MATH145 Readings

Johnson Ng

June 8, 2017

Introduction

Below is an introduction written by the author of the referred notes, Kenneth R. Davidson.

As a student entering university to study mathematics, you probably have encountered prime bumbers. Chances are great that you believe that every integer factors uniquely into a product of primes but have not seen a proof. This important fact, known as the Fundamental Theorem of Algebra, is of crucial importance in the theory of numbers. It is not easy to prove. More importantly, it is not *intuitively obvious*. Indeed, its significance is only realized with very large numbers beyond our real experience. The crucial fact that enables us to prove this with relative ease is the Euclidean Algorithm for finding greatest common divisors. The first two chapters deal with these basic properties of the integers and modular arithmetic.

It is worth noting that there are number systems not very much different from the intergers in which this unique factorization into primes fails. Far from being a disaster, this is an opportunity to investigate why this phenomena occurs. It shows us which properties of the integers themsevles are crucial to make the theory work. That is why we make a foray into quadratic number domains in chapter 3. Naturally, we merely touch the surface here as this theory lies in a rather deep connection between algebra and number theory.

A nice application of modular arithmetic is the Rivest-Shamir-Adelman (RSA) public key cryptography scheme. This code allows the author to publish the method of *encoding* a message in a public place, while keeping the method of *decoding* the message secret. This is a rather different idea of coding, as for all previously known codes, the method of decoding merely reversed the endoing method. The secret here is that it is very easy (with a computer) to find large primes (say 100-200 digits) but very difficult to factor the product of two large primes. If you believe that checking whether a number is prime involes trial division by all numbers up to the square root, it might be hard to imagine why determining if a number if prime should be any easier than finding factors. So we delve more deeply into methods used to determine whether a number is prime or composite. It quickly becomes clear that simple tests can determine beyond any doubt that a number is

composite without giving any information at all about the factors.

In chapter 5, we introduce the complex numbers. There is a tacit assumption that the student is already reasionably familiar with the real numbers from studying calculus. However, a section is devoted to a brief discussion of how the real numbers are developed. No attempt is made to separate algebra from analysis. Indeed, all of mathematics is integrated and it is foolish to pretend that there are natural walls. In particular, we prove the Fundamental Theorem of Algebra that every complex polynomial factors into a product of linear terms. In spite of its name, this is a theorem of analysis because it relies on the (topological) completeness of the complex numbers. The proof we give is one of the simplest, and relies on the Extreme Value Theorem. We also develop the complex exponential function. This again is really a theorem of analysis. But it is included because it plays such an important role in other applications of the compelx numbers.

In chapter 6, we show that the same theory applies to the algebra of polynomials. In particular, there is a Euclidean Algorithm and unique factorization into irreducible polynomials. We exanime various tests for irreducibility, and study connections with irrationality of the roots. Then we do a few special topics about real and complex polynomials such as Sturm's Theorem for counting real roots, and the formula for solving cubics. Then in chapter 7, we study finite fields in some detail. This is just doing modular arithmetic modulo an irreducible polynomial instead of modulo a prime integer. Many of the results for $\mathbb{Z}_p$ carry over to finite fields with the same ideas. A rather beautiful application of these ideas is an algorithm for factoring polynomials over the rationals. This algorithm is based on a method for factoring polynomial of degree d mod p is much easeier than factoring a d digit base p number.

Contents

List of Definitions

List of Theorems

Axioms and Principles

Chapter 1

The Integers

1.1 Basic Properties

The following list of properties is what a student taught in the 'modern' style would come up with when talking about properties of integers. We give the name Commutative Rings for sets of numbers that satisfy these properties.

Definition 1.1.1 (Commutative Rings)
A commutative ring is a set of numbers that satisfy these properties.

1. *The **integers** consist of a set $\mathbb{Z}$ together with two binary operations **addition** $(+)$ and **multiplication** $(\cdot)$*
2. *(**commutativity of addition**)* $\forall a, b \in \mathbb{Z} \quad a + b = b + a$
3. *(**associativity of addition**)* $\forall a, b, c \in \mathbb{Z} \quad (a + b) + c = a + (b + c)$
4. *(**additive identity**)* $\exists 0 \in \mathbb{Z} \ \forall a \in \mathbb{Z} \quad a + 0 = a = 0 + a$
5. *(**additive inverse**)* $\forall a \in \mathbb{Z} \ \exists (-a) \in \mathbb{Z} \quad a + (-a) = 0$
6. *(**commutativity of multiplication**)* $\forall a, b \in \mathbb{Z} \quad a \cdot b = b \cdot a$
7. *(**associativity of multiplication**)* $\forall a, b, c \in \mathbb{Z} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
8. *(**multiplicative identity**)* $\exists 1 \in \mathbb{Z} \ \forall a \in \mathbb{Z} \quad a \cdot 1 = a = 1 \cdot a$
9. *(**distributive law**)* $\forall a, b, c \in \mathbb{Z} \ (a + b) \cdot c = a \cdot c + b \cdot c$

But this does not fully distinguish integers from many other sets, for example:

1. The real numbers $\mathbb{R}$.
2. The set $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$
   See Exercise 1.1 for proof.
3. The set $\mathbb{Z} \oplus \mathbb{Z} := \{(a, b) \mid a, b \in \mathbb{Z}\}$ with coordinate-wise addition and multiplication.

Definition 1.1.2 (Ring)
A ring is a set of numbers that satisfy all properies of a commutative ring except for property 6, ***commutativity of multiplication****, and added with an additional distributive law*

$$\forall a, b, c \in \mathbb{Z} \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

Example 1.1.1
An example of a non-commutative ring is the set of 2×2 *matrices with integer entries. While addition is coordinate-wise, multiplication is defined by the rule:* $\forall a, b, c, d, w, x, y, z \in \mathbb{Z}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{bmatrix}$$

which is clearly non-commutative since

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} aw + cx & bw + dx \\ ay + cz & by + dz \end{bmatrix}$$

Example 1.1.2
Another important example is the set of integers ***modulo*** *n. Consider the ring* $\mathbb{Z}_2$ *consisting of two elements* $\{0, 1\}$ *with operations given by the tables:*

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

The above example gives us a clue about how to add further properties to our list in Definition 1.1.1 to ensure that the integers become our only example.

For instance, we declare the following property so as to distinguish many other commutative rings from the integers.

10. $\mathbb{Z}$ is generated by $\{0, 1\}$

With this, we have laid the foundations of starting our set starting with 0 and 1, then form the rest of the elements of $\mathbb{Z}$ so as to provide the *minimal* collection satisfying all our properties. In particular, since a ring is *closed* under addition and multiplication, we need all the numbers of the form $1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1, ...$

Note that such a construction ensures that the set is indeed closed under addition and multiplication. The set is closed under addition since

$$\forall a, b \in \mathbb{Z}$$
$$a + b = \underbrace{\underbrace{1 + 1 + \ldots + 1}_{\text{a many 1's}} + \underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}}_{\text{(a + b) many 1's}}$$

which thus implies that $a + b \in \mathbb{Z}$ since a ring is closed under addition. The set is closed under multiplication since

$$\begin{aligned} a \cdot b &= (\underbrace{1 + 1 + \ldots + 1}_{\text{a many 1's}}) \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) \\ &= \underbrace{1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) + 1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) + \ldots + 1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}})}_{\text{a times}} \end{aligned}$$

by the distributive law, and since each $1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) \in \mathbb{Z}$, we have, once again, that

$$a \cdot b = \underbrace{1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) + 1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}}) + \ldots + 1 \cdot (\underbrace{1 + 1 + \ldots + 1}_{\text{b many 1's}})}_{\text{a times}} \quad \in \mathbb{Z}$$

and thus our construction is closed under multiplication.

Next, in order to satisfy the **additive inverse property**, we *may* have to add in $-1, -(1+1), -(1+1+1), ...$ The proof that such a collection is enough to satisfy all the properties of a commutative ring is similar to our exercise above.

Our legwork is not done yet, since we still have, for example, $\mathbb{Z}_2$ also being generated by its 0 and 1. We can, fortunately, eliminate this group of sets by stating that $1, 1+1, 1+1+1, ...$ are all unique. If such a property holds in any ring, then the collection $S = \{1, 1+1, 1+1+1, ...\}$ will be indistinguishable from the **natural numbers** $\mathbb{N}$ (without the 0) by any mathematical property. In fact, to ensure that all the elements are distinct, it is important that none of them are 0, since for example:

$$0 = 1 + 1 + 1 + 1 \implies (1 + 1 + 1 + 1) + 1 = 1 \text{ but } (1 + 1) + (1 + 1 + 1) = 5$$

by the distributive law.

With that said, then $-S \cap S = \emptyset$, and thus $R = S \cup \{0\} \cup -S$ is a ring that has indistinguishable properties from $\mathbb{Z}$. To clarify the explanation above, we state the following as a property:

11. No nontrivial sum of 1's is equal to 0.

Some questions come into attention here (and will be hinted in Exercise 1.4 below):

1. What does it mean to say that two mathematical objects are the same?
2. What does it mean to say that two mathematical objects have the same properties?

Definition 1.1.3 (Order)
We define order as follows:

$$\begin{array}{lll} a < b & \text{if} & b - a \in \mathbb{N} \\ a = b & \text{if} & b - a = 0 \\ a > b & \text{if} & b - a \in \mathbb{N} \end{array}$$

This order satisfies some simple properties:

O1 $\forall a, b, c \in \mathbb{Z} \wedge a < b,\ a + c < b + c$

O2 $\forall a, b, c \in \mathbb{Z} \wedge a < b \wedge c > 0,\ ac < bc$

Exercises

1.1 Show that $\mathbb{Z}[\sqrt{3}]$ is a commutative ring.

1.2 Describe explicitly the ring $\mathbb{Z}[\sqrt[3]{5}]$.

1.3 What are the additive and multiplicative identities for $\mathbb{Z} \oplus \mathbb{Z}$? Show that there are non-zero elements which multiply to 0.

1.4 Consider the ring $R = \{2^n \mid n \in \mathbb{Z}\}$ with addition $\oplus$ given by $2^n \oplus 2^m = 2^{n+m}$, and multiplication $\odot$ given by $2^n \odot 2^m = 2^{nm}$. Show that this is a ring. Then show that the map taking 2^n to its logarithm base 2 (namely n) maps R one-to-one and onto $\mathbb{Z}$ and preverse addition and multiplication. We say that R is isomorphic to $\mathbb{Z}$.

1.5 What other properties of the integers can you think of? Can these properties be deduced from the ones given above?

1.6 Can an order be put on $\mathbb{Z}_2$ satisfying O1?

1.2 Well Ordering Principle

Principle 1.1 (Well Ordering Principle)
Every non-empty subset of $\mathbb{N}$ *has a least element.*

Theorem 1.2.1 (Generalized Principle of Induction)
For all integers n, let P(n) be the statement about n propositions. Suppose that proposition P(1) is true. Furthermore, suppose that if P(k) is true for $1 \leq k < n$*, then P(n) is true. Then P(n) is true for all* $n \geq 1$*.*

Proof
Let S be the set of all n such that P(n) is false. If S is empty, then we have our desired conclusion, i.e. P(n) is true for all $n \geq 1$*. Otherwise, S is non-empty. Then by the Principle of Induction, there exists an n in S such that n is the least element in S. By the hypothesis,* $n \neq 1$*. Since n is the smallest integer in S, we know that P(k) is true for all* $1 \leq k < n$ *(otherwise if there is an* $1 \leq l < n$ *such that P(l) is false, then* $l \in S \wedge l < n$ *will contradict the fact that n is the least element). But by the induction hypothesis, P(n) must be true. This contradicts that P(n) is false. Thus our assumption that S is non-empty is false. Therefore, S must be empty, and therefore P(n) is true for all* $n \geq 1$*.*

Example 1.2.1 (False Proof of Induction)
Let P(n) be the statement that every set of n people have all the same hair colour. This is evident for n = 1. Now look at larger n. Suppose that P(n - 1) is true. Given a group of n people, apply the induction hypothesis to all but the last person in the group. This group will have all the same hair colour. Now repeat this argument with all but the first person. We find that all the people have the same hair colour by combining these two facts. By induction, all people have the same hair colour.

Exercises

2.1 Find the error in the False Proof of Induction example above.

I believe the problem lies in the execution of "Now repeat this argument with all but the first person". The problem is that if the last person has a different hair colour, then the base case would have been false from the beginning, thus rendering the entire induction to be false.

2.2 Prove by induction that

$$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i \right)^2 .$$

The base case is true and easily verifiable, since $1^3 = (1)^2 = 1$. Now suppose that for all k where $1 \leq k < n$ such that

$$\sum_{i=1}^{k} i^3 = \left(\sum_{i=1}^{k} i \right)^2$$

is true. Now consider the case n = k + 1. Then

$$\begin{aligned}\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 \\ &= \left(\sum_{i=1}^{k} i\right)^2 + (k+1)^3 \\ &= \left(\sum_{i=1}^{k} i\right)^2 + k^3 + 3k^2 + 3k + 1\end{aligned}$$

$$\begin{aligned}\left(\sum_{i=1}^{k+1} i\right)^2 &= \left(\sum_{i=1}^{k} i + k + 1\right)^2 \\ &= \left(\sum_{i=1}^{k} i\right)^2 + 2(k+1)\left(\sum_{i=1}^{k} i\right) + (k+1)^2 \\ &= \sum_{i=1}^{k} i^3 + (k+1)\left(\sum_{i=1}^{k} 2i + k + 1\right)\end{aligned}$$

So

$$\sum_{i=1}^{k+1} i^3 - \left(\sum_{i=1}^{k+1} i\right)^2 = (k+1)^3 - 2(k+1)\left(\sum_{i=1}^{k} i\right) - (k+1)^2$$

2.3 Consider the Fibonnaci sequence, given by F(0) = F(1) = 1, and for $n \geq 0$, F(n + 2) = F(n) + F(n + 1). Let $r = (\sqrt{5}+1)/2$. Prove by induction that

$$F(n) = \frac{r^{n+1} - (\frac{-1}{r})^{n+1}}{\sqrt{5}}.$$

2.4 Define a sequence of real numbers by the rules

$$s_0 = 0 \quad \text{and} \quad s_{n+1} = \sqrt{3 + s_n} \text{ for } n \geq 0$$

(a) Show by induction that $s_n < s_{n+1} < 3$ for all $n \geq 0$.

(b) The least upper bound principle (chapter 5) shows that the sequence has a limit. Show that the limit should be $\sigma = \frac{1+\sqrt{13}}{2}$.

(c) Obtain a formula for $\sigma - s_{n+1}$ in terms of $\sigma - s_n$. Hence prove by induction that $0 < \sigma - s_n < \frac{3}{4^n}$ for all $n \geq 0$.