Modern Algebra and Geometry

Sriaditya Vedantam

Modern Algebra and Geometry

Sriaditya Vedantam
svedantam@zyphensvc.com

It has definitely been an eventful semester 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 semester, 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 semester 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.

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.

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 $\operatorname{Im} a = b$ written as $f(a)$. **Images** mean the range of the function. The **domain** of f is written as $\operatorname{dom} f$, 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 $S = \mathbb{Z}^{\geqslant 0}$. ■

1.5.1 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 1.5.2 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.

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 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 Z, a + b = b + a.
4. Associative Law: For all a,b,c Z, (a + b) + c = a + (b + c).
5. There exists a zero element 0 Z, called the additive identity, satisfying 0 + a = a for any a Z.
6. For all a Z, there exists a unique additive inverse, -a Z, satisfying a + (-a) = 0

Definition 2.1.2: Multiplicative Properties

Multiplication is well-defined. Given a,b Z, a · 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 Z, a · b Z.

Commutative Law: For all a,b Z, ab = ba.

Associative Law: For all a,b,c Z, (ab)c = a(bc)

1 Z is the multiplicative identity, satisfying 1 · a

Definition 2.1.3: Distributive Property

For all a,b,c 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 $n \in \mathbb{N}$ is true for all $n \in \mathbb{Z}$.

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 $p_1 = q_1 \ldots q_k, p_1$ prime, all q_i prime. So $s = 1, p_1 = q_1$.

Proof of Uniqueness: Assume uniqueness for k, prove for $k+1$. Suppose $n = p_1 \ldots p_r = q_1 \ldots q_s$, $min\{r, s\} = k + 1$, as we can assume that $r = k + 1$. Then $p_1 \ldots p_k p_{k+1} = q_1 \ldots q_s$. So $p_1 q_1 \ldots q_s$, assume $p_1 = q_1$. So $p_1 = -q_1, q_1$. Then let's replace this singular prime, $p_1 \ldots p_{k+1} = (p_1)q_2 \ldots q_s$. Then $p_1(p_2 \ldots p_{k+1}) = p_1(q_2 \ldots q_s)$. 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 $q_i = p_i$ 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

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 $m > k$.

$$\begin{aligned} u^m - u^k &= 0 \\ u^k(u^{m-k} - 1) &= 0 \end{aligned}$$

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

$$\begin{aligned} u^{m-k} - 1 &= 0 \\ u^{m-k} &= 1 \\ u(u^{m-k-1}) &= 1 \\ u^{-1} &= u^{m-k-1}. \end{aligned}$$

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. ■

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

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

Theorem 6.1.6 First Isomorphism Theorem

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

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

$$\begin{aligned} \phi(r) - \phi(s) &= 0 \\ \phi(r - s) &= 0. \end{aligned}$$

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 $s \in \operatorname{Im} \phi$, 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,

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

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 $\mathbb{Q}[r] = \mathbb{Q}(r)$. ■

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.

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

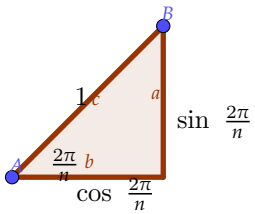
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

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. Suppose $\beta \in \mathbb{Q}[x]$, then $\exists f(x) \in \mathbb{Q}[x]$ such that $\beta = f(x)$, so $\phi(f(x)) = f(\alpha) = \beta$. Q.E.D ϕ is injective if and only if $\ker \phi = \{0\}$. This is a consequence of the first isomorphism theorem.

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.

Solutions to Exercises

Chapter 1

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

$$\begin{aligned} a - c &= nb + r - nd - r \\ a - c &= n(b - d) + r - r. \end{aligned}$$

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

$$\begin{aligned} a &= nk + c \\ c &= nq + r. \end{aligned}$$

Replace the values accordingly:

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

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 10. 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 $p \mid \binom{p}{k}$. ■