aut}(G)$ and $g \mapsto \phi_g$ is a homomorphism $\phi : G \to \text{Aut}(G)$.

$$\begin{aligned} \phi_g(xy) &= gxyg^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= \phi_g(x)\phi_g(y) \end{aligned}$$

ϕ_g is bijective because it is has inverse $\phi_g^{-1} = \phi_{g^{-1}}$. Check: $x \in G, (\phi_g \circ \phi_{g^{-1}}) = \phi_g(\phi_{g^{-1}}(x)) = \phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$. Similarly $\phi_{g^{-1}} \circ \phi_g$ = identity on G. Let $g, h \in G$ such that $gh \mapsto \phi_{gh}$ where for $x \in G$

$$\begin{aligned}\phi_{gh}(x) &= ghx(gh)^{-1}\\ &g(hxh^{-1})g^{-1}\\ &g\phi_h(x)g^{-1}\\ &\phi_g(\phi_h(x))\\ &\phi_g \circ \phi_h(x)\end{aligned}$$

Suppose G is abelian, would this still hold? NO. If $x \in G$, $\phi_g(x) = gxg^{-1} = x$. Note that ϕ_g is the identity map in $\mathrm{Aut}(G)$ for all $g \in G$ ■

Example 8.4.10

Let G be any group. Define $\mathrm{Inn}(G) := \{\phi_g : g \in G\}$ where $\phi_g(x) = gxg^{-1}$. The reason why we call it $\mathrm{Inn}(G)$ is because we call it the group of inner automorphisms of G.
Prove $\mathrm{Inn}(G) \leqslant \mathrm{Aut}(G)$.

Proof of Exercise 8.4.10: We have previously shown that $\phi_g \in \mathrm{Aut}(G)$, thus $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$. Since $g \mapsto \phi_g$ is a homomorphism, $\mathrm{Inn}(G) = \mathrm{Im}(\phi)$ is a subgroup of $\mathrm{Aut}(G)$. ■

Example 8.4.11

Compute $\mathrm{Inn}(S_3)$.

Proof of Exercise 8.4.11:

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Let $g = (12)$. $\phi_g(id) = id$. $\phi_g(12) = (12)$. $\phi_g(13) = (12)(13)(12) = (23)$. $\phi_g(23) = (12)(23)(12) = (13)$. $\phi_g(123) = (12)(123)(12) = (213) = (132)$. $\phi_g(132) = (123)$. ■

In fact in this case, we can check that $\mathrm{Inn}(G) \cong \mathrm{Aut}(G)$.

8.5 Symmetric and Alternating Groups

Theorem 8.5.1

Every element in S_n can be written as a product of disjoint cycles.

(123)(4567) is disjoint. (123)(426) is not disjoint.

Theorem 8.5.2

Every $\omega \in S_n$ can be written as a product of transpositions.

$$\begin{aligned}\sigma &= (12\ldots n)\\ &= (1n)(1(n-1))\ldots(13)(12)\end{aligned}$$

Theorem 8.5.3

Suppose $\sigma \in S_n$. with

$$\begin{aligned}\sigma &= \tau_1 \ldots \tau_k : \tau_i \text{ transpositions}\\ &= \lambda_1 \ldots \lambda_r : \lambda_i \text{ transposition}\end{aligned}$$

Then $k \equiv r \mod 2$.

Proof of Theorem 8.5.3: Suppose $\tau = (ab)$ is a transposition, then $\tau^{-1} = \tau$. Suppose $\sigma = \tau_1 \dots \tau_k$ transpositions, then $\sigma^{-1} = \tau_k \dots \tau_1$. First reduce to the case that $\sigma = e$. Suppose $\sigma = \tau_1 \dots \tau_k = \lambda_1 \dots \lambda_r$. Then $1 = \sigma\sigma^{-1} = \tau_1 \dots \tau_k \lambda_r \dots \lambda_1$. Which the number of transpositions is $k + r$. Thus $k \equiv r \mod 2 \iff k + r \equiv 0 \mod 2$. So $k \equiv r \mod 2 \iff k + r$ is even. We need to prove that $e = \tau_1 \dots \tau_k$.

Let's do a proof by contradiction. Suppose $e = \tau_1 \dots \tau_k$, with k odd. Some $a \in \{1, \dots, n\}$ appears in some τ_i of all such ways of writing e choose one with the fewest number of tanspositions as far left as possible. Of all the ways of doing this, choose one of the form $\dots (ad)(ac)(ab)(\ )(\ ) \dots$ with no a's to the right of this (ab). We will show this can either cancel $(ab)(ab)$ and get fewer transpositions or move a to the left.

$(cd)(ab)(\ )(\ ) \dots$

Possibilities for (cd) if $\{c, d\} \bigcap \{a, b\} = \varnothing$, then $(cd)(ab) = (ab)(cd)$ If $\{c, d\} = \{a, b\}$, then we could cancel and result in fewer transpositions.

The remaining case $c = a, d \neq b$ results in $(ad)(ab) = (ab)(bd) = (abd)$. You eventually must get $e = (ab)$ after cancelling out as much as possible, but $b \neq a$, so a contradiction. ■

Definition 8.5.1: Sign

The sign of σ is 1 if σ can be written as an even number of transpositions and -1 otherwise. Sign σ is denotated by $\operatorname{sgn}(\sigma)$ or $\epsilon(\sigma)$. The theorem says $\operatorname{sgn}(\sigma)$ is well-defined.

Definition 8.5.2: Even Symmetric Group

$A_n = \{\sigma \in S_n : (\sigma) = 1\}$

Theorem 8.5.4

A_n is a subgroup of S_n.

8.6 Exercises

Example 8.6.1 (Exercise 1)

23. Let $SL(2, \mathbb{R})$ be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a, b, c, d \in \mathbb{R}$ and $ad - bc = 1$. Prove that $SL(2, \mathbb{R})$ is a group under matrix multiplication. It is called the special linear group.

Example 8.6.2 (Exercise 2)

Let T be a set with at least three elements. Show that the permutation group $A(T)$ is nonabelian.[a]

[a] Note the following proof was an adaptation of class notes, I did not makeshift an entire permutation model. I used what was given to me to prove commutative being false.

Example 8.6.3 (Exercise 3)

If $f \in S_n$, prove that $f^k = I$ for some positive integer k, where f^k means $f \circ f \circ f \circ \dots \circ f(k \text{ times })$ and I is the identity permutation.

Example 8.6.4 (Exercise 4)

If $a, b \in G$, prove that $\operatorname{ord}(bab^{-1}) = \operatorname{ord}(a)$.

Example 8.6.5 (Exercise 5)

(a) Show that $a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ has order 3 in $GL(2, \mathbb{R})$ and $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4.
(b) Show that ab has infinite order.

Example 8.6.6 (Exercise 6)
Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Example 8.6.7 (Exercise 7)
If every non identity element of G has order 2, prove that G is abelian.

Example 8.6.8 (Exercise 8)
If $a, b \in G$, prove that $\text{ord}(ab) = \text{ord}(ba)$.

Example 8.6.9 (Exercise 9)
If $\text{ord}(G)$ is even, prove that G contains an element of order 2.

Example 8.6.10 (Exercise 10)
Assume that $a, b \in G$ and $ab = ba$. If $\text{ord}(a)$ and $\text{ord}(b)$ are relatively prime, prove that ab has order $\text{ord}(a)\,\text{ord}(b)$.

Example 8.6.11 (Exercise 11)
If $a, b \in G, b^6 = e$, and $ab = b^4a$, prove that $b^3 = e$ and $ab = ba$.

Example 8.6.12 (Exercise 12)
If $(ab)^i = a^i b^i$ for three consecutive integers i and all $a, b \in G$, prove that G is abelian.

Example 8.6.13 (Exercise 13)
Let G be an abelian group and let T be the set of elements of G with finite order. Prove that T is a subgroup of G; it is called the torsion subgroup. (This result may not hold if G is nonabelian[a].)

[a] See Exercise 5

Example 8.6.14 (Exercise 14)
Let G be a group and $a \in G$. The centralizer of a is the set $C(a) = \{g \in G \mid ga = ag\}$. Prove that $C(a)$ is a subgroup of G.

Example 8.6.15 (Exercise 15)
If G is a group, prove that $Z(G) = \bigcap_{a \in G} C(a)$ (notation as in Exercise 33).

Example 8.6.16 (Exercise 16)
Suppose that H is a subgroup of a group G and that $a \in G$ has order n. If $a^k \in H$ and $(k, n) = 1$, prove that $a \in H$.

Example 8.6.17 (Exercise 17)

If H is a subgroup of a group G, then the normalizer of H is the set $N(H) = \{x \in G \mid x^{-1}Hx = H\}$ (notation as in Exercise 27). Prove that $N(H)$ is a subgroup of G that contains H.

Example 8.6.18 (Exercise 18)

Let $G = \langle a \rangle$ be a cyclic group of order n.
(a) Prove that the cyclic subgroup generated by a^m is the same as the cyclic subgroup generated by a^d, where $d = (m, n)$. [Hint: It suffices to show that a^d is a power of a^m and vice versa. (Why?) Note that by Theorem 1.2, there are integers u and v such that $d = mu + nv$.]
(b) Prove that a^m is a generator of G if and only if $(m, n) = 1$.

Example 8.6.19 (Exercise 19)

Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $(m, n) = 1$.

Example 8.6.20 (Exercise 20)

Prove that the function $h : \mathbb{R} \to GL(2, \mathbb{R})$ defined by $h(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$ is an injective homomorphism.

Example 8.6.21 (Exercise 21)

Show that $\mathbb{Z}_5^*$ is isomorphic to $\mathbb{Z}_{10}^*$.

Example 8.6.22 (Exercise 22)

If $f : G \to H$ is a surjective homomorphism of groups and G is abelian, prove that H is abelian.

Example 8.6.23 (Exercise 23)

Prove that a group G is abelian if and only if the function $f : G \to G$ given by $f(x) = x^{-1}$ is a homomorphism of groups. In this case, show that f is an isomorphism.

Example 8.6.24 (Exercise 24)

Let N be a subgroup of a group G and let $a \in G$.
(a) Prove that $a^{-1}Na = \{a^{-1}na \mid n \in N\}$ is a subgroup of G.
(b) Prove that N is isomorphic to $a^{-1}Na$. [Hint: Define $f : N \to a^{-1}Na$ by $f(n) = a^{-1}na$.]

Example 8.6.25 (Exercise 25)

Assume that a and b are both generators of the cyclic group G, so that $G = \langle a \rangle$ and $G = \langle b \rangle$. Prove that the function $f : G \to G$ given by $f(a^i) = b^i$ is an automorphism of G.

Example 8.6.26 (Exercise 26)

If $G = \langle a \rangle$ is a cyclic group and $f : G \to H$ is a surjective homomorphism of groups, show that $f(a)$ is a generator of H, that is, H is the cyclic group $\langle f(a) \rangle$. [Hint: Exercise 15.]

Example 8.6.27 (Exercise 27)

$\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Example 8.6.28 (Exercise 28)

Prove that $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Example 8.6.29 (Exercise 29)

Prove that the cycle $(a_1 a_2 \cdots a_k)$ is even if and only if k is odd.

Example 8.6.30 (Exercise 30)

Prove Theorem 7.25: The order of a permutation τ in S_n is the least common multiple of the lengths of the disjoint cycles whose product is τ.

Example 8.6.31 (Exercise 31)

Let B_n denote the set of odd permutations in S_n. Define a function $f : A_n \to B_n$ by $f(\alpha) = (12)\alpha$.
(a) Prove that f is injective.
(b) Prove that f is surjective. [Hint: If $\beta \in B_n$, then $(12)\ \beta \in A_n$.] So f is bijective. Hence, A_n and B_n have the same number of elements.
(c) Show that $|A_n| = n!/2$. [Hint: Every element of S_n is in A_n or B_n (but not both) and $|S_n| = n!$.]

Example 8.6.32 (Exercise 32)

Prove that the center of $S_n (n > 2)$ is the identity subgroup.

Example 8.6.33 (Exercise 33)

If τ is the k-cycle $(a_1 a_2 \cdots a_k)$ and if $\sigma \in S_n$, prove that $\sigma\tau\sigma^{-1} = (\sigma(a_1)\,\sigma(a_2) \cdots \sigma(a_k))$.

Example 8.6.34 (Exercise 34)

Let G be a subgroup of S_n that contains an odd permutation τ.
(a) Prove that the number of even permutations in G is the same as the number of odd permutations in G.
(b) Explain why 2 divides $|G|$.
(c) If K is a subgroup of S_n of odd order, prove that K is actually a subgroup of A_n.

Example 8.6.35 (Exercise 35)

Prove that S_n is isomorphic to a subgroup of A_{n+2}.

Example 8.6.36 (Exercise 36)

Find the inverse of each permutation in S_3.

Example 8.6.37 (Exercise 37)

Find the multiplicative inverse of each nonzero element in
(a) $\mathbb{Z}_3$
(b) $\mathbb{Z}_5$

(c) $\mathbb{Z}_7$

Example 8.6.38 (Exercise 38)

Let $G = \{x \in \mathbf{R} \mid x > 0 \text{ and } x \neq 1\}$. Define the operation $*$ on G by $a * b = a^{\ln b}$, for all $a, b \in G$. Suppose G is a group under the operation $*$, prove it is abelian.

Chapter 9

Normal Subgroups and Quotient Groups

9.1 Congruences and Lagrange's

Definition 9.1.1: Left Congruence

Let $H \leqslant G$. Define a relation on G by $a \sim b, a \overset{\ell}{\sim} b \mod H$ if $b^{-1}a \in H$ if and only if $a^{-1}b \in H$ called "Left Congruence modulo H".

Theorem 9.1.1

Left congruence is an equivalence relation.

Proof of Theorem 9.1.5: **1)** It is reflexive. If $a \in G$, then $a^{-1}a = e \in H$.
2) Let $a, b \in G$ then $a \sim b \iff a^{-1}b \in H \iff b^{-1}a \in H$. Thus $a \sim b \iff b \sim a$. Hence $\sim$ is symmetric.
3) Suppose $a, b, c \in G$, then $a \sim b, b \sim c$ then $b^{-1}a, c^{-1}b \in H$ so $(c^{-1}b)(b^{-1}a) = c^{-1}a \in H$ so $a \sim c$. ■

What are the left equivalence classes?

Definition 9.1.2: Left Congruence Classes

$\{b \in G : b \equiv a \mod H\} = \{b \in G : \exists h \in H, b = ah\} = aH = \{ah : h \in H\}$. We call aH the left coset containing a which partition G. I.e. it is the union of left cosets and 2 cosets are either identical or disjoint.

Suppose $G = S_3$ and $H = \langle (12) \rangle = \{e, (12)\}$.
$(13)H = \{(13), (123)\}$
$(23)H = \{(23), (132)\}$
Then $S_3 = \{e, (12)\} \cup \{(13)(123)\} \cup \{(23), (132)\}$.

Proposition 9.1.1

All left cosets of H have $\#H$.

Proof of Proposition 9.1.1: Let $a \in G, aH = \{ah : h \in H\}$ be a left coset of H in G. We define a map $H \to aH$ which has inverse $H \leftarrow aH$. Since they are bijections, then $\#H = \#aH$. aH is not a group, this mapping is called a set map. ■

Definition 9.1.3: Index of H in G

$[G : H]$ is the number of distinct cosets of H in G called the index of H in G so $[G : H] = \frac{\text{ord}(G)}{\text{ord}(H)}$.

Theorem 9.1.2 Lagrange's Theorem

Suppose G is a finite group, $\text{ord}(G) = n$. If $H \leqslant G$, then $\text{ord}(H) | \text{ord}(G)$.

Proof of Theorem 9.1.6: Suppose $G = G \cup a_1 H \cup \cdots \cup a_k H$, $k = \#$ of distinct cosets, where each of the $a_i H$ are distinct left cosets of H in G such that $\#a_i H = \text{ord}(H)$ for all i. So $\text{ord}(G) = k\,\text{ord}(H)$, so $\text{ord}(H) | \text{ord}(G)$. ■

Proof of Theorem 9.1.6: ■

Corollary 9.1.1 Corollary of Theorem 8.5.6

Suppose you had a finite group G of prime order. If $H \leqslant G$, then $H = \{e\}$ or $H = G$.

Proof of Corollary 9.1.1: $\text{ord}(H) | p$ so $\text{ord}(H) = 1$ or $\text{ord}(H) = p$. ■

Corollary 9.1.2 Corollary of Corollary 9.1.1

Suppose a finite order G of prime order. Then G is cyclic $\cong (\mathbb{Z}_p, +)$.

Proof of Corollary 9.1.2: Let $1 \neq a \in G$. Let $H = \langle a \rangle$. By previous cor 2, it is not the trivial group, thus it must be $H = G$. ■

Corollary 9.1.3 Corollary of Fermat's Little Theorem

Let p be prime, $a \in \mathbb{Z}, p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

Proof of Corollary 9.1.3: Let $G =$. Let $a \in \mathbb{Z}, p \nmid a, [a] \neq [0] \in$. Then $\text{ord}(\langle [a] \rangle) | p - 1$. Then $[a]^{p-1} = [1] \in$. Hence $a^{p-1} \equiv 1 \mod p$. ■

Corollary 9.1.4 Corollary 2 of Fermat's Little Theorem

For all $a \in Z$, $a^p \equiv a \mod p$. Thus $\frac{a^p - a}{p} \in \mathbb{Z}$.

Example 9.1.1

Suppose $\text{ord}(G) = 4$. Let $1 \neq a \in G$. Since $\text{ord}(\langle a \rangle) | 4$, thus $\text{ord}(\langle a \rangle) = 2$ or $\text{ord}(\langle a \rangle) = 4$. Suppose $\text{ord}(a) = 2, \langle a \rangle = \{1, a\}$. Let $a, b \in G$ and $b \neq 1, \text{ord}(b) = 2$, thus $G = \{1, a, b, ab\} \cong C_2 \times C_2 = \bigvee$ called Klein-4 Group.

9.2 Normal Subgroup

We have previously defined Left Congruence as $H \leqslant G, a, b \in G$, then $a \overset{\ell}{\equiv} b \mod H$ if $b^{-1}a \in H$ if and only if $a^{-1}b \in H$. We also defined left cosets as

$$aH := \{ah : h \in H\}$$

Definition 9.2.1: Right Congruence

$a \overset{r}{\equiv} b \mod H$ if and only if $ba^{-1} \in H$ if and only if $ab^{-1} \in H$. Right congruence classes is an equivalence class relation with an equivalence. With right cosets defined by:

$$Ha := \{ha : h \in H\}$$

In fact note that $a \in aH \cap Ha$, but it may also be the only element in common. It's possible that $aH \neq Ha$.

Example 9.2.1

$G = S_3, H = \{1, (12)\} = \langle (12) \rangle$.

Our left cosets are:

$$H = \{1, (12)\} \quad (13)H = \{(13), (123)\} \quad (23)H = \{(23), (132)\}$$

What about right cosets?

$$H = \{1, (12)\} \quad H(13) = \{(13), (132)\} \quad H(23) = \{(23), (123)\}$$

Example 9.2.2

$N = \{1, (123), (132)\} = \langle (123) \rangle$.

Left Cosets:

$$N \quad (12)N = \{(12), (23), (13)\} = (23)N = (13)N$$

Right Cosets:

$$N \quad N(12)$$

Thus the Index, $[G : N] = 2$.

Remember that the number of left cosets always equals the number of right cosets for any group $:= \frac{\text{ord}(G)}{\text{ord}(H)} = [G : H]$.

Definition 9.2.2: Normal Subgroup

Suppose N is a subgroup of G, then N is a normal of G, if the left cosets are the same as the right cosets. Denoted by $N \trianglelefteq G$. $N \trianglelefteq G$ is a normal subgroup if $\forall a \in G, aN = Na := \{xa : x \in N\} = \{ax : x \in N\}$.

Theorem 9.2.1

Suppose $N \leqslant G$. Then $N \trianglelefteq G$;
(1) if and only if the set of left cosets is identical to the set of right cosets;
(2) if and only if for all $a \in G, aN = Na.$;
(3) if and only if for all $a \in G$, $aNa^{-1} = N$ called the normalizer;
(4) for all $a \in G, a^{-1}Na = N$;
(5) for all $a \in G, x \in N, axa^{-1} \in N$;
(6) for all $a \in G, x \in N, a^{-1}xa \in N$;
(7) if and only if multiplication of left cosets is well-defined, i.e. if aN, bN are left cosets of N in G and we try to define multiplication:

$$(aN)(bN) = abN$$

if $cN = aN, bN = dN$, then $abN = cdN$;
(8) if and only if right coset multiplication is well-defined.

Proof of Theorem 9.2.1: (2) implies (1) is trivial.

Suppose (1) implies (2). Since $a \in aN$, $e \in N, a = ae \in aN = Nb$, thus $a \in Nb$. If we choose a as our representative, then $Nb = aN$.

Suppose (2) implies (7). Suppose $aN = Na$ for all $a \in G$. Suppose $aN = cN, bN = dN$, prove $abN = cdN$. Since $aN = cN$ if and only if $c^{-1}a \in N$ and likewise for bN and dN. Then $(cd)^{-1}ab \in N$ if and only if $d^{-1}c^{-1}ab \in N$. ∎

Theorem 9.2.2

$N \trianglelefteq G$, then multiplication of cosets is well-defined if $aN = cN, bN = dN$ then $abN = cdN$.

Proof of Theorem 9.2.2: Given $a, b, c, d \in G$, $aN = cN, bN = dN$ if and only if $c^{-1}a \in N, d^{-1}b \in N$. We know that since $c^{-1}a \in N$, then $d^{-1}(c^{-1}a)d \in N$ by proposition. Multiply $(d^{-1}(c^{-1}a)d)(d^{-1}b) = d^{-1}c^{-1}ab \in N$ Thus $(cd)^{-1}ab \in N$. ■

Proposition 9.2.1

$N \trianglelefteq G$ if and only if $\forall a \in G$ and $x \in N$, then $axa^{-1} \in N$ if and only if $a^{-1}xa \in N$.

Proof of Proposition 9.2.1: ($\implies$). Suppose $N \trianglelefteq G$. Let $a \in G$, $x \in N$. Since $aN = Na$, for $x, y \in N$, let $ax \in aN$ such that $ax = ya$, thus $axa^{-1} = y \in N$.

($\impliedby$). Suppose $z = ax$ then $z^{-1} = x^{-1}a^{-1}$. then $az^{-1} = ax^{-1}a^{-1}$ thus $az^{-1} \in N$. ■

Definition 9.2.3: Characteristic

N is characteristic in G for any $\phi = \mathrm{Aut}(G)$ such that $\phi(N) = N, \phi : N \to N$. Denoted by $N \mathit{char} G$

Lemma 9.2.1

If N is a characteristic subgroup of G, then $N \trianglelefteq G$.

Lemma 9.2.2

The center of G is $\mathit{char} G$.

Proposition 9.2.2

If $N \trianglelefteq G$, then the right cosets are well-defined.

Proof of Prosition 9.2.2: Use Lagrange's Theorem.

$$[G : H] = \frac{\mathrm{ord}(G)}{\mathrm{ord}(H)}$$

■

Definition 9.2.4: Quotient Group

Let G/N be the set of cosets of N in G such that $\{gN : g \in G\}$

9.3 Homomorphisms and Isomorphisms

Definition 9.3.1: Center

$$Z(G) := \{x \in G : xa = ax \ \forall a \in G\} = \{x \in G : xax^{-1} = a \ \forall a \in G\} = \bigcap_{a \in G} C_G(a).$$

Note that the centralizer is only for one element of a: $C_G(a) := \{x \in G : xa = ax\}$
$Z(G) \trianglelefteq G$

Theorem 9.3.1

Suppose $G/Z(G)$ is cyclic, then G is abelian thus $Z(G) = G$.

Proof of Theorem 9.3.1: Denote $Z(G) = Z$. Let cZ be a generator for G/Z. c is some element in G, where cZ is the coset. $aZ = c^iZ$ and $bZ = c^jZ$ for $i, j \in Z$. Thus $abZ = c^ic^jZ = c^{i+j}Z = c^{j+i}Z = baZ$. Let $a = c^id \in aZ$ and $b = c^je \in bZ$ with $d, e \in Z$. Then $ab = c^idc^je = c^ic^jde = c^ic^jed = (ec^i)(dc^j) = ba$. ■

Definition 9.3.2: Kernel of Group Functions

Suppose $\phi : G \to H$ is a group homomorphism. Define the kernel of $\phi := \{g \in G : \phi(g) = 1_H\}$.

Proposition 9.3.1

$\ker \phi \trianglelefteq G$. 2. ϕ is injective if and only if $\ker \phi = \{1_G\}$

Proof of Proposition 9.3.1: $1 \in \ker \phi$ If $a, b \in G, a, b \in \ker \phi$ $\phi(a) = \phi(b) = 1$ then $\phi(ab) = \phi(a)\phi(b) = 1 \cdot 1 = 1$ $\phi(a^{-1}) = \phi(a)^{-1} = 1^{-1} = 1$

Suppose $g \in G, x \in \ker \phi$, thus $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g^{-1}) = \phi(gg^{-1}) = 1$. Thus $gxg^{-1} \in \ker \phi$. ■

Theorem 9.3.2 First Isomorphism Theorem

Suppose $\phi : G \to H$ is a group homomorphism, which may or may not be injective. Let $k = \ker \phi$. Then $G/K \cong \text{Im}(\phi)$. Let $\overline{\phi} : G/K \to H$ be defined by $\overline{\phi}(gk) = \phi(gk)$. Then $\overline{\phi}$ is a well-defined injective homomorphism whose image is $\text{Im}(\phi)$.

Proof of Theorem 9.3.2: Let G be a Group.
$\phi : G \to H$ is a group homomorphism
$K = \ker \phi = \{g \in G : \phi(g) = e_H\}$
$K \trianglelefteq G$ and $G/K \cong \text{Im}(\phi)$
So if ϕ is surjective then $G/K \cong H$ ■

Let $f : G/K \to \text{Im}\phi$ such that $f(gk) \mapsto \phi(g)$ is a well defined isomorphism.

Theorem 9.3.3

$g \to \phi_g$ is a homomorphism from G to $\text{Aut}(G)$.

Proof of Theorem 9.3.3: Let $a, b \in G$. Need to check that $ab \mapsto \phi_a\phi_b$ then $\phi_{ab} \mapsto \phi_a\phi_b$. Let $x \in G$, then

$$\begin{aligned}\phi_{ab}(x) &= abxab^{-1} \\ &= abxb^{-1}a^{-1} \\ &= a\phi_b(x)a^{-1} \\ \\ &= \phi_a \circ \phi_b(x)\end{aligned}$$

What is $\ker \phi$?

$$\begin{aligned}\ker \phi &= \{y \in G \mid \phi_g(x) = x \quad \forall x \in G\} \\ &= \{y \in G \mid gxy^{-1} = x \quad \forall x \in G\} \\ &= \{y \in G \mid yx = xy \quad \forall x \in G\} \\ &= Z(G)\end{aligned}$$

$\to$ center of G ■

Corollary 9.3.1

$$G/Z(G) \cong \text{Inn(G)}$$

inner automorphisms of G by 1st isomorphism theorem.

Proof of Corollary 9.3.1: If G is abelian, then $Z(G) = G$ and $Inn(G) = \{ID\}$. If $G = S_n, n \geqslant 3$ then $Z(G) = \{1\}$ so $G \cong$ subgroup of $\text{Aut}(G)$. Thus $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. ■

Theorem 9.3.4

Suppose $N \trianglelefteq G, K \trianglelefteq N, K \trianglelefteq G$ then $N/K \trianglelefteq G/K$ and $(G/K)/(N/K) \cong G/N$

Normal is not transitive. Suppose

$$N \trianglelefteq G \text{ and } K \trianglelefteq N \nRightarrow K \trianglelefteq G$$

$$G = \mathbb{Z}_3 + N = 6\mathbb{Z}, K = 12\mathbb{Z}$$
$$K \trianglelefteq N \trianglelefteq G, K \trianglelefteq G$$
$$G/N = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$$

it is possible for then to be true but $K \ntrianglelefteq G$ $N/K = 6\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_2$

$$G/K = \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}_{12}$$
$$(G/K)/(N/K) = \mathbb{Z}_{12}/\mathbb{Z}_2 \cong \mathbb{Z}_6$$
$$\text{so } G/N \cong (G/K)/(N/K)$$

Proof of Theorem 9.3.4: Define $\phi : G/K \to G/N$ by $\phi(gk) = gN$ for $g \in G$ Check well defined Suppose $aK = bK$ [Show $aN = bN$] So $b^{-1}a \in K \leqslant N$ so $b^{-1}a \in N$ thus $aN = bN$.

Show $\text{Ker}(\phi) = N/K$ Suppose $gk \in \ker(\phi)$ so $gN = N \iff y \in N$, so $gK \in N/K$ So $\phi(gK) = gN = N = N$ Thus all gk are elements of $\ker(\phi)$. $\implies N/K \leqslant \ker(\phi)$.

Show ϕ surjective Let $gN \in G/N, gK \in G/K$ $gK \xrightarrow{\Phi} gN$ Use 1st isomorphism theorem $(GK)/Ker\phi \cong G/N$ So every output gN has as input $gk \in G/K \iff (G/K)/(N/K) \cong GN$ ■

Theorem 9.3.5 4th Isomorphism Theorem

Suppose $N \trianglelefteq G$ then there is bijection between subgroups G/N and subgraphs of G containing N

Proof of Theorem 9.3.5: ($\implies$). Suppose $H \leqslant G$ Define $T = \{hN \mid h \in H\}$ Check that $T \leqslant G/N$

$1 \in H = G/N = N \in T$ Identity ✓. If $h_1, h_2 \in H$

$(h_1N)(h_2N) = (h_1h_2)N$ Closure under multiplication. ✓

If $h \in H$ $(hN)^{-1} = h^{-1}N \in T$ Closure under inverses ✓ so $\left(h^{-1}N\right) = (\ln N)^{-1}$.

($\impliedby$). Suppose $T \leqslant G/N$ Define $H = \{h \in G \mid hN \in T\}$ Check that $H \leqslant G$ $1 \in H$ because $1N \in T$

If $h_1, h_2 \in H$ then $h_1N, h_2N \in T$ $(h_1N)(h_2N)$ because T group So $(h_1h_2)N \in T \Rightarrow h_1h_2 \in H$ If $h \in H$, then $hN \in T$ $(hN)^{-1} \in T$ b/c T group $\Rightarrow h^{-1}N \in T \Rightarrow h^{-1} \in H$ ■

These maps are also inverses of one another. If we start with $H \leqslant G$ then $T = \{hN : h \in H\}$. Then we have $T \to H$. If we start with $T \leqslant G/N$ then let $H = \{h \in G : hN \in T\}$ thus $H \to T$.

Proposition 9.3.2

Under these maps $H \trianglelefteq G \Leftrightarrow T \trianglelefteq G/N$.

Proof of Proposition 9.3.2: ($\implies$). Let $xN \in T$ $gN \in G/N \Rightarrow gNxNg^{-1}N = gxg^{-1}N \in T \Rightarrow T \trianglelefteq G/N$

($\impliedby$). Let $T \trianglelefteq G/N, xN \in T$. Let $x \in H, y \in G$ and $(gN)(xN)(g^{-1}N) \in T$ because T group. Thus $(gxg^{-1})N \in T$ and $gxg^{-1} \in H$ so $H \trianglelefteq G$. ■

Definition 9.3.3: Simple Group

Suppose G group and $\{1\} \neq G$. G is simple if and only if $N \trianglelefteq G$ implies $N = G$ or $N = \{1\}$.

Theorem 9.3.6

If G abelian and simple, then $G \cong C_p$ with p prime.

Proof of Theorem 9.3.6: Since G is abelian and simple, then there are no proper subgroups. Suppose $a \in G$ and $1 \neq a$, then $\langle a \rangle = G$ due to the simple group structure. Thus G is cyclic. We claim that $G \ncong (\mathbb{Z}, +)$ due to $(\mathbb{Z}, +)$ having many proper subgroups. Thus $G \cong C_n$.

Suppose n is composite, $\exists k$ such that $k|n$, then $\langle a^k \rangle \triangleleft G = \langle a \rangle$, thus $\langle a^k \rangle$ is normal and not equal to G. But then G is not simple with this conclusion, thus a contradiction arose. Thus n prime. Hence $G \cong C_p$, p prime. ■

What does it mean when a graph is not simple? It will have a proper normal subgroup. Suppose G not simple, then $1 \neq N \triangleleft G$. Thus G/N is not simple and can **lift** any proper normal subgroup of G/N to G.

Now the correct thing to ask is what does lift mean...

Definition 9.3.4: Lift

By the 4th Isomorphism Theorem, there is a bijection between $T \leqslant G/N$ to $H \leqslant G$. We lift T by assigning T to its corresponding H.

Definition 9.3.5: Jordan-Holder Series [Composition Series]

If N is simple, we can find further proper subgroups of G contained in N. Do this process backwards:

$$\text{proper normal subgroup of G} \longrightarrow \text{proper normal subgroup of G/N} = \text{M}$$

$$\text{proper normal subgroup of (G/N)/M} \longrightarrow \dots$$

Eventually we run out of proper normal subgroups. This process creates a sequence of subgroups

$$\{1\} \leqslant G_1 \leqslant G_2 \leqslant G_3 \leqslant \dots \leqslant G_n \leqslant G$$

with $G_i \trianglelefteq G_{i+1}$ both simple. This sequence is called the JH-Series.

Example 9.3.1

$G = C_6 \cong C_3 \times C_2$ then $N_1 = C_3 \times \{1\} \trianglelefteq G$ and $N_2 = \{1\} \times C_2 \trianglelefteq G$. Thus $G/N_1 \cong C_2$ and $G/N_2 \cong C_3$. Have 2 composition series, and composition factors, $\{1\} \trianglelefteq N_1 \trianglelefteq G$. since $\{1\} \trianglelefteq N_2 \trianglelefteq G$ have the same composition factors C_2, C_3: $N_2/\{1\} \cong C_2, G/N_2 \cong C_3$ and $N_1/\{1\} \cong C_3, G/N_1 \cong C_2$.

9.4 Simplicity of A_n

Theorem 9.4.1

If $n \geqslant 5$ then A_n is simple.

Proof of Theorem 9.4.1: Outline of Pf. **1.** A_n is generated by the 3-cycles such that every product of A pair of transpositions is a product of 3-cycles or a 3-cycle.
2. Suppose $N \trianglelefteq A_n$ with $(123) \in N$, then N has every 3-cycle.
3. Suppose $n \geqslant 5$, and $1 \neq N \trianglelefteq A_n$. Prove that N has a 3-cycle that has some $\sigma \in N, 1 \neq \sigma$. By disjoint cycle decomposition in A_n suppose $\sigma = (123\dots r)(\dots)(\dots)$ for $r \geqslant 4$, pick some τ that only moves $1 \dots r$ such that τ is a 3-cycle: $\tau\sigma\tau^{-1}\sigma^{-1} = \tau(1\dots r)()()\dots\tau^{-1}()()\dots(r\dots 321) = \tau(123\dots r)\tau^{-1}(r\dots 321)$.

Let $\tau = (123)$. Then $(123)(123\dots r)(132)(r\dots 321) = (231456\dots r)(r\dots 654321) = (124)(3)(5)\cdots = (124) \in N$ Thus $N = A_n$.

Suppose $1 \neq N \trianglelefteq A_n$. We have shown that every cycle is a product of three cycle or a three cycle itself. Given $(abc) \in N$ then $N = A_n$. Let $\sigma = ()()$ be a product of cycles, atleast one of them are length of atleast 3 $\in N$ which implies $N = A_n$.

Then the remaining cases are $\sigma \in N$ and the cycle structure of σ which consists of 2-cycles and 3-cycles. Then σ^2 only has 3-cycles. Then we can assume that only 2-cycles or only 3-cycles

Every element of A_n (with $n \geqslant 3$) is a product of 3-cycles.
Every element of A_n is by definition the product of pairs of transpositions. But every such pair must be of one of these forms: $(ab)(cd)$ or $(ab)(ac)$ or $(ab)(ab)$. In the first case verify that $(ab)(cd) = (adb)(adc)$, in the second that $(ab)(ac) = (acb)$, and in the last that $(ab)(ab) = (1) = (abc)(acb)$. Thus every pair of transpositions is either a 3-cycle or a product of two 3-cycles. Hence, every product of pairs of transpositions is a product of 3-cycles.

Claim: If N is a normal subgroup of A_n (with $n \geqslant 3$) and N contains a 3-cycle, then $N = A_n$
Suppose we had a 3-cycle of any standard, for simplicity (WLOG), we choose $(123) \in N$. We have the inverse being $(132) \in N$ and because N is normal then we have that $x(132)x^{-1} \in N$ too, by theorem 8.11. Let $x = (12)(3k)$ and $x^{-1} = (3k)(12)$. Then

$$x(132)x^{-1} \quad = (12)(3k)(132)(3k)(12) \quad = (12k)$$

Case 1. N contains all 3-cycles of the form $(12k)$ with $k \geqslant 3$. Verify that every other 3-cycle can be written in one of these forms: $(1a2), (1ab), (2ab), (abc)$ where $a, b, c \geqslant 3$. By (*) and closure in N,

$$\begin{aligned}
&(1a2) = (12a)(12a) \in N;\\
&(1ab) = (12b)(12a)(12a) \in N;\\
&(2ab) = (12b)(12b)(12a) \in N;\\
&(abc) = (12a)(12a)(12c)(12b)(12b)(12a) \in N.
\end{aligned}$$

Thus N contains all 3 -cycles, and, hence, N contains all products of 3-cycles by closure. Therefore, $N = A_n$ by previous Lemma. Case 2. The inverse of the cycle $(a_1a_2a_3 \cdots a_k)$ is the cycle $(a_1a_ka_{k-1} \cdots a_3a_2)$. You can easily verify this. ■

Theorem 9.4.2

For each $n \neq 4$, the alternating group A_n is a simple group.

9.5 Exercises

Example 9.5.1 (Exercise 1)

If G is a group of order 25, prove that either G is cyclic or else every nonidentity element of G has order 5.

Example 9.5.2 (Exercise 2)

If G is an abelian group of order $2n$, with n odd, prove that G contains exactly one element of order 2.

Example 9.5.3 (Exercise 3)

(a) If a and b each have order 3 in a group and $a^2 = b^2$, prove that $a = b$. [Hint: What are a^{-1} and b^{-1} ?]
(b) If G is a finite group, prove that there is an even number of elements of order 3 in G.

Example 9.5.4 (Exercise 4)

If a prime p divides the order of a finite group G, prove that the number of elements of order p in G is a multiple of $p - 1$.

Example 9.5.5 (Exercise 5)

If G is a group, prove that every subgroup of $Z(G)$ is normal in G.

Example 9.5.6 (Exercise 6)

Prove that for any group G, the center $Z(G)$ is a characteristic subgroup.

Example 9.5.7 (Exercise 7)

If K is a normal subgroup of order 2 in a group G, prove that $K \subseteq Z(K)$. [Hint: If $K = \{e, k\}$ and $a \in G$, what are the possibilities for aka^{-1} ?]

Example 9.5.8 (Exercise 8)

(a) Let N and K be subgroups of a group G. If N is normal in G, prove that $NK = \{nk \mid n \in N, k \in K\}$ is a subgroup of G.
(b) If both N and K are normal subgroups of G, prove that NK is normal.

Example 9.5.9 (Exercise 9)

If K and N are normal subgroups of a group G such that $K \cap N = \langle e \rangle$, prove that $nk = kn$ for every $n \in N, k \in K$.

Example 9.5.10 (Exercise 10)

Let N be a subgroup of a group G of index 2. Prove that N is a normal subgroup as follows.
(a) If $a \notin N$, prove that the coset Na consists of all elements of G that are not in N.
(b) For each $a \in G$, prove that $a^{-1}Na \subseteq N$ and apply Theorem 8.11. [Hint: If $a \notin N$ and $n \in N, a^{-1}na$ is either in N or in Na by part (a). Show that the latter possibility leads to a contradiction.]

Example 9.5.11 (Exercise 11)

Let H be a subgroup of order n in a group G. If H is the only subgroup of order n, prove that H is normal.

Example 9.5.12 (Exercise 12)

Let G be an abelian group and T its torsion subgroup (see Exercise 19 of Section 7.3). Prove that G/T has no nonidentity elements of finite order.

Example 9.5.13 (Exercise 13)

Suppose that G is a simple group and $f : G \to H$ is a surjective homomorphism of groups. Prove that either f is an isomorphism or $H = \langle e \rangle$.

Example 9.5.14 (Exercise 14)

Let G be an abelian group.
(a) Show that $K = \{a \in G | \mid a \mid \leqslant 2\}$ is a subgroup of G.
(b) Show that $H = \left\{x^2 \mid x \in G\right\}$ is a subgroup of G.
(c) Prove that $G/K \cong H$. [Hint: Define a surjective homomorphism from G to H with kernel K.]

Example 9.5.15 (Exercise 15)

Prove that $(\mathbb{Z} \times \mathbb{Z})/\langle (1,1) \rangle \cong \mathbb{Z}$. [Hint: Show that $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, given by $f((a,b)) = a - b$, is a surjective homomorphism.]

Example 9.5.16 (Exercise 16)

$SL(2, \mathbb{R})$ is a normal subgroup of $GL(2, \mathbb{R})$. Prove that $GL(2, \mathbb{R})/SL(2, \mathbb{R})$ is isomorphic to the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

Example 9.5.17 (Exercise 17)

(Second Isomorphism Theorem) Let K and N be subgroups of a group G, with N normal in G. Then $NK = \{nk \mid n \in N, k \in K\}$ is a subgroup of G that contains both K and N.
(a) Prove that N is a normal subgroup of NK.
(b) Prove that the function $f : K \to NK/N$ given by $f(k) = Nk$ is a surjective homomorphism with kernel $K \cap N$.
(c) Conclude that $K/(N \cap K) \cong NK/N$.

Example 9.5.18 (Exercise 18)

Prove that no subgroup of order 2 in $S_n (n \geqslant 3)$ is normal.
Use : The center of S_n (n ¿ 2) is the identity subgroup;

Example 9.5.19 (Exercise 19)

Let N be a subgroup of S_n such that $\sigma\tau = (1)$ for all nonidentity elements $\sigma, \tau \in N$. Prove that $N = (1)$ or N is cyclic of order 2. [Hint: If $N \neq (1)$, let σ be a nonidentity element of N. Show that σ has order 2. If τ is any other nonidentity element of N, show that $\sigma = \tau$.]

Example 9.5.20 (Exercise 20)

If N is a normal subgroup of S_n and $N \bigcap A_n = A_n$, prove that $N = A_n$ or S_n. [Hint: Why is $A_n \subseteq N \subseteq S_n$?]
Use: A_n is a subgroup of S_n of order $n!/2$ and Lagrange's Theorem

Chapter 10

Topics in Group Theory

10.1 Direct Sums and Finite Abelian Groups

Definition 10.1.1: External Direct Product

Let H, K be groups. $G = H \times K = \{(h,k) : h \in H, k \in K\}$, G group. $\overline{H} = \{(h,1) : h \in H\} \trianglelefteq G$ $\overline{K} = \{(1,k) : k \in K\}$ In fact the intersection $\overline{H} \bigcap \overline{K} = \{(1,1)\}$.

Theorem 10.1.1

Suppose G is a group and two subgroups $H, K \leqslant G$. When is G actually isomorphic to the direct product of H and K.

Proof of Theorem 10.1.1: Define $HK = \{hk\}$. If $H, k \trianglelefteq G$, then HK is a group (Exercise). ■

Theorem 10.1.2

If $G = HK$ and $H \bigcap K = \{1\}$, then $G \cong H \times K$. Defined the Internal Direct Product since it is isomorphic to G.

Definition 10.1.2: Disjoint Group

If $H \bigcap K$ is disjoint, then $H \bigcap K = \{1\}$.

Proof of Theorem 10.1.2: Define $\phi : H \times K \to G$ defined by $\phi(h,k) = hk$. Since $G = hk$, ϕ is surjective.
Let $(h_1, k_1), (h_2, k_2) \in H \times K$.

$$\begin{aligned}\phi[(h_1,k_1)(h_2,k_2)] &= \phi[(h_1h_2, k_1k_2)] \\ &= (h_1h_2)(k_1k_2) \\ &= (h_1k_1)(h_2k_2) \\ &= \phi[(h_1,k_1)]\phi[(h_2,k_2)]\end{aligned}$$

Thus ϕ is a homomorphism.

Let $\ker(\phi) = \{(h,k) : hk = e\}$. If $hk = e$ then $h = k^{-1}$ and $k = h^{-1}$. So $k \in H$ and $h \in K$, so $k, h \in H \bigcap K = \{1\}$ then $k = h = 1$. So $\ker(\phi) = \{(1,1)\}$. A surjective homomorphism and trivial kernel implies injectivity. ■

Example 10.1.1 (Example 1.)
$G = \langle n = 2x \rangle, \text{ord}(x) = n$.

Proof of Example 1.: Suppose $n = ab, \gcd(a,b) = 1$. Let $H = \langle x^a \rangle, H \cong C_b, K = \langle x^b \rangle K \cong C_a$. If $x^r \in H \bigcap K$, then $a|r$ and $b|r$. Then $r = ai$ and $r = bj$ for $i, k \in \mathbb{Z}$. Since r is a multiple of a and b, then $n|r$, then $x^r = 1$. So $H \bigcap K = \{1\}$.

If $r \in \mathbb{Z}$ and $r = sa + tb$, then

$$\begin{aligned} x^r &= x^{sa+tb} \\ &= x^{sa}x^{tb} \\ &= (x^a)^s(x^b)^t, \end{aligned}$$

then $x^a \in H$ and $x^b \in K$. Thus $x^r \in HK$ for all r and $G = \langle x \rangle$. Hence $G = HK$. ■

Definition 10.1.3: Direct Sum

When G is an additive abelian group, the direct product is then called a direct sum.

Theorem 10.1.3 Fundamental Theorem

If $\text{ord}(G) \leqslant \infty$, G abelian, then

1. $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$;
2. $G \cong \mathbb{Z}_{p_1}^{k_1} \oplus \mathbb{Z}_{p_1}^{k_2} \oplus \mathbb{Z}_{p_2}^{l_2} \ldots$;
3. $G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k}$. With p_i^k being elementary divisors and d_i are invariant factors.

Proof of the Fundamental Theorem: (2) $\implies$ (1) is easy.

(2) $\implies$ (3) happens because $gcd(m,n) = 1$, then $\mathbb{Z}_{mn} \cong Z_m \oplus Z_n$. Thus by previous clause, (4) $\implies$ (3).

(3) $\implies$ (4), Use the following algorithm: Ex. $G = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Primes: 2,3,5

$2^2\ 3\ 5 \to 60 = d_3$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. $2^2\ 3\ 1 \to 12 = d_2$

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$. $2\ 1\ 1 \to 12 = d_1$

(1) $\implies$ (4). Suppose $x_1, \ldots, x_n$ generators. Map $\mathbb{Z}^n = \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \mathbb{Z} \to G$ such that $e_i \to x_i$. Let $e_1 = (1,0,0,\ldots,0) e_2 = (0,1,0,\ldots,0), \ldots, e_n = (0,0,0,\ldots,1)$. Every $y \in Z^n$ can be written as $y = y_1e_1 + \cdots + y_ne_n \in \mathbb{Z}$. Map $y \to \sum_{i=1}^{n} y_i x_i$ is surjective. Prove that its a homomorphism. If $K = \ker \phi$, then $Z^n/K \cong G$ by the first isomorphism theorem. ■

Definition 10.1.4: Free Abelian Group

G is a free abelian group if it has a basis.

Note:-

Recall from Linear Algebra:
Base for $\mathbb{Z}$ is $e_1, \ldots, e_n$ which generates and is linearly independent.

Lemma 10.1.1

Every subgroup of $\mathbb{Z}^n$ has a basis.

A direct product and direct sum are similar as basis but for groups.

Theorem 10.1.4

We have $\{f_1, \ldots, f_m\}$ as a base for K if for all $k \in K, K = \sum a_i f_i$ for all $a_i \in \mathbb{Z}$. And also if $\sum a_i f_i = 0$ implies $a_i = 0$ for all i.

We want to show that every element k can be written as a linear combination.

Proof of Theorem 10.1.5: Induction on n. Base Case: n = 1 Every subgroup of $\mathbb{Z}^1$ is cyclic and generated by $d \in \mathbb{Z}$. If $k \neq \{0\}$ is a subgroup of $\mathbb{Z}$, then $d \neq 0$, then $\{d\}$ is a base for $K \leqslant Z$. Let $K = \mathbb{Z}d = \{xd : x \in \mathbb{Z}\}$. So every subgroup of $\mathbb{Z}$ has a base.

Baby Induction: $n = 1 \implies n = 2$. Let $n = 2$. $K \leqslant \mathbb{Z}^2 = \mathbb{Z}e_1 + \mathbb{Z}e_2$. If $K \leqslant \mathbb{Z}e_1$, done. Since $n = 1$ is true. Assume not. Let $H = \{b \in \mathbb{Z} : \exists y \in \mathbb{Z}, (y, b) = ye_1 + be_2 \in K\}$. If $K \not\leq \mathbb{Z}e_1$, then $H \neq \{0\}$. So $H = \mathbb{Z}d, d \neq 0$. So $H \leqslant \mathbb{Z}$.

So there exists $y_1 \in \mathbb{Z}$ such that $y_1e_1 + de_2 = (y_1, d) \in K$. Let $f_2 = (y_1, d)$. $K \bigcap \mathbb{Z}e_1 = (y, 0) \in K$. If $K \bigcap \mathbb{Z}e_1 = \{(0, 0)\}$, then not in base. Otherwise it has base $(a, 0) = f_1$. ■

Lemma 10.1.2

(f_2) is a base for K. 2) (f_1, f_2) is a base for K.

Proof of Lemma 10.1.2: Let $k \in K$ span all K such that $k = z_1e_1 + z_2e_2 = (z_1, z_2) \in K$. Then $z_2 \in H$. Then H is generated by some integer d. So $z_2 = dk_2, k_2 \in \mathbb{Z}$. Then

$$\begin{aligned} k - k_2f_2 &= (z_1, z_2) - k_2(y_1, d) \\ &= (z_1 - k_2y_1, z_2 - k_2d) \\ &= (z_1 - k_2y_1, dk_2 - k_2d) \\ \\ &= (z_1 - k_2y_1, 0) \in K \bigcap \mathbb{Z}e_1 \end{aligned}$$

So

$$k - k_2f_2 = \begin{cases} 0 & \text{when } f_1 = (0, 0); \\ k_1f_1 & \text{else} \end{cases}$$

So

$$k = \begin{cases} k_2f_2 \\ k_1f_1 + k_2f_2 \end{cases}$$

In both cases, the vectors span K.

In order to check for linear independence, we can easily see that case one is obvious since there is only one vector. For Case Two: Let $f_1 = (a, 0), f_2 = (y_1, 0)$. If $a_1f_1 + a_2f_2 = (0, 0)$. $(a_1a, 0) + (a_2y, a_20) = (0, 0)$. $(a_1a + a_2y, a_20) = (0, 0)$.

Then $d \neq 0$, so $a_20 = 0$ implies $a_2 = 0$.

If $a \neq 0, a_2 = 0$, and $a_1a + a_2y = 0$ implies $a_1 = 0$. So $a_1f_1 + a_2f_2 = (0, 0)$ implies $a_1 = a_2 = 0$. So linearly independent in case two. ■

10.2 Group Actions

Let G be a finite group and let A be a set. G acts on A if there is a homomorphism $G \to \operatorname{sym} A$.

Definition 10.2.1: Left Translation Group Action

The most general group action is G acts on itself by left translation (Cayley Homomorphism) $(g \to \phi_g : \phi_g(x) = gx)$
In general G acts on A by left translation if for $g \in G$ and $a \in A$, there is an element $g \cdot a \in A$ such that $1 \cdot a = a$ and $(gh) \cdot a = g(ha)$

Definition 10.2.2: Right Conjugation Action

$g \in G$, $a \in A$. There is $a^g \in A$ such that $a^1 = a$ and $a^{gh} = (a^g)^h$.

Definition 10.2.3: Left Conjugation Action

$g \in G$, $a \in A$. There is ${}^{g}a \in A$ such that ${}^{1}a = a$ and ${}^{gh}a = {}^{h}({}^{g}a)$.

Definition 10.2.4: Orbit

Suppose G acts on A by left translation. Let $a \in A$, then the orbit of a under the action is $\{g \cdot a : g \in G\} =: O(a)$

Lemma 10.2.1

Cayley action G on G, then the orbit is all of G.

If the action is right exponential, then $O(a) = \{a^g : g \in G\}$.
If G acts on itself by right conjugation, then $O(a) = \{gxg^{-1} : g \in G\}$ = conjugacy class of $x \in C_x$.
If G is abelian then $C_x = \{x\}$ for any x.

Example 10.2.1

If $G = S_3$ $C_{(12)} = \{(12), (13), (23)\}$. $G = C_1 \sqcup C_{(12)} \sqcup C_{(123)}$

If G acts on A then we can define a relation on A such that $a \sim b$ if a, b are in the same orbit by left translation and right exponentiation.

Definition 10.2.5: Stabilizer

Suppose G acts on A. Let $a \in A$, then the stabilizer of A under the action: left translation : $\{g \in G : g \cdot a = a\}$ and; right exponentiation : $\{g \in G : a^g = a\}$ denoted by ${}_{g}a$.

G acts on G under conjugation then the stabilizer is infact just the centralizer of G on x.

Theorem 10.2.1 Orbit-Stabilizer Theorem

1. $H =_G (a) \leqslant G$;
2. $[G : H] = \text{ord}(O(a))$

Proof of the Orbit-Stabilizer Theorem: **(1).** If $a \in A$ and $a^1 = a$, so $1 \in_G (a)$. If $g, h \in (a)$, then $a^{gh} = (a^g)^h = a^h = a$. So $gh \in (a)$ So $(a) \leqslant G$. Suppose $g \in (a)$ then $a^g = a$, then $(a^g)^{g^{-1}} = a^{gg^{-1}} = a^1 = a = a^{g^{-1}}$. So $g^{-1} \in (a)$.

(2). Find a bijection. Let H cosets in $G = G \setminus H$. Then declare a bijection from $Hg \longleftrightarrow a^g$. We need to check $Hg_1 = Hg_2 \iff a^{g_1} = a^{g_2}$. Then $g_2 g_1^{-1} \in H \iff a^{g_2 g_1^{-1}} = a \iff (a^{g_2 g_1^{-1}})^{g_1} = a^{g_1} \iff a^{g_2} = a^{g_1}$. ∎

Definition 10.2.6: Class Equation

Let G act on itself by conjugation. G is the union of its disjoint conjugacy classes. Suppose these have representatives $z_1 = 1, z_2, \ldots, z_k, x_1, x_2, \ldots, x_r$. Let z_i be the center of G.
Let $\text{ord}(C_{z_1}) = 1$ and $\text{ord}(C_{x_i}) \geqslant 2$. Class Equation for G: $\text{ord}(G) = \text{ord}(Z(G)) + \text{ord}(C_{x_1}) + \ldots + \text{ord}(C_{x_r})$.
Or let $\text{ord}(C_{x_1}) = [G : C_G(x_1)]$, then $\text{ord}(G) = \text{ord}(Z(G)) + \sum_{i=1}^{r} [G : C_G(x_i)]$

Example 10.2.2

Suppose P is a group, then $\text{ord}(P) = p^n$, p prime, then $Z(P) \neq \{1\}$.

Proof of Example: From Class Equation: $\text{ord}(P) = \text{ord}(Z(P)) + \sum_{i=1}^{r} [P : C_P(x_i)]$. If:

$$\begin{aligned}[P : C_P(x_i)] &= \frac{p^n}{\text{ord}(C_P(x_i))} \geqslant 2 \\ &= p^{r_i}, r_i > 0\end{aligned}$$

then $p | [P : C_P(x_i)]$ for all i. Which implies that $p | Z(P)$ implying that $\text{ord}(Z(P)) \neq \{1\}$. ■

10.3 Sylow Theorems

Theorem 10.3.1 First Sylow Theorem

Suppose $\text{ord}(G) < \infty$ and $p | \text{ord}(G)$, then p^n is the highest power of p dividing G then $\exists P \leqslant G$ such that $\text{ord}(P) = p^n$ called the Sylow P Subgroup.

Example 10.3.1

Given $G = S_4$, Sylow Theorem One says $p^n \mid \text{ord}(S_4) = 24$. Then there exists P, Q with $\text{ord}(P) = 8$ if $p = 2$ and $\text{ord}(Q) = 3$ if $p = 3$.

Proof of Example: With $p = 3$, $3 \mid 24$ and there must be classes $3 \nmid \text{ord}(C_{x_i}$. Fine one: $\text{ord}(C_{x_i)} = 8$ with $x_i = (123)$. Try and find $\text{ord}(C_G(x_i))$ for $x_i = (123)$. If $p \nmid \text{ord}(C_{x_i})$, then $p^n \mid \text{ord}(C_G(x_i))$. Why?

$$\text{ord}(C_G(x_i)) = \frac{\text{ord}(G)}{\text{ord}(C_{x_i})}.$$

With $p = 2$

$3 = \text{ord}(C_{(12)(34)})$ $8 = \text{ord}(C_G[(12)(34)])$ ■

Example 10.3.2

Given $G = S_4$, then $Z(G) = \{e\}$. The possible cycle structures given by partitions of 4:

$$\begin{aligned}4 = 4 &\implies (1234) \\ 4 = 3 + 1 &\implies (123)(4) \\ 4 = 2 + 2 &\implies (12)(34) \\ 4 = 2 + 1 + 1 &\implies (12)(3)(4) \\ 4 = 1 + 1 + 1 + 1 &\implies (1)(2)(3)(4)\end{aligned}$$

How many distinct conjugacy classes are there? We need to keep in mind that 2-cycles may look different but still the same.

Proof of Example: $(34)(12) = (12)(34)$. We do not want this example above as separate conjugacy classes due

to abelian.

$$\begin{aligned} 4 &\implies 4!/4 = 6 \\ 3+1 &\implies \binom{4}{3} \cdot 3!/3 = 4(2) = 8 \\ 2+2 &\implies \binom{4}{2}/2 = 3 \\ 2+1+1 &\implies \binom{4}{2} = 6 \\ 1+1+1+1 &\implies 1 \end{aligned}$$

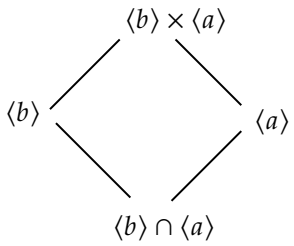
The right hand side if you have not noticed is the order of the conjugacy classes. We can add these together to get $6+8+3+6+1 = 24$, where $1 = \text{ord}(Z(G))$ and $6+8+3+6 = [G : C_G(x_i)]$. ■

Theorem 10.3.2 Cauchy's Theorem

If $p \mid \text{ord}(G)$, then G has a subgroup under p.

Proof of Cauchy's Theorem: By induction of order G, let $a \in G$ and $1 \neq a$ and $p \mid \text{ord}(G)$. If $p \mid \text{ord}(a) = n$, then $a^{n/p}$ has order p, implies there exists a group with order p. Suppose $p \nmid \text{ord}(a)$, then $p \mid \text{ord}(G/\langle a \rangle) < \text{ord}(a)$.

By Induction $b = b\langle a \rangle$, there exists $b \in G$ with $\text{ord}(\bar{b}) = p$. We claim that $p \mid \text{ord}(b)$.



Based on the second isomorphism theorem. $\langle b \rangle \times \langle a \rangle / \langle a \rangle \cong \langle b \rangle / \langle b \rangle \cap \langle a \rangle$. So $p \mid \text{ord}(b) = m$. So $b^{m/p}$ has order p. ■

Example 10.3.3

If $G = S_4$. Then $24 = 1+8+3+6+6$. Made up of $(1) + (123) + (12)(34) + (12) + (1234)$.

Proof of Example: **Case 1**. If $p \mid \text{ord}(Z(G))$, then $Z(G)$ has a subgroup N of order p. This is by Cauchy's Theorem for Abelian Groups. If $g \in G$ and $n \in N$, then $gng^{-1} = n \in N$. So $N \trianglelefteq G$. Mod out by N. Then let $\bar{G} = G/N$ such that $\text{ord}(\bar{G}) < \text{ord}(G)$, then $p^{n-1} \mid\mid \text{ord}(\bar{G})$. So by Induction Hypothesis $\bar{G}$ contains a subgroup T of order p^{n-1}. By the fourth isomorphism theorem: $\text{ord}(H) = \text{ord}(N)\,\text{ord}(T) = p \cdot p^{n-1} = p^n$.

Case 2. Suppose $p \nmid \text{ord}(Z(G))$. Since $p \mid \text{ord}(G)$, if $p \mid [G : C_G(x_i)]$ for all i, then $p \mid \text{ord}(Z(G)) = \text{ord}(G) \setminus \sum_{i=1}^{r} [G : C_G(x_i)]$, but $p \nmid \text{ord}(Z(G))$. So there exists an i, such that $p \nmid [G : C_G(x_i)] = \frac{\text{ord}(G)}{\text{ord}(C_G(x_i))}$. So $p^n \mid \text{ord}(G) = \text{ord}(C_G(x_i)) * [G : C_G(x_i)]$, thus $p^n \mid\mid \text{ord}(C_G(x_i))$ where $\text{ord}(C_G(x_i)) < \text{ord}(G)$. By induction hypothesis $C_G(x_i)$ has a subgroup $P \leqslant C_G(x_i)$ of order $p^n, P \leqslant G$. ■

Theorem 10.3.3 Second Sylow Theorem

All Sylow-p's are conjugate in G. I.e. if $P, Q \leqslant G$, then both Sylow-p's there exists g inG sucht hat $Q = P^g = gPg^{-1} = \{gxg^{-1} : x \in P\}$.

Theorem 10.3.4 Third Sylow Theorem

The number of Sylow-p subgroups of $G \equiv 1 \mod p$ and equal to $[G : N_G(p)]$ where p is any Sylow-p. So this number divides $[G : P]$ where $N_G(p) := \{g \in G : gxg^{-1} \in P, \forall x \in P\}$ and $[G : P] = [G : N_G(p)][N_G(P) : P]$.

Let P be a Sylow-p. Let $S := \{P^g = \{gxg^{-1} : x \in P\}\}$. G acts on S by right exponentiation such that $g : P \xrightarrow{\phi_g} P^g$ and $1 : P \to P^1 = P$. Then $P^{gh} = \{ghx(gh)^{-1} : x \in P\} = \{g(hxh^{-1})g^{-1} : x \in P\} = \{gP^{hg^{-1}} : hxh^{-1} \in P^{h}\} = (P^h)^g$.

Orbit under G of this action is S. Size of the orbit is $\text{ord}(S)$. The stabilizer of P is $\{g \in G : P^g = P\} = \{g \in G : gPg^{-1} = P\} = N_G(P) \leqslant G$. Then the Orbit-Stabilizer $\text{ord}(S) = [G : N_G(P)]$. Since $\text{ord}(G) = [G : N_G(P)]\,\text{ord}(N_G(P))$. Then $|N_G(P) = [N_G(P) : P]\,\text{ord}(p) = p^n$. So $p \nmid \text{ord}(S)$.

Goal. Let Q be any Sylow-p prove Q is one of these P^g i.e. $Q \in S$.

What are the sizes of orbits? If $T = P^h \in S$, $(h \in G)$. Then $\text{ord}(T) = \text{ord}(P) = p^n$. Then $P^h = \text{ord}(hPh^{-1}) = \text{ord}(P)$. THen the size of orbit under action of Q, $\text{ord}(Q) = p^n$. $[Q :_Q (T)]$,$_Q(T)$ = the stabilizer in Q of T under this action.

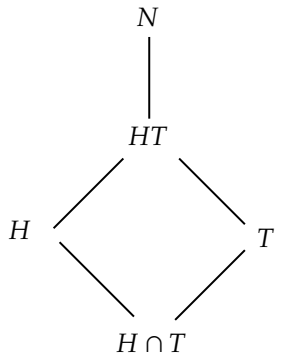
Each orbit must then have size p^k for some k since $p \nmid \text{ord}(S)$ not all $k \geqslant 1$. Atleast one $k = 0$.

Goal. $k = 0$ if and only if $Q = T$.

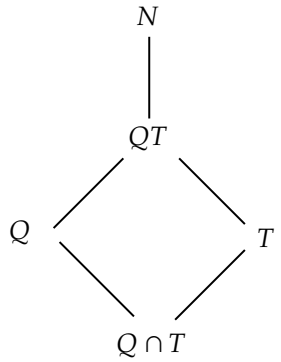
Lemma 10.3.1

If Q, T are both Sylow-p's , then $_Q(T) = Q$ if and only if $T = Q$.

Proof of Lemma: $_Q(T) = \{g \in G : T^g = T\} = Q \bigcap N_G(T) = N$. Let $T \trianglelefteq N$.



Note that $p \nmid \{H, H \cap T\}$ thus $p \nmid \text{ord}(HT/T)$



Then $Q \cap T = Q$. Hence $Q = T$. ■

Theorem 10.3.5

Suppose $\text{ord}(G) = 2q$ and q odd prime and G not abelian, then $G \cong (H \leqslant S_q)$ = q-cycle and an element of order two.

Proof of Theorem: Given $\text{ord}(G) = 2q$, G has a sylow-2, say $\langle x \rangle$ with $\text{ord}(x) = 2$. The number of Sylow-2 groups which is not 1 divides $\frac{\text{ord}(G)}{2} = q$. So there are q Sylow-2 groups. Say $P_1 = \langle x_1 \rangle, P_2 = \langle x_2 \rangle, \ldots, P_q = \langle x_q \rangle$ with x_i distinct elements of order 2. We define $\phi : G \to$ Permutations of $\{x_1, \ldots, x_q\} \cong S_q$, defined by $g \mapsto \phi_g$ such that $\phi_g(x_i) = x_i^g = gx_ig^{-1}$. The kernel of ϕ is trivial, which implies ϕ is an isomorphism. So there exists an isomorphism $G \to$ the subgroup of S_q with order of $2q$. ■

Example 10.3.4

Let $g \in G, \text{ord}(g) = q$. Let $x_1 = x, x_2 = x_1^g, x_3 = x_2^g, \ldots, x_q = x_{q-1}^g, x_1 = x_q^g$. g is mapped to the q-cycle, which x is mapped to elements of order 2. Thus it is isomorphic to the dihedral group.

Example 10.3.5 (Why is the kernel trivial? Claim: $K = \ker \phi = \{1\}$.)

$\text{ord}(K) \neq 2q$ nor is $\text{ord}(K) \neq q$ or $\text{ord}(K) \neq 2$. If $y \in K, \text{ord}(y) = 2$. Thus $yx_i = x_i y$ for all x_i in $\mathbb{Z}_2 \times \mathbb{Z}_2$. This creates a subgroup of order 4. There cannot exist order 4 since $4 + 2q$. So there is no $y \in K$ with $\text{ord}(y) = 2$. Hence $\text{ord}(K) \neq 2$.

10.4 Exercises

Example 10.4.1 (Exercise 1)

Let K be a subgroup of $\mathbb{Z} \oplus \mathbb{Z}$. Let $H = \{b \in \mathbb{Z} \mid \exists y \in \mathbb{Z}, (y, b) \in K\}$. Prove that H is a subgroup of $\mathbb{Z}$.

Example 10.4.2 (Exercise 2)

Let G be an abelian group and T the set of elements of finite order in G. Prove that
(a) T is a subgroup of G (called the torsion subgroup).
(b) Every nonzero element of the quotient group G/T has infinite order,

Example 10.4.3 (Exercise 3)

How many isomorphism types are there of abelian groups of order 32? Write down a representative for one of each isomorphism type.

Example 10.4.4 (Exercise 4)

Find the invariant factors of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Example 10.4.5 (Exercise 5)

Let $G = A_5$.
(a) Find a representative for each conjugacy class in G.
(b) How many elements are there in the various conjugacy classes?
(c) What is the size of the centralizer of each of your elements in (a).
(d) What is the class equation for G?

Example 10.4.6 (Exercise 6)

Let K be a Sylow p-subgroup of G and N a normal subgroup of G. If K is a normal subgroup of N, prove that K is normal in G.

Example 10.4.7 (Exercise 7)

Let N be a normal subgroup of $G, a \in G$, and C the conjugacy class of a in G.
(a) Prove that $a \in N$ if and only if $C \subseteq N$.
(b) If C_i is any conjugacy class in G, prove that $C_i \subseteq N$ or $C_i \cap N = \emptyset$.
(c) Use the class equation to show that $|N| = |C_1| + \cdots + | C_k |$, where $C_1, \ldots, C_k$ are all the conjugacy classes of G that are contained in N.

Example 10.4.8 (Exercise 8)

If $N \neq \langle e \rangle$ is a normal subgroup of G and $|G| = p^n$, prove that $N \cap Z(G) \neq \langle e \rangle$. [Hint: Exercise 7(c) may be helpful.]

Example 10.4.9 (Exercise 9)

If K is a Sylow p-subgroup of G, prove that $N(N(K)) = N(K)$.

Example 10.4.10 (Exercise 10)

If $|G| = p^n$, prove that G has a normal subgroup of order p^{n-1}. [Hint: You may assume Theorem 9.27 below. Use induction on n. Let $N = \langle a \rangle$, where $a \in Z(G)$ has order p (Why is there such an a ?); then G/N has a subgroup of order p^{n-2}; use Theorem 8.24.]

Example 10.4.11 (Exercise 11)

Prove that there are no simple groups of order 30.

Example 10.4.12 (Exercise 12)

Let K be a Sylow p-subgroup of G and N a normal subgroup of G. Prove that $K \cap N$ is a Sylow p-subgroup of N.

Chapter 11

Galois Theory

11.1 Field Extensions

Refer to Chapter 7.2 for all of the theory on Field Extensions. We will be continuing this on behalf of learning Galois Theory.

Definition 11.1.1

Given $u \in \mathbb{E} \supseteq \mathbb{F}$, $\mathbb{F}(u)$ is the intersection of all subfields of $\mathbb{E}$ containing u.

$$\mathbb{F}(u) = \bigcap_{u \in \mathbb{E}\mathbb{E}_i \subseteq \mathbb{E}}$$

is a field containing u, which is the smallest field extension of $\mathbb{F}$ containing u. I.e. If $\mathbb{K}$ is afield, then $\mathbb{F} \subset \mathbb{K}$, $u \in \mathbb{K}$, then $\mathbb{F}(u) \subseteq \mathbb{K}$

Thus if u is algebraic over $\mathbb{F}$, then $\mathbb{F}[u]$ is a field extension of $\mathbb{F}, u \in \mathbb{F}[u]$. Hence $\mathbb{F}(u) \subseteq \mathbb{F}[u]$ Let $f(u) \in \mathbb{F}[u]$, then $f(x) \in \mathbb{F}[x]$. Then it is always true $f(u) \in \mathbb{F}(u)$, which has to contain every polynomial in u. Thus $\mathbb{F}[u] \subseteq \mathbb{F}(u)$.

Let $f(x) \in \mathbb{F}[x]$. If $p(x)$ is an irreducible factor of $f(x)$, then $\frac{\mathbb{F}[x]}{p(x)}$ is a field containing $\mathbb{F}$ (really a copy consisting of classes of constant polynomials). Which has a root of $f(x)$ namely α is equal to the class of x. Ex. $f(x) = x^2 - 2$ in $\mathbb{Q}[x]$, then $\mathbb{Q}[\sqrt{2}] \cong \frac{\mathbb{Q}[x]}{(x^2-2)}$. Thus $\sqrt{2}$ cooresponds to the class of x. Map $\mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ defined by $f(x) \mapsto f(\sqrt{2})$, thus $x \mapsto \sqrt{2}$.

Then $p(\alpha)$ is equal to the class of $p(x)$, but since we mod'd out by $p(x)$, that is equal to $0 \in \frac{\mathbb{F}[x]}{(p(x))}$.

Theorem 11.1.1

Let $f(x) \in \mathbb{F}_1$ where $f(x)$ is irreducible factor of $p(x)$. And $\mathbb{K}_1 = \frac{\mathbb{F}_1[x]}{p(x)}$ is a field extension of $\mathbb{F}_1$ such that $f(x)$ hsa a root of $\alpha \in \mathbb{K}_1$. Where α is the class of $x \in \mathbb{K}_1$.
Suppose $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ is a field isomorphism, then $\sigma f(x) \in \mathbb{F}_2[x]$. If $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ where $a_i \in \mathbb{F}_1$, then $\sigma f(x) = \sigma(a_0) + \ldots + \sigma(a_n)x^n \in \mathbb{F}_2[x]$. Which is irreducible $p(x) \in \mathbb{F}_1[x] \to \sigma p(x)$ is irreducible in $\mathbb{F}_2[x]$. Let $u \in \mathbb{E}_1$, and u is a root of $p(x) \in \mathbb{E}_1$. Suppose v is a root of $\sigma p(x) \in \mathbb{F}_2[x]$, then there exists $\bar{\sigma} : \mathbb{F}_1(u) \to \mathbb{F}_2(v)$ is an extension of $\sigma(\bar{\sigma} \mid_{\mathbb{F}_1} = \sigma)$ such that $\sigma(u) = v$.

Proof of Theorem: $\mathbb{F}_1(u) \cong \frac{\mathbb{F}_1[x]}{p(x)} \cong \frac{\mathbb{F}}{\sigma p(x)} \cong \mathbb{F}_2(v)$ defined by $u \mapsto$ class of x in $\mathbb{F}_1 \longleftrightarrow$ class of x in $\mathbb{F}_2 \longleftrightarrow v$ Then $\sigma(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_2}$. ∎

Corollary 11.1.1

The number of such extensions is the number of distinct roots of $\sigma p(x)$ in $\mathbb{E}_2$.

Definition 11.1.2: Splitting Field

A splitting field for $f(x) \in \mathbb{F}[x]$ is an extension field $\mathbb{E}$ of $\mathbb{F}$ such that $\mathbb{E}[x]\ f(x) = c(x-a_1)\dots(x-a_n), a_i \in \mathbb{E}$ factors and $E = F(a_1, \dots, a_n)$.

Theorem 11.1.2

There exists a splitting field for $f(x) \in \mathbb{F}[x]$.

Sketch of Proof: By Induction we will prove this. We know there is a proof of induction on $\deg(f) = n$ and there exists a class of an extension field of $\mathbb{E}_1$, where $n = 1$ then f is linear. If it is an extension field of $\mathbb{F}$ such that $f(x)$ has a root $u \in \mathbb{E}_1$ ($\mathbb{E}_1 = \frac{\mathbb{F}[x]}{p(x)}, p(x)$ irreducible factor of $f(x)$) in $\mathbb{E}_1[x]$, $f(x) = (x-u)g(x)$, $\deg(g(x)) < \deg(f(x))$. By induction hypothesis, there is a splitting field for $g(x)$ over $\mathbb{E}$. ■

Theorem 11.1.3

Any 2 splitting fields for $f(x)$ are isomorphic.

Proof of Theorem 11.1.2: Suppose $\mathbb{F}_1 \overset{\sigma}{\tilde{\to}} \mathbb{F}_2$, where $\sigma : \mathbb{F}_1 \to \mathbb{F}_2$ is also an isomorphism. If $f(x) \in \mathbb{F}[x]$, then $\mathbb{E}_1$ is a splitting field for $f(x)$ over $\mathbb{F}$ and $\sigma f(x) \in \mathbb{F}_2[x]$ over $\mathbb{F}_2$. $\mathbb{E}_2$ is a splitting field for $\frac{\sigma f(x)}{\mathbb{F}_2}$. Then σ can be extended to an isomorphism such that $\bar{\sigma} : \mathbb{E}_1 \to \mathbb{E}_2$. If $\mathbb{F}_1 = \mathbb{F}_2$, then $\sigma = e$ and $\mathbb{E}_1 \cong \mathbb{E}_2$, thus splitting fields are unique up to isomorphism. If $f(x)$ has a distinct root in $\mathbb{E}_1$, then the number of such extensions is $[\mathbb{E}_1 : \mathbb{F}_1]$.

Assume $[\mathbb{E}_1 : \mathbb{F}_1] > 1$. Let $p(x) \in \mathbb{F}[x]$ be an irreducible factor $f(x)$. Then $p(x)$ has a root r in an extension field of $\mathbb{F}$. If v is any root of $\sigma p(x) \in F_2[x]$ Then there exists an extension of σ such that $\sigma_1 : F_1(r) \tilde{\to} F_2(v)$. Then the number of such $\mathbb{F}_1(r) \to \mathbb{E}_2$ is $\deg(p(x))$ under assumption that all roots of $p(x)$ are distinct. Note that $\deg(p(x)) = [\mathbb{F}_1(r) : \mathbb{F}_1]$.

Base Case: $[\mathbb{E}_1 : \mathbb{F}_1] = 1$, thus $f(x)$ is the product of linear polynomials. Since $[\mathbb{E}_1 : \mathbb{F}_1(r)]$ are extensions of σ, then the number of extensions of σ to an isomorphism $\mathbb{E}_1 \to \mathbb{E}_2$ is $[\mathbb{E}_1 : \mathbb{F}_1(r)][\mathbb{F}_1(r) : \mathbb{F}_1] = [\mathbb{E}_1 : \mathbb{F}_1] = [\mathbb{E}_2 : \mathbb{F}_2]$. Suppose that $\bar{\sigma} : \mathbb{E}_1 \to \mathbb{E}_2$ is an extension of σ, then if $f(x_i) = 0$, then $\sigma f(x_i) = 0$. ■

11.2 Galois Theory

Define a homomorphism $\phi : \mathbb{Z} \to \mathbb{F}$ where $1 \mapsto 1$ and $n \mapsto n1$ and $n + m \mapsto n1 + m1$ and $nm \mapsto n1m1$ and $\mathrm{Im}\phi$ is a subring of $\mathbb{F}$ where the $\frac{Z}{\ker\phi} \cong \mathrm{Im}\phi$ where $\ker\phi$ is an ideal of $\mathbb{Z}$ if the $\ker\phi = \{0\}$ then then there is subring isomorphic to $\mathbb{Z}$ where Φ is a isomorphism, so a subfield isomorphic to $\mathbb{Q}$.

If $char(\mathbb{F}) = p$ then $\mathbb{F}$ has a subfield isomorphic to $\mathbb{Z}_p = \frac{Z}{p\mathbb{Z}}$ We say that $\mathbb{F}$ has characterisitc 0 fi it hsa a kerphi = n in nZZ, then $\mathbb{F}$ has a subring isomorphic to $Z_{n=\frac{\mathbb{Z}}{n\mathbb{Z}}}$ since $\mathbb{F}$ is a field n must be prime p say $\mathbb{F}$ has characterisitc p.

Definition 11.2.1: Formal Derivative

In $f(x) \in \mathbb{F}[x]$, $f'(x) = Df(x)$ if $f(x) = x^n$ then $Df(x) = nx^{n-1}$ and extend to $\mathbb{F}[x]$ by linearity.

Alternatively in $\mathbb{F}[x, h]$ where h is trancendental where $g(x, h) = f(x + h) - f(x)$ where $g(x, 0) = 0$.
By the factor therem h is a factor of $g(x, h)$.

Definition 11.2.2

$Df(x) = \frac{g(x,h)}{h}$ evaluated at $h = 0$.

Definition 11.2.3: Repeated Root

If we have $f(x) \in \mathbb{F}[x]$ and E is a splitting field for $f(x)$, we say a is a repeated root of $f(x)$, if $f(x) = (x-a)^2 g(x)$ in $\mathbb{E}[x]$.
If $Df(x)$ has repeated root then $f(a) = 0$, so a is also a root of $Df(x)$.

Given $f(x) \in \mathbb{F}[x]$ is irreducible and $\mathbb{F}$ is an extension field of $\mathbb{Q}$, then $\mathbb{E}$ is a splitting field.
If $u \in \mathbb{E}$, then $f(u) = 0$, then u is not a repeated root for $f(x)$
If $u \in \mathbb{E}$, then $f(u) = 0$, then u is not a repeated root for $f(x)$. ie. $f(x) = (x-u)^2 g(x) \in \mathbb{F}[x]$ (not possible)
If u is a repeated root, then

$$(Df)(u) = 0$$

So $(x-u)$ is a factor of $Df(x)$. Also $f(x)$ is minimal polynomial of U over $\mathbb{F}$ $\deg(Df(x)) < \deg(f(x))$ If $Df(u) = 0 \implies f(x)$ such that $(Df(x)) \implies Df(x) = 0$
Assume $\mathbb{E}$ is a finite dimensional extension of $\mathbb{Q}$ (char. 0) Let $\mathbb{F}$ be a subfield of $\mathbb{E}$.

Definition 11.2.4: Normal Extension

$\mathbb{F}$ is a normal extension of $\mathbb{F}$ if $u \in \mathbb{E}, f(x) \in \mathbb{F}[x]$ is the minimal poly. of $u/\mathbb{F} \in \mathbb{F}[x]$, then $f(x)$ splits in $E[x]$.

Any $f(x) \in \mathbb{F}[x]$ which has a root in $\mathbb{E}$ has all its roots in $\mathbb{E}$.

Example 11.2.1

If $\mathbb{E}$ is a splitting field for $f(x) \in \mathbb{F}[x]$, then it is normal $/\mathbb{F}$:
Given $p = e^{\frac{2i\pi}{3}}$
$\mathbb{Q}\left[2^{\frac{1}{3}}, 2^{\frac{1}{3}} e^{\frac{n\pi}{3}}\right] = \mathbb{Q}\left[2^{1/3}, p\right]$ = splitting field for $x^3 - 2/Q$ is normal over $\mathbb{Q}$. But $\mathbb{Q}\left[2^{1/3}\right]$ is not normal / Q.

Definition 11.2.5: Automorphism

$\mathrm{Aut}(\mathbb{E})$ = group of field automorphisms of $\mathbb{E}$.

Definition 11.2.6: Galois Group

$\mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) := \{\sigma \in \mathrm{Aut}(E) : \sigma(a) = a, \forall a \in \mathbb{F}\} = \mathrm{Gal}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$.

Definition 11.2.7: Fixed Field

Let $G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$. The fixed field of G is $\{u \in \mathbb{E} : \sigma(u) = u, \forall \sigma \in G\} = \mathrm{Inv}(G)$

Note that $\mathbb{F} \subseteq \mathrm{Inv}(G)$, but it is not necessarily $\mathrm{Inv}(G) \subseteq \mathbb{F}$.

Example 11.2.2

$\mathbb{F} = \mathbb{Q}$, $\mathbb{E} = \mathbb{Q}(2^{\frac{1}{3}})$, and $G = \mathrm{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) = e$ such that $2^{\frac{1}{3}} = 2^{\frac{1}{3}}$.

Theorem 11.2.1 Fundamental Theorem of Galois

Given $\frac{\mathbb{E}}{\mathbb{F}}$ has *char* 0 and finite-dimensional, then we will prove that all the following is equivalent.

1. $\mathrm{Inv}\left(aut\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = F$;
2. $\mathbb{F} = \mathrm{Inv}(G)$ for some $G \leqslant aut(\mathbb{E})$;
3. $\mathbb{E}$ is normal to any separable over $\mathbb{F}$;

4. $\mathbb{E}$ is a splitting field of a separable polynomial in $\mathbb{F}[x]$;

5. $\text{ord}\left(aut\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = [\mathbb{E} : \mathbb{F}]$

Proof of FTGT: . We have already shown that **(4)** $\implies$ **(5)**. **(1)** $\implies$ **(2)** is obvious since $\mathbb{F} = \text{Inv}(G)$. Suppose **(3)** $\implies$ **(4)**, then $\frac{\mathbb{E}}{\mathbb{F}}$ is finite dimensional thus $\mathbb{E} = \mathbb{F}[u_1, \ldots, u_n]$. Let $p_i(x) \in \mathbb{F}[x]$ be the minimal polynomial of $u_i/\mathbb{F}$. Let $f(x)$ be the product of distinct $p_i(x)$. Then $\mathbb{E}$ is the splitting field for $f(x) \in \mathbb{F}[x]$.

(**(2)** $\implies$ **(3)**).Assume that $\mathbb{F} = \text{Inv}(G)$ for some $G \leqslant \text{Aut}(E)$, where $\text{ord}(G) < \infty$. Suppose $\mathbb{E}$ is a field, G is a finite subgroup of $\text{Aut}(\mathbb{E})$. Let $\mathbb{F} = \text{Inv}(G) \subseteq \mathbb{E}$. If $u \in \mathbb{E}$ and $f(x)$ is the minimal polynomial of u over $\mathbb{F}$, then $f(x)$ splits $\mathbb{E}[x]$.

Let $u \in \mathbb{E}$. $\frac{\mathbb{E}}{\mathbb{F}}$ is finite, so it is algebraic over $\mathbb{F}$. Let $f(x)$ be a minimal polynomial of u and $\text{ord}(G) < n$. Consider the orbit under G of u which is equal to the set of distinct $\sigma_i u$, where $\sigma_i \in G$, and $\{u = u_1, \ldots, u_m\}$. Let $g(x) = (x - u_1)\ldots(x - u_m) \in \mathbb{E}[x]$. Let $u_1 = u$. We claim that $g(x) \in \mathbb{F}[x]$:

Claim. Let $\sigma_i \in G$, then $(\sigma_i g)(x) = g(x)$, so σ_i fixes all coefficients of $g(x)$ expanded for all i. So each coefficient is in $\text{Inv}(G) = \mathbb{F}$, so $g(x) \in \mathbb{F}[x]$. Then $g(0) = 0$ implies $g(x) = f(x)$. So $\frac{\mathbb{E}}{\mathbb{F}}$ is normal. Thus $g(x) \mid f(x)$ in $\mathbb{E}[x]$ ■

Lemma 11.2.1

Let $\mathbb{E}$ be an extension field of $\mathbb{F}$, and let $G = \text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$ and let $\mathbb{K} = \text{Inv}(G)$, then $\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right) = \text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right) = G$.

Continued Proof of FTGT: . (**(5)** $\implies$ **(1)**). Now, suppose **(5)**, i.e. $\text{ord}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = [\mathbb{E} : \mathbb{F}]$. We need to show that $\text{Inv}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right) = \mathbb{F}$. Pf. Let $\mathbb{K} = \text{Inv}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right)$. By lemma, $\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right) = \text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)$, so $\text{ord}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = \text{ord}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{F}}\right)\right)$. Apply **(2)** $\mathbb{F} = \text{Inv}(G)$ for some $G \leqslant \text{Aut}(E)$ where $\text{ord}(G) < \infty$ implies **(3)** implies **(4)** implies **(5)**, with $\mathbb{K}$ in place of $\mathbb{F}$. We get that $\text{ord}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = [\mathbb{E} : \mathbb{K}]$. Thus $\text{ord}\left(\text{Aut}\left(\frac{\mathbb{E}}{\mathbb{K}}\right)\right) = [\mathbb{E} : \mathbb{K}]$. Hence $\mathbb{F} = \mathbb{K} = \text{Inv}(G)$. ■

Definition 11.2.8: Galois

$\frac{\mathbb{E}}{\mathbb{F}}$ is Galois any of these conditions above hold.

Theorem 11.2.2

Given $G \leqslant \text{Aut}(\mathbb{E})$ and $\mathbb{K} \subset \mathbb{E}$, then we have $[\mathbb{E} : \mathbb{K}] \leqslant \text{ord}(G) < \infty$.

Proof of Theorem: linearly dependent over $\mathbb{K}$. Write $G = \{1, \sqrt{2}, \sqrt{3}, \ldots, \sqrt{n}\}$ and let $1 = \sigma$. Define an $n \times m$ matrix A such that $A_{ij} = \sigma_j(u_i) \in \mathbb{E}$.

$$A = \begin{bmatrix} u_1 & u_2 & \cdots & & u_m \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2 & (u_m) \\ \vdots & & & & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_m) & \end{bmatrix}_{n \times m}$$

What do we know about A? Each $\sigma_j(u_i) \in \mathbb{E}$, but $\sigma_j(u_i)$ does not necessarily equal u_i. Why? $u_i \in \mathbb{E}$, not necessarily an element of $\mathbb{K}$. Then $\sigma(u_i) = u_i, \forall \sigma \in G$ iff $u_i \in \mathbb{K}$. This matrix is rectagular since $m > n$. The systems of equations $A\vec{x} = \vec{0}$ is underdetermined meaning there are more variables than equations. So we have many (possibly infinite) non-trivial solutions.

Pick a random non-trivial solution with a minimal number of non-zero elements. We can always assume the solution has the form

$$\vec{b} = \begin{bmatrix} 1 \\ \vdots \end{bmatrix}$$

Why can we assume this? We can scale the solution by a constant. We can also permute the variables of A and still get a solutions. Thus we can permute such that x_1 is non-zero.

Let $A\vec{b} = \vec{0}$. We claim: $\vec{b} \in \mathbb{K}^m$. In a proof by contradiction, suppose

$$\vec{b} = \begin{bmatrix} 1 \\ b_2 \\ \vdots \\ \end{bmatrix}$$

We do we want to show this? If all elements of $\vec{b} \in \mathbb{K}$, then we have an linear combination over $\mathbb{K}$ with constants b_i equalling 0. But at least one $b_i \neq 0$. So the set $\{u_1, u_2, \ldots, u_m\}$ is not linearly independent over $\mathbb{K}$

Then there exists a $\sigma_\ell \in G$ such that $\sigma_\ell(b_2) \neq b_2$. Define $\sigma_\ell(A)$ to be the matrix where $\sigma_\ell(A)_{ij} = \sigma_\ell(\sigma_j(u_i))$ and it will apply σ_ℓ to all elements of A. This will just permute the rows of A. Why? Because $\sigma_\ell \circ \sigma_j = \sigma_\omega$ for some $\sigma_\omega \in G$ because G is a group.

Thus $\sigma_\ell(A)\vec{x} = \vec{0}$ has the same solution as $A\vec{x} = \vec{0}$. Thus $\sigma_\ell(\vec{b})$ is also in the solution set because $\sigma_\ell(A)\sigma_\ell(\vec{b}) = \sigma_\ell(A\vec{b}) = \sigma_\ell(0) = 0$. If $\vec{b}$ and $\sigma_\ell(\vec{b})$ are in the solution set, then $\vec{b} - \sigma_\ell(\vec{b})$ is also in the solution set.

$$\begin{bmatrix} 1 \\ b_2 \\ \vdots \\ \end{bmatrix} - \begin{bmatrix} 1 \\ \sigma_\ell(b_2) \\ \vdots \\ \end{bmatrix} = \begin{bmatrix} 0 \\ \text{not } 0 \end{bmatrix}$$

Hence a contradiction with $\vec{b}$ has fewest non-zero elements. So $\vec{b} \in \mathbb{K}^m$. ∎

Another Proof of FTGT: . Suppose $\mathbb{E}/\mathbb{F}$ is galois, so one of the conditions are true, then $G = \text{Aut}(\mathbb{E}/\mathbb{F}) = \text{Gal}(\mathbb{E}/\mathbb{F})$ is the galois group. Then $\mathbb{E}/\mathbb{K}$ is galois for any intermediate field $\mathbb{K}$. Let $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$. Then there is a bijection between the intermediate fields $\mathbb{K}$ and subgroups $H \leqslant G$. These maps are order reversing under inclusion, i.e. $\mathbb{K}_1 \leqslant \mathbb{K}_2 \implies \text{Aut}(\mathbb{E}/\mathbb{K}_1) \supseteq \text{Aut}(\mathbb{E}/\mathbb{K}_2)$ and if $H_1 \subseteq H_2 \implies \text{Inv}(H_1) \supseteq \text{Inv}(H_2)$.

Let $K \to \text{Aut}(\mathbb{E}/\mathbb{F})$ and $\text{Inv}(H) \leftarrow H$. Let $\mathbb{K} := \{u \in H : \sigma(u) = u, \forall \sigma \in H\}$ where σ are the automorphisms. These maps are inverses to each other i.e. $\text{Inv}(\text{Aut}(\mathbb{E}/\mathbb{F})) = \mathbb{K}$ and $\text{Aut}(\mathbb{E}/\text{Inv}(H)) = H$.

If $\mathbb{K} \to \text{Aut}(\mathbb{E}/\mathbb{F})$ and $G \leqslant \text{Aut}(\mathbb{E}/\mathbb{F})$ and $\mathbb{K}$ is the set of intermediate fields. Then $H \to \text{Inv}(H)$ where $\text{Inv}(H)$ is the fixed field of H and H is the set of subgroups of $G \leqslant \text{Aut}(\mathbb{E}/\mathbb{F})$. We have a bijection between groups and fields.

Then $\mathbb{K}$ is galois over $\mathbb{F}$ if and only if $\sigma(K) = K, \forall \sigma \in G$, if and only if $H = \text{Inv}(K) \trianglelefteq G$. In this case $[\mathbb{K} : \mathbb{F}] = \text{ord}(G/H)$. ∎

Example 11.2.3 (Galois Groups Fork)

When is $\mathbb{K}$ galois over $\mathbb{F}$? Let $\mathbb{F} = \mathbb{Q}$ adn $\mathbb{E} = \mathbb{Q}\left(2^{\frac{1}{3}}, \exp\left(\frac{2\pi i}{3}\right) = \omega\right)$. $\mathbb{E}$ is galois because it meats condition (**2**). Which means it is splitting field for $f(x) = x^3 - 2$ over $\mathbb{Q}$. What is $[\mathbb{K} : \mathbb{F}]$? $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

$$\mathbb{E} \underset{\mathbb{E}=\text{Inv}(1)}{\overset{\text{Aut}(\mathbb{E}/\mathbb{E})}{\longleftrightarrow}} 1$$

$$\mathbb{K} \underset{\mathbb{K}=\text{Inv}(H)}{\overset{\text{Aut}(\mathbb{E}/\mathbb{K})}{\longleftrightarrow}} H$$

$$\mathbb{F} \underset{\mathbb{F}=\text{Inv}(G)}{\overset{\text{Aut}(\mathbb{E}/\mathbb{F})}{\longleftrightarrow}} G$$

What does these mean? When $\mathbb{E}/\mathbb{F}$ is galois, then all these maps have it where starting from $\mathbb{K} \subset \mathbb{F}$, when we apply both ways. We always end up at $\mathbb{K}$ again!
Now what we have to do is show that $H \leqslant G$ by applying both maps resulting in H again! Once we prove this, we know the maps are inverses.

Continued Another Proof of FTGT: . Given $\mathbb{E}/\mathbb{F}$ is galois and $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$. By (**4**), $\mathbb{E}$ is a splitting field for $f(x) \in \mathbb{F}[x]$ because $\mathbb{E}/\mathbb{F}$ is galois. Since $\mathbb{F} \subset \mathbb{K}$, then $f(x) \in \mathbb{K}[x]$ as well. So $\mathbb{E}$ is a splitting field for $f(x) \in \mathbb{K}[x]$ as well. Thus $\mathbb{E}/\mathbb{K}$ is also galois.

Let $H \leqslant \text{Aut}(E), \text{ord}(H) \leqslant \infty$, then $\mathbb{K} = \text{Inv}(H)$. By Artin's Lemma, $[\mathbb{E} : \mathbb{K}] \leqslant \text{ord}(H)$ and $H \leqslant \text{Aut}(\mathbb{E})$ and $K = \text{Inv}(H)$ implying $H \leqslant \text{Aut}(\mathbb{E}/\mathbb{K})$. So $\text{ord}(H) \leqslant \text{ord}(\text{Aut}(\mathbb{E}/\mathbb{K}))$. Thus $\mathbb{E}/\mathbb{K}$ is galois, thus by (**5**), then $\text{ord}(\text{Aut}(\mathbb{E}/\mathbb{K})) = [\mathbb{E} : \mathbb{K}]$, so $[\mathbb{E} : \mathbb{K}] \leqslant \text{ord}(H) \leqslant [\mathbb{E} : \mathbb{K}]$. So $\text{ord}(H) = [\mathbb{E} : \mathbb{K}] = \text{ord}(\text{Aut}(\mathbb{E}/\mathbb{K}))$. Thus $\text{ord}(H) = \text{ord}(\text{Aut}(\mathbb{E}/\mathbb{K}))$ and $H \leqslant \text{Aut}(\mathbb{E}/\mathbb{K})$ implying $H = \text{Aut}(\mathbb{E}/\mathbb{K})$. Thus $\mathbb{K}$ and H are inverse maps. ■

Example 11.2.4 (Application of Theorems)

Suppose $\mathbb{K}$ is galois over $\mathbb{F}$ if and only if $\sigma(\mathbb{K}) = \mathbb{K}$ for all $\sigma \in G$ if and only if $H = \text{Inv}(\mathbb{K})$ is normal. Then the splitting field of $x^3 - 2$ over $\mathbb{Q}$ results in three cosets generated by $2^{\frac{1}{3}}$ and ω. Thus $\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ is our splitting field. Look at the fields and automorphisms that fix these fields

$$\begin{array}{cc} \mathbb{Q}\left(2^{\frac{1}{3}}, \omega\right) & 1 \\ |\cap & \cup| \\ \vdots & \vdots \\ |\cap & \cup| \\ \mathbb{Q} & G \end{array}$$

What is the degree of $\mathbb{Q}(2^{\frac{1}{3}}, \omega)$? We get $\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ from $x^3 - 2$ containing 3 roots. Automorphisms we know permute the roots, so the size could be up to $\text{ord}(S_3) = 6$, but may be smaller.

Let $\mathbb{F} = \mathbb{Q}(2^{\frac{1}{3}}, \omega)$, what are the isomorphisms in G? If $\sigma : \mathbb{F} \to \mathbb{F}$, then σ be conjugation. Thus $\sigma(z) = \bar{z}$. Then $\bar{z} + \bar{w} = z \mp w$, likewise for multiplication.

Let $\sigma(2^{\frac{1}{3}}) = 2^{\frac{1}{3}}$ because $2^{\frac{1}{3}} \in \mathbb{R}$. Then $\sigma(\omega) = \bar{\omega} = \omega^{-1} = \omega^2$. Then $\sigma^{2(\omega)} = \sigma(\bar{\omega}) = \bar{\bar{\omega}} = \omega$. So $\sigma^2 = 1_G$.

11.3 Exercises

Example 11.3.1 (Exercise 1)

Let $\mathbb{K}$ be a splitting field of $f(x)$ over $\mathbb{F}$. If $[\mathbb{K} : \mathbb{F}]$ is prime, $u \in \mathbb{K}$ is a root of $f(x)$, and $u \notin \mathbb{F}$, show that $\mathbb{K} = \mathbb{F}(u)$.

Example 11.3.2 (Exercise 2)

Find and describe a splitting field of $x^4 + 1$ over $\mathbb{Q}$.

Example 11.3.3 (Exercise 3)

Find a splitting field of $x^4 - 2$
(a) over $\mathbb{Q}$.
(b) over $\mathbb{R}$.

Example 11.3.4 (Exercise 4)

(a) If $f(x) = cx^n \in F[x]$ and $g(x) = b_0 + b_1x + \cdots + b_kx^k \in F[x]$, prove that $(fg)'(x) = f(x)g'(x) + f'(x)g(x)$.
(b) If $f(x), g(x)$ are any polynomials in $F[x]$, prove that $(fg)'(x) = f(x)g'(x) + f'(x)g(x)$. [Hint: If $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then $(fg)(x) = a_0g(x) + a_1xg(x) + \cdots + a_nx''g(x)$; use part (a) and Exercise 4.]

Example 11.3.5 (Exercise 5)

If $f(x) \in F[x]$ and n is a positive integer, prove that the derivative of $f(x)^n$ is $nf(x)^{n-1}f'(x)$. [Hint: Use induction on n and Exercise 5.]

Example 11.3.6 (Exercise 6)

Prove that $u \in K$ is a repeated root of $f(x) \in F[x]$ if and only if u is a root of both $f(x)$ and $f'(x)$. [Hint: $f(x) = (x-u)^m g(x)$ with $m \geqslant 1, g(x) \in K[x]$, and $g(u) \neq 0_F, u$ is a repeated root of $f(x)$ if and only if $m > 1$. Use Exercises 4 and 5 to compute $f'(x)$.]

Example 11.3.7 (Exercise 7)

Prove that $f(x) \in F[x]$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime.

Example 11.3.8 (Exercise 8)

Let $p(x)$ be irreducible in $F[x]$. Prove that $p(x)$ is separable if and only if $p'(x) \neq 0_F$.

Example 11.3.9 (Exercise 9)

Let E and F be fields. Assume that E is a Galois extension of F, so it satisfies each of the 5 conditions in Galois 1 . Let G = Aut(E/F) be the Galois group of E over F. Let H be any subgroup of G. Let K = Inv(H). The following problem asks you to give the details finishing the proof of The Fundamental Theorem of Galois Theory.

(a)Let $\tau \in G$. Prove that Inv $\left(\tau H \tau^{-1}\right) = \tau(K)$.

(b)Prove that H is normal in G if and only if for every $\tau \in G, \tau(K) = K$.

(c) Suppose that for every $\tau \in G, \tau(K) = K$. Let u be an element of K and let f(x) be its minimal polynomial. Prove that f(x) splits in K.

(d)Use parts (b) and (c) and Galois 1 to prove that if H is normal in G then K is Galois over F. State clearly which criterion in Galois 1 for being Galois you are using.

(e)Suppose that for each element u in K, the minimal polynomial of u splits in K. Prove that for every $\tau \in G, \tau(K) = K$.

(f)Use parts (b) and (e) and Galois 1 to prove that if K is Galois over F then H is normal in G. State clearly which criterion in Galois 1 for being Galois you are using.

(g) Let $\sigma \in Aut(E/F)$. Let $\sigma|_K$ denote the restriction of σ to K. In general $\sigma|_K$ is clearly a monomorphism (injective homomorphism) with domain K and codomain $\sigma(K)$. Prove that if K is Galois over F, then $\sigma|_K$ is in Aut(K/F).

(h) Suppose that K is Galois over F. Prove that the map $\sigma \to \sigma|_K$ is a homomorphism from the group Aut(E/F) to the group Aut(K/F).

(i) Suppose that K is Galois over F. Prove that the kernel of the homomorphism $\sigma \to \sigma|_K$ is Aut(E/K).

(j)Suppose that K is Galois over F. Use Theorem 11.14:

Let $\sigma : F \to E$ be an isomorphism of fields, $f(x)$ a nonconstant polynomial in $F[x]$, and $\sigma f(x)$ the corresponding polynomial in $E[x]$. If K is a splitting field of $f(x)$ over F and L is a splitting field of $\sigma f(x)$ over E, then σ extends to an isomorphism $K \cong L$.

to prove that the homomorphism $\sigma \to \sigma|_K$ from the group Aut(E/F) to the group Aut (K/F) is surjective. Show clearly how you are using Theorem 11.14.

(k)Suppose that K is Galois over F. Use the previous parts of this problem and the First Isomorphism Theorem to prove that Aut (K/F) is isomorphic to G/H.

Solutions to Exercises

Chapter 1

Proof of Exercise 1: We know that $0 + 0 = 0$. Given $a \in \mathbb{Z}$, then:

$$\begin{aligned}(0+0)a &= 0a\\ 0a + 0a &= 0a\\ 0a + 0a - 0a &= 0a - 0a\\ 0a + 0a - 0a &= 0a - 0a\\ 0a &= 0\end{aligned}$$

■

Chapter 2

Proof of Exercise 1: Let

$$a = qb + r \quad \text{and} \quad 0 \leqslant r < b.$$

If ac is divided by bc, then we could multiply all sides by c such that

$$ac = (qb)c + rc,$$

then rearrange to so associativity. Then

$$ac = q(bc) + rc,$$

thus showing that when ac is divided by bc, we have the remainder rc. ■

Proof of Exercise 2: Let

$$ac = qb + r \quad \text{and} \quad 0 \leqslant r < b.$$

Suppose q is divided by c results in the equation

$$q = kc + r_2.$$

Let this value of q replace q in the ac divided by b.

$$\begin{aligned}a &= (kc + r_2)b + r\\ &= kbc + br_2 + r.\end{aligned}$$

Claim. Since $r_2 < c$, then $r_2 < bc$, and since $r < b$, then we also have that $br_2 + r < bc$.
$br_2 \leqslant b(c-1)$, and $r \leqslant b - 1$, thus we have the equation $b(c-1) + b - 1 < bc$.

$$\begin{aligned}bc - b + b - 1 &< bc\\ bc - 1 &< bc.\end{aligned}$$

Thus we have shown that the remainders can never be greater than bc, our divider. Thus this satisfies the statement that when a is divided by bc, then the quotient is also k. ■

Proof of Exercise 3: ($\Longrightarrow$). Given that $a = nb + r$ and $c = nd + r$, as they have the same remainder, then let

$$a - c = nb + r - nd - r$$
$$a - c = n(b - d) + r - r.$$

Let there exist an integer $k = b - d$ such that $a - c = nk$. ($\Longleftarrow$). Suppose $a - c = nk$, then we can rewrite this in the form of the division algorithm such that

$$a = nk + c$$
$$c = nq + r.$$

Replace the values accordingly:

$$a = nk + nq + r$$
$$= n(k + q) + r.$$

Since r is the remainder for n dividing c, and as shown we also have it such that it is the remainder for a. Thus showing that it is the same remainder. ■

Proof of Exercise 4.: ($\Longrightarrow$). Given $a = bn$, then $a = (-b)(-n)$, which shows that $(-b)|a$.
($\Longleftarrow$). Given $a = (-b)n$, then $a = b(-n)$, thus $b|a$. ■

Proof of Exercise 5: Given $b = an$ and $c = bm$, then $c = anm$. Therefore $c = a(nm)$, thus $a|c$. ■

Proof of Exercise 6: Given $b = an$ and $c = am$, then $b + c = an + am$. Therefore $b + c = a(n + m)$, thus $a|(b + c)$. ■

Proof of Exercise 7: Given $b = an$ and $c = am$, then $br + ct = anr + amt$. Therefore $br + ct = a(nr + mt)$, thus $a|(br + ct)$. ■

Proof of Exercise 8: Let $b = am$ and $a = bn$. Then $a = amn$, when we substitute in b. Thus $mn = 1$, and since we are in the integers, the only divisors of 1 are $-1, 1$. Thus $a = \pm b$. ■

Proof of Exercise 9: Let $b = an$ and $d = cm$, then $bd = ancm$. Therefore $bd = (ac)(nm)$, thus $ac|bd$. ■

Proof of Exercise 10: Using the extended gcd algorithm:

$$0 = aq + r$$

Let $q = 1$ and $r = -a$.

$$0 = a(1) - a$$
$$a = a(1) + 0.$$

Then the gcd of $(a, 0)$ is a. ■

Proof of Exercise 11: Using the extended gcd algorithm, let

$$n + 1 = n(1) + 1.$$

Thus we have found that the gcd of $(n, n + 1)$ is 1. ■

Proof of Exercise 12: Given $c = am$ and $c = bn$, then a, b are two divisors of c. ■

Proof of Exercise 13: Given $n \in Z$,

$$n + 2 = n(1) + 2$$
$$n = 2q + r$$

Case 1: n is even.
Then 2 is the greatest common divisor of $(n, n + 2)$. This is due to 2 being able to evenly divide n.

Case 2: n is odd.

$$n = 2q + 1$$
$$2 = 1(2)$$

Then 1 is the greatest common divisor of $(n, n+2)$. This is due to 1 being able to continue the extended gcd algorithm and we find 1 can evenly divide 2.
Thus the only solutions are that $gcd(n, n+2) = 1$ or 2. ■

Proof of Exercise 14: By the linear combination of $gcd(a,b) = d$, we find that $ax + by = d$. Therefore

$$\frac{a}{d}x + \frac{b}{d}y = 1.$$

Thus $gcd(\frac{a}{d}, \frac{b}{d}) = 1$. ■

Proof of Exercise 15: Let $c = bn$, therefore $a|bn$, but since $gcd(a,b) = 1$, then $a|n$. Therefore $ab|bn$, thus $ab|c$. ■

Proof of Exercise 16: Let $ax + cy = 1$ and $bn + cm = 1$. Then

$$(ax + cy)(bn + cm) = 1 \cdot 1.$$
$$ab(xn) + c(byn + axm + cym) = 1$$

Thus the gcd of $(ab, c) = 1$. ■

Proof of Exercise 17: Suppose that $a|c$ and $b|c$ and the $gcd(a,b) = d$. If the greatest common divisor of a and b is d, then a and b can be written in terms of d and some integer $x, y \in \mathbb{Z}$, and also c in terms of $m, n \in \mathbb{Z}$ with a and b, such that

$$\begin{aligned} d|a &\iff a = dx \\ d|b &\iff b = dy \\ a|c &\iff c = am \\ b|c &\iff c = bn. \end{aligned}$$

Therefore, given $t \in \mathbb{Z}$ when we have the equivalence of $ab|cd$, we can substitute values into a and b to show divisibility. Hence

$$\begin{aligned} ab|cd &\iff cd = abt \\ &\iff cd = (dx)bt \\ &\iff cd = a(dy)t \end{aligned}$$

It can also be done the other way by replacing c with some value with a or b:

$$\begin{aligned} ab|cd &\iff cd = abt \\ &\iff (am)d = abt \\ &\iff (bn)d = abt. \end{aligned}$$

Also note that since a and b also divide c, since the multiplication of c and d result in some multiple of each other, a and b can also divide any multiple of c, regardless of the statement that $d|a$ and $d|b$. ■

Proof of Exercise 18: Suppose $a > 0$ and $b > 0$. Then $ab > 0$, therefore ab is some common multiple of a and b, but nothing to show that it is the least common multiple of ab. Suppose there exists $m, x, y \in \mathbb{Z}$, then $m|a$ and $m|b$, such that $m|ab$. Thus

$$\begin{aligned} m|a &\iff a = mx \\ m|b &\iff b = my \\ m|ab &\iff ab = (mx)(my) \end{aligned}$$

So there is a common divisor of a and b, which is m. Now suppose that there exists a d such that $d|a$, $d|b$, and $d|m$, but $d \leqslant m$. Because of this, given some $t \in \mathbb{Z}$,

$$d|m \iff m = dt$$

Thus,

$$gcd(a,b) = m = dt.$$

Now that we have an integer representation of the $gcd(a,b)$, then let us rearrange the problem to satisfy this new standing:

$$\begin{aligned} lcm[a,b] &= \frac{ab}{gcd(a,b)} \\ lcm[a,b] &= \frac{(mx)(my)}{m} \\ lcm[a,b] &= \frac{(dtx)(dty)}{dt} \\ lcm[a,b] &= dtxy \\ lcm[a,b] &= mxy \\ &\iff (mx)y \\ &\iff x(my). \end{aligned}$$

Given some value for ab and the $gcd(a,b)$, if we are to divide such numbers, then we would get the least representation of such numbers such that, they are the least common multiple of a and b. If we are to take the divisors of a and b, which are: m and x, or m and y. Then the least common divisor is equal to the product of m, x, and y as they make up a and b. This is because it can be rearranged into some multiple of a or b, as shown, $lcm[a,b] = mxy$. Hence $lcm[a,b] = \frac{ab}{gcd(a,b)}$. ■

Proof of Exercise 19: This is something that I spent time focusing personal research on. The prime omega function, which counts how many primes factors there are for a specified integer, can be restricted to the square root of that integer, as there cannot be any prime integer greater than $\lfloor\sqrt{2^5-1}\rfloor = 5$. Therefore, we can test 2,3, and 5, and none of them divide $2^5 - 1 = 31$ evenly. Therefore, it is prime.

Similarly, $\lfloor\sqrt{2^7-1}\rfloor = 11$, $2 \nmid 127, 3 \nmid 127, 5 \nmid 127, 7 \nmid 127, 11 \nmid 127$. ■

Proof of Exercise 20: If the $gcd(p,10) = 2$, then it must be even thus p cannot be even. And even if it is not specifically 2, but instead also 4, 6, or 8, then we should note that 2 is still a divisor of such "prime" above 5, which means the integer must still be even. Thus we can rule out all even remainders. Now consider $r = 5$, for some remainder, r. Thus the $gcd(p,10) = 5$, which comes to show that p is not prime. ■

Proof Of Exercise 21: ($\implies$). If p is prime and $a < p$, then the $gcd(a,p) = \pm 1, \pm p$. Since the only divisors of p prime is these two factors. If $a \geqslant p$, then $gcd(a,p) = p$.
($\impliedby$). If $gcd(a,p) = 1$, or $p|a$, then this shows that the only divisors of p is in fact, ± 1 and $\pm p$. ■

Proof of Exercise 22: Let's assume that p is not prime. Then p would have some divisors $d, t \in \mathbb{Z}$, such that

$$p = dt.$$

Then according to our assumption, if p is not prime, then $p|d$ or $p|t$. Therefore, when $p \mid d$, then $d = \pm p$ and $t = \pm 1$. Or when $p \mid t$, then $t = \pm p$, and $d = \pm 1$. Thus p is prime. ■

Proof of Exercise 23: The idea of this question is that there exists an integer $d \in \mathbb{Z}$ such that

$$d = p_1^{n_1} p_2^{n_2} \dots p_k^{n_i},$$

where the $gcd(a,b) = d$. This integer is some common divisor of both a and b, such that each n_i is the minimum count of r_i and s_i. If we are to see a more literal viewing of this statement, then we can readjust the value of a as:

$$\begin{aligned} a &= p_1^{n_1} p_1^{r_1-n_1} p_2^{n_2} p_2^{r_2-n_2} \dots p_k^{n_i} p_k^{r_i-n_i} \\ &= d(p_1^{r_1-n_1} p_2^{r_2-n_2} \dots p_k^{r_i-n_i}). \end{aligned}$$

However, how do we know that n_i is the minimum between r_i and s_i. Suppose that there is a divisor $q \in \mathbb{Z}$, such that:

$$q = p_1^{v_1} p_2^{v_2} \dots p_k^{v_i}.$$

Then if $v_i < min\{r_i, s_i\}$, then q will not be the greatest common divisor, as there is some divisor that includes more power in a kth prime. And if $v_i > min\{r_i, s_i\}$, then the same powers of a or b will result in $p_k^{r_i-v_i}$, which may become a negative power, which will create a fractional value instead of an integer prime, thus also not possible. Therefore v_i must be $v_i = min\{r_i, s_i\} = n_i$. Continuing back with the proof (from $a = \dots$), similarly, we can do the same for b, such that it will contain the common divisors of both a and b. Therefore, the $gcd(a,b) = d$. ■

Proof of Exercise 24: Consider a $lcm[x,y]$, given some $x, y \in \mathbb{Z}$, then this lcm will be equal to the lowest possible multiple of both x and y. In problem 33, we prove that the $lcm[a,b] = \frac{ab}{gcd(a,b)}$, and this statement further proves this statement, which we can break up into simpler statements. Since a and b are a product of primes, then what we do in the numerator of the previous fraction is add all powers of primes together, and then divide it by the greatest common divisors of each, which will lead to a least common multiple. Since we have proved in the previous part of this question, the $gcd(a,b)$ is equal to some integer $d \in \mathbb{Z}$, such that d contains the minimum power common divisor in both a and b.
Now that we have broken down the problem into ideas we can actually use, we can proceed to prove the problem. Given that

$$\begin{aligned} a &= p_1^{r_1} p_2^{r_2} \dots p_k^{r_i} \\ b &= p_1^{s_1} p_2^{s_2} \dots p_k^{s_i} \\ ab &= p_1^{r_1} p_1^{s_1} p_2^{r_2} p_2^{s_2} \dots p_k^{r_i} p_k^{s_i} \\ \frac{ab}{gcd(a,b)} &= \frac{p_1^{r_1} p_1^{s_1} p_2^{r_2} p_2^{s_2} \dots p_k^{r_i} p_k^{s_i}}{p_1^{n_1} p_2^{n_2} \dots p_k^{n_i}} \\ &= p_1^{r_1+s_1-n_1} p_2^{r_2+s_2-n_2} \dots p_k^{r_i+s_i-n_i}. \end{aligned}$$

Note that when we subtract n_i from $r_i + s_i$, we are left with the maximum of r_i or s_i. This is because we are subtracting the lesser of r_i and s_i from each power, and that means we are left with the other term. To understand this in simpler terms, let's suppose that $n_4 = min\{r_4, s_4\} = s_4$. Therefore, the fourth integer in the factorization will equal $p_4^{r_4+s_4-s_4} = p_4^{r_4}$, and similarly, we can do the same for each of the factors in ab.
Therefore we have just shown that

$$\begin{aligned} lcm[a,b] &= p_1^{r_1+s_1-min\{r_1,s_1\}} p_2^{r_2+s_2-min\{r_2,s_2\}} p_3^{r_3+s_3-min\{r_3,s_3\}} \dots p_k^{r_i+s_i-min\{r_i,s_i\}} \\ &= p_1^{max\{r_1,s_1\}} p_2^{max\{r_2,s_2\}} p_3^{max\{r_3,s_3\}} \dots p_k^{max\{r_i,s_i\}} \\ &= p_1^{t_1} p_2^{t_2} p_3^{t_3} \dots p_k^{t_i}. \end{aligned}$$

Thus we have reached the conclusion that $lcm[a,b] = p_1^{t_1} p_2^{t_2} p_3^{t_3} \dots p_k^{t_i}$, where $t_i =$ maximum of r_i, s_i. ■

Proof of Exercise 25: Suppose that $a \mid b$, then given some $x \in \mathbb{Z}$

$$b = ax.$$

Since this is the case, then we can square both sides and simplify given that $y = x^2$

$$\begin{aligned} b^2 &= a^2 x^2 \\ &= a^2 y, \end{aligned}$$

which comes to show that b^2 is divisible by a^2.
We can show this in the reverse direction to show a bi-conditional iff. Given $a^2 \mid b^2$ and $w, z \in \mathbb{Z}$, then

$$b^2 = a^2 w,$$

and we can split the factors, and set $z = aw$, show that,

$$\begin{aligned} b(b) &= a(aw) \\ b(b) &= az \\ a &\mid b * b \end{aligned}$$

Thus $a \mid b \iff a^2 \mid b^2$. ■

Proof of Exercise 26: Given that $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, then we can split this fractions into terms such that $p!$ is divisible by p.

$$\frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{k!(p-k)!}$$

Note that since, $(p-1), k, \ and \ (p-k)$ are all less than p, they are not divisible due to the definition of a prime and what we proved in Question 21. Note that, $(p-1), k, \ and \ (p-k)$ are integers, and since they are multiples of numbers that are less than p, then p cannot divide these integers. However, there is a problem, we don't know if the fraction $\frac{(p-1)!}{k!(p-k)!}$ is also an integer. Consider that

$$\begin{aligned} \frac{p!}{k!(p-k)!} &= m \\ p! &= mk!(p-k)! \\ p(p-1)! &= mk!(p-k)! \\ p &\mid mk!(p-k)! \end{aligned}$$

Then p divides $m, k!, \ or \ (p-k)!$, and as we stated before, all but m are less than p, therefore indivisible. And since $p \mid m$, and $m = \frac{p!}{k!(p-k)!} = \binom{p}{k}$, then $p \mid \binom{p}{k}$. ■

Chapter 8

Proof of Exercise 1: Let $SL(2, \mathbb{R})$ be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $a, b, c, d \in \mathbb{R}$ and the determinate is equal to 1, which is non-zero. We know the identity matrix exists in $SL(2, \mathbb{R}) \ni I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We can check this by first checking $\det\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] = 1$, and if $A \in SL(2, \mathbb{R})$, then $AI = IA = A$, which it does. Thus I is the identity element. Since the determinate is nonzero, there exists an inverse by properties of matrices since if the determinate is non-zero, then let

$$A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

such that $AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Which is the identity element, thus proving an inverse. To prove associativity, we can show this by determinants. Let $A, B, C \in SL(2, \mathbb{R})$

$$\begin{aligned} \det(A)(\det(B)\det(C)) &= \det(A)(1) \\ &= (1)(1) \\ &= 1; \\ (\det(A)\det(B))\det(C) &= (1)\det(C) \\ &= (1)(1) \\ &= 1, \end{aligned}$$

thus also showing associativity, but if we let $A = B = C$, then it also shows closure under multiplication. Thus $SL(2, \mathbb{R})$ is a group. ■

Proof of Exercise 2: Suppose A abelian, denote it $\begin{pmatrix} 1 & 2 & 3 \\ A(1) & A(2) & A(3) \end{pmatrix}$.

We can show this by showing examples of such permutations

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, A_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

We have

$$A_1 A_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

however,

$$A_2 A_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

, thus a contradiction arises since $A_1 A_2 \neq A_2 A_1$, thus not abelian. ■

Proof of Exercise 3: Given $f \in S_n$, suppose $f^m = f^n$, $m < n$, then if we take the inverse of f^m

$$f^m f^{-m} = f^n f^{-m}.$$

Then $I = f^{n-m}$. Let $k = n - m$ proving $f^k = I$. ■

Proof of Exercise 4: Suppose $\text{ord}(bab^{-1}) = k$ and $\text{ord}(a) = t$ such that $k \neq t$. If we take $(bab^{-1})^t$, then by exercise 12, then it would equal to $ba^t b^{-1}$. Continuing the group operations, we will get:

$$\begin{aligned} ba^t b^{-1} &= beb^{-1} \\ &= bb^{-1} \\ &= e. \end{aligned}$$

Note that $e = a^t$, thus $(bab^{-1})^t = a^t$. If we take $(bab^{-1})^k$, then it would equal to $ba^k b^{-1}$, which is equal to the identity due to the order. Continuing on:

$$\begin{aligned} ba^k b^{-1} &= e \\ (b^{-1}b)(a^k)(b^{-1}b) &= b^{-1}eb \\ ea^k e &= b^{-1}b \\ a^k &= e. \end{aligned}$$

Thus $a^k = e$. If $a^k = e = a^t$, then $a^k = a^t$. Hence $k = t$, a contradiction. ■

Proof of Exercise 5: **(a)** Given $a = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, then we can find the order by doing matrix multiplication in the general linear group.

$$\begin{aligned} \left[\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\right]\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} &= \left[\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\right]\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Thus $a^3 = e$ and is the least power of a that equals the identity, hence $\text{ord}(a) = 3$. Given $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, then we can find the order similarly.

$$\begin{aligned} \left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right]\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] &= \left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right]\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right] \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Thus $b^4 = e$, hence $\text{ord}(b) = 4$.
(b) Let's do a couple of powers to see if we notice a pattern. Let $c = ab$ and do a couple of base cases.

$$c = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$
$$c^2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$
$$c^3 = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$$
$$c^4 = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}.$$

We now can hypothesize, in fact, an Induction Hypothesis, that $c^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$, where $n \in \mathbb{N}$.

Define $S := \{n \in \mathbb{N} : c^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}\}$. We have proven multiple base cases, therefore we know $1, 2, 3, 4 \in S$. Now suppose $k \in S$, our goal is to show $k + 1 \in S$.

$$\begin{aligned} c^k &= \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \\ c^k c &= \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -(k+1) & 1 \end{pmatrix} \\ &= c^{k+1}. \end{aligned}$$

Thus we have shown that $c^{k+1} = \begin{pmatrix} 1 & 0 \\ -(k+1) & 1 \end{pmatrix}$, thus $k + 1 \in S$ by PMI. ■

Proof of Exercise 6: ($\Longrightarrow$) Given G is abelian, let $(ab)(ab)^{-1} = e$. Using group operations of the abelian variety, we get that

$$\begin{aligned} (ab)(ab)^{-1} &= e \\ (a^{-1}a)b(ab)^{-1} &= a^{-1}e \\ eb(ab)^{-1} &= a^{-1}e \\ b(ab)^{-1}b^{-1} &= a^{-1}eb^{-1} \\ (ab)^{-1}(bb^{-1}) &= a^{-1}b^{-1} \\ (ab)^{-1}e &= a^{-1}b^{-1} \\ 0(ab)^{-1} &= a^{-1}b^{-1}. \end{aligned}$$

Therefore $(ab)^{-1} = a^{-1}b^{-1}$.
($\Longleftarrow$) Given $(ab)^{-1} = a^{-1}b^{-1}$, then

$$\begin{aligned} (ab)(a^{-1}b^{-1}) &= e \\ (ab)a^{-1}(b^{-1}b) &= eb \\ (ab)(a^{-1}a) &= eba \\ ab &= ba. \end{aligned}$$

Thus, since $ab = ba$, then G is abelian. ■

Proof of Exercise 7: Given for all $x \in G$ and $x \neq e$, $\text{ord}(x) = 2$, if we have any arbitrary element in G, $a, b \in G$, then similar to exercise 25, we have the following setup:

$$\begin{aligned} (ab)(ab) &= e \\ (ab)a(bb) &= eb \\ (ab)aa &= ba \\ ab &= ba. \end{aligned} \tag{11.1}$$

To explain what was just done, Equation 11.1 is possible due to the order 2 of two group elements grouped under the group operation, which allows us to equal to the identity. From there, it is similar to exercise 25. ■

Proof of Exercise 8: Given $\text{ord}(ab) = k$, if $(ab)^k = e$ and $(aa^{-1})^k = e$, then

$$\begin{aligned} (ab)^k(aa^{-1})^k &= ee \\ &= e. \end{aligned}$$

Note that we could combine these powers together such that

$$(ab)^k(aa^{-1})^k = (abaa^{-1})^k,$$

but by exercise 19, we get the following:

$$\begin{aligned} (ab)^k &= (a(ba)a^{-1})^k \\ &= (ba)^k. \end{aligned}$$

Hence $(ab)^k = (ba)^k$. ■

Proof of Exercise 9: Given $\text{ord}(G) = n$ is even, suppose $m_x \in G$, with $x \in \mathbb{N}$, such that $\text{ord}(m_x) = p$ is some odd strictly positive value strictly greater than 1. Then for each $m_x \in G$ there exists an inverse m_x^{-1}, that $m_x \neq m_x^{-1}$, plus some identity element $e \in G$. If this is true, then $\text{ord}(G)$ is odd, which is a contradiction to the order of G being even. Thus there exists $k \in G$ such that $k = k^{-1}$, this considers all even ordered values in G. Hence, there exists a order 2 element k. ■

Proof of Exercise 10: Suppose $\text{ord}(a) = n$ and $\text{ord}(b) = m$. If m, n are relatively prime, then by theorem 7.9, as long as $n|k$ in a^k, and $m|l$ in b^l, then n and m divides $lcm(m, n) = nm$. Thus the $\text{ord}(ab) = \text{ord}(a)\,\text{ord}(b) = mn$. ■

Proof to Exercise 11: By Theorem 7.9, we know if $\text{ord}(b) = n$ and $n|6$, then b^6 is an identity element. Thus our divisors of 6 are $2, 3, 6$. Since, $ab = b^4a$, then we know that $2|4$, thus the identity is not b^2. Given $ab = b^4a$, then:

$$\begin{aligned} b &= a^{-1}b^4a \\ b^2 &= a^{-1}b^8a \text{ by Exercise 12} \\ b^3 &= a^{-1}b^{12}a \\ &= a^{-1}a \\ &= e. \end{aligned}$$

Thus we have shown that b^3 is the identity. Since we know that b^3 is the identity, then by Theorem 7.7,

$$\begin{aligned} ab &= b^3ba \\ ab &= eba \\ ab &= ba. \end{aligned}$$

Hence $ab = ba$. ■

Proof to Exercise 12: Given $(ab)^i = a^i b^i$, then let

$$\begin{aligned} a^i(b^i a)b &= a^{i+1}b^{i+1} \\ &= a^i(ab^i)b. \end{aligned}$$

Thus $b^i a = ab^i$ by Theorem 7.5. Since

$$\begin{aligned} a^{i+1}(b^{i+1}a)b &= a^{i+2}b^{i+2} \\ &= a^{i+1}(ab^{i+1})b. \end{aligned}$$

Thus $b^{i+1}a = ab^{i+1}$. Then given these two equalities, then

$$\begin{aligned} ab^{i+1} &= (ab)b^i \\ b^{i+1}a &= b(b^i a) \\ &= (ba)b^i \\ (ab)b^i &= (ba)b^i. \end{aligned}$$

Hence $ab = ba$. ■

Proof of Exercise 13: Given that T has elements of finite order that are in G, then we know identity $e \in G$ is also in T since $\text{ord}(e) = 1$. Thus T is nonempty. Suppose $a \in G$ and $\text{ord}(a) = n$ such that $a^n = e$. Then we know by a class lemma[1], that $\text{ord}(a) = \text{ord}(a^{-1})$, thus there exists the inverse of a.

Suppose $a, b \in T$, $\text{ord}(a) = n, \text{ord}(b) = m$, thus by Exercise 31 in 7.2, $\text{ord}(ab) = mn$ such that $(ab)^{mn} = e$. Thus $ab \in T$, showing closure under multiplication. Thus by Theorem 7.11, T is a subgroup of G. ■

Proof of Exercise 14: Given that $C(a)$ is a set of abelian products by a and some element in G, we know that identity $e \in C(a)$, since by the property of identities $ea = ae = a$. Thus $C(a)$ is non-empty. Since $a, a^{-1} \in G$, then by properties of inverses $a^{-1}a = aa^{-1}$, thus there exists inverses in $a^{-1} \in C(a)$.

Suppose $b, c \in C(a)$, then:

$$\begin{aligned} a(bc) &= (ab)c \\ &= (ba)c \\ &= b(ac) \\ &= b(ca) \\ &= (bc)a. \end{aligned}$$

Thus $bc \in C(a)$ showing closure under multiplication. Thus by Theorem 7.11, $C(a)$ is a subgroup of G. ■

Proof of Exercise 15: Given G is a group and for some $a \in G$, $C(a)$ is the centralizer in group G with a, we need to show that $Z(G) = \bigcap_{a \in G} C(a)$. We have previously defined

$$C(a) := \{g \in G : ga = ag\}$$

and

$$Z(G) = \{g \in G : ga = ag, \forall a \in G\}.$$

Define $S = \bigcap_{a \in G} C(a)$. If $c \in C(a)$ but $c \notin C(b)$, then $c \notin S$. Suppose $x \in S$, then $x \in C(f), xf = fx \forall f \in G$, which follows the definition of the centre. Thus $x \in S$. Suppose $y \in Z(G)$, then $\forall a \in G$, $ya = ay$, which satisfies the restriction of S, thus $y \in S$. Thus $Z(G) = \bigcap_{a \in G} C(a)$. ■

[1] Dr. Chastkofsky allowed me to use this on the homework when asked in Office Hour

Proof of Exercise 16: Suppose H is a subgroup of G, $\text{ord}(a) = n$, $a^k \in H$, $\gcd(k, n) = 1$. Since $\gcd(k, n) = 1$, then we can rewrite this as a linear combination $1 = rk + sn$. Thus $a^1 = a^{rk+sn} \in G$. We know that $a^k \in H$, thus $(a^k)^r \in H$ due to closure under multiplication. And

$$\begin{aligned}(a^k)^r(a^n)^s &= (a^k)^r e \\ &= (a^k)^r.\end{aligned}$$

Thus $a^{rk+sn} \in H$, thus $a \in H$. ■

Proof of Exercise 17: Given H is a subgroup of G and normalizer $N(H) := \left\{x \in G \mid x^{-1}Hx = H\right\}$, we know $e \in N(H)$ since $e \in G$ and $e^{-1}ae = a$ for all $a \in H$. Thus $N(H)$ is nonempty. Suppose $a \in H$, let we know $a^{-1} \in G$, then $(a^{-1})^{-1}aa^{-1} = a$, thus $a^{-1} \in H$ for all $a \in H$. Thus this set is closed under inverses.

Recall given $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$. Suppose $b, c \in N(H)$, then

$$\begin{aligned}(bc)^{-1}abc &= c^{-1}b^{-1}abc \\ &= c^{-1}(b^{-1}ab)c \\ &= c^{-1}ac \\ &= a.\end{aligned}$$

Thus $bc \in N(H)$ which shows closure under multiplication. Thus $N(H)$ is a subgroup of G that contains H. ■

Proof of Exercise 18.a: Given $G = \langle a \rangle$ and $\text{ord}(G) = n$, we claim that $\text{ord}(a) = n$. This is because there are only n elements in G which is generated by a, thus all the elements in G range from $a^1, a^2, \ldots, a^{n-1}, a^n$. Of which a^n must be the identity e, since G is a group. Suppose $d = \gcd(m, n)$, such that $d = rm + sn$. Similar to the proof of Exercise 16:

$$\begin{aligned}a^d &= a^{rm+sn} \\ &= (a^m)^r(a^n)^s \\ &= (a^m)^r(e)^s \\ &= (a^m)^r.\end{aligned}$$

Thus $\langle a^d \rangle = \langle a^m \rangle$ by closure under multiplication. ■

Proof of Exercise 18.b: ($\implies$). Given a^m is a generator of G, and $\text{ord}(G) = n$ and as we have shown earlier, $\text{ord}(a) = n$, then define

$$S := \{w \in \mathbb{N} : 1 \leqslant w \leqslant n \text{ and } a^{mw} \text{ must be unique}\}$$

Suppose $n|m$, then $a^{mw} = e$ by Theorem 7.9, thus this does not satisfy $\#S \neq n$. This is an example of how we will be approaching the rest of this proof.
Suppose $\gcd(n, m) = d \neq 1$, then by definition of $\text{lcm}(n, m) = \frac{nm}{d} = x \neq nm$. Thus $\#S \neq n$, since there is some multiple of m and n that is not mn and w cannot reach past x. Thus $\gcd(n, m) = 1$, thus $\text{lcm}(n, m) = nm$, thus all a^{mw} are unique and w reaches n such that $\#S = n$.

($\impliedby$). Given $\gcd(n, m) = 1$, then $\text{lcm}(n, m) = nm$ and $\#S = n$. Thus a^m is a generator of G. ■

Proof of Exercise 19: ($\implies$). Define $S = \mathbb{Z}_m \times \mathbb{Z}_n$. Suppose $gcd(m, n) = d \neq 1$, then as we have shown in similar fashion to the proof of Exercise 18, $\text{lcm}(m, n) = x < mn$. Thus for $a \in S$, $a^x = (0, 0)$, which means $\text{ord}(a) < mn$ and $\text{ord}(S) = mn$, thus is not cyclic.

($\impliedby$). Suppose $\gcd(m, n) = 1$. If $a \in S$, let $\text{ord}(a) = p$. Since $\text{ord}(S) = mn$, thus $mn \geqslant p$. Since $\text{lcm}(m, n) = mn$, by the proof of Exercise 18, $mn \leqslant p$. Thus $mn = p$. Since $\text{ord}(S) = \text{ord}(a)$, then S is cyclic. ■

Proof of Exercise 20: First we must check that h is indeed a homomorphism.

$$\begin{aligned} h(a)h(b) &= \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ a+b & 1 \end{pmatrix} \\ &= h(a+b). \end{aligned}$$

Thus h is a homomorphism. Now to check if h is also injective, suppose we have $h(x) = h(y)$:

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

then as shown, $x = y$. ■

Proof of Exercise 21:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Set $f(1) = 1, f(2) = 3, f(3) = 7, f(4) = 9$, and it can be seen that these two groups are indeed isomorphic. ■

Proof of Exercise 22: Given f is a subjective homomorphism and G is abelian, suppose $f(a) = c, f(b) = d$. Since f is a homomorphism, then $f(ab) = cd$, but $f(ab) = f(ba) = dc$. Thus $cd = dc$. Hence H is abelian. ■

Proof of Exercise 23: ($\implies$). Given G is abelian, suppose $f(x) = x^{-1}$. Then:

$$\begin{aligned} f(xy) &= xy^{-1} \\ &= y^{-1}x^{-1} \\ &= x^{-1}y^{-1} \\ &= f(x)f(y). \end{aligned}$$

Thus f is a homomorphism.
($\impliedby$). Suppose f is a homomorphism.

$$\begin{aligned} xy &= f(x^{-1})f(y^{-1}) \\ &= f(x^{-1}y^{-1}) \\ &= f(yx^{-1}) \\ &= yx. \end{aligned}$$

Thus G is abelian. ■

Proof of Exercise 24.a: Define $S = a^{-1}Na$. Given N is a subgroup of G and $a \in G$, suppose $b, c \in N$, then:

$$a^{-1}baa^{-1}ca = a^{-1}(bc)a.$$

Thus $a^{-1}(bc)a \in S$. Thus S is closed under multiplication. Suppose $a^{-1}ba \in S$, since $b^{-1} \in N$, then

$$\begin{aligned} a^{-1}baa^{-1}b^{-1}a &= a^{-1}bb^{-1}a \\ &= a^{-1}a \\ &= e. \end{aligned}$$

Thus $(a^{-1}ba)^{-1} = a^{-1}b^{-1}a \in S$. Hence S is a subgroup of G. ■

Proof of Exercise 24.b: Suppose we have a function $f : N \to S$. In the effort to show a subgroup, we have already shown that this function is a homomorphism. If we have $b, c \in N$, $a^{-1}ba = a^{-1}ca$, thus by cancellation law, $b = c$. Thus f is injective. Suppose for all $b \in S$, such that there exists a $c \in N$ such that $f(c) = b$. Let $b = a^{-1}ca$, then by group operations:

$$\begin{aligned} b &= a^{-1}ca \\ aba^{-1} &= c. \end{aligned}$$

Thus $f(c) = f(aba^{-1}) = a^{-1}(aba^{-1})a = b$. Hence, f is isomorphic. ■

Proof of Exercise 25: Given $G = \langle a \rangle$ and $G = \langle b \rangle$ and $f : G \to G$ given by $f\left(a^i\right) = b^i$, we must show that f is first a homomorphism.

$$\begin{aligned} f(a^i a^j) &= b^{i+j} \\ &= b^i b^j \\ &= f(a^i)f(a^j). \end{aligned}$$

If we had $f(a^i) = f(a^j)$, then $b^i = b^j$, and since G is cyclic, then i and j are unique, thus $i = j$. Thus we have shown that f is homomorphic and injective.

Suppose $\text{ord}(G) = n$, then $\text{ord}(a) = \text{ord}(b) = n$, and as we have proved that f is indeed injective, then a finite order G would make f surjective.
Suppose $\text{ord}(G) = \infty$, then $\text{ord}(a) = \text{ord}(b) = \infty$, and similarly due to injectivity, we have surjectivity. Hence, f is an automorphism of G. ■

Proof of Exercise 26: Given G is a cyclic group generated by $\langle a \rangle$ and $f : G \to H$ is a surjective homomorphism of groups, then by exercise 15, we know that $f(a^n) = (f(a))^n$. Since f is surjective, thus $H = \langle f(a) \rangle$. ■

Proof of Exercise 27: Note that all elements in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has at most order 2, as all elements are under modulo 2. But given $(1, 1) \in \mathbb{Z}_4 \times \mathbb{Z}_2$, $\text{ord}(1, 1) = 4$, which shows a contrast in properties. Thus $\mathbb{Z}_4 \times \mathbb{Z}_2 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ■

Proof of Exercise 28: Since the only generators of $\mathbb{Z}$ are 1 and -1, thus by exercise 25 and 26, $\text{ord}(\text{Aut}(\mathbb{Z})) = 2$, thus $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$. ■

Proof of Exercise 29: Let's do a couple of tests to see if we can come to any observations.

$$\begin{aligned} (12) &= (12) \\ (123) &= (13)(12) \\ (1234) &= (14)(13)(12) \\ (12345) &= (15)(14)(13)(12). \end{aligned}$$

We can notice that the claim seems to be holding true that the cycle is even when k is odd.

($\Longleftarrow$). Given that the cycle $(a_1 a_2 \cdots a_k)$, suppose k is odd. Since a_1 repeats itself in all pairings with a_2 through a_k, then there are a total $k - 1$ transpositions, which is an even number. Therefore the cycle is even if k is odd.

($\implies$). Given the cycle is even, suppose k is even. As we have said before, there are only $k-1$ transpositions, and since k is even, then the cycle must be odd. A contradiction has risen. By Theorem 7.28, the cycle cannot be both even and odd, thus k must be odd for the cycle to be even. Hence proving this biconditional relationship. ■

Lemma 11.3.1 Exercise 7.2.33

Assume that $a, b \in G$ and $ab = ba$. If $\text{ord}(a)$ and $\text{ord}(b)$ are relatively prime, prove that ab has order $\text{ord}(a)\,\text{ord}(b)$.

Proof of Exercise 7.2.33: Suppose $\text{ord}(a) = n$ and $\text{ord}(b) = m$. If m, n are relatively prime, then by theorem 7.9, as long as $n|k$ in a^k, and $m|l$ in b^l, then n and m divides $lcm(m,n) = nm$. Thus the $\text{ord}(ab) = \text{ord}(a)\,\text{ord}(b) = mn$. ■

Corollary 11.3.1 Corollary of Exercise 7.2.33

The order of the product of two elements is $\text{ord}(ab) = \text{lcm}[\text{ord}(a), \text{ord}(b)]$.

Proof of Exercise 30: From Exercise 7.5.17 from the Textbook[2], we know that the order of a k-cycle in group S_n has order k. From Exercise 7.5.18 from the Textbook, we also know that the product of disjoint cycles are commutative. Look at the proof of the lemma above. Consider the corollary of the lemma.

Define $\tau := \prod_{i=1}^{n} \sigma_i$. By 7.5.17, suppose we are trying to find the order of $\tau = \sigma_1\sigma_2$. Let $\text{ord}(\sigma_1) = c, \text{ord}(\sigma_2 = d$. Then by the corollary of the lemma, $\text{ord}(\sigma_1\sigma_2) = \text{lcm}[c,d]$.
Our next base case is suppose we have $\tau = \prod_1^3 \sigma_i$. Let $i = 1, 2$ remain the same orders of c, d respectively, and let $\text{ord}(\sigma_3) = e$. Then our order is $\text{ord}\left(\prod_1^3 \sigma_i\right) = \text{lcm}[\text{lcm}[c,d], e]$ by corollary of lemma.
Our last base case is suppose we have $\tau = \prod_1^4 \sigma_i$, similarly let all the previous orders remain as is, and let $\text{ord}(\sigma_4) = f$. Then let $\text{ord}\left(\prod_1^4 \sigma_i\right) = \text{lcm}[\text{lcm}[c,d]\,\text{lcm}[e,f]]$ by corollary of lemma.

We now can hypothesize, in fact, an Induction Hypothesis, that

$$\text{ord}\left(\prod_1^n \sigma_i\right) = \text{lcm}\left[\text{ord}\left(\prod_1^{n-1} \sigma_i\right), \text{ord}(\sigma_n)\right]$$

for all $n \in \mathbb{N}$. Define $S := \{n \in \mathbb{N} : \text{ord}\left(\prod_1^n \sigma_i\right) = \text{lcm}\left[\text{ord}\left(\prod_1^{n-1} \sigma_i\right), \text{ord}(\sigma_n)\right]\}$. By our base cases, we know that $1, 2, 3, 4 \in S$. Now suppose $1, \ldots, k \in S$, our goal is to show that $k+1 \in S$:

$$\begin{aligned}\text{ord}\left(\prod_1^{k+1} \sigma_i\right) &= \text{ord}\left[\left(\prod_1^{k} \sigma_i\right)\sigma_{k+1}\right] \\ &= \text{lcm}\left[\text{ord}(\prod_1^{k} \sigma_i), \text{ord}(\sigma_{k+1})\right].\end{aligned}$$

Thus $k+1 \in S$ by PMI. ■

Proof of Exercise 31: **(a)**. Suppose $f(a) = f(b)$:

$$\begin{aligned}(12)a &= (12)b \\ (12)(12)a &= (12)(12)b \qquad (11.2)\\ a &= b. \qquad (11.3)\end{aligned}$$

The reason we could go from Equation 11.2 to Equation 11.3, is due to Exercise 17, of a k-cycle group being order of the elements in the group.
(b). Since $b \in B_n$, then b is an odd cycle. Thus $(12)b$ is an even cycle such that $(12)b \in A_n$.

$$\begin{aligned}f((12)b) &= (12)(12)b \\ &= b.\end{aligned}$$

[2]From Hungerford Abstract Algebra

Thus f is bijective.
(c) Since A_n and B_n is disjoint cycles, by Theorem 7.28, the union of A_n and B_n is equal to S_n. Since $\text{ord}(S_n) = n!$ and since f is bijective, then the orders of A_n and B_n are equal, then $\text{ord}(A_n) = n!/2$. ■

Proof of Exercise 32: Note that by Theorem 7.24, all permutations can be written as a product of disjoint cycles, and by Theorem 7.23, all disjoint cycles are commutative. Therefore, for all $n \geqslant 3$ in S_n, there does not exist an element that is commutative for all elements in S_n, unless it is the identity. For example, there will always exist an element $(1 \dots n)$ which will show as non-disjoint for any cycle. ■

Proof of Exercise 33: Given τ is a k-cycle $(a_1 a_2 \cdots a_k)$ and $\sigma \in S_n$, then suppose there exists an element b is not an element of $(\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$ and $i \in \mathbb{N}^{\leqslant k}$. Then $\sigma\tau\sigma^{-1}\sigma(a_i) = \sigma\tau(a_i) = \sigma(a_i)$. Thus $\sigma\tau\sigma^{-1}(b) = \sigma\sigma^{-1}(b) = b$. Therefore, $\sigma\tau\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$ ■

Proof of Exercise 34: **(a)** Suppose $f : A_G \to B_G$ with $\sigma \mapsto \sigma\tau$, with A_G and B_G being the set of even and odd permutations respectively. Suppose $f(a) = f(b)$, then:

$$\begin{aligned} a\tau &= b\tau \\ a\tau\tau^{-1} &= b\tau\tau^{-1} \\ a &= b. \end{aligned}$$

Thus f is injective. For $b \in B_G$, $b\tau^{-1} \in A_G$, thus $f(b\tau^{-1}) = b$, thus f is a bijection. Thus $\text{ord}(A_G) = \text{ord}(B_G)$.
(b) By (a), since $\text{ord}(A_G) = \text{ord}(B_G)$, and since these partition G, then $\text{ord}(G) = 2\,\text{ord}(A)$. Thus by the division algorithm, $2 | \text{ord}(G)$.
(c) Given K is a subgroup of S_n of odd order, if K has an odd permutation, then by the previous part, half of K is odd. Then it can be written that K is even, which is a contradiction. Thus $K \leqslant A_n$. ■

Proof of Exercise 35: Suppose $f : S_n \to A_{n+2}$ with

$$\sigma \mapsto \begin{cases} \sigma & \text{if } even \\ \sigma(n+1\ n+2) & \text{if } odd \end{cases}$$

Suppose a and b are elements in S_n. $f(ab) = ab = f(a)f(b)$, since ab is even as well. If a is even and b is odd, then $f(ab) = ab(n+1\ n+2) = f(a)f(b)$. If a and b are odd, then $f(ab) = ab$, since ab is even. If a is even and b is odd, then $f(ba) = ba(n+1\ n+2)$, and since $(n+1n+2)$ are disjoint to all elements in S_n, then by Theorem 7.23, $ba(n+1\ n+2) = b(n+1\ n+2)a = f(b)f(a)$.

The function is also injective since if a and b is even, then $f(a) = f(b)$ implies $a = b$. If a and b is odd, then $f(a) = f(b)$ implies $a(n{+}1\ n{+}2) = b(n{+}1\ n{+}2)$, and by Exercise 17, $a(n{+}1\ n{+}2)(n{+}1\ n{+}2) = b(n{+}1\ n{+}2)(n{+}1\ n{+}2)$ implies $a = b$. Thus since f is a injective homomorphism, then S_n is isomorphic to the image of f, which is a subgroup of A_{n+2}. ■

Proof of Exercise 36: $(123)^{-1} = (321)$. Every other element has the inverse of itself, other than the identity which is already the inverse. ■

Proof of Exercise 37: I found a trick while doing this. Split the index in half, denoted h, then convert each element from $(-h) - (h)$, which should be in symmetric order. Then multiply the digits to get a product of one. The first and last element will always be their own inverse.

In $\mathbb{Z}_7$:

$$\begin{aligned} 2 &\to 2 \\ 4 &\to -3 \\ 2(-3) = -6 &\to 1 \end{aligned}$$

■

Proof of Exercise 38: Given G is a group, suppose we have with $a, b \in G$, $a * b$:

$$\begin{aligned} a * b &= a^{\ln b} \\ &= \exp\left(\ln a^{\ln b}\right) \\ &= \exp\left(\ln b \ln a\right) \\ &= b^{\ln a} \\ &= b * a \end{aligned}$$

Thus G is abelian. ■

Chapter 9

Proof of Exercise 1: Given G is a group of order 25, our goal is to show that G is cyclic or an element in G has order 5. By Corollary 8.6, since G is a finite group, then the order of all $a \in G$ must divide the order of G. The possible factors of G is $1, 5, 25$. If $\text{ord}(a) = 1$, then $a = e$. If $\text{ord}(a) = 5$, then we know that each element in G has an order of 5. If $\text{ord}(a) = 25$, then there is one generating element of G making it cyclic. Thus this proves the claim. ■

> **Lemma 11.3.2** Reduction of Possible Divisors of 2n
>
> The maximum divisor of $2n$ is n.

Proof of Lemma: Note that the total cap to integer divisors is $\lfloor\sqrt{2n}\rfloor$. What can we do to reduce this range in relation to n. Could we have a possible divisor of $2n$ put into relation of n? That is the question this lemma attempts to answer. By the Fundamental Theorem of Arithmetic, all divisors of n divide $2n$. However, if n is built up of primes $n = p_1 p_2 \dots p_k$, then the only difference between n and $2n$ is the prime 2. Thus $2n = 2p_1 p_2 \dots p_k$.

■

Proof of Exercise 2: Given G is an abelian group of order $2n$, with n odd, suppose G contains more than one element of order 2. By Exercise 8.1.31, we know that since $\text{ord}(G) = 2n$, which is even, then G contains at least one element of order 2. By the previous Lemma, there are no greater divisor of $2n$ than n. Thus the only divisors of n have to be odd by the Fundamental Theorem of Arithmetic leaving only one even divisor, which is order 2. ■

Proof of Exercise 3: **(a)**. Suppose a and b has order 3 in group and $a^2 = b^2$.

$$\begin{aligned} a^2 a^2 &= b^2 b^2 \\ a^4 &= b^4 \\ a^3 a &= b^3 b \\ ea &= eb \\ a &= b. \end{aligned}$$

Thus by these statements, $a = b$.

(b) Given G is a finite group, then for $a \in G$, $\text{ord}(a^2) = 3$:

$$\begin{aligned} (a^2)^3 &= (a^3)^2 \\ &= e^2 \\ &= e. \end{aligned}$$

As we have proved in the proof of **(a)**, a has order 3 already. Thus since a and a^2 have order 3, then without loss of generality, all elements of order 3 have an even number to such elements, being included in the set

$$\{b, b^2 : \forall b \in G \text{ and } \text{ord}(b) = 3$$

. ■

Proof of Exercise 4: Given p prime and $p|\operatorname{ord}(G)$, let $S := \{a \in G : \operatorname{ord}(a) = p\}$. By Exercise 8.1.34, there are exactly $p-1$ distinct elements of order p in the subgroup of G generated by $\langle a\rangle$. Define a relation on S such that $\langle a\rangle = \langle b\rangle$ denoted $a \sim b$. This relation creates clearly[3] distinct classes with each $p-1$ elements, $[a] = \{b \in S : a \sim b\}$, hence $p-1|S$. In fact we learn that the number of these elements are $n(p-1)$, with n counting the number of distinct classes under this relation. ■

Proof of Exercise 5: Denote $Z = Z(G)$. Given G is a group, suppose we have an element $c \in Z$. Then by the definition of Z, we have that c commutes with all elements in G. Thus we have that Z is a normal subgroup of G. Suppose $C \leqslant Z$, then every element in C still commutes with every element in G. Thus subgroup C is normal to G. ■

Proof of Exercise 6: Given group G, we have previously proved that Z is a normal subgroup of G. Let f be a automorphism of G. Given an element $c \in Z$, then:

$$\begin{aligned} f(c)f(a) &= f(ca) \\ &= f(ac) \\ &= f(a)f(c). \end{aligned}$$

And since f is an automorphism, then we know that this function is also an isomorphism, thus unique and has an inverse. Thus $f(c) \in Z$, since $f(c) \in G$ and $f(a) \in G$ for all $a \in G$. Thus Z is a characteristic subgroup. ■

Proof of Exercise 7: Given K is a normal subgroup of order 2 in group G, then given $k \in G$ and $\operatorname{ord}(k) = 2$, let $K = \{e, k\}$. Suppose $K \nsubseteq Z$, then $k \in K$ is not commutative with all elements in G. We know since $\operatorname{ord}(k) = 2$, then we know that k is commutative with $k \in G$. By Theorem 8.11, $Ka = aK$, thus by weak commutativity $ka = ak_1$ for all $a \in G$. However, by our assumption this is only possible if $k, k_1 = e$, thus a contradiction arises. Thus $K \subseteq Z$. ■

Proof of Exercise 8: **(a)**. Given N and K are subgroups of group G and N is normal to G, suppose $NK = \{nk : n \in N, k \in K\}$. Let $a = n_1k_1, b^{-1} = k_2^{-1}n_2^{-1}$. Since $k_1k_2 \in K$ due to closure, then $k_1k_2^{-1}n_2^{-1} = n_3k_1k_2^{-1}$ by weak commutativity. Thus:

$$\begin{aligned} ab^{-1} &= n_1k_1k_2^{-1}n_2^{-1} \\ &= n_1n_3k_1k_2^{-1}. \end{aligned}$$

Since $n_1n_3 \in N$ and $k_1k_2 \in K$, then $ab^{-1} \in NK$.

(b). Given N and K are normal subgroups of G, then for $a = n_1k_1, b^{-1} = k_2^{-1}n_2^{-1}$, then:

$$\begin{aligned} ab^{-1} &= n_1k_1k_2^{-1}n_2^{-1} \\ &= n_1k_1n_2^{-1}n_2k_2^{-1}n_2^{-1} \\ &= n_1k_1n_2^{-1}(n_2k_2^{-1}n_2^{-1}) \\ &= n_1k_1n_2^{-1}k_3 \\ &= n_1n_2^{-1}n_2k_1n_2^{-1}k_3 \\ &= n_1n_2^{-1}(n_2k_1n_2^{-1})k_3 \\ &= n_1n_2^{-1}k_4k_3. \end{aligned}$$

Since $n_1n_2^{-1} \in N$ and $k_4k_3 \in K$, then $ab^{-1} \in NK$. ■

Proof of Exercise 9: Given K and N are normal subgroups of group G such that $K \cap N = \langle e\rangle$, suppose we have $a = k^{-1}n^{-1}kn$. By using properties of normal subgroups, we have it that $a \in N$ but also that $a \in K$, since $(k^{-1}n^{-1}k)n = k^{-1}(n^{-1}kn)$. By the end of it, $a = e$, which satisfies $K \cap N$, then:

$$\begin{aligned} (k^{-1}n^{-1})kn &= e \\ (nk)^{-1}kn &= e \\ nk(nk)^{-1}kn &= nke \\ kn &= nk. \end{aligned}$$

[3] Allowed to state by Dr. Chastkofsky.

Thus $nk = kn$. ■

Proof of Exercise 10: **(a)**. Given N is a subgroup of G of index 2, then by Theorem 8.4, there are only two distinct elements a can be that are not in N, thus $Na_1 \cup Na_2 = G$ for all $n \in N$. Since a_1 and a_2 are not in N, and we know that N is a subgroup that is also closed under multiplication, thus $Na \notin N$.

(b). Suppose for $a \notin N$ and $n \in N$, then $a^{-1}Na \in Na$ and $a^{-1}Na \notin N$. Then $a^{-1}N \in N$ due to closure under multiplication to satisfy Na coset properties. Since $a^{-1} \in N$, then $a \in N$, and as we proved by part (a), thus a contradiction. Since Na makes up all elements that are not in G, then it must be the case that $a^{-1}Na \in N$. Thus N is a normal subgroup by Theorem 8.11, since $a^{-1}Na \subseteq N$. ■

Proof of Exercise 11: Given $\text{ord}(H) = n$ and H is the only subgroup of this order, then we know that all elements of H have finite order also. By Exercise 7.4.20, $a^{-1}Ha \leqslant G$ and $H \cong a^{-1}Ha$, given that $a \in G$. Thus the orders of H and $a^{-1}Ha$ are also the same due to this isomorphism, but we are given that H is the only subgroup of order n. Thus $a^{-1}Ha = H$. Hence H is normal. ■

Proof of Exercise 12: By properties of right cosets, suppose $Ta \in G/T$, then:

$$(Ta)^n = T(a^n).$$

If $a \in T$ and $\text{ord}(a) = n$, then $a^n = e$, thus $Te = T$, which does not have finite order. If $\text{ord}(a) = \infty$ then $T(a^n)$ will never have finite order for any $n \in \mathbb{N}$. ■

Proof of Exercise 13: Given that G is a simple group and $f : G \to H$ is a surjective homomorphism of groups, then let K be the kernel of this function. By Theorem 8.4.16, K is a normal subgroup of G, however since G is simple, this could either mean the trivial group or G itself. If K is trivial then $K = \langle e \rangle$, thus by Theorem 8.4.17 f is isomorphic due to injectivity. If K equals the G group itself, then all elements in G have to map to e_H, which means $H = \langle e \rangle$. ■

> **Lemma 11.3.3** Exercise 7.2.33
>
> Assume that $a, b \in G$ and $ab = ba$. If $\text{ord}(a)$ and $\text{ord}(b)$ are relatively prime, prove that ab has order $\text{ord}(a)\,\text{ord}(b)$.

Proof of Exercise 7.2.33: Suppose $\text{ord}(a) = n$ and $\text{ord}(b) = m$. If m, n are relatively prime, then by theorem 7.9, as long as $n|k$ in a^k, and $m|l$ in b^l, then n and m divides $lcm(m, n) = nm$. Thus the $\text{ord}(ab) = \text{ord}(a)\,\text{ord}(b) = mn$. ■

> **Corollary 11.3.2** Corollary of Exercise 7.2.33
>
> The order of the product of two elements is $\text{ord}(ab) = \text{lcm}[\text{ord}(a), \text{ord}(b)]$.

Proof of Exercise 14: **(a)**. Note that the only element of order 1 is the identity, thus K is closed under the identity. Given how $\text{ord}(a) = 2$, then it is also closed under inverses due to the inverse also having the same order as the element. Suppose $a, b \in K$, then ab^{-1} has order less than 2 due to $\text{lcm}(\text{ord}(a), \text{ord}(b)) \leqslant 2$ by Corollary 9.1.1. Thus K is closed under multiplication, thus a subgroup of G.
(b). H is closed under identity since $e^2 = e \in H$. H is closed under inverses since given $a \in G$, $a^2, (a^{-1})^2 \in H$, but $(a^{-1})^2 = (a^2)^{-1}$. Given $a, b \in G$, then $(ab^{-1})^2 = (b^{-1})^2a^2 = a^2(b^{-1})^2 \in H$. Thus H is closed under multiplication. Hence H is a subgroup of G.
(c). Define a map $f : G \to H$ by $x \mapsto x^2$ with kernel K. We claim f is a homomorphism: Given $x, y \in G$

$$\begin{aligned} f(xy^{-1}) &= (xy^{-1})^2 \\ &= (y^{-1})^2x^2 \\ &= x^2(y^{-1})^2 \\ &= f(x)f(y^{-1}) \end{aligned}$$

Since H is composed of all squares of G, then f is surjective. Given that $\ker(f) = \{x \in G : f(x) = e_H\}$, note that $f(x) = x^2$, which follows our requirement for K being the kernel holding all orders of 2 or less. Hence by the First Isomorphism Theorem, $G/K \cong H$. ■

Proof of Exercise 15: Define $G = \mathbb{Z} \times \mathbb{Z}$ and define a map $f : G \to \mathbb{Z}$ by $(a, b) \mapsto a - b$. We claim that f is a homomorphism: Given $(a, b), (c, d) \in G$

$$\begin{aligned} f((a,b)+(c,d)) &= f(a+c, b+d) \\ &= a + c - (b + d) \\ &= a - b + c - d \\ &= f(a,b) + f(c,d). \end{aligned}$$

Thus f is a homomorphism. Suppose $(a, 0) \in G$, then $f(a, 0) = a - 0 = a$, thus f is a surjective function. Given $\ker(f) = \{(a, b) \in G : f(a, b) = e_H\}$, but this is only true when $a = b$, thus we have a kernel of $K = \langle(1, 1)\rangle$. Hence by the First Isomorphism Theorem, $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 1)\rangle \cong \mathbb{Z}$. ∎

Proof of Exercise 16: Define a map of $f : GL(2, \mathbb{R}) \to \mathbb{R}^*$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$. We claim f is a homomorphism: Given $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in GL(2, \mathbb{R})$

$$\begin{aligned} f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] &= f\left[\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\right] \\ &= (ae + bg)(cf + dh) - (af + bh)(ce + dg) \\ &= ad(eh - fg) + bc(fg - eh) \\ &= (ad - bc)(eh - fg) \\ &= f\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] f\left[\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \end{aligned}$$

Thus f is a homomorphism. We claim that f is a surjective function: Given $\begin{pmatrix} \sqrt{x} & 0 \\ 0 & \sqrt{x} \end{pmatrix} \in GL(2, \mathbb{R})$, then $f\left[\begin{pmatrix} \sqrt{x} & 0 \\ 0 & \sqrt{x} \end{pmatrix}\right] = x$, thus f is surjective. We defined the $\ker(f) = \{x \in GL(2, \mathbb{R}) : f(x) = 1\}$, which the special linear group accomplishes due to the determinate equalling 1. Thus $GL(2, \mathbb{R})/SL(2, \mathbb{R}) \cong \mathbb{R}^*$. ∎

Proof of Exercise 17: Given K and N both subgroups of G with N normal in G, let $NK = \{nk \mid n \in N, k \in K\}$ be a subgroup of G that contains both K and N.
(a). Since N is normal to G, then N is also normal to NK since $k \in K$ also means $k \in G$.
(b). Given $a, b \in K$:

$$\begin{aligned} f(ab) &= Nab \\ &= NaNb \\ &= f(a)f(b). \end{aligned}$$

Thus f is a homomorphism. Given $n \in N, k \in K$, then $Nnk = Nk = f(k)$, thus f is surjective. We defined the $\ker(f) = \{x \in K : f(x) = N\}$, but note that $Nx = N$ means that also $x \in N$. Thus $K \bigcap N$ is our kernel, thus f is a surjective homomorphism with the restrictions as stated.
(c). By **(b)**, the First Isomorphism Theorem makes $K/(N \cap K) \cong NK/N$. ∎

Proof of Exercise 18: Suppose $N \trianglelefteq S_n$ such that $\text{ord}(N) = 2$. Then let $N = \{e, a\}$, then $ea = ae$, $aa = e$. Thus $N \leqslant Z(S_n)$. By the lemma provided above, since $N \leqslant Z(S_n)$, $\text{ord}(N) \leqslant \text{ord}(Z(S_n))$. Hence a contradiction. $2 \nleq 1$. Thus there is no subgroup of order 2 in n greater than 3 in S_n. ∎

Proof of Exercise 19: Given $N \leqslant S_n$ and $\sigma\tau = (1)$ for all $\sigma, \tau \neq (1) \in N$, let $N \neq (1)$ and $\sigma \neq (1) \in N$, then $\sigma\sigma = (1)$ which is order 2. Thus $\tau = \sigma$. Hence $N = (1)$ or N is cyclic of order 2. ∎

Proof of Exercise 20: Given $N \trianglelefteq S_n$ and $N \bigcap A_n = A_n$, then $A_n \subseteq N$ since N is exactly A_n or $\text{ord}(N) \geqslant \text{ord}(A_n)$. Since $\text{ord}(A_n) = n!/2$, and the order of S_n is $n!$. Hence N can either be order $n!$ or $n!/2$, which is either A_n or S_n. ∎

Chapter 10

Proof of Exercise 1: Given $K \leqslant \mathbb{Z} \oplus \mathbb{Z}$, then $(0,0) \in K$, thus by definition of H, $0 = e \in H$. Given $(a,b) \in K$, then $(a,b)^{-1} = (a^{-1}, b^{-1}) \in K$. Thus $b, b^{-1} \in H$. Since K is closed under multiplication by $(a,b)(c,d) = (ac, bd) \in K$, then H is also closed under multiplication since given $b, d \in H$, $bd \in H$. ■

Proof of Exercise 2: **(a).** Given G is an abelian groups and T is the torsion subgroup, then $e \in T$ since the identity has finite order of 1. Given $a \in T$, $a^{-1} \in T$ since the inverse has the same order as a. $(a^{-1})^{|a|} = (a^{|a|})^{-1} = e^{-1} = e$. Given $a, b \in T$:

$$\begin{aligned}(ab)^{|a||b|} &= (a^{|a|})^{|b|}(b^{|b|})^{|a|} \\ &= e^{|b|}e^{|a|} \\ &= e\end{aligned}$$

Thus $ab \in T$.

(b). Given $0 \neq Ta \in G/T$, then suppose $a \notin T$ and Ta has finite order m. $(Ta)^m = Ta^m = e$. Thus $a^m = e$ so $a \in T$. Thus $a \in T$, a contradiction arose. Hence all nonzero element of the quotient group G/T have infinite order ■

Proof of Exercise 3: The isomorphism types of abelian groups are:

1. 2^5
2. $2^4 \times 2$
3. $2^3 \times 2^2$
4. $2^3 \times 2 \times 2$
5. $2^2 \times 2^2 \times 2$
6. $2^2 \times 2 \times 2 \times 2$
7. $2 \times 2 \times 2 \times 2 \times 2$

The representatives for each respectively of these are:

1. $\mathbb{Z}_{32}$
2. $\mathbb{Z}_{16} \times \mathbb{Z}_2$
3. $\mathbb{Z}_8 \times \mathbb{Z}_4$
4. $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
5. $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
6. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
7. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

■

Proof of Exercise 4:

$$\begin{aligned}2,2,2,8,9,5,5 \to 2,2,2,2^3,3^2,5,5 \\ \implies d_1 = 2^3 \cdot 3^2 \cdot 5 = 360 \\ 2,2,2,5 \implies d_2 = 2 \cdot 5 = 10 \\ 2,2 \implies d_3 = 2\end{aligned}$$

Thus

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{360} \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_2$$

■

Proof of Exercise 5: Given $G = A_5$.
(a).

$$\begin{aligned} 5 &\implies (12345) \\ 5_2 &\implies (12354) \\ 3+1+1 &\implies (123)(4)(5) \\ 2+2+1 &\implies (12)(34)(5) \\ 1+1+1+1+1 &\implies (1) \end{aligned}$$

(b).

$$\begin{aligned} 5 &\implies 5!/10 = 12 \\ 5_2 &\implies 5!/10 = 12 \\ 3+1+1 &\implies 5(4) = 20 \\ 2+2+1 &\implies 5!/2^3 = 15 \\ 1+1+1+1+1 &\implies 1 \end{aligned}$$

Note that we needed to split 5 into two different subgroups due to $24 \nmid 60$. In all summed up, these elements equal 60, which is the total element of A_5.

(c). The size of the centralizer for each element in part (a) is associated with the number of elements above, except for the identity, which is the size of the center.

(d).

$$\text{ord}(G) = \text{ord}(Z(G)) + [G : C_G(12345)] + [G : C_G(12354)] + [G : C_G(123)] + [G : C_G(12)]$$

■

Proof of Exercise 6: Given K is a Sylow p-subgroup of G and N, which N is also a normal subgroup of G, then suppose K is normal to N. Since K is normal to N, then K is the only Sylow p-subgroup to N by the corollary of the Second Sylow Theorem. Let $N = gNg^{-1}$, then $gKg^{-1} \leqslant N$, which is also a Sylow p-subgroup. Since K is normal and a Sylow p-subgroup, then it must be the only subgroup of this kind, thus $K = gKg^{-1}$. Hence $K \trianglelefteq G$. ■

Proof of Exercise 7: **(a).** Given N is a normal subgroup of G, and C is the conjugacy class of a in G, then:
$(\impliedby)$. suppose $C \subseteq N$. Let $C := \{b \in G : gbg^{-1} = a\}$, then since conjugacy classes are symmetric, it is also the case that $gag^{-1} = b$, thus $a \in C$. Hence $a \in N$.
$(\implies)$. Suppose $a \in N$, then let $N := \{n \in G : \forall x \in G,\ n, m \in N, xnx^{-1} = m\}$. Since $xaa^{-1} = m$, then by the equivalence class of C, we have that $m \sim a$. Hence $C \subseteq N$, as we have all relationships such that $C \ni ymy^{-1} = a$.

(b). Suppose C_i is the conjugacy class of $c \in G$. By the previous part, we have learned if $c \in N$, then $C_i \subseteq N$. However, by the contrapositive, if $C_i \nsubseteq N$, then $c \notin N$, thus C_i and N are disjoint sets.

(c). The class equation of G, is $|Z(N)| + \sum_{i=1}^{j} \text{ord}(C_i)$. If C_i is not in N, then we can rearrange these terms such that $k \leqslant j$ such that $\bigcup_{i=1}^{k} C_i = N$. Since N is only comprised of conjugations of elements in G. By part **(b)**, we have that either these conjugation classes are a subset of N or the intersects resulting in the empty set. Thus by definition of a normal subgroup, we have that this class equation: $\sum_{i=1}^{k} \text{ord}(C_i) = \text{ord}(N)$ must hold true. ■

Proof of Exercise 8: Given $N \neq \langle e \rangle$ is a normal subgroup of G and $\text{ord}(G) = p^n$, then $\text{ord}(N) = p^k$ such that $k \leqslant n$. Due to Theorem 9.21, since N is made of Conjugacy classes, which we learned in our previous proof of Exercise 7, then there must be some $p^k | \text{ord}(G) = p^n$. Then it follows that there is some $e \neq a \in N$ such that $gag^{-1} = a$, thus $a \in Z(G)$. Hence $N \cap Z(G) \neq \langle e \rangle$ ■

Proof of Exercise 9: Given that $N(N(K))$ results in all $x \in N(N(K))$ such that $xN(K)x^{-1} = N(K)$, since $N(K) = K$. Hence $N(N(K)) = N(K)$. ■

Proof of Exercise 10: Given $\text{ord}(G) = p^n$, suppose $k = 1$, then a subgroup of $p^{k-1} = p^{1-1} = p^0 = 1$ is $\{e\}$. Assume that all $1 \leqslant i \leqslant k$ is true, and let $i = k + 1$. By Theorem 9.27, either $\text{ord}(Z(G)) = p^n$ or $\text{ord}(Z(G)) < p^n$. If this is the case, then $\text{ord}(G/Z(G)) = p^{n-k+1}$ which we can then take the normal subgroup $N/Z(G)$ which has order p^{n-1} due to induction since by Exercise 12, N is also a normal subgroup of G. Hence G has a normal subgroup of order p^{n-1}. ■

Proof of Exercise 11: A group of order 30 has the elementary divisors of $2, 3, 5$. If we are to take divisors of such an order, we get $1, 2, 3, 5, 6, 10, 15, 30$, but numbers of the form $1 + 2k$ are $1, 3, 5, 7, 9, 11, 13, 15$, which have a common number list of $1, 3, 5, 15$. If there is exactly one Sylow 2-subgroup, then this must be normal and, thus cannot be simple. Thus there are at least three Sylow 2-subgroups. Similarly, if we are to take $1 + 3k = 1, 4, 7, 10, 13, 16$ which have a common list of $1, 10$, which means there is at least 10 Sylow 3-subgroups. For $1 + 5k = 1, 6, 11, 16$, which result in at least 6 Sylow 5-subgroups. Since these subgroups are all disjoint, then there are exactly $m(p-1)$ elements of each order, where m is the number of minimum Sylow p-subgroups which result in $3, 20, 24$ elements. These added up result in a total of 47 elements of prime order, which is not 30. Thus a simple group of order 30 is not possible. ■

Proof of Exercise 12: Given K is a Sylow p-subgroup and N is normal to G, by Lagrange's Theorem and Exercise 15, we have that $[N : K \cap N] = [KN : K]$. Thus $[G : K] = [G : KN][KN : K]$. Then $[KN : K] \mid [G : K]$ which $[G : K]$ is not divisible by p, by the definition of Sylow p-subgroups. Thus $p \nmid [N : K \cap N]$, thus $K \cap N$ is a Sylow p-subgroup of N. ■

Chapter 11

Proof of Exercise 1: Given $\mathbb{K}$ is a splitting field of $f(x)$ over $\mathbb{F}$, suppose $u_1, \ldots, u_n \in \mathbb{K}$ be roots of f over $\mathbb{F}$. Then since K is a splitting field of $f(x)/\mathbb{F}$, then $K = \mathbb{F}(u_1, \ldots, u_n)$. Thus $\mathbb{F} \subseteq \mathbb{F}(u_1) \subseteq \mathbb{F}(u_1, u_2) \subseteq \ldots \subseteq \mathbb{F}(u_1, \ldots, u_n)$. Since $[\mathbb{K} : \mathbb{F}] = [\mathbb{F}(u_1) : \mathbb{F}][\mathbb{K} : \mathbb{F}(u_1)]$ and $[\mathbb{K} : \mathbb{F}]$ is prime, then if $[\mathbb{F}(u_1) : \mathbb{F}]$ is 1, then $\mathbb{F} = \mathbb{F}(u_1)$, which is a contradiction since u_1 is supposed to be an extension of $\mathbb{F}$. Thus $[\mathbb{K} : \mathbb{F}(u_1)]$ is 1, hence $\mathbb{K} = \mathbb{F}(u_1) = \mathbb{F}(u)$, given $u_1 = u$. ■

Proof of Exercise 2:

$$\begin{aligned} x^4 + 1 &= (x^2 - i)(x^2 - i) \\ &= (x - \sqrt{i})(x + \sqrt{i})(x - \sqrt{-i})(x + \sqrt{-i}) \qquad = (x - e^{i\pi/4})(x + e^{i\pi/4})(x - e^{3i\pi/4})(x + e^{3i\pi/4}) \\ &\implies \mathbb{Q}(e^{i\pi/4}) \\ &\implies \mathbb{Q}(i, \sqrt{2}) \end{aligned}$$

■

Proof of Exercise 3:

$$\begin{aligned} x^4 - 2 &= (x - 2^{1/4}e^{i\pi/4})(x - 2^{1/4}e^{3i\pi/4})(x - 2^{1/4}e^{5i\pi/4})(x - 7^{1/4}e^{i\pi/4}) \\ &\implies \mathbb{Q}(2^{1/4}, i) \\ &\implies \mathbb{R}(i) \end{aligned}$$

■

Proof of Exercise 4: **(a).** Given $f(x) = cx^n \in F[x]$ and $g(x) = b_0 + b_1x + \cdots + b_kx^k \in F[x]$, then:

$$\begin{aligned}
D(f(x)g(x)) &= D[(cx^n)(a_0 + a_1x + \ldots + a_kx^k)] \\
&= D[(ca_0x^n + ca_1x^{n+1} + \ldots + ca_kx^{n+k})] \\
&= nca_0x^{n-1} + (n-1)ca_0x^n + \ldots + (n+k)ca_kx^{n+k-1} \\
&= nca_0x^{n-1} + nca_1x^n + ca_1x^n + \cdots + nca_kx^{n+k-1} + kca_kx^{n+k-1} \\
&= ncx^{n-1}\left(a_0 + a_1x + \cdots + a_kx^k\right) + \left(ca_1x^n + \cdots + kca_kx^{n+k-1}\right) \\
&= ncx^{n-1}\left(a_0 + a_1x + \cdots + a_kx^k\right) + cx^n\left(a_1 + \cdots + ka_kx^{k-1}\right) \\
&= Df(x)g(x) + f(x)Dg(x).
\end{aligned}$$

(b). Given $f(x), g(x)$ are any polynomials in $F[x]$, then:

$$f(x) = a_0 + a_1x + \ldots + a_mx^m,$$

$$g(x) = b_0 + b_1x + \ldots + b_nx^n$$

$$\begin{aligned}
D(f(x)g(x)) &= D\left[(a_0 + a_1x + \ldots + a_mx^m)(b_0 + b_1x + \ldots + b_nx^n)\right] \\
&= D\left[a_0(b_0 + b_1x + \ldots + b_nx^n) + a_1x(b_0 + b_1x + \ldots + b_nx^n) + \ldots + a_mx^m(b_0 + b_1x + \ldots + b_nx^n)\right. \\
&= D\left[a_0(b_0 + b_1x + \ldots + b_nx^n)\right] + D\left[a_1x(b_0 + b_1x + \ldots + b_nx^n)\right] + \ldots + D\left[a_mx^m(b_0 + b_1x + \ldots + b_nx^n)\right] \\
&= Da_0(b_0 + b_1x + \ldots + b_nx^n) + D(a_1x)(b_0 + b_1x + \ldots + b_nx^n) + (a_1x)D(b_0 + b_1x + \ldots + b_nx^n) + \ldots + \\
&D(a_mx^m)(b_0 + b_1x + \ldots + b_nx^n) + (a_mx^m)D(b_0 + b_1x + \ldots + b_nx^n) \\
&= (a_0 + a_1x + \ldots + a_mx^m)D(b_0 + b_1x + \ldots + b_nx^n) + D\left[(a_1x) + \ldots + (a_mx^m)\right](b_0 + b_1x + \ldots + b_nx^n) \\
&= f(x)Dg(x) + Df(x)g(x)
\end{aligned}$$

■

Proof of Exercise 5: Given $f(x) \in F[x]$ and n is a positive integer, then let:

$$Df(x)^n = nf(x)^{n-1}Df(x)$$

Let's take a couple of steps to see if we notice a pattern. If $n = 1$, then:

$$\begin{aligned}
Df(x)^1 &= f(x)^0Df(x) \\
&= Df(x).
\end{aligned}$$

Which is true. If we let $n = 2$, then:

$$Df(x)^2 = 2f(x)Df(x)$$

Which followed our definition of a derivative. We now can hypothesize, in fact, an Induction Hypothesis, that $Df(x)^n = nf(x)^{n-1}Df(x)$ where $n \in \mathbb{N}$. Define

$$S := \{n \in \mathbb{N} : Df(x)^n = nf(x)^{n-1}Df(x)\}.$$

We have proven two base cases, therefore we know $1, 2 \in S$. Now suppose $k \in S$, our goal is to show $k + 1 \in S$. Assume $n = k$, and note that due to the product rule from the previous exercise, we have that:

$$\begin{aligned}
D[f(x)^k \cdot f(x)] &= kf(x)^{k-1}D[f(x)]f(x) + f(x)^kD[f(x)] \\
&= kf(x)^kD[f(x)] + f(x)^kD[f(x)] \\
&= (k+1)f(x)^kD[f(x)] \\
&= D[f(x)^{k+1}]
\end{aligned}$$

Hence $(k + 1) \in S$ by PMI. ■

Proof of Exercise 6: ($\Longrightarrow$). If. $u \in \mathbb{K}$ is a repeated root of $f(x) \in \mathbb{F}[x]$, then for some $n > 1$ and $g(x) \in \mathbb{K}[x]$ we have

$$f(x) = (x-u)^n g(x)$$

Thus:

$$Df(x) = n(x-u)^{n-1} g(x) + (x-u)^n Dg(x).$$

Note that $Df(u) = 0$, thus u is a root of $Df(x)$, thus a repeated root of $f(x)$ and $Df(x)$.

($\Longleftarrow$). Given u is a root of both $f(x)$ and $f'(x)$, then $f(x) = (x-u)g(x)$. Thus:

$$Df(x) = (x-u)Dg(x) + g(x).$$

Since u is a root of both, then $Df(u) = 0$. Thus $g(u) = (x-u)h(x)$ for some $h(x)$. Thus $Df(x) = (x-u)^2 h(x)$. Hence u is a repeated root. ■

Proof of Exercise 7: ($\Longrightarrow$). Given $f(x) \in F[x]$ is separable, then $f(x)$ has no multiples roots in $\mathbb{F}[x]$. Suppose $f(x), Df(x)$ are not relatively prime, then utilizing the previous exercise we have that

$$\begin{aligned} Df(x) &= (x-u)Dg(x) + g(x) \\ f(x) &= (x-u)^2 h(x), \end{aligned}$$

for some $h(x)$ and $g(x) \in \mathbb{F}[x]$. Thus it is shown that u is a multiple root of $f(x)$, thus a contradiction. Hence $f(x)$ and $Df(x)$ are relatively prime.

($\Longleftarrow$). Given $f(x)$ and $f'(x)$ are relatively prime, suppose u is a multiple root of $f(x) \in \mathbb{F}[x]$. Then:

$$f(x) = (x-u)^n g(x)$$

over splitting field $\mathbb{K}$. Thus

$$Df(x) = n(x-u)^{n-1} g(x) + (x-u)^n Dg(x).$$

Then it contradicts that u is a multiple root since $f(x)$ and $Df(x)$ are relatively prime. Hence $f(x)$ is separable. ■

Proof of Exercise 8: ($\Longrightarrow$). Given $p(x)$ is separable, then by the previous exercise, it is relatively prime. Thus $Dp(x)$ is a irreducible polynomial, hence $Dp(x) \neq 0_F$.

($\Longleftarrow$). Given $Dp(x) \neq 0_F$, then $p(x)$ is irreducible and $Dp(x)$ has a lesser degree. Thus $p(x)$ is relatively prime. Hence, separable. ■

Proof of Exercise 9: Let $\ell = \tau H \tau^{-1}$.

(a). Given $\tau \in G$ is a automorphism, let $\sigma \in \tau H \tau^{-1}$ be an element that fixes $\sigma(x) = x$ for all $x \in \tau(\mathbb{K})$. Because we have that $\mathbb{K}$ is a fixed field of H, then $\tau^{-1}(x) = x$. Since x is fixed by every element of H, then it must be the case that also $h(x) = x$ for all $x \in \mathbb{K}$. Thus $\sigma(x) = \tau(x)$ for all $x \in \tau(\mathbb{K})$. Hence $\mathrm{Inv}(\tau H \tau^{-1}) = \tau(\mathbb{K})$.

(b). ($\Longrightarrow$). Given H is normal in G, then for all $\tau \in G$, we have that $\tau H \tau^{-1} = H$, due to the definition of normal subgroup. What we have established in part **(a)** is that $\mathrm{Inv}(\tau H \tau^{-1}) = \tau(\mathbb{K})$. Since H is normal;, then we have that $\mathrm{Inv}(H) = \mathbb{K} = \tau(\mathbb{K})$.
($\Longleftarrow$). Given for all $\tau \in G$, if $\tau(\mathbb{K}) = \mathbb{K}$, then suppose by part **(a)**, we have that $\mathrm{Inv}(\tau H \tau^{-1}) = \tau(\mathbb{K})$. Thus since we have by the definition of $\mathbb{K}$, that $\tau(\mathbb{K}) = \mathbb{K}$, then we must have that $\mathrm{Inv}(\tau H \tau^{-1}) = \mathbb{K}$. Thus ℓ fixes every element of $\mathbb{K}$. Since $\mathbb{K}$ is the fixed field of H, it only naturally follows that H is normal to G.

(c). Given for all $\tau \in G$ and $\tau(\mathbb{K}) = \mathbb{K}$ and $u \in \mathbb{K}$ such that $f(X)$ be its minimal polynomial, then suppose since $u \in \mathbb{K}$, then all the conjugates of u: $u_1, u_2, U_3, \ldots, u_\tau$ are also in $\mathbb{K}$ under the action of G. If $f(x)$ splits linear factors into a splitting field $\mathbb{E}$ over $\mathbb{F}[x]]$, then $f(x) = (x-u_1)(x-u_2)\ldots(x-u_\tau)$. Since $\mathbb{K}$ is the

fixed field of H, then if $\tau \in H$, then $\tau(u) = u$ for all $u \in \mathbb{K}$. Hence $f(x)$ is fixed under for all $h \in H$. Thus all roots of $f(x)$ are also in $\mathbb{K}$. Hence, $f(x)$, a minimal polynomial of u splits in $\mathbb{K}$.

(d). Given H is normal over G, then since a field extension $\mathbb{E}/\mathbb{F}$ is galois if and only if it is normal and separable, then it must be the case that since H is normal in G, then every conjugate of $k \in \mathbb{K}$ under action G is also in $\mathbb{K}$. Thus $\mathbb{K}$ has all of it's conjugates, thus $\mathbb{K}$ is normal over $\mathbb{F}$. For all $a \in \mathbb{K}$, by the last part, we have shown that $f(x)$ splits into linear factors in $\mathbb{K}$, implying that $f(x)$ has distinct roots in $\mathbb{K}$. Thus $\mathbb{K}$ is separable over $\mathbb{F}$. Hence $\mathbb{K}$ is normal and separable over $\mathbb{F}$. Hence $\mathbb{K}$ is galois over $\mathbb{F}$.

(e). Given that for all elements $u \in \mathbb{K}$, the minimal polynomial of u splits in $\mathbb{K}$, then suppose for some $\tau \in G$, let $u \in \mathbb{K}$ also be arbitrary. If minimal polynomial $f(x)$ of u splits in $\mathbb{K}$, then by part **(c)**, all of its roots are also in $\mathbb{K}$. Hence $\tau(u) \in \mathbb{K}$ for all $u \in \mathbb{K}$. Since, τ is an automorphism. Then it follows that $\tau(\mathbb{K}) \subseteq \mathbb{K}$. If for some $v \in \mathbb{K}$, we have $\mathbb{K}$ is the fixed field of H, then for any $\sigma \in H$, we have that $\sigma(v) = v$. Since τ is a automorphism and H is a subgroup of G, then we also have by part **(b)** that H is normal to G, thus $\tau H \tau^{-1} = H$ meaning $\tau^{-1} H \tau$. Hence $\tau^{-1}(H) = H$. Thus $\tau^{-1}(v) = v$, implying that $\tau(v) = v$, due to bijectivity. Thus $\mathbb{K} \subseteq \tau(\mathbb{K})$. Hence for all $\tau \in G$, $\tau(\mathbb{K}) = \mathbb{K}$.

(f). Given that $\mathbb{K}$ is galois over $\mathbb{F}$, then since a field extension $\mathbb{E}/\mathbb{F}$ is galois if and only if $\mathbb{E}$ is the splitting field of some separable polynomial in $\mathbb{F}[x]$. As we have stated earlier in part **(d)**, since a field is galois if and only if it normal and separable, we have the quality that $\mathbb{K}$ is normal a separable over $\mathbb{F}$. Let for some $\tau \in G$, for all u of $f(x)$ in $\mathbb{K}$, we have that it's conjugates under G are also in $\mathbb{K}$ since $\mathbb{K}$ is also normal. By the previous part, we have that for these circumstances of a minimal polynomial of u splits in $\mathbb{K}$, then we must have $\tau(\mathbb{K}) = \mathbb{K}$ for all $\tau \in G$. Since H and also $\ell = \tau H \tau^{-1}$, then by part **(b)**, if H is normal in G, then we must have for all $\tau \in G$, then since $\tau(\mathbb{K}) = \mathbb{K}$. Since $\tau(\mathbb{K}) = \mathbb{K}$, we have that $\ell = H$. Hence H is normal in G.

(g). Given $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ and the definition of $\sigma \mid_{\mathbb{K}}$, then suppose $\mathbb{K}$ is galois over $\mathbb{F}$. If σ is an automorphism of $\mathbb{E}/\mathbb{F}$, then it fixes $\mathbb{F}$. Thus if $a, b \in \mathbb{K}$ such that $a = b$ if and only if $\sigma(a) = \sigma(b)$ if and only if $\sigma \mid_{\mathbb{K}} (a) = \sigma \mid_{\mathbb{K}} (b)$, because a and b are fixed by σ since it is an automorphism fixing $\mathbb{E}$ over $\mathbb{F}$. Thus it is well defined and injective. If $\sigma \mid_{\mathbb{K}} (a + b) = \sigma(a + b) = \sigma(a) + \sigma(b) = \sigma \mid_{\mathbb{K}} (a) + \sigma \mid_{\mathbb{K}} (b)$, and likewise we have that $\sigma \mid_{\mathbb{K}} (ab) = \sigma(ab) = \sigma(a)\sigma(b) = \sigma \mid_{\mathbb{K}} (a) \sigma \mid_{\mathbb{K}} (b)$. Thus it is closed under addition and multiplication as a homomorphism. Since $\sigma \mid_{\mathbb{K}}$ is a homomorphic injective function, and also since $\mathrm{Im}(\sigma \mid_{\mathbb{K}}) = \mathbb{K}$, then it is also surjective. Thus $\sigma \mid_{\mathbb{K}}$ is an automorphism of $\mathbb{K}$ over $\mathbb{F}$. Thus $\sigma \mid_{\mathbb{K}} \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$.

(h). Given $\mathbb{K}$ is galois over $\mathbb{F}$, then let $\sigma, \tau \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, such that $(\sigma \circ \tau) \mid_{\mathbb{K}} = \sigma(\tau(\mathbb{K})) = \sigma \mid_{\mathbb{K}} \circ \tau \mid_{\mathbb{K}}$ for all $\sigma, \tau \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. Thus $\sigma \to \sigma \mid_{\mathbb{K}}$ is a homomorphism from $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ to $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$.

(i). Let $\mathbb{L} = \ker(\sigma \to \sigma \mid_{\mathbb{E}})$. Given $\mathbb{K}$ is galois over $\mathbb{F}$, then let $\tau \in \mathrm{Aut}(\mathbb{E}/\mathbb{K})$. For all $u \in \mathbb{K}$, let $\tau(u) = u$. Thus τ is a identity map on $\mathbb{K}$, thus $\tau \in \mathbb{L}$ for all $\tau \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$. If $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ be in the kernel $\mathbb{L}$, then $\sigma(u) = u$, for all $u \in \mathbb{K}$. Thus $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{K})$. Since every element in $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ is in $\mathbb{L}$, and every element in $\mathbb{L}$ is in $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$, then it must be that $\mathbb{L} = \mathrm{Aut}(\mathbb{E}/\mathbb{K})$.

(j). Given $\mathbb{K}$ is galois over $\mathbb{F}$, and given theorem 11.14, since $\mathbb{K}$ is the splitting field of some seperable polynomial $f(x)$ over $\mathbb{F}$. Let $\mathbb{L}$ be the splitting field of $\sigma f(x)$ over $\mathbb{E}$. Suppose $\phi : \mathbb{K} \to \mathbb{L}$ defined by Theorem 11.14, then $\mathbb{L}$ is a splitting field of $\sigma f(x)$ over $\mathbb{E}$, then let $\psi : \mathbb{E} \to \mathbb{E}$, where ψ is the identity on $\mathbb{F}$ and maps $\mathbb{K} \to \mathbb{L}$ in an isomorphism. For all $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$, let $\tau = \psi \circ \sigma \circ \psi^{-1}$, as a conjugation by functions. Since τ fixes $\mathbb{F}$ and maps $\mathbb{K}$ to itself, then for all $u \in \mathbb{K}$, we have that $\tau(u) = \psi(\sigma(\psi^{-1}(u))) = \psi(\sigma(\phi(\psi^{-1}(u)))) = \psi(\sigma(u) = \sigma(u)$. Thus $\tau \mid_{\mathbb{K}} = \sigma$. Hence for all τ of $\mathbb{K}$ over $\mathbb{F}$, there exists some $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ such the mapping of the homomorphism $\sigma \to \sigma|_K$ from the group $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ to the group $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ is surjective.

(k). Given $\mathbb{K}$ is galois over $\mathbb{F}$ and the first isomorphism theorem, since we have a surjective homorphism $\phi : G \to \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ defined by $\sigma \mapsto \sigma \mid_{\mathbb{K}}$. Then by the first isomorphism theorem, $G/\ker(\phi) \cong \mathrm{Aut}(\mathbb{K}/\mathbb{F})$. Since we know from part **(i)**, $\ker(\phi) = \mathrm{Aut}(\mathbb{E}/\mathbb{K})$, then by the fundamental theorem of galois, $\mathrm{Aut}(\mathbb{E}/\mathbb{K}) \cong G/H$. Hence $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \cong G/H$ ∎