

MTH 311
Introduction
to
Higher Mathematics

Dr. Adam S. Sikora
based on notes of dr. Michael Cowen.

0. PREFACE FOR THE TEACHER BY A.S. SIKORA

These notes follow the traditional development of numbers, starting with Peano's Axioms for naturals and then successive definitions of integers, rationals, reals, and complex numbers. Students learn a variety of topics along the way: Fibonacci numbers and other recursive series, equivalence relations, Fermat's Little Theorem, Fermat's Last Theorem, Twin Prime and Goldbach's Conjectures. Additionally, there is a number of more advanced topics presented, like Russel's Paradox, fractals, Cantor's Hypothesis and its independence from Peano's axioms, algebraic and transcendental numbers, cardinal numbers.

Finally, some rudimentary notions of algebra are introduced: a ring (including $\mathbb{Z}[\sqrt{d}]$, rings of functions, rings of matrices) and a field, including $\mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{R}, \mathbb{C}$ as examples. Our hope is to use this course as a gentle introduction into some topics of current mathematical research. A significant number of proofs and examples is included in the notes.

The sections are presented in chronological order as taught by me in Fall 2009, except that fractals were presented at the very end of the course. One may consider moving sets ahead of Peano's axioms and, furthermore, replacing Peano's axioms by a set theory definition of natural numbers.

Finally, it may be desirable to add a section on infinite sequences and series, including the monotonic sequence convergence principle as an application of the least upper bound principle, as M. Cowen does. (We didn't find enough time for that.)

1. PREFACE FOR THE STUDENT BY M. COWEN

This booklet is an outline of the material presented in MTH 311 Introduction to Higher Mathematics, together with problem sets on each section. It is designed to be used in conjunction with the lecture material in MTH 311.

Notice the emphasis on *precision*. Mathematics is a precise language. It matters what the inverse image $f^{-1}(Y)$ of a set *means*; students will not be able to do any of the problems involving the inverse image of a set if they do not know what the inverse image is.

To get the most from this course, you need to accomplish at least the following 2 tasks:

(1) LEARN THE DEFINITIONS THOROUGHLY

- Memorize each definition.
- Go over each definition, giving examples and non-examples, until you understand the idea behind the definition.
- Review each definition, its meaning, its examples, and its non-examples, until you can recite all this information *in your sleep*.

(2) LEARN THE PROPOSITIONS AND THE IDEAS BEHIND THEM THOROUGHLY

- Memorize the statement of each proposition (theorem, lemma, corollary).
- Go over each proposition until you understand the central idea behind it.
- Learn the flow of the proof: what comes first, what comes last.
- Memorize the central ideas behind the proofs. Do not memorize proofs.
- Work through a proof of each proposition *while* referring to your lecture notes.
- Work through a proof of each proposition *without* referring to your lecture notes.

Neither of these tasks is easy. You may find that flashcards of definitions and propositions are a useful tool. Practice and repetition will make the tasks easier. The purpose of this outline is to provide a place to start. Together with the lecture notes, it specifies what you need to know.

The problems vary from easy (follows directly from a definition or proposition) to sophisticated (requires an idea you have to come up with on your own). Don't expect to look at a problem and solve it immediately, as you may have done with most calculus problems. If you can't solve a problem immediately, come back to it after a few hours or the next day. In the meanwhile, go

on to the next problems; often they will not be linked together. Note this means that you need to start doing the homework assignments early, to give yourself enough time to think.

CONTENTS

0. Preface for the teacher by A.S. Sikora	1
1. Preface for the student by M. Cowen	1
2. Basic Logic	4
3. Sets	8
4. Functions	12
5. Inverse Functions	14
6. Natural Numbers	16
7. Integers	20
8. More Induction	22
9. Divisibility	27
10. Binary Relations	34
11. Rational Numbers	36
12. Real Numbers	39
13. Largest Lower and Least Upper Bounds	44
14. Additional Topics on Real Numbers: Archimedean Principle, Density	46
15. Monotone Sequence Property	48
16. Decimal Expansions	50
17. Rings and Fields	52
18. Complex Numbers	56
19. Application of Complex Numbers: Fractals	58
20. Equivalence of sets	59
21. Algebraic Numbers	63
22. Cardinal Numbers	65

2. BASIC LOGIC

Definition 2.1 (Statement). A statement P is a sentence that is either true or false (but not both).

For example, “Chickens are birds” is a statement.

However, “Most cows have four legs” is not a statement, since the word “most” does not have a precise meaning.

Definition 2.2 (Negation). If P is a statement, then the negation of P is $\neg P$, read “not P .” The negation of P is defined to be true if P is false and false if P is true.

P	$\neg P$
T	F
F	T

Definition 2.3 (Conjunction). If P and Q are statements, then their conjunction $P \wedge Q$, read “ P and Q ,” is true if P and Q are both true; otherwise their conjunction is false.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Note the similarity between the symbol “ \wedge ” and the letter “A” for “and”.

Definition 2.4 (Disjunction). If P and Q are statements, then their disjunction $P \vee Q$, read “ P or Q ,” is true if either P or Q or both are true; otherwise their disjunction is false.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Note that \vee is the inclusive “or”, eg. “ $1 + 1 = 2$ ” \vee “ $2 \times 2 = 4$ ” is true. In common (non-mathematical) use, one also encounters the exclusive “or”: “do you want coke or pepsi?”

Definition 2.5 (Formal implication). If P and Q are statements, then the implication $P \Rightarrow Q$, read “if P then Q ”, is the statement that if P is true then Q is true. P is called the premise and Q is called the conclusion. Other ways of expressing $P \Rightarrow Q$ are “ P implies Q ”, “ P only if Q ”, “ Q if P ”, “ P is sufficient for Q ”, “ Q is necessary for P ”.

Note that implication in this formal sense is only concerned with the truth or falsity of P and Q as statements, not with the meaning of P and Q or with a chain of reasoning between P and Q . For example,

“Cows are mammals \Rightarrow 7 is a prime number”

is true.

We say $P \Rightarrow Q$ is true when P is false, regardless of whether Q is true. The reason for that is that a false statement can imply truth, eg. $1 = -1$ (false) squared yields $1^2 = (-1)^2$ (true).

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Definition 2.6 (Converse). The converse of an implication $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.

Note that the converse of a true implication could be false and the converse of a false implication could be true.

Definition 2.7 (Equivalence). If P and Q are statements, then P and Q are equivalent, written $P \Leftrightarrow Q$ and read “ P if and only if Q ” or “ P is equivalent to Q ”, if $P \Rightarrow Q$ and $Q \Rightarrow P$. The words “if and only if” are often abbreviated to “iff”. Hence, P iff Q is another way to state equivalence of P and Q .

Theorem 2.8 (De Morgan’s Laws).

- $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$
- $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$

Definition 2.9 (Contrapositive). The contrapositive of the implication $P \Rightarrow Q$ is the implication $\neg Q \Rightarrow \neg P$.

Theorem 2.10 (An implication and its contrapositive are equivalent).

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P).$$

Proof. by constructing a truth table. □

The above theorem implies that for the purpose of proving $P \Rightarrow Q$, it is enough to show its contrapositive, $\neg Q \Rightarrow \neg P$.

An expression “ $(P \vee Q) \wedge \neg(P \Rightarrow Q)$ ” is called a compounded statement. P and Q are its components.

A statement which is true for all possible values of its components is called a tautology. For example, $P \vee \neg P$ is a tautology.

Definition 2.11. A sentence whose truth value depends on the values of some variable is an open sentence.

We write $P(x)$, $P(x, y)$, etc. for open sentences depending on the variables x or x and y , etc.

Definition 2.12 (Existential Quantifier). The existential quantifier is denoted by the symbol \exists , read “there exists.”

Definition 2.13 (Universal quantifier). The universal quantifier is denoted by the symbol \forall , read “for all” or “for every.”

For example the existence of $\sqrt{2}$ can be stated as

$$\exists x \in \mathbb{R} \text{ such that } x^2 = 2,$$

or, more compactly, as

$$\exists_{x \in \mathbb{R}} x^2 = 2.$$

(Note that you put the part of the sentence before words “such that” in subscript after \exists .)

Additionally, a quantifier $\exists!$ is used to state the existence of a unique element with certain property. For example,

$$\exists!_{x \in (0, \infty)} x^2 = 2$$

holds, but

$$\exists!_{x \in \mathbb{R}} x^2 = 2$$

does not (since $x^2 = 2$ for two real x ’s: $\sqrt{2}$ and $-\sqrt{2}$).

The fact that $\sqrt{2}$ is irrational can be written as

$$\forall_{x \in \mathbb{Q}} x^2 \neq 2$$

or

$$\forall_{x \in \mathbb{R}} x \in \mathbb{Q} \Rightarrow x^2 \neq 2$$

(The set of rational numbers is traditionally denoted by \mathbb{Q} , coming from the word “quotient”.)

Theorem 2.14. Let $P(x)$ and $Q(x)$ be open sentences. Then

- (1) $\neg(\forall x, P(x)) \Leftrightarrow (\exists x, \neg P(x))$
- (2) $\neg(\exists x, P(x)) \Leftrightarrow (\forall x, \neg P(x))$
- (3) $\neg(\forall P(x) \Rightarrow Q(x)) \Leftrightarrow (\exists x, (P(x) \wedge \neg Q(x)))$

\forall is usually stronger than \exists . For example, “there exists a black cat” is true and “every cat is black” is false. However, that is not always the case. For example,

P=“there exists a white unicorn”

is false because it implies the existence of a unicorn. However,

Q=“every unicorn is white”

Q is true. Indeed, $\neg Q$ means “not every unicorn is white”. By Proposition 2.14, that is “there is a unicorn which is not white”. Hence, $\neg Q$ is false and, consequently, Q is true.

By the same token, the statement

P=“ $x = 5$ for all real x such that $x^2 + 1 < 0$ ”

is true. Indeed, note that the set of x 's such that $x^2 + 1 < 0$ is empty. Therefore P says “ $x = 5$ for all $x \in \emptyset$ ” and, consequently, $\neg P$ says

“ $x \neq 5$ for some element $x \in \emptyset$ ”

Since there are no elements in \emptyset , the above statement is false. Hence P is true.

Mathematical Notation in Proofs.

Besides the mathematical symbols explained above, there is a number of additional symbols used in mathematical proofs:

- The end of a proof is usually denoted by the letters “QED” for the Latin phrase “quod erat demonstrandum” or, more commonly by \square . (Occasionally, different symbols are used, like a triangle in your Calculus Textbook.)
- “Therefore” is sometimes abbreviated by \therefore .
- “Contradiction” is sometimes abbreviated by $\#$ (or $\Rightarrow\Leftarrow, \perp$.)

Avoid using the symbols for “Therefore” and “Contradiction” as they are not universal and many mathematicians are not familiar with them.

PROBLEMS 2.

Problem 2.1. For each of the following statements, find P and Q so that the statement is equivalent to the implication $P \Rightarrow Q$:

- (1) I am happy if I am listening to music.
- (2) I am happy only if I am listening to music.
- (3) Being at least 30 years old is necessary for serving in the U.S. Senate.
- (4) Being born in US is a sufficient condition for being US citizen.

Problem 2.2. (a) Write the negation of the statement “There exists a cat with 9 lives” in standard English. (You cannot start it with “It is not true that...”)

(b) Write the negation of the statement “All cats have 9 lives.” (You cannot start it with “It is not true that...” nor “Not all cats...”).

Problem 2.3. Prove that $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$ is a tautology.

Problem 2.4.

- (1) Let P be the statement “ $x^2 + 2 = 11$ for all real numbers x such that $x^3 + 32 = 5$.” Is P true? Why or why not?
- (2) Let Q be the statement “ $x^3 + 32 = 5$ for all real numbers x such that $x^2 + 2 = 11$.” Is Q true? Why or why not?

(3) Let R be the statement “ $x^3 + 32 = 5$ for all real numbers x such that $x^2 + 32 = 0$.” Is R true? Why or why not?

Problem 2.5. As you should remember from Calculus, every cubic polynomial with real coefficients has a real root. Express that statement using \forall , \exists quantifiers and other math symbols but without using any words. (By the way, note though that not every quadratic polynomial has a real root.)

3. SETS

According to Wikipedia, “A set is a collection of distinct objects, considered as an object in its own right.”

Examples:

- \emptyset (set with no elements)
- {apple, horse, 2}

We use the Greek letter epsilon, \in , to write that a certain object is an element of a set, e.g. $2 \in \{\text{apple, horse, 2}\}$.

Definition 3.1 (Subset). Let A and B be sets. We say that A is contained in B or A is a subset of B , written $A \subset B$ or $A \subseteq B$, if whenever $x \in A$, then $x \in B$. As an alternative, we sometimes say that B contains A , written $B \supset A$ or $B \supseteq A$.

Note: Notation $A \subseteq B$ (consistent with writing $x \leq y$) is sometimes used to accentuate the possibility that A coincides with B . However, \subset and \subseteq always mean the same.

Note: $\emptyset \subset A$ for all sets A .

If A is a set then we often define its subsets by writing $\{x \in A : x \text{ satisfies some condition}\}$, e.g. $\{x \in \mathbb{Z} : 3|x^2 + x\}$ is the set of all integers x such that $x^2 + x$ is divisible by 3.

Definition 3.2 (Equality of Sets). We say that A equals B , written $A = B$, if $A \subset B$ and $A \supset B$.

Hence

$$\{\text{apple, horse, 2}\} = \{\text{horse, 2, apple}\} = \{\text{horse, 2, apple, horse}\}.$$

Sets can be elements of other sets, eg. $A = \{\{3, 5, 7\}, 1\}$ is a set of two elements, one of which is a set itself. If $B = \{1, 3, 5, 7\}$, then $A \neq B$, since B has 4 elements. Also, $A \neq \{\{1, 3, 5\}, 7\}$, since 7 is not an element of A .

The above intuitive notion of sets was taken for granted until 1901, when a British philosopher Bertrand Russell found a deadly flaw in it. Before we explain it, notice that according to wikipedia definition, the collection of all sets is a set in itself. This set contains itself as its own element! One might be willing to accept that as a fact of life, if not for the fact that the following argument of Russell leads to a contradiction:

Let us say that a set A is *wild* if A contains A as its own element. Otherwise A is *tame*. Hence the set of all sets is wild. Let Ω be the set of all tame sets. (Ω being the last letter of the Greek alphabet is often used to denote “large” sets.) Is Ω tame? If it is, then it belongs to Ω and hence, Ω is wild. On the other hand, if Ω is wild then, Ω is its element. Since by definition, all elements of Ω are tame, Ω is tame as well. Therefore, we proved that wildness of Ω implies its tameness and tameness of Ω implies its wildness.

This is the famous Russel’s Paradox which led the early 20th century mathematicians to rewrite the foundations of mathematics. Their efforts were not completely satisfactory, since they were unable to formulate a rigorous definition of a set. (The difficulty lies in the fact that every definition describes a notion in terms of simpler ones. One cannot define a “set” since it is the most basic notion of mathematics.)

Unable to define sets, mathematicians settled on the next best thing and described sets by axioms – fundamental properties upon which we all agree on. The most common set of axioms was formulated by Zermelo and Fraenkel. We will not discuss their axioms here, since they are more complicated than one would expect, c.f. http://en.wikipedia.org/wiki/Zermelo-Fraenkel_set_theory

Remark 3.3. (1) In simple terms, these axioms imply that there exists “a lot” of sets, but not everything is a set.

(2) All mathematical knowledge of human civilization can be derived from these axioms. (3) In

particular all mathematical notions (except sets) can be rigorously defined on the basis of set theory.

(4) We do not know if these axioms are consistent (i.e. do not lead to a contradiction, analogous to Russell's paradox). However, most mathematicians believe that they are since no contradiction have been found in the last 100 years.

(5) Axiomatic approach to set theory has its limitations. In particular we will see that the validity of some statements cannot be either proved or disproved on the basis of these axioms, c.f. Section 22.

Here are further operations on sets:

Definition 3.4 (Union and intersection). The union $A \cup B$ of two sets A and B is defined by $A \cup B = \{x : x \in A \text{ or } x \in B\}$. Note that 'or' in mathematics means 'and/or.' The intersection $A \cap B$ is defined by $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

Sometimes infinite unions come useful. For example, the set of all real numbers x such that $\sin(x) > 0$ can be written as $\{x \in \mathbb{R} : \sin(x) > 0\}$ or, more explicitly, as $\bigcup_{k \in \mathbb{Z}} (2\pi k, 2\pi k + \pi)$, meaning a union of intervals $(2\pi k, 2\pi k + \pi)$ for all possible integral values of k .

Definition 3.5 (Disjoint). Sets A and B are disjoint if $A \cap B = \emptyset$.

Definition 3.6 (Power set). The power set of a set A , denoted 2^A , is the set of all subsets of A . That is, $2^A = \{X : X \subset A\}$.

Mathematicians use the term "Proposition" to mean a true statement of lesser importance than a "Theorem." They also use the term "Lemma" to denote true statements which are of little importance as statements on their own, but are needed for proofs of Propositions and Theorems. We will encounter them in Sec. 6.

Proposition 3.7 (Basic properties of sets). *If A, B, C are sets, then*

- (1) $\emptyset \cap A = \emptyset$; $\emptyset \cup A = A$
- (2) $A \cap B \subset A$
- (3) $A \subset A \cup B$
- (4) $A \cup B = B \cup A$; $A \cap B = B \cap A$
- (5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (6) $A \cup A = A \cap A = A$
- (7) If $A \subset B$, then $A \cup C \subset B \cup C$ and $A \cap C \subset B \cap C$

Proof. The proofs are obvious. For example, if $x \in A \cap B$ then $x \in A$ and $x \in B$. Hence, in particular $x \in A$, implying $A \cap B \subset A$. □

Proposition 3.8 (Distributive Rules). *If A, B, C are sets, then*

- (1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof. Proof of (1): To prove that two sets, X and Y coincide (i.e. are equal), one usually needs to show separately that $X \subset Y$ and $Y \subset X$.

Proof of $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$: Let $x \in A \cap (B \cup C)$ then $x \in A$ and, furthermore, $x \in B$ or $x \in C$. Hence, $x \in A \cap B$ in the first case and $x \in A \cap C$ in the other. Therefore, $x \in A \cap B \cup A \cap C$ for all such x .

Proof (2): in class or HW. □

Definition 3.9 (Complement). If X and A are sets, the complement, $X - A$, of A in X is defined by $X - A = \{x \in X : x \notin A\}$

Proposition 3.10 (de Morgan's laws). *If A, B and X are sets then*

- (1) $X - (A \cup B) = (X - A) \cap (X - B)$
- (2) $X - (A \cap B) = (X - A) \cup (X - B)$

The proofs of these properties can be visualized by use of Venn diagrams.

As mentioned in Remark 3.3, all mathematical notions can be defined in terms of set theory. Let us take the first challenge then of defining a pair (a, b) , like the one used to denote the coordinates of a point on a plane. Note that $(a, b) \neq \{a, b\}$ since $(a, b) \neq (b, a)$ for $a \neq b$.

Definition 3.11 (Formal definition of ordered pair). Let A and B be sets, let $a \in A$, $b \in B$. Then we define the ordered pair (a, b) by $(a, b) = \{\{a\}, \{a, b\}\}$.

The following proposition shows that (a, b) behaves as “a pair”.

Proposition 3.12 (Fundamental property of ordered pairs). *Let a and c be in A ; and b and d be in B . Then $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.*

Proof. Since \Leftarrow implication is obvious, we need to prove \Rightarrow only.

Let $a, c \in A$ and $b, d \in B$ be such that $(a, b) = (c, d)$. Observe that (a, b) is a set of 1 or 2 elements depending on whether a equals b or not. Indeed, if $a = b$ then

$$(3.12.1) \quad (a, b) = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$$

and if $a \neq b$ then (a, b) contains two different elements. (Why?)

For the proof, assume first that $a = b$. Then $(a, b) = (c, d)$ is a 1 element set and, hence, $c = d$. Furthermore, by (3.12.1), $\{a\} = \{c\}$. Hence $a = c$ and the implication follows.

If $a \neq b$ then (a, b) contains 2 elements: a 1 element set, $\{a\}$, and a 2 element set, $\{a, b\}$. By assumption $(a, b) = (c, d)$. Therefore (c, d) is also a 2 element set, i.e. $\{c, d\} \neq \{c\}$. Since a 1 element set cannot equal a 2 element set (recall that two sets equal if they have the same elements), our assumptions imply that $\{a\} = \{c\}$ and $\{a, b\} = \{c, d\}$. Hence $a = c$ and $b = d$. \square

Definition 3.13 (Cartesian Product). The Cartesian product $A \times B$ of sets A and B is defined by $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

Note: writing $(a, b) \in A \times B$ implies that $a \in A$ and $b \in B$.

We define $A^1 = A$, and A^2, A^3, \dots recursively by $A^{n+1} = A^n \times A$. For simplicity, we denote $((a, b), c)$ in $A^3 = A^2 \times A$ by (a, b, c) . Hence A^3 is the set of all triples of elements of A . Similarly we define n -tuples as elements of A^n .

Since every point in space can be uniquely identified (in given system of coordinates) by its X-, Y-, and Z-coordinates which are real numbers, the infinite 3-dimensional space is often denoted by \mathbb{R}^3 .

PROBLEMS 3.

Problem 3.1. Prove that if $A \subset B$ and $C \subset D$ then

- a) $A \cup C \subset B \cup D$.
- b) $A \cap C \subset B \cap D$.

Problem 3.2. Prove that $A \cup B = A$ if and only if $B \subset A$.

Problem 3.3. Prove that if A is a subset of X , then

- a) $A \cap (X - A) = \emptyset$.
- b) $A \cup (X - A) = X$.
- c) $X - (X - A) = A$. Hint: use a) and b).

Problem 3.4. Prove that if A and B are subsets of X , then

- a) $A - B = A \cap (X - B)$.
- b) $X - (A \cap B) = (X - A) \cup (X - B)$.
- c) $A \subset B$ if and only if $X - B \subset X - A$.

Problem 3.5. Prove that for any sets A, B, C , $A \cap (B - C) = (A \cap B) - (A \cap C)$.

Problem 3.6. List all elements of 2^A for $A = \{a, b, c\}$.

Problem 3.7. Let A and B be sets. Prove that $A \times \emptyset = \emptyset \times B = \emptyset$.

Problem 3.8. Let A, B, C be non-empty sets, with $B \subset C$. Prove that $A \times B \subset A \times C$.

Problem 3.9. Let A, B, C be non-empty sets. Prove that

(i) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(ii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Problem 3.10. Let A and B be non-empty sets. Prove that $A \times B = B \times A$ if and only if $A = B$. Where do you use that A and B are non-empty?

4. FUNCTIONS

We mentioned before that all mathematical notions can be defined rigorously on the basis of set theory. Can we define functions as sets then? Yes! For that, we use the fact that each function is determined by its graph.

Definition 4.1. A function is a triple (A, B, f) , where A, B are sets and f is a subset of $A \times B$ with the following properties:

- (1) If $x \in A$, then there exists $y \in B$ such that $(x, y) \in f$.
- (2) If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

Note that using the quantifier $\exists!$ introduced in Sec 2, we can combine these conditions into one: $\forall x \in A \exists! y \in B (x, y) \in f$.

We call A the domain of the function and B its codomain. The more traditional notation for a function (A, B, f) is $f : A \rightarrow B$. (From now on we will use this notation.) We write $f(x) = y$ if $(x, y) \in f$. Note that (1) means that for each $x \in A$, $f(x)$ exists. Condition (2) means that $f(x)$ has unique value. (“unique” = “only one”). In other words (2) is the vertical line test. Functions are also often referred to as maps.

Definition 4.2 (Composition). If $f : A \rightarrow B$ and $g : B \rightarrow C$ then the composition, $g \circ f$, of g with f is a function from A to C defined by $(g \circ f)(x) = g(f(x))$.

Definition 4.3 (Image). Let $f : A \rightarrow B$ be a function and let X be a subset of A . Then the image of X under f , denoted $f(X)$, is defined by $f(X) = \{f(a) : a \in X\}$. Alternatively, $f(X) = \{y \in B : y = f(x) \text{ for some } x \in X\}$.

Note 4.4. The image of f is $f(A)$, i.e. it is the image of A under f , often called the range of f . That is, the image of f and the range of f are each $\{f(a) : a \in A\}$.

Definition 4.5 (Inverse image). Let $f : A \rightarrow B$ be a function and let Y be a subset of B . Then the inverse image of Y under f , denoted $f^{-1}(Y)$, is defined by $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$.

Preimages of one element sets, $f^{-1}(\{y\})$, are sometimes abbreviated to $f^{-1}(y)$.

Example 4.6. If $f(x) = x^3 - x$, $f : \mathbb{R} \rightarrow \mathbb{R}$, then $f^{-1}(0) = \{-1, 0, 1\}$.

Proposition 4.7 (Image of inverse image is a subset). $f(f^{-1}(Y)) \subset Y$ for all $Y \subset B$.

PROBLEMS 4.

Problem 4.1. Let $A = \{1, 2, 3, 4\}$ and $B = \mathbb{Z}$. Using the formal definition of function, check whether the following subsets of $A \times B$ correspond to functions of A to B . Give your reasons why these are or are not functions

- (1) $f = \{(1, 4), (2, 3), (1, -2), (3, 1), (4, 1)\}$
- (2) $f = \{(1, 0), (2, -1), (3, 1)\}$.

Problem 4.2. Let $A = B = \mathbb{R}$. Using the formal definition of function, check whether the following subsets of $A \times B$ correspond to functions of A to B . Give your reasons why these are or are not functions:

- (1) $f = \{(x, y) \in \mathbb{R}^2 : \text{and } x = y^4\} \subset \mathbb{R}^2$
- (2) $f = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1 \text{ and } y \geq 0\} \subset \mathbb{R} \times \mathbb{R}$
- (3) $f = \{(x, y) \in \mathbb{R}^2 : \text{and } x = y^5 + 4y^3 + 7\}$ (You will need to use calculus to solve this problem)

Problem 4.3. Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$. Write down all functions from A to B .

Problem 4.4. Let A be a finite set with m elements, and B be a finite set with n elements. Find a formula expressing the number of different functions from A to B . Prove your result. What notation does this suggest for “the set of all functions from A to B ”.

Problem 4.5. If A is a finite set, then the set of all functions from A to $\{0, 1\}$ has the same number of elements as the power set of A , by Problem 4.4 above and by Problem 3.3.6. So let A be a set (finite or not). Show that each function of A to $\{0, 1\}$ determines a subset of A and vice-versa.

Problem 4.6. Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4, 5\}$. Define a function $f : A \rightarrow B$ by $f(1) = 2, f(2) = 2, f(3) = 5, f(4) = 4$.

- i. Find the image of f .
- ii. Find $f^{-1}(\{3, 4\})$.
- iii. Find $f(\{1, 2, 4\})$.
- iv. Find $f^{-1}(\{3\})$.
- v. Find $f(f^{-1}(\{2, 3\}))$.

Problem 4.7. Let $A = \{1, \dots, 5\}, B = \{1, \dots, 6\}, C = \{1, \dots, 4\}$. Define $f : A \rightarrow B$ by $1, 2, 3, 4, 5 \rightarrow 2, 4, 3, 6, 1$ and $g : B \rightarrow C$ by $1, 2, 3, 4, 5, 6 \rightarrow 4, 4, 1, 3, 2, 2$. Find $g \circ f$.

Problem 4.8. Let $f, g : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^3 + 1$ for all $x \in \mathbb{R}$ and $g(t) = 1 - t$ for all $t \in \mathbb{R}$. Find $(f \circ g)(3)$ and $(g \circ f)(3)$.

Problem 4.9. Let $f : A \rightarrow B$ be a function.

- i. Let $Y \subset B$ be a subset. Prove that $f(f^{-1}(Y)) = Y$ if and only if $Y \subset \text{image } f$.
- ii. Prove that $X \subset f^{-1}(f(X))$ for all $X \subset A$.

Problem 4.10. Let $f : A \rightarrow B$ be a function. Let X_1 and X_2 be subsets of A and Y_1 and Y_2 be subsets of B . Prove the following:

- i) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$
- ii) $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$
- iii) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$
- iv) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$
- v) Give an example where $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$.

Problem 4.11. Let A be a set and let $f : A \rightarrow \{1, 2, 3, 4\}$ be a function. Let $A_i = f^{-1}(\{i\})$ for $i = 1, 2, 3$, and 4 . Note: f is not assumed to be one to one or onto.

- i) Prove that $A_i \cap A_j = \emptyset$ for $i \neq j$.
- ii) Prove that $A = A_1 \cup \dots \cup A_4$.

Problem 4.12. Describe the set $\sin^{-1}(1)$ explicitly using math symbols only (no words).

5. INVERSE FUNCTIONS

Definition 5.1 (One to one). A function $f: A \rightarrow B$ is one to one (or, “1-1” or “injective”) if $f(x_1) = f(x_2)$ for some x_1 and x_2 in A always implies that $x_1 = x_2$.

Definition 5.2 (Onto). A function $f: A \rightarrow B$ is onto (or, “surjective”) if for each $y \in B$ there is an $x \in A$ such that $f(x) = y$.

Note that f is onto if and only if $f(A) = B$.

Definition 5.3 (Identity function). The identity function $id_A: A \rightarrow A$ is defined by $id_A(x) = x$ for all $x \in A$.

Definition 5.4 (Inverse). Let $f: A \rightarrow B$ be a function. Define $f^{-1} = \{(b, a) \in B \times A : (a, b) \in f\}$.

Proposition 5.5. f^{-1} is a function from B to A if and only if f is one to one and onto.

Proposition 5.6. If f is one to one and onto, then our f^{-1} satisfies the Calculus definition of inverse function: $f^{-1} \circ f$ is the identity on A and $f \circ f^{-1}$ is the identity on B .

From now on we will usually use the (more intuitive) Calculus definition of the inverse function. In particular, we will say “ f has an inverse” rather than “ f^{-1} is a function”.

If f has an inverse then the convention of abbreviating the preimage of $\{y\}$ under f by $f^{-1}(y)$ (c.f. Example 4.6) leads to an ambiguity: $f^{-1}(y)$ can mean x such that $f(x) = y$ (i.e. the value of f^{-1} at y) or the preimage of $\{y\}$ under f . However, this ambiguity is not too bad since that preimage is $\{x\}$.

Proposition 5.7. Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be one to one and onto functions. Then $g \circ f: A \rightarrow C$ is one to one and onto; and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Remark 5.8. If A is a finite set then

(a) every 1-1 function $f: A \rightarrow A$ is onto.

(b) every onto function $f: A \rightarrow A$ is 1-1.

These statements are called “Pigeonhole principle”. Pigeonhole principle does not hold for infinite A .

PROBLEMS 5.

Problem 5.1. Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4, 5\}$. Define a function $f: A \rightarrow B$ by $f(1) = 2, f(2) = 2, f(3) = 5, f(4) = 4$.

i. Is f one to one? Why or why not?

ii. Is f onto? Why or why not?

Problem 5.2. Let $f: A \rightarrow B$ be a one to one function. Let $X \subset A$ be a subset. Let x be an element of A . Prove that if $f(x) \in f(X)$ then $x \in X$.

Problem 5.3. Let $f: A \rightarrow B$ be a function. Prove that $X = f^{-1}(f(X))$ for all $X \subset A$ if and only if f is one to one. Note: part of the problem was done in Problem 4.9.ii of Section 4.

Problem 5.4. Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 3, 4, 5\}$. Define $f: A \rightarrow B$ by $1, 2, 3, 4 \rightarrow 4, 2, 5, 3$. Check that f is one to one and onto and find the inverse function f^{-1} .

Problem 5.5. Let $f: A \rightarrow B$ and $g: B \rightarrow A$ be functions.

i) Prove that $g \circ f = id_A$ implies f is one to one.

ii) Prove that $f \circ g = id_B$ implies f is onto.

Problem 5.6. Let $f: A \rightarrow B$ be one to one and onto.

i) If $g: B \rightarrow A$ satisfies $g \circ f = id_A$, prove that $g = f^{-1}$.

ii) If $g: B \rightarrow A$ satisfies $f \circ g = id_B$, prove that $g = f^{-1}$.

Problem 5.7. Let $f : A \rightarrow B$ be a function, where A and B are non-empty sets. If f is one to one, prove there exists a function $g : B \rightarrow A$ such that $g \circ f = id_A$. *Hint: define g on $f(A)$ to make $g \circ f = id_A$. Then define g on $B - f(A)$. Does it matter how you define g on $B - f(A)$?*

Problem 5.8. Prove Proposition 5.7.

Problem 5.9. Give an example showing that Remark 5.8(a) does not hold for the natural numbers $A = \{1, 2, \dots\}$ and an example showing that Remark 5.8(b) does not hold for $A = \{1, 2, 3, \dots\}$.

Problem 5.10. Let $f : A \rightarrow B$ be a function, where A and B are non-empty sets. If f is onto, prove there exists a function $g : B \rightarrow A$ such that $f \circ g = id_B$.

Problem 5.11. Which of the following functions is 1-1? Which of them is onto?

- (1) f is the set of all points of the form (x, x^2) in $\mathbb{R} \times \mathbb{R}$
- (2) f is the set of all points of the form (x, x^2) in $[0, \infty) \times \mathbb{R}$
- (3) f is the set of all points of the form (x, x^2) in $\mathbb{R} \times [0, \infty)$

6. NATURAL NUMBERS

As we have mentioned in Section 3, all mathematical notions can be defined in terms of set theory. That applies to numbers too. For $1, 2, \dots$ the definition goes like this: $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, and so on.

More generally, we say that a successor of a set A is

$$A' = A \cup \{A\}.$$

The set, \mathbb{N} , of natural numbers is the smallest set containing 1 and such that for every n in \mathbb{N} also n' is in \mathbb{N} . (The existence of such set is guaranteed by one of the Zermelo-Frankel axioms of set theory.) Some mathematicians (but not us) include 0 in the set of natural numbers.

An alternative approach to natural numbers is through five axioms formulated by a 19th century Italian mathematician, G. Peano. For simplicity, we will use his approach in these notes. Later we will define rational and, more generally, real and complex numbers on the basis of natural numbers.

Preliminary Axioms

Let n, m be numbers.

- (a) $n=n$ for every n .
- (b) If $n=m$ then $m=n$.
- (c) If $n=m$, $m=k$ then $n=k$.

Peano's axioms for natural numbers.

Axiom 1: 1 is a natural number. (That is, our set is not empty.)

Axiom 2: For each n there exists exactly one natural number, called the successor of n , which will be denoted by n' . (We cannot call it $n + 1$ since $+$ is not defined yet.)

Axiom 3: For every n , we have $n' \neq 1$.

Axiom 4: If $n' = m'$ then $n = m$. (We will often use its contrapositive: If $n \neq m$ then $n' \neq m'$.)

Axiom 5 (Axiom of Induction): If M is a set of natural numbers, with the following properties:

- 1 belongs to M ("the base assumption")
- If k belongs to M then so does k' ("the inductive assumption")

then M contains all the natural numbers.

All known properties of natural numbers can be defined and derived from Peano's axioms.

We denote $1'$ by 2. By Axiom 3, $2 \neq 1$. Similarly, we define $3 = 2'$, $4 = 3'$, $5 = 4'$, $6 = 5'$, $7 = 6'$, $8 = 7'$, $9 = 8'$.

We are going to see later that if m is obtained from n by taking a sequence of its successors, then $m \neq n$. Let us start with a simple instance of this claim:

Proposition 6.1. $3 \neq 1$ and $3 \neq 2$.

Proof. $3 \neq 1$ by Axiom 3. We prove $3 \neq 2$ "by contradiction"

Suppose that the statement is false, i.e. $3 = 2$. Then, by Axiom 4, $2 = 1$, contradicting Axiom 3 since $2 = 1'$. □

Axiom 5 says that the only natural numbers are $1, 2, 3, 4, 5, \dots$

We denote the set of all natural numbers by \mathbb{N} . Hence $\mathbb{N} = \{1, 2, 3, 4, \dots\}$.

One uses Axiom 5 to prove various statements about natural numbers, as illustrated below:

Theorem 6.2. $\forall_{n \in \mathbb{N}} n' \neq n$.

Proof. (by Axiom of Induction).

Let M be the set of $n \in \mathbb{N}$ such that $n' \neq n$. We need to prove that $M = \mathbb{N}$. Using Axiom of Induction, it is enough to prove that

- (base step) $1 \in M$, and
- (induction step) if $k \in M$ then $k' \in M$.

Base step says that $2 \neq 1$. This fact follows from Axiom 3.

Induction step says that if $k' \neq k$ then $(k')' \neq k'$. This implication follows from Axiom 4 for $n = k$ and $m = k'$. \square

Theorem 6.3. *For every $n \neq 1$, there exists m such that $n = m'$.*

Proof left as HW.

Theorem 6.4 (Existence of addition). *To every pair of numbers n, m we may assign in exactly one way a natural number, written $n + m$, such that*

- (1) $n + 1 = n'$ for every n ,
- (2) $n + m' = (n + m)'$ for every n and every m .

Theorem 6.5 (Associativity Law). $\forall a, b, c \in \mathbb{N} \quad (a + b) + c = a + (b + c)$

We often denote $(a + b) + c$ and $a + (b + c)$ by $a + b + c$.

Theorem 6.6 (Commutativity Law). $\forall a, b \in \mathbb{N} \quad a + b = b + a$

The proofs of Theorems 6.4-6.6 are by Axiom of Induction as well, see E. Landau, Foundations of Analysis. We skip these proofs since they are too lengthy for inclusion here.

From now on we will use a simplified version of the inductive argument, which does not invoke the set “ M ” explicitly, based on the following version of Axiom of Induction:

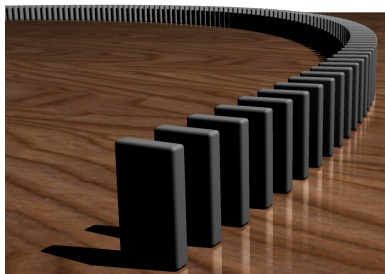
Theorem 6.7 (Principle of Mathematical Induction). *Let $P(n)$ be a statement for each integer $n \in \mathbb{N}$. If both of the following hold:*

- (1) $P(1)$ is true (*the base step*)
- (2) For each $k \in \mathbb{N}$ if $P(k)$ is true then $P(k + 1)$ is true (*the inductive step*)

then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let M be the set of those n for which $P(n)$ holds. Then $1 \in M$ and if $k \in M$ then $k + 1 \in M$. Since $k + 1 = k'$ by Theorem 6.4(1), the assumptions of Axiom of Induction are satisfied and $M = \mathbb{N}$. This means that $P(n)$ holds for all n . \square

This principle is often explained by analogy with falling domino:



If

- the first domino falls, and
- any falling domino trips its next neighbor

then all dominos fall.

We will apply this principle to the proof of the following:

Theorem 6.8. $\forall a, b \in \mathbb{N} \quad a + b \neq b$.

Proof. Fix $a \in \mathbb{N}$. Let $P(b)$ be the statement “ $a + b \neq b$.” We are going to prove $P(b)$ for all $b \in \mathbb{N}$ by the Principle of Mathematical Induction:

By Theorem 6.4(1) and Axiom 3, $a + 1 = a' \neq 1$. Hence, the base step, $P(1)$, holds.

Inductive Step: Assume that $P(k)$ holds. Then $a + k \neq k$. By Axiom 4, $(a + k)' \neq k'$. Therefore, by Theorem 6.4, $a + k' \neq k'$. Since $k' = k + 1$, $P(k + 1)$ holds. Since both, the base step and the inductive step hold, the statement $P(b)$ is true for all $b \in \mathbb{N}$ by the Principle of Induction (Theorem 6.7). \square

Definition 6.9.

- $a > b$ if $a = b + c$ for some c . Equivalently, we write $b < a$.
- $a \geq b$ iff $a > b$ or $a = b$. Similarly, $a \leq b$ iff $a < b$ or $a = b$.

Theorem 6.10. *For every a, b exactly one of the below must be the case:*

- (1) $a = b$
- (2) $a > b$
- (3) $b > a$.

Theorem 6.11. $\forall_{n \in \mathbb{N}} n \geq 1$.

Proof. By Thm 6.3, either $n = 1$ or $n = m + 1$ for some m . The later case implies that $n > 1$. \square

Theorem 6.12 (+Def.). *If $a > b$ then there is a unique c such that $a = b + c$. We denote such c by $a - b$.*

Theorem 6.13 (Well-ordering Principle). *For every non-empty set $A \subset \mathbb{N}$*

$$\exists_{a \in A} \forall_{a' \in A} a \leq a'.$$

The element a as above is the smallest element of A . In other words, every set of natural numbers has the smallest element. Note that many other sets, eg. $(0, 1)$, do not have the smallest element.

Proof of Thm 6.13: If $1 \in A$ then the statement follows from Thm 6.11. Hence assume that $1 \notin A$. Now we continue our proof by contradiction:

Assume that A has no smallest element. Let B be the set of all $b \in \mathbb{N}$ such that $\forall_{a \in A} b < a$.

We claim that $B = \mathbb{N}$. Proof by induction:

- $1 \in B$. Proof: Since $1 \notin A$, $\forall_{a \in A} 1 < a$. Hence $1 \in B$.
- Now we need to prove the induction step: if $b \in B$ then $b + 1 \in B$.

Proof: If $b \in B$ then $\forall_{a \in A} b < a$. If $b < a$ then $a - b \in \mathbb{N}$. If $a - b = 1$ then $a = b + 1 \in A$. Since $b \in B$, $b + 1$ is the smallest element of A – contradiction. Therefore, we can assume that $a - b > 1$ for every $a \in A$. Hence $b + 1 \in B$. This complete the proof of the inductive step.

Hence, $B = \mathbb{N}$. If $a \in A$ then $a \notin B$. Hence $A = \emptyset$, contradicting the assumption of the theorem. \square

Note that the proof of Well-ordering Principle is based on the Induction Principle. Conversely, it can be shown that Peano’s Axioms 1-4, Theorem 6.3, and the Well-ordering Principle imply the Induction Principle.

PROBLEMS 6.

Problem 6.1. Using your knowledge (not restricted to these notes) show that the set $[0, \infty)$ (the non-negative real numbers) does not satisfy the Well-ordering principle. In other words, show that it contains a subset A which does not contain the smallest element.

When solving these problems you can only refer to axioms and statements made in these notes only.

Problem 6.2. Prove Thm 6.3.

Hint: Let A be a set composed of 1 and of all n such that $n = m'$ for some m .

Prove by induction that $A = \mathbb{N}$.

Problem 6.3. Prove the following piece of Thm 6.10: For every $a, b \in \mathbb{N}$ at most of one of the three alternatives of Thm 6.10 holds. Hint: Use Thm 6.8.

7. INTEGERS

For each natural number, n , consider a new number (symbol), $-n$. The numbers $1, 2, 3, \dots, -1, -2, -3, \dots$ and zero, 0 , are called integers.

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

(\mathbb{Z} stands for German “Zahlen” – numbers.)

We call $1, 2, \dots$ positive integers and the numbers $-1, -2, -3, \dots$ negative integers.

Definition 7.1 (The absolute value). If $n \in \mathbb{N}$ then $|n| = n$ and $|-n| = n$. Additionally, $|0| = 0$.

Definition 7.2. We define addition of integers as follows,

$$a + b = \begin{cases} a + b & \text{if } a, b \text{ are positive} \\ -(|a| + |b|) & \text{if } a, b \text{ are negative} \\ a & \text{if } b = 0 \\ b & \text{if } a = 0. \end{cases}$$

If a is positive and b negative, then

$$(7.2.1) \quad a + b = \begin{cases} a - |b| & \text{if } a > |b| \\ -(|b| - a) & \text{if } |b| > a \\ 0 & \text{if } |b| = a. \end{cases}$$

If a is negative and b positive, then we define $a + b$ similarly.

Theorem 7.3 (Associativity Law for Integers). $\forall a, b, c \in \mathbb{Z} \quad (a + b) + c = a + (b + c)$.

Theorem 7.4 (Commutativity Law for Integers). $\forall a, b \in \mathbb{Z} \quad a + b = b + a$.

We often denote $a + (-b)$ by $a - b$.

By definition of addition, we have $\forall a \in \mathbb{Z} \quad a - a = 0$.

Let $-(-n) = n$ for every $n \in \mathbb{Z}$. In particular, we always have $-n = 0 - n$.

Proposition 7.5. *If $a = b + c$ then $c = a - b$.*

Proof. If $a = b + c$ then $a + (-b) = c + b + (-b) = c$. □

Corollary 7.6 (Cancellation Property). *If $a + c = b + c$ then $a = b$.*

Proof. $a = (a + c) + (-c) = (b + c) + (-c) = b$. □

Multiplication.

Theorem 7.7 (Existence of multiplication). *For every $a, b \in \mathbb{Z}$ we can assign a unique integer, called $a \cdot b$, such that*

- $\forall a \in \mathbb{Z} \quad a \cdot 1 = a$
- $\forall a, b, c \in \mathbb{Z} \quad a \cdot (b + c) = a \cdot b + a \cdot c$.

The second property is called the Distributivity Law. We often abbreviate $a \cdot b$ to ab .

Theorem 7.8 (Associativity of Multiplication). $\forall a, b, c \in \mathbb{Z} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Theorem 7.9 (Commutativity of Multiplication). $\forall a, b \in \mathbb{Z} \quad a \cdot b = b \cdot a$.

Proposition 7.10. (1) $\forall a \in \mathbb{Z} \quad a \cdot 0 = 0$.

(2) $\forall a \in \mathbb{N} \quad a \cdot (-1) = -a$.

(3) $\forall a, b \in \mathbb{N} \quad a \cdot b \in \mathbb{N}$.

(4) $\forall a, b \in \mathbb{N} \quad (-a) \cdot b = a \cdot (-b) = -(ab)$.

(5) $(-a)(-b) = ab$.

Theorem 7.11. $\forall a, b \in \mathbb{Z}$ if $a \neq 0$ and $b \neq 0$ then $a \cdot b \neq 0$.

Corollary 7.12 (Cancellation of multiplication). *If $a \neq 0$, then $a \cdot b = a \cdot c$ implies $b = c$.*

Ordering of integers

Definition 7.13. For any $a, b \in \mathbb{Z}$ we say that $a > b$ iff $a - b \in \mathbb{N}$.

Note that this definition agrees with the previous one for $a, b \in \mathbb{N}$.

Theorem 7.14 (Properties of inequalities).

- (1) *If $a < b$ and $b < c$ then $a < c$.*
- (2) *If $a < b$ then $a + c < b + c$*
- (3) *If $a < b$ and $c > 0$ then $ac < bc$.*
- (4) *If $c < 0$ and $a < b$, then $ac > bc$.*
- (5) *If $c > 0$ and $ac < bc$, then $a < b$.*
- (6) *If $c < 0$ and $ac < bc$, then $a > b$.*
- (7) *If $0 < a < b$ and $0 < c < d$, then $a \cdot c < b \cdot d$.*

Theorem 7.15. *For every $a, b \in \mathbb{Z}$ exactly one of the following must be the case: $a > b$ or $a < b$ or $a = b$.*

PROBLEMS 7.

When solving these problems you can only refer to axioms and statements made in these notes only.

Problem 7.1. Prove the following easier version of Thm 7.11: $\forall_{a,b \in \mathbb{N}} a \cdot b \neq 0$. Hint: Prove the statement by induction with respect to b .

Problem 7.2. Prove Thm. 7.10(1),(2),(3). Hint: Proof of (3) is by induction on a or b .

Problem 7.3. Prove Corollary 7.12. Hint: Use Thm 7.11.

Problem 7.4. Prove Prop. 7.14(1)-(3).

Problem 7.5. The formulas $a - |b|$ and $-(|b| - a)$ in the first two cases on the right hand side of (7.2.1) “look” the same. Why do we need to write them in these two ways? (A single sentence answer is sufficient.)

8. MORE INDUCTION

Definition 8.1. For any integer x , let x^n be defined as follows: $x^1 = x$ and $x^{n+1} = x^n \cdot x$ for all $n \in \mathbb{N}$.

Proposition 8.2.

- (1) $\forall x, y \in \mathbb{Z}, n \in \mathbb{N} \quad (xy)^n = x^n y^n.$
- (2) $\forall x \in \mathbb{Z}, n, m \in \mathbb{N} \quad x^m x^n = x^{m+n}.$
- (3) $\forall x \in \mathbb{Z}, n, m \in \mathbb{N} \quad (x^m)^n = x^{mn}.$
- (4) $\forall x, y \in \mathbb{N}, n \in \mathbb{N} \quad \text{if } x < y \text{ then } x^n < y^n.$

Proof. (1) in class. Proofs of (2), (3), (4) are HW. All these proofs are by induction. □

Although so far we have defined natural numbers and integers only, in the rest of this section we assume the existence of real numbers and we take their basic arithmetic properties for granted.

Problem 8.3. Use induction to prove that

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{n^2} \leq 2 - \frac{2}{n+1}$$

for all $n \geq 1$.

Solution: Let $P(n)$ be the inequality above. We carry the proof by induction.

Base step: $P(1)$ reads " $\frac{1}{1^2} \leq 2 - \frac{2}{1+1}$." Hence $P(1)$ is true.

Inductive Step: Assume that $P(k)$ holds. We need to prove $P(k+1)$, i.e.

$$(8.3.1) \quad \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}.$$

We will use here a very useful approach called "a forward-backward proof."

By the inductive assumption,

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{k^2} \leq 2 - \frac{2}{k+1}.$$

Hence

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+1} + \frac{1}{(k+1)^2}.$$

Therefore, **it is enough to prove**¹ that

$$2 - \frac{2}{k+1} + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}.$$

This is equivalent to

$$-\frac{2}{k+1} + \frac{1}{(k+1)^2} \leq -\frac{2}{k+2}.$$

By multiplying both sides by -1 we get (remember to change the inequality sign!)

$$\frac{2}{k+1} - \frac{1}{(k+1)^2} \geq \frac{2}{k+2},$$

i.e.

$$\frac{2k+1}{(k+1)^2} \geq \frac{2}{k+2}.$$

By multiplying both sides by $(k+1)^2(k+2)$, we get

$$(2k+1)(k+2) \geq 2(k+1)^2.$$

Expanding, we get

$$2k^2 + 5k + 2 \geq 2k^2 + 4k + 2.$$

¹Note that I didn't write: "We must prove" here. Why?

This is equivalent to $k \geq 0$. Therefore we proved $P(k + 1)$ (assuming $P(k)$). In other words, we proved the inductive step. By the Principle of Induction, (Thm 6.7), $P(n)$ holds for all $n \in \mathbb{N}$. \square

Remarks:

- The above proof of the inductive step is written in the way a mathematician will usually derive it: by a sequence of successive simplifications of the statement which needs to be proved, until it becomes obvious. This is a special case of a forward-backward proof – it works forward from A and backward from B; the proof concludes when these two sequences of statements converge. It is not the most elegant type of proof. We present an elegant version of that proof below.

- Note the bold faced words “it is enough to prove”. It is important to realize that these words cannot be replaced by “we have to prove”. Why?

Here is an **elegant version** of the above proof of the inductive step:

By the inductive assumption,

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{k^2} \leq 2 - \frac{2}{k+1}.$$

Hence

$$(8.3.2) \quad \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+1} + \frac{1}{(k+1)^2}.$$

Now, notice that since $k \geq 0$, we have

$$2k^2 + 5k + 2 \geq 2k^2 + 4k + 2.$$

By factoring we get,

$$(2k+1)(k+2) \geq 2(k+1)^2.$$

Now, by dividing both sides by $(k+1)^2(k+2)$, we get

$$\frac{2k+1}{(k+1)^2} = \frac{2}{k+1} - \frac{1}{(k+1)^2} \geq \frac{2}{k+2}.$$

Hence

$$-\frac{2}{k+1} + \frac{1}{(k+1)^2} \leq -\frac{2}{k+2}$$

and

$$(8.3.3) \quad 2 - \frac{2}{k+1} + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}.$$

Since \leq is transitive (i.e. $a \leq b$ and $b \leq c$ implies $a \leq c$), and the right side of (8.3.2) is the left side of (8.3.3), we get

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots + \frac{1}{(k+1)^2} \leq 2 - \frac{2}{k+2}.$$

This is $P(k + 1)$. This completes the proof of the inductive step. \square

Notice that this proof starts from simple statements (e.g. $k > 0$) and concludes more complicated ones from them until it achieves its goal (proof of $P(k + 1)$). In writing this proof, we were guided by the previous one. (We rewrote it in reverse order.)

Factorials and Binomial Coefficients.

Definition 8.4 (Factorials). $0! = 1! = 1$. For every $n \in \mathbb{N}$, $n! = (n - 1)! \cdot n$.

A definition of this type is called “recursive”.

Definition 8.5 (Binomial coefficients). Let k and n be integers, $0 \leq k \leq n$. Define the binomial coefficient $\binom{n}{k}$, by:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

$\binom{n}{k}$ is often read “ n choose k ”, since it is the number of all k element subsets of an n element set. For example $\binom{4}{2} = 6$ is the number of 2 element subsets of $\{1, 2, 3, 4\}$. (These subsets are $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$.)

Remark 8.6. For every integer $n \geq 0$, $\binom{n}{0} = \binom{n}{n} = 1$.

Proposition 8.7 (Pascal’s Triangle). If $0 < k < n$, then $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Proof. in class, by direct computation. □

Proposition 8.8. $\binom{n}{k}$ is an integer, for every integers, $0 \leq k \leq n$.

Proof. by induction on n , in class. □

Theorem 8.9 (Binomial Theorem). For every $x, y \in \mathbb{R}$ and every $n \in \mathbb{N}$,

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

Proof of this theorem is assigned as HW.

Proposition 8.10. $\sum_{k=0}^n \binom{n}{k} x^k y^{n-k} = 2^n$.

In Theorem 6.7 both conditions, (1) and (2), are equally important. Consider for example, the following statement $P(n) = “n = n + 1”$. By adding 1 to both sides, we get $n + 1 = (n + 1) + 1$. Hence $P(n)$ implies $P(n + 1)$. However $P(1)$ is false and, therefore, the Principle of Induction does not apply.

Here is another interesting example of faulty logic in an induction proof:

“Theorem” All cats have the same color.

”Proof”: Take any group of n cats, where $n = 1, 2, \dots$. We need to prove that all cats in this group have the same color. It is an obvious statement for $n = 1$.

Inductive step: Assume that the statement holds for n . We need to prove it for $n + 1$.

Consider a group of $n + 1$ cats. Label them by numbers from 1 to $n + 1$. By the inductive assumption, cats $1, \dots, n$ have the same color. Similarly, by the inductive assumption cats $2, \dots, n + 1$ have the same color, since there is n of them. Since these two sets intersect, all $n + 1$ cats have the same color. □

Where is the error in this proof? (We answer that in the class).

Below are two useful generalizations of the Principle of Induction.

Theorem 8.11 (Induction with base m). Let $P(n)$ be a statement for each integer $n \geq m$. If both of the following hold:

(1) $P(m)$ is true (the base case)

(2) For each $k \geq m$, $P(k + 1)$ is true under the assumption that $P(k)$ is true (the induction step)

then $P(n)$ is true for all $n \geq m$.

Theorem 8.12 (Complete Induction). Let $Q(n)$ be a statement for each integer $n \geq 1$. If both of the following hold:

(1) $Q(1)$ is true (the base case)

(2) For each $k \geq 1$, $Q(k + 1)$ is true under the assumption that $Q(1), \dots, Q(k)$ are all true (the complete induction step)

then $Q(n)$ is true for all $n \geq 1$.

Proof of this theorem is assigned as HW.

Application of the complete induction will be seen in the next section.

Fibonacci numbers.

The Fibonacci numbers are defined by the following recursive definition: $F_1 = 1$, $F_2 = 1$, and $F_{n+2} = F_n + F_{n+1}$ for all $n \in \mathbb{N}$. Hence F_3, F_4, \dots are $2, 3, 5, 8, 13, 21, 34, \dots$. These numbers appear in various disciplines of science and even in the sunflower seed pattern! See e.g. <http://www.math.ntnu.no/~jarlet/Douady96.pdf>

We want a closed formula for the n -th Fibonacci number. ("closed" means non-recursive.)

Proposition 8.13. $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$

Proof. We use a version of the proof by complete induction. Denote the above formula by $Q(n)$. We check that the formula holds for $n = 1$ and $n = 2$ by direct computation. (The detailed computations were done in class.)

Now we will prove the complete induction step. That is, we prove that if all $Q(1), P(2), \dots, Q(k)$ hold then $Q(k+1)$ holds as well.

Assume that $Q(1), P(2), \dots, Q(k)$ are true. (In fact, it is enough for us to assume that $Q(k-1)$ and $Q(k)$ are true, and we do not need to worry about $Q(1), \dots, Q(k-2)$.) Let

$$x_1 = \frac{1 + \sqrt{5}}{2}, \quad x_2 = \frac{1 - \sqrt{5}}{2}.$$

Since x_1, x_2 are roots of $x^2 - x - 1 = 0$, we have

$$x_1^2 = x_1 + 1, \quad x_2^2 = x_2 + 1 \text{ and, consequently, } x_1^{k+1} = x_1^k + x_1^{k-1}, \quad x_2^{k+1} = x_2^k + x_2^{k-1}.$$

Therefore,

$$\frac{x_1^{k+1}}{\sqrt{5}} - \frac{x_2^{k+1}}{\sqrt{5}} = \left(\frac{x_1^k}{\sqrt{5}} - \frac{x_2^k}{\sqrt{5}} \right) + \left(\frac{x_1^{k-1}}{\sqrt{5}} - \frac{x_2^{k-1}}{\sqrt{5}} \right).$$

By the inductive assumption the right hand side of the above equality is $F_k + F_{k-1}$. By definition of Fibonacci numbers, it is F_{k+1} . Hence we proved that

$$\frac{x_1^{k+1}}{\sqrt{5}} - \frac{x_2^{k+1}}{\sqrt{5}} = F_{k+1}.$$

This completes the proof of the inductive step. By the Principle of Complete Induction, the statement of the proposition holds for all $n \in \mathbb{N}$. \square

Recursive sequences.

Fibonacci numbers are an example of a recursive sequence.

More generally, fix complex numbers c_1, \dots, c_N and s_1, \dots, s_N . Consider an infinite sequence whose first N terms are s_1, \dots, s_N and all subsequent terms are defined by the recursive relation

$$(8.13.1) \quad s_{n+1} = c_1 s_n + c_2 s_{n-1} + \dots + c_N s_{n-N+1}.$$

The proof of Proposition 8.13 suggests an idea for finding a closed formula for the n -term of this sequence: If x is a solution of

$$(8.13.2) \quad x^N - c_1 x^{N-1} - \dots - c_N = 0,$$

then the sequence $1, x, x^2, \dots$ satisfies the recursive relation (8.13.1), but not necessarily the initial conditions. One can prove however that if (8.13.2) has N different solutions x_1, \dots, x_N then there exist constants d_1, \dots, d_N such that

$$s_n = d_1 x_1^n + \dots + d_N x_N^n$$

for every n . One can find d_1, \dots, d_N by solving N linear equations

$$\begin{cases} s_1 = d_1x_1 + \dots + d_Nx_N \\ s_2 = d_1x_1^2 + \dots + d_Nx_N^2 \\ \dots \\ s_N = d_1x_1^N + \dots + d_Nx_N^N. \end{cases}$$

For Fibonacci sequence, we have

$$N = 2, \quad c_1 = c_2 = s_1 = s_2 = 1, \quad x_1 = \frac{1 + \sqrt{5}}{2}, \quad x_2 = \frac{1 - \sqrt{5}}{2},$$

The equations

$$\begin{cases} s_1 = d_1x_1 + d_2x_2 \\ s_2 = d_1x_1^2 + d_2x_2^2 \end{cases}$$

yield

$$d_1 = \frac{1}{\sqrt{5}}, \quad d_2 = -\frac{1}{\sqrt{5}}.$$

PROBLEMS 8.

Problem 8.1. Guess at a formula for $1 + 3 + 5 + \dots + (2n - 1)$, and prove your result by induction for $n \geq 1$.

Problem 8.2. Use induction to prove that $1^3 + \dots + n^3 = (1 + \dots + n)^2$.

Problem 8.3. Use induction to prove Proposition 8.2 (2) and (3).

Problem 8.4. Use induction to prove Proposition 8.2 (4).

Problem 8.5. Prove Theorem 8.9. (Hint: Use induction on n .)

Problem 8.6. Prove that $2^n \geq n^2$ for all integers $n \geq 4$. (Hint: use induction with base step $n = 4$.)

Problem 8.7. Prove Theorem 8.12. Hint: Let $P(k)$ be the statement “ $Q(1), Q(2), \dots, Q(k)$ are true.” Show that the complete induction step for $Q(k)$ implies induction step for $P(k)$.

Problem 8.8. Let $s_1 = 1$, $s_2 = 1$, and $s_{n+1} = 2s_n + s_{n-1}$ for $n \geq 2$. Find a closed formula for s_n following the recipe described above. (You need to show the computations which lead you to this formula, but you do not need to prove that this formula is correct.)

9. DIVISIBILITY

We are again assuming nothing more than Peano's axioms and the results derived from them in the previous Sections.

Definition 9.1. We say that an integer a divides an integer n if there exists an integer b such that $n = a \cdot b$. We write $a \mid n$.

Note. The following are all equivalent ways of writing the same thing:

- (1) a divides n
- (2) a is a factor of n
- (3) a is a divisor of n
- (4) n is a multiple of a

Note. If $a \mid n$ then $-a \mid n$ and $a \mid -n$.

Proposition 9.2. If a and n are positive integers such that $a \mid n$, then $a \leq n$.

Proof. left as HW □

Definition 9.3. A positive integer n is a prime number (or a prime) if $n > 1$ and the only positive factors of n are 1 and n . *Note:* because of tradition (and some more advanced reasons), 1 is not a prime.

Proposition 9.4. 2, 3, 5, 7 are prime numbers.

Proof. By Proposition 9.2, the only positive divisors of 2 are 1 and 2. Hence 2 has no positive divisors other than 1 and itself. Proof of primeness of 3, 5, 7 is left as HW. □

Theorem 9.5. Every natural number $n > 1$ is either a prime or a product of prime numbers.

Proof. in class, by complete induction. □

Such a decomposition is called a prime factorization of a number. For example, $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$.

Theorem 9.6. [Unique Factorization of Natural Numbers] If $n = p_1 \cdot \dots \cdot p_r$ and $n = q_1 \cdot \dots \cdot q_s$ are two prime factorizations of $n \in \mathbb{N}$ then $r = s$ and the primes p_1, \dots, p_r coincide with q_1, \dots, q_s up to a permutation (i.e. reordering).

Proof – later in this section.

Congruences, Integral Division.

Definition 9.7. We say that integers m_1, m_2 are congruent modulo n and we write

$$m_1 = m_2 \pmod{n}$$

iff $m_1 - m_2$ is divisible by n .

For example, $7 = -8 \pmod{5}$.

Proposition 9.8. If $a_1 = b_1 \pmod{n}$ and $a_2 = b_2 \pmod{n}$ then

- (1) $a_1 + a_2 = b_1 + b_2 \pmod{n}$, and
- (2) $a_1 a_2 = b_1 b_2 \pmod{n}$.

Corollary 9.9. If $a = b \pmod{n}$ then $a^k = b^k \pmod{n}$ for every $k \in \mathbb{N}$.

Proof. follows by induction from Proposition 9.8(2). □

Proposition 9.8 and Corollary 9.9 have many useful applications:

Problem 9.10. Prove that $3^{300} - 1$ is divisible by 31.

Mathematica computation shows that $(3^{300} - 1) = 31 \cdot N$, where $N = 4415854163180270193268581528454461805369796633075401176499360970269967650887066986896780843731901335104854336793483678800435894605345024986000$, but can it be trusted? Certainly we cannot verify these computations “by hand”. Besides that, we want a method to deal with even larger numbers which cannot be handled by computers. Here is a solution based on Proposition 9.8 and Corollary 9.9:

$$3^{300} - 1 = (3^3)^{100} - 1 = 27^{100} - 1 = (-4)^{100} - 1 \pmod{31}.$$

Now $(-4)^{100} - 1 = ((-4)^5)^{20} - 1 = (-1024)^{20} - 1$. Since $1024 = 33 \cdot 31 + 1$, the remainder of the division of 1024 by 31 is 1. Hence

$$3^{300} - 1 = (-1024)^{20} - 1 = (-1)^{20} - 1 = 0 \pmod{31}.$$

This means that $3^{300} - 1$ is divisible by 31.

Although the above sequence of simplifications of $3^{300} - 1 \pmod{31}$ was chosen ad hoc, every sequence of simplifications will yield the same result.

There is an alternative approach to the above problem using Fermat’s Little Theorem, see below.

Remainders and Integral Quotients.

Theorem 9.11. *Let $n \in \mathbb{N}$. For every $m \in \mathbb{Z}$ there exists $a, r \in \mathbb{Z}$ such that*

$$(9.11.1) \quad m = a \cdot n + r \quad \text{and} \quad 0 \leq r < n.$$

Furthermore such a and r are unique.

Proof. (1) Existence of a and r : Let $A = \{a \in \mathbb{Z} : a \cdot n \leq m\}$. Since $n \geq 1$,

$$\forall_{a \in A} a = a \cdot 1 \leq an \leq m.$$

Hence A is bounded from above and, therefore, it contains the largest element, a_M , by Theorem 9.16(2). Let $r = m - a_M \cdot n$. By our construction, $a_M \cdot n \leq m$. Hence $r \geq 0$. Since a_M is the largest element of A , $a_M + 1 \notin A$ and, hence, $(a_M + 1)n > m$. This implies that $a_M n + n > a_M n + r$, i.e. $n > r$. \square

(2) Uniqueness of a and of r . We need to prove that if $a, r \in \mathbb{Z}$ and $a', r' \in \mathbb{Z}$ satisfy condition (9.11.1) then $a = a'$ and $r = r'$.

Proof: We prove first that $r = r'$: Assume that $r \neq r'$. Then either $r' > r$ or $r > r'$, by Theorem 7.15. Without loss of generality, we can assume that $r' > r$. We have

$$a \cdot n + r = m = a' \cdot n + r'.$$

Since $r' - r = (a - a')n$, the number $r' - r$ is divisible by n . Since $r' - r \in \mathbb{N}$, by Proposition 9.2, $n \leq r' - r$. But then $n \leq n + r \leq r' \leq n - 1$. This is a contradiction. Therefore, we have proved that $r = r'$.

Now $a \cdot n + r = m = a' \cdot n + r'$ implies that $(a - a')n = 0$. By Theorem 7.11, $a - a' = 0$ (since $n \in \mathbb{N}$ and, hence $n \neq 0$.) Therefore $a = a'$. \square

If m, n, a, r are as above then a is called the integral quotient of m by n and r is called the remainder of the division of m by n . We clearly have $m = r \pmod{n}$.

By Theorem 9.11 for $n = 2$, every integer m equals to $2n + r$ for $r = 0$ or 1. Integers of the form $2n$ are called even and those of the form $2n + 1$ are called odd. By the above theorem every integer is either even or odd, but not both.

Note that:

- the sum of two even numbers is even,
- an even number plus an odd one is odd,
- the sum of two odd ones is even,
- the product of an even number with any number is even,
- the product of two odd numbers is odd.

The following is an application of Theorem 9.11.

Proposition 9.12. *Each natural number a can be written uniquely in the form*

$$a = b_n 10^n + b_{n-1} 10^{n-1} + \dots + b_2 10^2 + b_1 10 + b_0,$$

where b_0, \dots, b_n are integers from 0 to 9.

Proof. omitted – uses Theorem 9.11. □

Greatest Common Divisor.

Definition 9.13 (Greatest common divisor). Let m and n be non-zero integers. The greatest common divisor of m and n , denoted by $\gcd(m, n)$, is the largest integer that divides both m and n .

Note that the gcd is always positive.

Proposition 9.14. *Any two non-zero integers have their unique greatest common divisor.*

For the proof of Proposition 9.14 we need the following.

Definition 9.15. (1) We say that a set $A \subset \mathbb{Z}$ is bounded from below iff there exists $n \in \mathbb{Z}$ such that $\forall a \in A \ n \leq a$. Such n is called a lower bound.

(2) Similarly, $A \subset \mathbb{Z}$ is bounded from above iff there exists $n \in \mathbb{Z}$ such that $\forall a \in A \ a \leq n$. Such n is called an upper bound.

Theorem 9.16. (1) *Every $A \subset \mathbb{Z}$ bounded from below contains the smallest element, i.e. an element $m \in A$ such that $\forall a \in A \ m \leq a$.*

(2) *Every $A \subset \mathbb{Z}$ bounded from above contains the largest element, i.e. an element $m \in A$ such that $\forall a \in A \ a \leq m$.*

Note. (1) Note that Theorem 9.16 is a generalization of the Well-Ordering Principle.

(2) The above theorem does not hold if \mathbb{Z} is replaced by \mathbb{R} . For example, the open interval $(1, \infty)$ is bounded from below (for example by -5 , but the largest lower bound for A is 1). However, $(1, \infty)$ does not have the smallest element, since for every $a \in (1, \infty)$ the number $\frac{1+a}{2}$ is in A and it is smaller than a .

Proof of Theorem 9.16: Motivation: If $A \subset \mathbb{N}$ then the statement follows from the well-ordering principle, Thm 6.13. Therefore our goal is to define a new set $B \subset \mathbb{N}$ such that the existence of the smallest element in B is equivalent to the existence of the smallest element in A .

Here is the formal proof: Assume that A is bounded from below by n . If $n \in A$ then n is the smallest element of A and the statement holds. Therefore, assume now that $n \notin A$. Let $B \subset \mathbb{Z}$ be the set of all numbers of the form $a - n$, where $a \in A$.

$\forall a \in A \ n \leq a$ implies (by subtracting n from both sides) that $\forall a \in A \ 0 \leq a - n$. Since $a - n \neq 0$, we have $\forall a \in A \ 0 < a - n$, i.e. $B \subset \mathbb{N}$. By Well-ordering principle, Thm 6.13, B has the smallest element. Let us denote it by b_m . (Subscript “m” stands for “minimum”.) By definition of B , $b_m = a_m - n$ for some $a_m \in A$. We claim that a_m is the smallest element of A . Indeed, for every $a \in A$, $a - n \in B$ is greater or equal to $b_m = a_m - n$. Hence $\forall a \in A \ a - n \geq a_m - n$. By adding n to both sides of this inequality, we see that a_m is the smallest element of A .

Proof of (2) is analogous – left as HW. □

Now we are ready for the proof of Proposition 9.14: Let A be the set of common divisors of n and m . For every $a \in A$, a divides $|n|$ and, hence, by Proposition 9.2, $a \leq |n|$. Therefore A is bounded from above. By Theorem 9.16(2), A contains the largest element. This element satisfies the definition of the greatest common divisor of n and m . □

Definition 9.17. Let m and n be non-zero integers. We say that m and n are relatively prime (or coprime) if $\gcd(m, n) = 1$.

Note that m and n are relatively prime iff they have no common divisors other than 1 and -1 .

Lemma 9.18 (Bézout's Lemma). *For any integers a, b there exist integers x, y such that $ax + by = \gcd(a, b)$.*

Proof. Fix $a, b \in \mathbb{Z}$. Let $M = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$. Since M is a subset of a well ordered set, \mathbb{N} , it contains its smallest element. Denote it by d . By definition, $d = ax_0 + by_0$, for some $x_0, y_0 \in \mathbb{Z}$.

Lemma 9.19. *d divides a and b .*

Proof. $a = kd + r$ for some $k \in \mathbb{Z}$ and some $0 \leq r < d$ by Theorem 9.11. If d does not divide a then $r > 0$. Since $r = a - kd = a(1 - kx_0) + b(-ky_0)$, $r \in M$. This contradicts the assumption that d is the smallest element of M . Hence d divides a . Proof of $d|b$ is analogous. \square

Continuation of the proof of Bézout's Lemma: It is easy to see that d is the largest common divisor of a and b . Indeed, if d' is any other common divisor of a and b then d' divides $d = ax_0 + by_0$ as well. If d' is negative, then it is smaller than d . If d' is positive then it is not larger than d by Proposition 9.2. \square

Example 9.20. *By Bézout's Lemma, the equation $11x + 13y = 1$ has at least one solution $x, y \in \mathbb{Z}$. (Note that a solution to this equation consists of two numbers, x and y .) This may look surprising, since no such x and y immediately come to mind. Finding such integers is left as HW.*

Proposition 9.21. *If $\gcd(n, a) = 1$ and $n|a \cdot b$ then $n|b$.*

Proof. Suppose that $\gcd(n, a) = 1$ and n divides $a \cdot b$. By Bézout's Lemma $nx + ay = 1$ for some $x, y \in \mathbb{Z}$. Multiplying both sides by b we get $nxb + aby = b$. Since n divides both terms on the left, it divides b as well. \square

The following statement is known as Euclid's lemma (or Euclid's first theorem). It appears as Proposition 30 in Book VII of Euclid's Elements, written c. 300 BC.

Corollary 9.22 (Euclid's lemma). *If p is prime dividing $a \cdot b$ then $p|a$ or $p|b$.*

Proof. left as HW. \square

Now we are ready for

Proof of Unique Factorization Theorem (by contradiction): Let s be the smallest natural number that can be written as (at least) two different products of prime numbers. Denote these two factorizations of s as $p_1 \cdot \dots \cdot p_m$ and $q_1 \cdot \dots \cdot q_n$. Hence

$$(9.22.1) \quad p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_n.$$

By Euclid's Lemma either p_1 divides q_1 or p_1 divides $q_2 \cdot \dots \cdot q_n$. Both q_1 and $q_2 \cdot \dots \cdot q_n$ have unique prime factorizations, since both are smaller than s . Therefore, $p_1 = q_j$ (for some j). By removing p_1 from the left side of (9.22.1) and q_j from the right side of (9.22.1), we obtain two different factorizations of a smaller integer, contradicting our initial assumption. \square

Fermat's Little Theorem.

Lemma 9.23. *For every prime p and every $1 \leq k \leq p - 1$, $\binom{p}{k}$ is divisible by p .*

Proof. in class. \square

For example, $\binom{5}{1} = \binom{5}{4} = 5$, $\binom{5}{2} = \binom{5}{3} = 10$ are divisible by 5.

Proposition 9.24. *For every prime p , $\forall_{a,b \in \mathbb{Z}} (a + b)^p = a^p + b^p \pmod{p}$.*

Proof. By Binomial Theorem (Thm 8.9),

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \dots + \binom{p}{p-1}ab^{p-1} + b^p.$$

By Lemma 9.23, all terms on the right are divisible by p except for the first and the last one. Hence $(a + b)^p = a^p + b^p \pmod{p}$. \square

Corollary 9.25. *For every prime p and all $a_1, a_2, \dots, a_n \in \mathbb{Z}$,*

$$(a_1 + a_2 + \dots + a_n)^p = a_1^p + \dots + a_n^p \pmod{p}.$$

Proof. by induction, using Proposition 9.24. \square

By taking $a_1 = a_2 = \dots = a_n = 1$ we obtain the following neat result:

Theorem 9.26 (“Fermat’s Little Theorem”). *If p is prime then $n^p = n \pmod{p}$ for every $n \in \mathbb{Z}$. In other words, $p \mid n^p - n$.*

The word “little” is used to distinguish that theorem from the Fermat’s “great” one, discussed later. See <http://en.wikipedia.org/wiki/RSA> for the discussion of applications of Fermat’s Little Theorem to internet security.

Alternative Solution to Problem 9.10: By Fermat’s Little Theorem, $31 \mid 3^{31} - 3 = 3(3^{30} - 1)$. By Corollary 9.22, $3 \mid 3^{30} - 1$. Hence $3^{30} = 1 \pmod{31}$. By Corollary 9.9,

$$3^{300} = (3^{30})^{10} = 1^{10} = 1 \pmod{31}.$$

\square

Rings, non-uniqueness of factorization and Fermat’s Last Theorem.

For a given $d \in \mathbb{Z}$, denote by $\mathbb{Z}[\sqrt{d}]$ be the set of all numbers of the form $a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$. These numbers are real if $d \geq 0$ and complex if $d < 0$.

Proposition 9.27. $\mathbb{Z}[\sqrt{d}]$ is closed under addition, subtraction, and multiplication, i.e. if $x, y \in \mathbb{Z}[\sqrt{d}]$ then $x + y$, $x - y$ and $x \cdot y$ are elements of $\mathbb{Z}[\sqrt{d}]$.

Proof. – left as HW. \square

A set which is closed under addition, subtraction and multiplication, and such that the addition is distributive with respect to multiplication ($a(b + c) = ab + ac$) is called a ring.

For technical reasons let us assume that $d \neq -1, 3$. As before, we can define the prime numbers in $\mathbb{Z}[\sqrt{d}]$ to be these x which are divisible by ± 1 and $\pm x$ only. One can proof that each number has a prime factorization. But unlike for integers, such factorization does not have to be unique!

Example 9.28. *One can show that $2, 1 + \sqrt{5}, -1 + \sqrt{5}$ are all prime in $\mathbb{Z}[\sqrt{5}]$. However, we have $4 = 2 \cdot 2$ and $4 = (1 + \sqrt{5})(-1 + \sqrt{5})$.*

Despite much of mathematicians effort, it is unknown to this day for which $d \in \mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]$ has the unique factorization property.

We finish this section with the “great” theorem of Fermat:

Theorem 9.29 (“Fermat’s Last Theorem”). *For every $n > 2$ there are no $a, b, c \in \mathbb{N}$ such that $a^n + b^n = c^n$.*

The assumption of $n > 2$ is essential since the statement does not hold for $n = 2$. For example, $3^2 + 4^2 = 5^2$.

Fermat wrote his theorem on a margin of a book, together with a comment that he has an easy proof but this margin is too small to include it there. It took mathematicians 300 years to figure a proof of this theorem – it is an enormously difficult and complicated argument. Therefore, it is

very unlikely that Fermat's proof was correct. Most mathematicians believe that Fermat took the unique factorization of numbers in $\mathbb{Z}[\sqrt{d}]$ for granted for every d . Using that, one indeed can prove Fermat's Last Theorem.

Open Problems in Number Theory.

We end with two examples (among many) of famous conjectures in number theory, which still open and subject of research at present time:

Conjecture 9.30. (*Goldbach's Conjecture*) *Every even integer n greater than 2 is a sum of two prime numbers.*

For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 7 + 3 = 5 + 5$,
 $12 = 5 + 7$, $14 = 3 + 11 = 7 + 7$. Goldbach's conjecture have been verified for all numbers $n < 10^{18}$ by computers.

Conjecture 9.31. (*Twin Prime Conjecture*) *There are infinitely many pairs of primes of the form $p, p + 2$.*

Here are a few examples of pairs of "twin" primes: $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$. The conjecture is quite surprising since the differences between consecutive primes grow on average, as the numbers grow. For example, $113, 127$ is a pair of consecutive primes, since all 13 numbers between them are composite. The Twin Prime Conjecture states that, nonetheless, there are infinitely many pairs of primes of distance 2 only!

PROBLEMS 9.

Problem 9.1. Prove that $\forall_{a \in \mathbb{Z}} a \mid a$.

Problem 9.2. If a, b , and c are non-zero integers, prove that $a \mid b$ and $b \mid c$ implies $a \mid c$.

Problem 9.3. Let a and b be non-zero integers such that $a \mid b$ and $b \mid a$. Prove that $b = a$ or $b = -a$.

Problem 9.4. Proof Proposition 9.2.

Problem 9.5. Proof that 3 is prime.

Problem 9.6. Proof Proposition 9.8.

Problem 9.7. Prove Theorem 9.16(2).

Problem 9.8. Find $x, y \in \mathbb{Z}$ satisfying the equation of Example 9.20.

Problem 9.9. Prove Euclid's Lemma.

Problem 9.10. Let k be a positive integer. Prove that if $k^2 + 3$ is prime, then k is even.

Problem 9.11. Is it true that if k is even then $k^2 + 3$ is prime? Why or why not?

Problem 9.12. Use induction to prove that $n^3 - n$ is divisible by 6 for all $n \geq 0$.

Problem 9.13. Use induction to prove that $3^{2n-1} + 1$ is divisible by 4 for all $n \in \mathbb{N}$.

Problem 9.14. Use induction to prove that $11^{n+1} + 12^{2n-1}$ is divisible by 133 for all $n \in \mathbb{N}$.

Problem 9.15. (1) Does $7a + 11b = 1$ have an integral solution, i.e. $a, b \in \mathbb{Z}$ satisfying this equation? If yes, then find at least one such pair a, b . Otherwise, explain such pair does not exist.

(2) Do the same problem for $15a + 12b = 7$

(3) Do the same problem for $15a + 12b = 3$

Hint: Use Bézout's Lemma.

Problem 9.16. Find the last digit of 3^{100} .

Problem 9.17. Prove that for all $a \in \mathbb{Z}$ not divisible by 7, $a^{12} + a^6 + 5$ is divisible by 7. Hint: Use Fermat's Little Theorem and Corollary 9.22.

Problem 9.18. Prove Proposition 9.27.

10. BINARY RELATIONS

A binary relation on a set A is a certain property of pairs of some of its elements.

- Examples 10.1.** (1) A is the set of all people alive. R is the “fatherhood relation” – aRb if a is the father of b .
 (2) A is as above. S is the relation on A such that aSb iff a and b have the same mother.
 (3) A is the set of all Math 311 class students. aTb iff a and b are in the same study group.
 (4) A is as above. J is the relation on A such that aJb iff a is younger than b .
 (5) \leq is a relation on $A = \mathbb{Z}$. Eg. $2 \leq 4$
 (6) $m \in \mathbb{Z}$ is in the “divisibility relation” with $n \in \mathbb{Z}$ iff $n \mid m$. Eg. 4 is in divisibility relation with 2, but not vice versa.
 (7) Fix $n \in \mathbb{N}$. Then $m_1, m_2 \in \mathbb{Z}$ are in “mod n congruence relation” iff $m_1 = m_2 \pmod n$.

A formal definition is as follows:

Definition 10.2. A relation on a set A is a subset of $A \times A$.

In Example (1) above, the relation R on A is defined by the set of all pairs (father,son) in $A \times A$, i.e.

$$R = \{(a, b) \in A \times A : a \text{ is the father of } b\}.$$

We identify the relation R with this set. Hence, we write aRb iff $(a, b) \in R$.

Relation R on A is reflexive if $\forall a \in A \ aRa$. R is symmetric if $\forall a, b \in A \ aRb \Rightarrow bRa$. Finally, R is transitive if $\forall a, b, c \in A \ (aRb \wedge bRc) \Rightarrow aRc$.

For the seven examples above we have:

Example	Ref	Sym	Trans
1	N	N	N
2	Y	Y	Y
3	Y	Y	Y
4	N	N	Y
5	Y	N	Y
6	Y	N	Y
7	Y	Y	Y

A reflexive, symmetric, and transitive relation is called an equivalence relation. Hence, examples (2),(3) and (7) above are equivalence relations.

Equivalence relations are very important in mathematics. The most important one is the equality relation, “=”. (Note that the Preliminary Axioms in Section 6 are to make sure that = is an equivalence relation.) We will see below, that equivalence relations are used for identifying different objects. For that reason we often denote them by \sim or \simeq (by analogy with “=”).

Definition 10.3. Let \sim be an equivalence relation on A . The equivalence class of an element a of A , denoted by $[a]$ is the set $[a] = \{b \in A : b \sim a\}$.

For every $a \in A$, $[a]$ is a subset of A .

Example 10.4. For congruence mod 3 (Example 10.1(7)),

$$[0] = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}, \quad [1] = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\},$$

$$[2] = \{\dots, -7, -4, -1, 2, 5, 8, 11, 14, \dots\}.$$

Observe also that

$$\dots = [-6] = [-3] = [0] = [3] = [6] = \dots,$$

i.e. all numbers divisible by 3 have the same equivalence class. Similarly,

$$\dots = [-5] = [-2] = [1] = [4] = [7] = \dots, \quad \text{and} \quad \dots = [-4] = [-1] = [2] = [5] = [8] = \dots$$

Example 10.5. Let T be the equivalence relation of Example 10.1(3). The equivalence class of a student is the set of all students in his/her study group.

Observe that in Example 10.4 there are only three distinct equivalence classes, $[0]$, $[1]$, and $[2]$. They are disjoint and their union is the set of all integers. Similarly, in Example 10.5 there are 9 distinct equivalence classes, since there are 9 study groups in Math 311. They are disjoint and their union is the set of all Math 311 students. More generally, we have:

Proposition 10.6. Let \sim be an equivalence relation on A . For every $a, b \in A$,

- (a) if $a \sim b$ then $[a] = [b]$
 (b) if $a \not\sim b$ then $[a] \cap [b] = \emptyset$.

Proof of this proposition is assigned as HW.

Definition 10.7. A collection P of non-empty subsets of a set A is a partition of A iff

- (1) $\forall a \in A \exists S \in P \ a \in S$, and
 (2) for every $S, T \in P$, either $S = T$ or $S \cap T = \emptyset$.

For example, $\{\{1, 2\}, \{3, 4, 5\}, \{6, 7\}\}$ is a partition of $\{1, 2, 3, 4, 5, 6, 7\}$ but $\{\{1, 2, 3\}, \{3, 4, 5\}, \{6, 7\}\}$ is not.

Proposition 10.6 implies now

Corollary 10.8. For every equivalence relation \sim on a set A , the set of all equivalence classes of \sim is a partition of A .

Mod 3 congruence of Example 10.4 partitions \mathbb{Z} into three subsets

$$\{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}, \quad \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}, \quad \{\dots, -7, -4, -1, 2, 5, 11, 14, \dots\}.$$

The equivalence relation of Example 10.5 partitions all Math 311 students into 9 study groups.

The partitioning property of equivalence relations is very useful for “identifying” different elements of a set. For example, 2 is never equal to 5, but $[2] = [5]$ in Example 10.4! This method of identifying (or equating) different elements of a set is very important in advanced algebra and topology, as well as in many other areas of mathematics. We will use it in the next section to define rational numbers.

Definition 10.9. If \sim is an equivalence relation on A then the quotient set of A by \sim , denoted by A/\sim , is the set of all equivalence classes of \sim .

For example, let \sim be the mod 3 congruence on \mathbb{Z} . Then \mathbb{Z}/\sim has three elements.

PROBLEMS 10.

Problem 10.1. Find an example of a relation (on a set of your choice) which is symmetric, transitive, but not reflexive. (Try to make this example as simple as you can.)

Problem 10.2. Which of the following are relations on $A = \{1, 2, 3\}$ are symmetric, reflexive, transitive? Justify your answer whenever you claim that one of these properties fails.

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$$

$$R_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$$

$$R_3 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (1, 3)\}.$$

Problem 10.3. Prove Proposition 10.6.

11. RATIONAL NUMBERS

In elementary mathematics education we are taught that a rational number $1/3$ is a number characterized by the following property:

$$1/3 + 1/3 + 1/3 = 1.$$

This definition is not precise enough for us. Indeed, how do we know that such number exists? Or, more precisely, we do not know if declaring the existence of $1/3$ and of all other rational numbers (with their “well known” properties) does not lead to a contradiction in mathematics. (Remember the story of a barber who shaves all people who don’t shave themselves? The assumptions in this story seem very reasonable and yet they are contradictory.)

For that reason, we, mathematicians, need to define rational numbers in a precise way, on the basis of notions which we have already: the arithmetic of integers and the set theory. That is not an easy task!

In order to do that, let us ignore for now the fact the bar in $1/3$ means division. We will treat it as a formal symbol for now. With this approach, one could try to define a rational number as a formal expression: an integer followed by a bar “/”, followed by a non-zero integer, eg. $1/3$. Alternatively, we write this formal expression as $\frac{1}{3}$.

Any such expression is really a pair of numbers and, therefore, can be thought as an element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. This preliminary definition has one major fault: $1/3$ and $2/6$ are different formal expressions. We want them to be equal. We are going to “identify” them using the method of the last section. For that we need an equivalence relation \sim on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ such that

$$(a, b) \sim (c, d) \text{ iff } a/b = c/d$$

Although right side is not defined properly (since we didn’t define rational numbers yet), by multiplying both sides by bd we obtain an equality which makes formal sense in the context of the integers:

Definition 11.1. Let \sim be a relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ such that

$$(a, b) \sim (c, d) \text{ iff } ad = bc.$$

Proposition 11.2. *The relation \sim is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.*

Proof of this proposition is assigned as HW.

The equivalence class of $(1, 3)$ with respect to this relation is $[(1, 3)] = \{(1, 3), (2, 6), (3, 9), \dots, (-1, -3), (-2, -6), (-3, -9), \dots\}$.

Now are ready for the correct definition of a rational number:

Definition 11.3. A rational number (or “rational” for short) is an equivalence class of the relation \sim on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. We denote the equivalence class $[(a, b)]$ by a/b or $\frac{a}{b}$.

This is the most abstract construction you have seen in this class! It says that $1/3$ is an infinite set. More precisely, it is a subset of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$,

$$1/3 = [(1, 3)] = \{(1, 3), (2, 6), (3, 9), \dots, (-1, -3), (-2, -6), (-3, -9), \dots\}.$$

Notice that

$$2/6 = [(2, 6)] = \{(1, 3), (2, 6), (3, 9), \dots, (-1, -3), (-2, -6), (-3, -9), \dots\},$$

Hence $1/3 = 2/6$. Therefore, we have achieved our goal of identifying $1/3$ and $2/6$!

We denote the set of all rational numbers by \mathbb{Q} . (\mathbb{Q} stands for “Quotients”.) In other words, \mathbb{Q} is the quotient set

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} - \{0\}) / \sim,$$

c.f. last Section. Now we need to define the addition and the multiplication of rational numbers.

Definition 11.4. If $x = [(a, b)]$ and $y = [(c, d)]$ then

$$x + y = [(ad + bc, bd)] \quad \text{and} \quad xy = [(ac, bd)].$$

For example $1/3$ is the equivalence class of $(1, 3)$, $1/2$ is the equivalence class of $(1, 2)$ hence $1/3 + 1/2 = [(5, 6)] = 5/6$ and $1/3 \cdot 1/2 = [(1, 6)] = 1/6$. Therefore, the above definition works as expected. Unfortunately, there is a hidden potential problem with this definition. The definition of $x + y$ and $x \cdot y$ requires a choice of (a, b) and (c, d) such that $x = [(a, b)]$ and $y = [(c, d)]$. For that purpose, we can choose any element of x and any element of y . For example $(2, 6)$ is an element of the equivalence class $1/3$ and, hence, $1/3 = [(2, 6)]$. We need to make sure that the formulas for $1/3 + 1/2$ and $1/3 \cdot 1/2$ do not change if we replace $(1, 3)$ by $(2, 6)$. (Of course, we could always consider the simplest representation of $1/3$, i.e. $(1, 3)$, but that would make proving the properties of addition and multiplication in Theorem 11.6 very difficult.)

Luckily we have

Proposition 11.5. *The above definition of $x + y$ and $x \cdot y$ does not depend on the choice of a representative (a, b) of x and the choice of a representative (c, d) of y .*

Proof. We need to prove that if $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$ then

$$[(ad + bc, bd)] = [(a'd' + b'c', b'd')] \quad \text{and} \quad [(ac, bd)] = [(a'c', b'd')].$$

The premise of this implication says that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. The conclusion says

$$(ad + bc, bd) \sim (a'd' + b'c', b'd') \quad \text{and} \quad (ac, bd) \sim (a'c', b'd').$$

We leave the details of the proof out. □

From now on we will identify an integer n with the rational number $\frac{n}{1}$. Hence $\mathbb{Z} \subset \mathbb{Q}$. Observe that

$$\frac{n}{1} + \frac{m}{1} = \frac{n+m}{1}.$$

In other words, the addition of n and m thought as rational numbers coincides with the addition of integers defined in Section 7. Similarly,

$$\frac{n}{1} \cdot \frac{m}{1} = \frac{n \cdot m}{1}$$

implies that multiplication of integers thought as rational numbers coincides with the multiplication of integers defined in Section 7. These observations fully justify identifying integers n with rational numbers $\frac{n}{1}$.

Now we are ready for stating the fundamental arithmetic properties of rational numbers.

Theorem 11.6. (1) *addition of rational numbers is commutative and associative,*

(2) $\forall x \in \mathbb{Q} \ x + 0 = x$ (i.e. $0 = \frac{0}{1}$ is the “additive identity”),

(3) *multiplication of rational numbers is commutative and associative,*

(4) $\forall x \in \mathbb{Q} \ x \cdot 1 = x$ (i.e. $1 = \frac{1}{1}$ is the “multiplicative identity”),

(5) $\forall x, y, z \in \mathbb{Q} \ (x + y)z = xz + yz$ (i.e. *multiplication is distributive over addition*).

Since $(-m, n) \sim (m, -n)$ for every $m, n \in \mathbb{Z}$, $n \neq 0$, we have $\frac{-m}{n} = \frac{m}{-n}$. We denote it by $-\frac{m}{n}$ and call it the additive inverse of $\frac{m}{n}$, since $\frac{m}{n} + (-\frac{m}{n}) = 0$. A multiplicative inverse of a number x is a number y such that $x \cdot y = 1$. The multiplicative inverse of $\frac{m}{n}$ is $\frac{n}{m}$, as long as $m \neq 0$. Therefore, every non-zero rational number has a multiplicative inverse.

We denote the multiplicative inverse of x by x^{-1} and, more generally, the multiplicative inverse of x^n by x^{-n} . For any $x, y \in \mathbb{Q}$, we denote $x \cdot y^{-1}$ by x/y or $\frac{x}{y}$. This is the division (or quotient) of x by y . Therefore, $2/3$ means two things: (a) rational number $[(2, 3)]$ and (b) the quotient of 2 by 3. It is not difficult to prove that these two definitions coincide.

Definition 11.7. We say that $\frac{a}{b} < \frac{c}{d}$ iff either $(bd > 0$ and $ad < bc)$ or $(bd < 0$ and $ad > bc)$.

Note that this is not a self-referential definition, since the right side of “iff” above involves inequality relation among integers only, which was defined in Section 7.

As usual, $y > x$ is equivalent to $x < y$ and $x \leq y$ means $x < y$ or $x = y$.

Proposition 11.8. (1) For every $x, y \in \mathbb{Q}$, exactly one of the following cases holds: $x = y$,
 $x > y$, or $y > x$.

(2) $<$ is transitive,

(3) $\forall x, y, z \in \mathbb{Q} \ x < y \Rightarrow x + z < y + z$,

(4) $\forall x, y, z \in \mathbb{Q}$ if $z > 0$ and $x < y$ then $x \cdot z < y \cdot z$.

PROBLEMS 11.

Problem 11.1. Prove Proposition 11.2.

Problem 11.2. Which of the following are true? Justify your answer.

(1) A rational number is an element of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.

(2) A rational number is an infinite set.

(3) Every infinite subset of $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ is a rational number.

Problem 11.3. Write the definition of $2/5$.

Problem 11.4. Proof that if rational numbers x and y are not equal to zero, then $x \cdot y \neq 0$. (Hint: Use Theorem 7.11.)

12. REAL NUMBERS

There are real numbers which are not rational.

Proposition 12.1. *(due possibly to Hippasus, 5 century BC.)*

$\sqrt{2}$ is irrational.

Proof. Suppose that $\sqrt{2} = \frac{m}{n}$. By dividing m and n by $\gcd(m, n)$ if necessary, we can assume that m and n are relatively prime. We have $m^2 = 2n^2$ and, therefore, $2 \mid m \cdot m$. By Corollary 9.22, 2 divides m . Hence m^2 is divisible by 4. But $m^2 = 2n^2$. Hence n is divisible by 2. Therefore m and n are both even, contradicting relative primeness. \square

Therefore $\sqrt{2}$ is an example of a real number which is not rational. But how do we define real numbers? The challenge is to do it in a way which involves only notions defined rigorously already – that is integers, rational numbers, and sets. Our approach will rely on the fact that each real number can be “approximated” by rational numbers.

Let us start with the following informal definition: A “Dedekind cut” is a pair of sets

$$(12.1.1) \quad A = \mathbb{Q} \cap (-\infty, \alpha), \quad B = \mathbb{Q} \cap [\alpha, \infty),$$

for some real (rational or irrational number) α . The motivation for this construction is that a Dedekind cut describes a real number in terms of rational ones – it divides all rational numbers into those which lie below α and those which lie above it. This is the reason for the term “cut”.

The set A is called a Dedekind set. Since $B = \mathbb{Q} - A$, the Dedekind cut (A, B) is determined by the Dedekind set A . Every Dedekind set A has the following properties:

- (1) $A \subset \mathbb{Q}$ is non-empty and not equal to \mathbb{Q} ,
- (2) For every $x \in A$ and every $y \in \mathbb{Q} - A$, $x < y$.
- (3) A does not contain the largest element.

Definition 12.2. A Dedekind set is subset of \mathbb{Q} satisfying the properties (1), (2), and (3). A Dedekind cut is a pair (A, B) where A is a Dedekind set and $B = \mathbb{Q} - A$.

Remark 12.3. *Condition (2) implies that if x belongs to a Dedekind set A , then for every $y < x$, $y \in A$ as well. (Indeed, if $y \in \mathbb{Q} - A$ then $y > x$ by condition (2) above.)*

Lemma 12.4. **+Definition** For every $\alpha \in \mathbb{Q}$, $\{x \in \mathbb{Q} : x < \alpha\}$ is a Dedekind set. We denote it by $\underline{\alpha}$.

The statement follows from the discussion above. Here is a formal proof: Condition (1) holds since $\alpha - 1 \in \underline{\alpha}$ and $\alpha + 1 \notin \underline{\alpha}$.

If $a \in \underline{\alpha}$ and $b \in \mathbb{Q} - \underline{\alpha}$ then $a < \alpha \leq b$ – hence condition (2) holds as well.

To prove condition (3), we need to show that for every element $a \in \underline{\alpha}$ there is an element $a' \in \underline{\alpha}$ larger than a . We claim that $a' = \frac{a+\alpha}{2} \in \underline{\alpha}$ is such an element. Indeed a' is the arithmetic average of a and α . Hence it is always between a and α . Here is a formal version of this argument: $a < \alpha \Rightarrow a + \alpha < 2\alpha \Rightarrow \frac{a+\alpha}{2} < \alpha$. Hence $a' \in \underline{\alpha}$. On the other hand, $a < \alpha \Rightarrow 2a < \alpha + a \Rightarrow a < \frac{a+\alpha}{2} = a'$. \square

Remark 12.5. *Assuming knowledge of real numbers, observe that furthermore $\underline{\alpha}$ is a well-defined subset of \mathbb{Q} for all real numbers α . This will motivate us to define real numbers as Dedekind sets (or, equivalently, Dedekind cuts)!*

Intuitively, we would like to identify $\sqrt{2}$ with the Dedekind set

$$\{x \in \mathbb{Q} : x < \sqrt{2}\}$$

but of course such definition would be self-referential, since this expression involves $\sqrt{2}$. However, we can rewrite this set as

$$\{x \in \mathbb{Q} : x^2 < 2 \vee x < 0\}.$$

Let us denote it by $\sqrt{2}$. Note that the part “ $x < 0$ ” of the condition is important, since $x^2 < 2$ means $x \in (-\sqrt{2}, \sqrt{2})$ and we need $(-\infty, \sqrt{2})$. Here is a formal verification of the fact that this is a Dedekind set:

Lemma 12.6. $\sqrt{2} = \{x \in \mathbb{Q} : x^2 < 2 \text{ or } x < 0\}$ is a Dedekind set.

Proof. Condition (1) holds since $1 \in A$ and $2 \notin A$.

Proof of condition (2): Let $x \in A$ and $y \in \mathbb{Q} - A$. Then $y^2 \geq 2$ and $y \geq 0$. There are two possibilities: (a) $x < 0$ or (b) $x > 0$ and $x^2 < 2$. The first one implies $x < 0 < y$ and the second one implies $y^2 > x^2$. In other words $y^2 - x^2 = (y - x)(y + x) > 0$. Since $y + x > 0$, also $y - x > 0$. Therefore, we proved that in both cases, (a) and (b), $y > x$.

Proof of condition (3): Let $x \in \sqrt{2}$. We need to find an element of $\sqrt{2}$ which is larger than x . If $x < 0$ then 1 is such an element. Therefore assume that $x > 0$ and $x^2 < 2$. We are going to complete the proof by showing that there exists a natural number n such that

$$x + \frac{1}{n} \in \sqrt{2}.$$

This inequality can be rewritten as

$$x^2 + 2x\frac{1}{n} + \frac{1}{n^2} < 2,$$

or as

$$(2 - x^2)n^2 - 2xn - 1 > 0.$$

Since x is constant, the left side is a quadratic function in n with positive leading coefficient. Hence indeed the above expression is positive for sufficiently large n . \square

Linear Ordering of Dedekind sets.

Proposition 12.7. For every Dedekind sets A, B either $A \subset B$ or $B \subset A$.

Proof. Suppose that $A \not\subset B$. Then there is $a \in A$ such that $a \notin B$. By condition (2) of definition of a Dedekind set, since $a \notin B$, $\forall b \in B$ $b < a$. By Remark 12.3, all $b \in B$ belong to A . Hence $B \subset A$. \square

Definition 12.8. We write $A \leq B$ iff $A \subset B$ and we write $A < B$ iff $A \subsetneq B$.

The above proposition implies that for all Dedekind sets A, B precisely one condition holds: $A < B$ or $A = B$ or $B < A$.

Addition of Dedekind sets.

Definition 12.9. If $A, B \subset \mathbb{Q}$ then $A + B = \{x + y : x \in A, y \in B\} \subset \mathbb{Q}$.

For example, we claim that

$$\underline{1/2} + \underline{1} = \underline{3/2}.$$

To see that, we need to prove two inclusions. Proof of $\underline{1/2} + \underline{1} \subset \underline{3/2}$: Every element of $\underline{1/2} + \underline{1}$ is of the form $x + y$ where $x < 1/2$ and $y < 1$. Since $x + y$ is rational number lower than $3/2$, it belongs to $\underline{3/2}$.

Proof of $\underline{1/2} + \underline{1} \supset \underline{3/2}$: Every element z of $\underline{3/2}$ can be written as $z/3 + 2z/3$. Since these summands are rational and $z/3 < 1/2$, $2z < 1$, $z/3 \in \underline{1/2}$ and $2z/3 \in \underline{1}$. Hence, $z \in \underline{1/2} + \underline{1}$. \square

The following is a generalization of the above example:

Proposition 12.10. If A and B be Dedekind sets then $A + B$ is a Dedekind set as well.

Proof. Proof of condition (1): Since A, B are non-empty, $A + B$ is non-empty as well. By condition (1) of Dedekind sets, there are $x \in \mathbb{Q} - A$, $y \notin \mathbb{Q} - B$. We are going to complete the proof of condition (1) for $A + B$ by showing that $x + y \notin A + B$. Proof: Suppose that $x + y \in A + B$. Then $x + y = a + b$ for some $a \in A$, $b \in B$ and $(x - a) + (y - b) = 0$. Hence either $x - a \leq 0$ or $y - b \leq 0$ (since $x - a > 0$ and $y - b > 0$ would mean $(x - a) + (y - b) = 0$). In the first case, $x \leq a$, implying that $x \in A$, by

Remark 12.3, and hence contradicting the fact that $x \in \mathbb{Q} - A$. In the second case, $y \leq b$ implying that $y \in B$ and contradicting the fact that $y \in \mathbb{Q} - B$.

Proof of Condition (2): Let $c \in A + B$ and $d \in \mathbb{Q} - (A + B)$. We need to show that $c < d$. By definition of $A + B$, $c = a + b$ for some $a \in A, b \in B$. Note that $d - a \notin B$, since if $d - a = b' \in B$ then $d = a + b' \in A + B$. Hence by condition (2) applied to B , $b < d - a$. Therefore $c = a + b < d$.

Proof of condition (3): left as HW. \square

Recall that $\underline{0} = \{x \in \mathbb{Q} : x < 0\}$.

- Theorem 12.11.** (1) For all Dedekind sets A , $\underline{0} + A = A$ (i.e. $\underline{0}$ is the additive identity)
(2) For all Dedekind sets A, B , $A + B = B + A$ (i.e. addition is commutative)
(3) For all Dedekind sets A, B, C , $(A + B) + C = A + (B + C)$ (i.e. addition is associative)
(4) For every Dedekind set A there is a Dedekind set, denoted by $-A$, such that $A + (-A) = \underline{0}$ (i.e. every Dedekind set has an additive inverse).
(5) If $A < B$ then $A + C < B + C$.
(6) For every $x, y \in \mathbb{Q}$, $\underline{x} + \underline{y} = \underline{x + y}$.

Multiplication of Dedekind sets. Now we are going to define multiplication of Dedekind sets. The informal idea is as follows: by Remark 12.5, every Dedekind set is of the form $\underline{\alpha} = \{a \in \mathbb{Q} : a < \alpha\}$ for some real α . We want to define a multiplication of $\underline{\alpha}$ with $\underline{\beta} = \{b \in \mathbb{Q} : b < \beta\}$, so that

$$\underline{\alpha} \cdot \underline{\beta} = \underline{\alpha \cdot \beta} = \{c \in \mathbb{Q} : c < \alpha \cdot \beta\}.$$

Unfortunately, we cannot use it as a formal definition, since we didn't define real numbers yet, and we cannot use Remark 12.5.

The definition of addition of Dedekind sets suggests to define $A \cdot B$ as $\{a \cdot b : a \in A, b \in B\}$. Indeed, if $a \in \underline{x}$ and $b \in \underline{y}$ and $a > 0$ or $b > 0$ then $ab \in \underline{xy}$. Unfortunately this definition does not work if $a, b < 0$. Eg. $-10 \in \underline{2}$, $-10 \in \underline{3}$ but $(-10)(-10) \notin \underline{6}$. Therefore, the definition of multiplication needs to take into account signs of a and b . Hence for every $A, B \subset \mathbb{Q}$, we define

$$A \cdot B = \begin{cases} \{x \cdot y : x \in A, x > 0, y \in B\} & \text{if } A > \underline{0} \\ \{x \cdot y : x \in A, y \in B, y > 0\} & \text{if } B > \underline{0} \end{cases}$$

and $A \cdot B = (-A) \cdot (-B)$ for $A \leq \underline{0}$ and $B \leq \underline{0}$.

Theorem 12.12. If A, B are Dedekind sets then $A \cdot B$ is.

Theorem 12.13. For all Dedekind sets A, B, C

- (1) $A \cdot \underline{1} = A$
(2) $A \cdot B = B \cdot A$
(3) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.
(4) $A(B + C) = AB + AC$.
(5) If $A < B$ and $C > 0$ then $A \cdot C < B \cdot C$.

For any Dedekind sets $A, B > \underline{0}$ we define

$$A/B = \{a/b \in \mathbb{Q} : a \in A, b \in \mathbb{Q} - B\}.$$

Proposition 12.14. For all Dedekind sets $A, B > \underline{0}$,

- (1) A/B is a Dedekind set.
(2) $A/B \cdot B = A$.

For all Dedekind sets A and $B \neq \underline{0}$, we define

$$A/B = \begin{cases} \underline{0} & \text{if } A = \underline{0} \\ -((-A)/B) & \text{if } A < \underline{0}, B > \underline{0} \\ -(A/(-B)) & \text{if } A > \underline{0}, B < \underline{0} \\ (-A)/(-B) & \text{if } A < \underline{0}, B < \underline{0} \end{cases}$$

The point of this definition is that the quotients on the right side involve positive Dedekind sets only and, hence, are defined by Proposition 12.14. Therefore, A/B is a Dedekind set for all Dedekind sets A and $B \neq \underline{0}$. Furthermore, we have the following generalization of Proposition 12.14:

Proposition 12.15. *For all Dedekind sets A and $B \neq \underline{0}$ we have $A/B \cdot B = A$.*

Summarizing the discussion above, we see that

- (1) every rational number defines a Dedekind set
- (2) our intuition about irrational real numbers tells us that each of them defines a Dedekind set as well
- (3) Dedekind sets can be added, multiplied, and divided, and that these operations satisfy the properties of addition, multiplication and of division of real numbers.
- (4) one can define inequalities $A < B$ between Dedekind sets.

Therefore, applying the principle:

“if it looks like a duck, swims like a duck and quacks like a duck, then it is a duck”
we define real numbers as Dedekind sets.²

Definition 12.16. A real number is a Dedekind set. We denote the set of all real numbers by \mathbb{R} . Real numbers of the form \underline{x} for $x \in \mathbb{Q}$ are called rational real numbers. The real numbers which are not rational are called irrational.

By our earlier definition,

$$\underline{\sqrt{2}} = \{x \in \mathbb{Q} : x^2 < 2 \vee x < 0\}$$

Indeed, one can prove that

$$(12.16.1) \quad \underline{\sqrt{2}} \cdot \underline{\sqrt{2}} = \underline{2} \text{ and } \underline{\sqrt{2}} > \underline{0}.$$

Therefore, denoting the above set by $\underline{\sqrt{2}}$ is fully justified. By Proposition 12.1, $\underline{\sqrt{2}}$ is an irrational real number.

Definition 12.17. For every positive $x \in \mathbb{R}$ and for every $n \in \mathbb{Z}$ let

$$\sqrt[n]{x} = \{a \in \mathbb{Q} : a \leq 0 \vee a^n < x\}.$$

It is called the n -th root of x .

Theorem 12.18. *For every positive $x \in \mathbb{R}$ and for every $n \in \mathbb{N}$,*

- (1) $\sqrt[n]{x}$ is a Dedekind set.
- (2) $\sqrt[n]{x}$ is the unique positive real number such that $(\sqrt[n]{x})^n = x$.

Sketch of Proof:

We leave part of (1) as HW.

We prove (2) by contradiction. Suppose that $A \neq \sqrt[n]{x}$ and $A^n = x$, $A > 0$. If $A < \sqrt[n]{x}$, then by Proposition 12.13,

$$A < \sqrt[n]{x} \Rightarrow A^2 < A \cdot \sqrt[n]{x} < (\sqrt[n]{x})^2 \Rightarrow \dots \Rightarrow A^n < (\sqrt[n]{x})^n,$$

by an inductive argument (similar to that of the proof of Proposition 8.2(4)), leading to contradiction. If $\sqrt[n]{x} < A$ then the proof is analogous. \square

Given real numbers $x < y$, we define

$$(x, y) = \{z \in \mathbb{R} : x < z < y\}, \quad [x, y) = \{z \in \mathbb{R} : x \leq z < y\}, \quad (x, y] = \{z \in \mathbb{R} : x < z \leq y\}, \\ [x, y] = \{z \in \mathbb{R} : x \leq z \leq y\}.$$

Therefore (a, b) may mean either an ordered pair, $\{a, \{b\}\}$, or an open interval from a to b . Usually the specific meaning of (a, b) is obvious from the context.

²There is one exception to this principle: It may look like a duck, swim like a duck and quack like a duck, but if Chuck Norris says it is a chicken, then it is a damn chicken. To the best of our knowledge, however, Chuck Norris does not claim that Dedekind sets are chicken.

Although $\pm\infty$ is not a number, it is useful and natural to expand the above notation to

$$(x, \infty) = \{z \in \mathbb{R} : x < z\}, [x, \infty) = \{z \in \mathbb{R} : x \leq z\}, \\ (-\infty, y) = \{z \in \mathbb{R} : z < y\}, (-\infty, y] = \{z \in \mathbb{R} : z \leq y\}, (-\infty, \infty) = \mathbb{R}.$$

PROBLEMS 12.

Problem 12.1. (1) How would you define $-\sqrt{2}$?

(2) Proof that your definition satisfies conditions (1) and (2) of Dedekind sets.

Problem 12.2. Complete the remaining part of the proof of Proposition 12.10. That is, if A, B are Dedekind sets then $A + B$ satisfies condition (3) of Dedekind sets.

Problem 12.3. Proof Theorem 12.11(1). *Hint:* Proof two inclusions: $A + \underline{0} \subset A$ (easy) and $A + \underline{0} \supset A$ (harder). To prove the second inclusion, use the fact that for every $a \in A$ there is $a' \in A$ larger than a .

Problem 12.4. Let $\underline{\sqrt{2}} = \{x \in \mathbb{Q} : x^2 < 2 \vee x < 0\}$. Prove that

(a) $\underline{\sqrt{2}} > \underline{1}$

(b) $\underline{\sqrt{2}} \cdot \underline{\sqrt{2}} \leq \underline{2}$. (In fact, we have $\underline{\sqrt{2}} \cdot \underline{\sqrt{2}} = \underline{2}$, c.f. eq. (12.16.1), but to make things simpler for you, I do not ask to prove it.)

Problem 12.5. Prove $\underline{1/2} = \underline{1}/\underline{2}$ using the definition of A/B (without referring to Proposition 12.14).

Problem 12.6. Let $x > 0$ and $n \in \mathbb{N}$. Prove a piece of Theorem 12.18(1) by showing that $\sqrt[n]{x}$ satisfies the following properties of Dedekind sets:

(1) $\sqrt[n]{x} \neq \emptyset$ and $\sqrt[n]{x} \neq \mathbb{Q}$.

(2) if $a \in \sqrt[n]{x}$ and $b \in \mathbb{Q} - \sqrt[n]{x}$ then $a < b$.

Problem 12.7. Find irrational real numbers x, y such that $x + y$ is rational. (*Hint:* You can take $x = \sqrt{2}$, which is irrational by Proposition 12.1. You need to prove that your y is irrational.)

Problem 12.8. Using your calculus knowledge, show that that $\{x \in \mathbb{Q} : x^3 + 3x < 1\}$ is a Dedekind set.

13. LARGEST LOWER AND LEAST UPPER BOUNDS

As in Definition 9.15, we say that l is a lower bound of a set $A \subset \mathbb{R}$ if $\forall a \in A, l \leq a$. A is bounded from below if such l exists. Similarly, u is an upper bound of $A \subset \mathbb{R}$ if $\forall a \in A, a \leq u$. A is bounded from above if such u exists.

We say that u is the least upper bound for A if u is the smallest upper bound for A . We define the largest lower bound analogously.

$$\begin{aligned} \sup A &= \begin{cases} \text{least upper bound of } A & \text{if } A \text{ is bounded from above,} \\ \infty & \text{otherwise.} \end{cases} \\ \inf A &= \begin{cases} \text{largest lower bound of } A & \text{if } A \text{ is bounded from below,} \\ -\infty & \text{otherwise.} \end{cases} \end{aligned}$$

Example 13.1. *There are infinitely many upper bounds on $A = \{1, 3, 5\} \subset \mathbb{R}$, e.g. $5, 7, 17/2, \dots$. The least upper bound is 5 .*

Proposition 13.2. *If the least upper bound exists then it is unique.*

Proof. Suppose that $u_1 \neq u_2$ are least upper bounds for A . Then either $u_1 < u_2$ and u_2 is not the smallest upper bound or $u_1 > u_2$ and, then, u_1 is not the least upper bound. \square

Theorem 13.3. *(Proof below.) If A is a non-empty subset of real numbers bounded from above then*

- (1) $u_0 = \bigcup_{a \in A} a$ is a Dedekind set, i.e. a real number.
- (2) Furthermore, u_0 is the least upper bound of A .

Similarly, we have:

Theorem 13.4. *If A is a non-empty subset of real numbers bounded from below, then*

- (1) $l_0 = \bigcap_{a \in A} a$ is a Dedekind set, i.e. a real number.
- (2) Furthermore, l_0 is the largest lower bound of A .

Corollary 13.5. *“Least Upper Bound Principle” Let A be a non-empty subset of real numbers.*

- (1) *If A is bounded from above then it has the least upper bound. This is the “Least Upper Bound Principle”.*
- (2) *If A is bounded from below then it has the largest lower bound.*

This statement is not as obvious as it may appear at first sight. In appreciate it, observe that subsets of \mathbb{Q} do not have the least upper bound property (in \mathbb{Q}). Consider for example a subset $A = \{x \in \mathbb{Q} : x < \sqrt{2}\}$ of rational numbers, \mathbb{Q} . This set is bounded from above (in the rationals), e.g. by 2. However, it does not have the least upper bound inside \mathbb{Q} . Indeed, the set of upper bounds of A in \mathbb{Q} ,

$$\{x \in \mathbb{Q} : x \geq \sqrt{2}\},$$

does not have the smallest element.

Proof of Theorem 13.3(1): We need to prove that u_0 satisfies the three properties of Dedekind sets:

- (i) Since A is non-empty, u_0 is non-empty. By assumption, $\forall a \in A, a < u$. By definition, $a < u$ means $a \subset u$. Hence $u_0 = \bigcup_{a \in A} a \subset u$. Since u is a Dedekind set, $u \subsetneq \mathbb{Q}$ and, hence, $u_0 \subsetneq \mathbb{Q}$.
- (ii) Let $x \in u_0$ and $y \in \mathbb{Q} - u_0$. We need to prove that $x < y$. Since $u_0 = \bigcup_{a \in A} a$, $x \in a$, for some $a \in A$. Also, $y \in \mathbb{Q} - u_0 \subset \mathbb{Q} - a$. Since a is a Dedekind set, by property (2), $x < y$. Hence we proved property (2) for u_0 .
- (iii) Left as HW.

Proof of Theorem 13.3(2): For every upper bound, u , of A and for every $a \in A$ we have $a \leq u$. By definition of inequality for real numbers, it means that $a \subset u \subset \mathbb{Q}$. Hence $u_0 = \bigcup_{a \in A} a \subset u$, implying that $u_0 \leq u$. Therefore, u_0 is the lowest upper bound. \square

PROBLEMS 13.

Problem 13.1. Finish the proof of Theorem 13.3(1). That is, prove that u_0 satisfies the third property of Dedekind sets i.e. that u_0 does not have the largest element.

Problem 13.2. (1) Prove that if a non-empty set $X \subset \mathbb{R}$ is bounded from above and below then $\inf X \leq \sup X$.

(2) What is the simplest characterization of sets $X \subset \mathbb{R}$ such that $\inf X = \sup X$?

Proposition 14.1. For every real number x there is an integer p larger than x .

Proof. If $x \leq 0$ then $p = 1$ satisfies the statement. Therefore, assume that $x > 0$. Since $x \notin \mathbb{Q}$, there is a rational number $p/q \notin x$, $p, q \in \mathbb{Z}$. Since x contains zero and all negative numbers, $p/q > 0$ and, hence, we can assume that $p, q > 0$. Then by multiplying both sides of $1 \leq q$ by x , we get $x \leq q \cdot x = p$. If $x < p$ then we are done. Otherwise, we take $p + 1$. \square

Corollary 14.2.

(1) If x and y are positive real numbers, then there exists a positive integer p such that $px > y$. This statement is called *Archimedean Principle*.

(2) For every positive $\varepsilon \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.

Proof is left as HW.

Remark 14.3. Traditionally the Greek epsilon, ε , has been used to designate a “very small” quantity. More precisely, ε can be an arbitrary real number, but the statement containing ε is interesting only if ε is very small. Corollary 14.2(2) is an example.

Definition 14.4. For every real number x ,

(1) $\lfloor x \rfloor$ is the largest integer not greater than x .

(2) $\lceil x \rceil$ is the smallest integer not less than x .

$\lfloor x \rfloor$ is sometimes called the largest integer in x . Examples: $\lfloor \sqrt{10} \rfloor = 3$, $\lceil \sqrt{10} \rceil = 4$, $\lfloor -\sqrt{10} \rfloor = -4$, $\lceil -\sqrt{10} \rceil = -3$.

Proposition 14.5. For every $x \in \mathbb{R}$, $\lceil x \rceil$ and $\lfloor x \rfloor$ exist.

Proof. (1) Let $A \subset \mathbb{Z}$ be the set of all integers larger or equal to x . By Proposition 14.1, $A \neq \emptyset$. By Well Ordering Principle, there exists the smallest element in A . It is $\lceil x \rceil$.

(2) Let $A \subset \mathbb{Z}$ be the set of all integers larger or equal to $-x$. By Proposition 14.1, $A \neq \emptyset$. By Well Ordering Principle, there exists the smallest element a in A . Then $\lfloor x \rfloor = -a$. \square

$\lfloor \cdot \rfloor, \lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}$ are called the floor and ceiling functions, respectively.

Remark 14.6. (1) If $x \in \mathbb{Z}$ then $\lceil x \rceil = \lfloor x \rfloor = x$.

(2) If $x \notin \mathbb{Z}$ then $\lceil x \rceil = \lfloor x \rfloor + 1$.

Dense subsets of \mathbb{R} .

Definition 14.7. We say that a set $S \subset \mathbb{R}$ is dense in \mathbb{R} if for all $x, y \in \mathbb{R}$, $x < y$ there exists $s \in S$ such that $x < s < y$.

Clearly, \mathbb{R} is dense in \mathbb{R} but $(0, 1) \subset \mathbb{R}$ is not. (There are no elements of $(0, 1)$ between $x = 2$ and $y = 3$.)

Proposition 14.8.

(1) \mathbb{Q} is a dense subset of \mathbb{R}

(2) the set of irrational numbers is dense in \mathbb{R} .

Proof. (1) Let $x < y$, $x, y \in \mathbb{R}$. We need to prove that there exists a rational number p/q between x and y . By Corollary 14.2(2), there exists $q \in \mathbb{N}$ such that $\frac{1}{q} < \frac{y-x}{2}$. Then $2 < qy - qx$. We claim that $p = \lfloor qx \rfloor + 1$ is an integer such that

$$(14.8.1) \quad qx < p < qy$$

and, hence, $x < p/q < y$. Therefore, we only need to prove inequality (14.8.1). The left one, follows from $qx < \lfloor qx \rfloor + 1 = p$. To prove the right inequality, observe that $p = \lfloor qx \rfloor + 1 \leq qx + 1 + 1 < qy$.

(2) For every $a \in \mathbb{Q}$, $a \neq 0$, $a\sqrt{2}$ is irrational. (If $b = a\sqrt{2}$ was rational then $\sqrt{2}$, being the quotient

of rational numbers b and a , would be rational as well, contradicting Proposition 12.1.) Therefore, it is enough to prove that for all real numbers $x < y$ there is $a \in \mathbb{Q}$ such that $x < a\sqrt{2} < y$. Since this double inequality is equivalent to $\frac{x}{\sqrt{2}} < a < \frac{y}{\sqrt{2}}$, the statement follows from part (1) of the proposition. \square

PROBLEMS 14.

Problem 14.1. Prove Corollary 14.2.

Problem 14.2. Let x and y denote real numbers. In terms of the greatest integer:

- a) Show that $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.
- b) Give an example where $\lfloor x \rfloor + \lfloor y \rfloor < \lfloor x + y \rfloor$.
- c) Show that $x + y < \lfloor x \rfloor + \lfloor y \rfloor + 2$.
- d) Give an example where $x + y = \lfloor x \rfloor + \lfloor y \rfloor + 1.99$.

Problem 14.3. (1) Can a set bounded from below be dense in \mathbb{R} ?

(2) Find an example of a subset of \mathbb{R} which is unbounded from below and from above and which is not dense.

Problem 14.4. Prove that if $S \subset \mathbb{R}$ is dense then for all $x < y$ in \mathbb{R} there are infinitely many elements $s \in S$ such that $x < s < y$. *Hint:* Suppose that there are finitely many of them only. Label them s_1, \dots, s_n in an increasing order. Derive a contradiction.

15. MONOTONE SEQUENCE PROPERTY

An infinite sequence (of real numbers) is a function $f : \mathbb{N} \rightarrow \mathbb{R}$, often denoted by $f(1), f(2), \dots$ or by $\{f(n)\}$. For example, $f(n) = 1/n$ is often written as $1, 1/2, 1/3, \dots$ or $\{1/n\}_{n=1}^{\infty}$. Hence, $\{a_n\}_{n=1}^{\infty}$ denotes the function $f(n) = a_n$.

A sequence $\{a_n\}_{n=1}^{\infty}$ is bounded from above (or below) if the set $\{a_n : n \in \mathbb{N}\}$ is.

Definition 15.1. $\{a_n\}_{n=1}^{\infty}$ converges to a real number L , denoted by $\lim_{n \rightarrow \infty} a_n = L$, if for every $\varepsilon > 0$ there exists N such that $|a_n - L| < \varepsilon$ for all $n > N$.

We say that a property $P(n)$, where $n \in \mathbb{N}$, holds for large n if there is $N \in \mathbb{N}$ such that $P(n)$ holds for all $n > N$. Hence, $\lim_{n \rightarrow \infty} a_n = L$, if for every $\varepsilon > 0$, $|a_n - L| < \varepsilon$ for large n .

Example 15.2. $\{1/n\}_{n=1}^{\infty}$ converges to 0. (Proof in class or HW.)

Proposition 15.3. A convergent sequence is bounded.

Definition 15.4. A sequence $\{a_n\}_{n=1}^{\infty}$ is non-decreasing if $a_{n+1} \geq a_n$ for all $n \in \mathbb{N}$ and increasing if $a_{n+1} > a_n$ for all $n \in \mathbb{N}$. Similarly, the sequence is non-increasing if $a_{n+1} \leq a_n$ for all $n \in \mathbb{N}$ and decreasing if $a_{n+1} < a_n$ for all $n \in \mathbb{N}$. A sequence is monotone if either it is non-increasing or non-decreasing.

Proposition 15.5 (The Monotone Sequence Property).

- (1) Every non-decreasing sequence bounded above converges to its least upper bound.
- (2) Every non-increasing sequence that is bounded below converges to its largest lower bound.

Proposition 15.6. +Defn. Given a sequence $\{a_n\}_{n=1}^{\infty}$, let $m_n := \inf\{a_k : k \geq n\} \in \mathbb{R} \cup \{-\infty\}$ and let $M_n := \sup\{a_k : k \geq n\} \in \mathbb{R} \cup \{\infty\}$. Then $\{m_n\}_{n=1}^{\infty}$ is non-decreasing and $\{M_n\}_{n=1}^{\infty}$ is non-increasing,

We define

$$\begin{aligned} \liminf a_n &:= \lim_{n \rightarrow \infty} m_n \quad \text{and} \\ \limsup a_n &:= \lim_{n \rightarrow \infty} M_n. \end{aligned}$$

Example 15.7. (1) $\liminf a_n = -1$ and $\limsup a_n = 1$ for $a_n = (-1)^n + 1/n$.

(2) $\liminf a_n = \limsup a_n = L$ for $a_n = (-1)^n/n$.

(3) Numerical evidence suggests that $\liminf a_n = -1$ and $\limsup a_n = 1$ for $a_n = \sin(n)$. (You may be asked to prove it in HW.)

Proposition 15.8. (1) If $\liminf a_n, \liminf b_n$ are finite then $\liminf a_n + b_n$ is finite and $\liminf a_n + b_n \geq \liminf a_n + \liminf b_n$.

(2) If $\limsup a_n, \limsup b_n$ are finite then $\limsup a_n + b_n$ is finite and $\limsup a_n + b_n \leq \limsup a_n + \limsup b_n$.

(We assume here that $\infty + x = \infty$ and $-\infty + x = -\infty$.)

Proof is left as HW.

Proposition 15.9. $a_n \rightarrow L$ if and only if $\liminf a_n = L$ and $\limsup a_n = L$.

Proposition 15.10. Let A and x_1 be positive real numbers. Define a sequence by $x_n := \frac{1}{2}(x_{n-1} + \frac{A}{x_{n-1}})$ for $n \geq 2$. Then $x_n \rightarrow \sqrt{A}$.

Proof in class

□

PROBLEMS 15.

Problem 15.1. Let $a_n := 1/1 + 1/2 + \dots + 1/n - \ln n$. Show that $\{a_n\}$ is decreasing. Note that $\ln n := \int_1^n 1/x dx$. (You may find it useful to look at the picture accompanying the proof of the integral test in any calculus book.)

Problem 15.2. (continuation of Problem 15.1) Let $b_n := 1/1 + 1/2 + \dots + 1/(n-1) - \ln n$ for $n \geq 2$. Show that $b_n \geq 0$ for all $n \geq 2$. Hint: this is similar to the integral test. Use the result on b_n to conclude that $\{a_n\}$ is bounded below.

Problem 15.3. (continuation of Problem 15.1) Show that $\{a_n\}$ converges. The limit is called Euler's Constant or the Euler-Mascheroni Constant and is denoted by γ . The value of γ is approximately $.5772157\dots$; it is unknown whether γ is irrational.

Problem 15.4. Prove that $\limsup_{n \rightarrow \infty} \sin(n) = 1$.

Problem 15.5. (1) Proof Proposition 15.8(1).

(2) Can $\liminf a_n + b_n$ be not equal to $\liminf a_n + \liminf b_n$?

16. DECIMAL EXPANSIONS

Numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 are called **digits**. A decimal numeral system is a method of denoting real numbers as sequences of digits. A sequence

$$\pm b_m \dots b_0 . a_1 a_2 a_3 \dots$$

denotes the sum

$$(16.0.1) \quad x = \pm(b_m \cdot 10^m + \dots + b_1 \cdot 10 + b_0 + a_1 \cdot 10^{-1} + a_2 \cdot 10^{-2} + a_3 \cdot 10^{-3} \dots)$$

There are finitely many b 's (in front of the decimal point) but there may be a finite or infinite number of a 's. Using your calculus knowledge, you should be able to prove that even if the number of a 's is infinite the sum is convergent (i.e. adds up to a finite number). The right side of (16.0.1) is called a decimal expansion or decimal representation of x .

Remark 16.1. If $a_k = 0$ for all $k > n$ then $b_m \dots b_0 . a_1 a_2 a_3 \dots$ (infinite decimal expansion) is equal to and identified with $b_m \dots b_0 . a_1 a_2 a_3 \dots a_n$ (finite expansion).

Lemma 16.2. For every $x \in \mathbb{R}$ there is the largest $m \in \mathbb{Z}$ such that $x \geq 10^m$

Proof. in class □

If $x > 0$ then such expansion of x can be constructed as follows:

- Let m be the largest integer such that $x \geq 10^m$. Its existence is implied by Lemma 16.2
- Let $b_m = \lfloor x/10^m \rfloor$, $b_{m-1} = \lfloor (x - b_m \cdot 10^m)/10^{m-1} \rfloor$, $b_{m-2} = \lfloor (x - b_m \cdot 10^m - b_{m-1} \cdot 10^{m-1})/10^{m-2} \rfloor$, and so on. Finally, let

$$\bullet b_0 = \lfloor x - (b_m \cdot 10^m + b_{m-1} \cdot 10^{m-1} + \dots + b_1 \cdot 10) \rfloor.$$

Let $x_0 = x - b_m \cdot 10^m - b_{m-1} \cdot 10^{m-1} - \dots - b_1 \cdot 10 - b_0$. Note that $0 \leq x_0 < 1$ and that $x - x_0 \in \mathbb{Z}$. Therefore $x_0 = x - \lfloor x \rfloor$.

Now we define a_1, a_2, \dots inductively:

$$\bullet a_1 = \lfloor x_0 \cdot 10 \rfloor, a_2 = \lfloor x_0 \cdot 10^2 - a_1 \cdot 10 \rfloor.$$

Suppose that a_1, \dots, a_n are defined. Then

$$\bullet a_{n+1} = \lfloor (x_0 \cdot 10^{n+1} - (a_1 \cdot 10^n + \dots + a_{n-1} \cdot 10 + a_n \cdot 10)) \rfloor.$$

Proposition 16.3. For every real number $x \geq 0$, $b_m, \dots, b_0, a_1, a_2, a_3 \dots \in \{1, 2, \dots, 9\}$. Hence the above sequence defines a decimal expansion of x .

A negative number x has a decimal expansion $-b_m \dots b_0 . a_1 a_2 a_3 \dots$ where $b_m \dots b_0 . a_1 a_2 a_3 \dots$ is the decimal expansion of $|x|$.

A decimal expansion is finite iff $a_n = 0$ for large n . (Recall from Sec. 15 that it means that there is N such that $a_n = 0$ for all $n \geq N$.) Such zeros are usually omitted in the notation.

We say that a decimal expansion $b_m \dots b_0 . a_1 a_2 a_3 \dots$ is repeating or recurring of period $p \in \mathbb{N}$ if $a_{n+p} = a_n$ for large n . We denote such decimal expansion by $b_m \dots b_0 . a_1 a_2 a_3 \dots a_n \overline{a_{n+1} \dots a_{n+p}}$. For example $1/3 = 0.\overline{3}$, $1/7 = 0.\overline{142857}$, $1/12 = 0.08\overline{3}$.

Remark 16.4. Some real numbers have more than one decimal expansion. Recall that the infinite geometric series $a + aq + aq^2 + \dots$ converges iff $|q| < 1$ and, in this case, its sum is $\frac{a}{1-q}$. Therefore $0.\overline{9} = 0.9 \cdot (1 + 10^{-1} + 10^{-2} + \dots)$ is a converging infinite geometric series and its sum is $0.9 \cdot \frac{1}{1-10^{-1}} = 1$. Hence $0.\overline{9} = 1$!

Theorem 16.5. Every real number x has a unique decimal expansion without repeating 9.

Theorem 16.6. Every rational number has either finite or a repeating expansion.

Proof. in class. □

Theorem 16.7. Every real number with repeating decimal expansion is rational.

Proof. Assume first that $x = 0.\overline{a_1 \dots a_p}$. Then

$$x = 0.a_1 \dots a_p + 0.a_1 \dots a_p \cdot 10^{-p} + \dots = 0.a_1 \dots a_p (1 + 10^{-p} + 10^{-2p} + \dots)$$

is a converging geometric series whose sum is

$$x = 0.a_1 \dots a_p \cdot \frac{1}{1 - 10^{-p}} = \frac{a_1 \dots a_p}{10^p(1 - 10^{-p})} = \frac{a_1 \dots a_p}{10^p - 1}.$$

It is a rational number.

Suppose now that $x = b_m \dots b_0.a_1 \dots a_n \overline{a_{n+1} \dots a_{n+p}}$. Clearly,

$$x_0 = b_m \dots b_0.a_1 \dots a_n = b_m \cdot 10^m + \dots + b_0 + a_1 \cdot 10^{-1} + \dots + a_n \cdot 10^{-n}$$

is a finite sum of rational numbers and, hence, a rational number itself.

We have also proved above already that $0.\overline{a_{n+1} \dots a_{n+p}}$ is rational. Therefore, $10^{-n} \cdot 0.\overline{a_{n+1} \dots a_{n+p}}$ is also rational and, hence, $x = x_0 + 10^{-n} \cdot 0.\overline{a_{n+1} \dots a_{n+p}}$ is rational as well. \square

Corollary 16.8. *A real number is rational if and only if it has a finite or repeating decimal expansion.*

PROBLEMS 16.

Problem 16.1. Find the rational presentation, p/q of the number $0.\overline{123}$.

Problem 16.2. Give an actual, explicit example of a non-repeating (non-terminating) decimal. Your answer should be such that you could determine without a computer what the thousandth decimal place would be. ‘The decimal expansion of π or of $\sqrt{2}$ ’ is not an answer, since you can’t describe these decimal expansions explicitly (what is the thousandth decimal place of $\sqrt{2}$?).

17. RINGS AND FIELDS

The operation of addition associates with any two real numbers, x, y , their sum, $x + y$. Therefore, addition can be thought as a function defined on the set of all pairs of real numbers, i.e. a function from $\mathbb{R} \times \mathbb{R}$ to \mathbb{R} . Any such function is called a binary operation. (“Binary” refers to the two numbers, x, y in the input. “Operation” means that the output is in \mathbb{R} , unlike in a relation, xRy , where the output is either “truth” or “false”.) Clearly, multiplication is a binary operation as well.

We say that a set R is a ring if

- (1) there are two binary operations defined on R , addition: $+$: $R \times R \rightarrow R$ and multiplication: \cdot : $R \times R \rightarrow R$.
- (2) these operations are associative, i.e. $(a + b) + c = a + (b + c)$, and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
- (3) addition is commutative, $a + b = b + a$.
- (4) multiplication is distributive over addition, i.e. $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$ for all $a, b, c \in R$.
- (5) There are two different distinguished elements $0, 1 \in R$ such that $0 + a = a$ and $1 \cdot a = a \cdot 1 = a$ for all a .
- (6) Every $a \in R$ has its additive inverse in R i.e. an element $b \in R$ such that $a + b = 0$. (such b is denoted by $-a$).

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are rings. Note that we denote by R any ring and by \mathbb{R} the ring of real numbers. Since $\mathbb{Q} \subset \mathbb{R}$ we say that \mathbb{Q} is a subring of \mathbb{R} . Similarly, \mathbb{Z} is a subring of \mathbb{Q} and of \mathbb{R} . On the other hand, \mathbb{N} is not a ring, since its elements do not have additive inverses. The reason for introducing the notion of a ring is that it encompasses properties of many important algebraic objects in mathematics. We describe below several important and interesting rings which you encountered already.

Example 17.1. Recall from Section 9, that $\mathbb{Z}[\sqrt{d}]$ denotes the set of all numbers of the form $a + b\sqrt{d}$, where $a, b \in \mathbb{Z}$. By Proposition 9.27, $\mathbb{Z}[\sqrt{d}]$ satisfies property (1). Properties (2)-(6) are easy to verify as well. Therefore, $\mathbb{Z}[\sqrt{d}]$ is a ring.

Example 17.2. For any $n \in \mathbb{N}$, we denote by \mathbb{Z}/n the quotient of \mathbb{Z} by the equivalence relation $\text{mod } n$, c.f. Section 10. Hence $\mathbb{Z}/3$ has three elements: the equivalence classes of 0, 1, and 2:

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}, \quad [1] = \{\dots, -5, -2, 1, 4, 7, \dots\}, \quad [2] = \{\dots, -4, -1, 2, 5, \dots\}.$$

Of course, $[0] = [3] = [6] = \dots$, $[1] = [4] = [7] = \dots$ etc.

We want to define addition and multiplication in \mathbb{Z}/n by the following formula:

$$(17.2.1) \quad [a] + [b] = [a + b] \quad [a] \cdot [b] = [a \cdot b]$$

for any $a, b \in \mathbb{Z}$. A priori, however, it is not clear if these operations can be defined in such a way since each element of (i.e. equivalence class in) \mathbb{Z}/n can be written as $[a]$ for many different a 's. For that reason we need:

Lemma 17.3. For any given $x, y \in \mathbb{Z}/n$, $[a + b] \in \mathbb{Z}/n$ and $[a \cdot b] \in \mathbb{Z}/n$ do not depend on the choice of $a \in x$ and $b \in y$.

Proof. (1) We need to prove that if $a, a' \in x$ and $b, b' \in y$ then $[a + b] = [a' + b']$ and $[a \cdot b] = [a' \cdot b']$. Our assumptions imply that $a = a' \text{ mod } n$ and $b = b' \text{ mod } n$. These congruences imply that $a - a'$ and $b - b'$ are divisible by n . Since $a - a' + b - b'$ is divisible by n , we have $a + b = a' + b' \text{ mod } n$. Hence $[a + b] = [a' + b']$.

(2) The proof of $[a \cdot b] = [a' \cdot b']$ is similar: We need to prove that $a \cdot b - a' \cdot b'$ is divisible by n . Since $a \cdot b - a' \cdot b' = a \cdot (b - b') + (a - a') \cdot b'$, the claim follows from the fact that $b - b'$ and $a - a'$ are divisible by n . □

Definition 17.4. For every $x, y \in \mathbb{Z}/n$ we define

$$x + y = [a + b] \quad \text{and} \quad x \cdot y = [a \cdot b]$$

for any $a \in x$ and $b \in y$.

Now indeed the equation (17.2.1) is satisfied! For example, $[2] + [3] = [0]$ and $[2] \cdot [3] = [1]$ in $\mathbb{Z}/5$.

It is straightforward to check, that \mathbb{Z}/n is a ring, with the zero element $[0]$ and the identity element $[1]$. We call that ring “ $\mathbb{Z} \bmod n$ ”. For simplicity, we will skip the brackets from now on. Hence, we will say that $1 = 4$ in $\mathbb{Z}/3$.

Example 17.5. Let X be a set and let $F(X)$ denote the set of all functions $f : X \rightarrow \mathbb{R}$. We can add and multiply functions together. If f, g are functions from X to \mathbb{R} then $f + g, f \cdot g : X \rightarrow \mathbb{R}$ are functions such that

$$(f + g)(x) = f(x) + g(x) \in \mathbb{R}, \quad (f \cdot g)(x) = f(x) \cdot g(x) \in \mathbb{R}.$$

It is not difficult to verify conditions (1)-(6) above and, hence, to see that $F(X)$ is a ring.

Example 17.6. Let $C(\mathbb{R})$ be the set of continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$. Since the set of continuous functions is closed under addition and multiplication and the conditions (1)-(6) hold, $C(\mathbb{R})$ is a ring. It is a subring of $F(\mathbb{R})$.

Example 17.7. A polynomial is a function of the form $f(x) = a_n x^n + \dots + a_1 x + a_0$. a_0, \dots, a_n are called coefficients of f . Denote the set of polynomials with coefficients in \mathbb{R} by $\mathbb{R}[x]$. This set is closed under addition and multiplication. Furthermore the constant functions 0 and 1 are the zero and the identity in $\mathbb{R}[x]$. Since $\mathbb{R}[x]$ satisfies conditions (1)-(6) above, it is a ring as well. Since every polynomial is continuous, $\mathbb{R}[x]$ is a subring of $C(\mathbb{R})$.

We say that $a \in R, a \neq 0$, is a zero divisor if there exists $b \in R, b \neq 0$ such that $a \cdot b = 0$. We know that \mathbb{Z}, \mathbb{Q} , or \mathbb{R} are rings with no zero divisors. However, the rings \mathbb{Z}/n have zero divisors for some n 's. For example $2, 3 \neq 0$ in $\mathbb{Z}/6$ but $2 \cdot 3 = 0$ in $\mathbb{Z}/6$.

Proposition 17.8. \mathbb{Z}/n does not have zero divisors iff n is prime.

Proof. was given in class. □

Note that the definition of the ring does not require that multiplication is commutative. In fact there are interesting examples of rings with non-commutative multiplication.

Example 17.9. You have learned in Vector Calculus that vectors in \mathbb{R}^3 can be added, eg. $\langle 2, -1, 3 \rangle + \langle 1, 2, -2 \rangle = \langle 3, 1, 1 \rangle$ and multiplied via “cross product” or “vector product”, eg.

$$\langle 2, -1, 3 \rangle \times \langle 1, 2, -2 \rangle = \begin{vmatrix} i & j & k \\ 2 & -1 & 3 \\ 1 & 2 & -2 \end{vmatrix} = -4i + 7j + 5k = \langle -4, 7, 5 \rangle.$$

(You have also learned about the dot product, but that one is irrelevant here.) Alternatively, the cross product is defined geometrically by the following two properties:

(1) $v \times w$ is a vector of length $|v| \cdot |w| \cdot \sin(\alpha)$, where $|v|$ and $|w|$ are lengths of v and w and α is the angle between v and w .

(2) $v \times w$ orthogonal to v and to w and pointing in the direction determined by “right hand rule”.

The cross product is associative and distributive over addition. Therefore, \mathbb{R}^3 is a ring! However, it is not commutative. In fact, for every $v, w \in \mathbb{R}^3$ we have $v \times w = -w \times v$.

The ring with commutative multiplication is called a commutative ring. Hence $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}[\sqrt{d}], \mathbb{Z}/n$ are examples of commutative rings. \mathbb{R}^3 (with cross product) is a non-commutative ring.

Example 17.10. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices is a non-commutative ring for $n \geq 2$. For $n = 2$ the addition and multiplication are defined as follows:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix},$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Remark 17.11. If R is a commutative ring then the left distributivity law,

$$(17.11.1) \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

is equivalent to the right one,

$$(17.11.2) \quad c \cdot (a + b) = c \cdot a + c \cdot b.$$

Indeed,

$$c \cdot (a + b) = (a + b) \cdot c = a \cdot c + b \cdot c = c \cdot a + c \cdot b.$$

If R is non-commutative then these conditions are independent, as seen in the example below.

Example 17.12. Consider the set S of all functions $f : \mathbb{R} \rightarrow \mathbb{R}$ with the usual addition and with the “multiplication” being composition of functions, i.e. the “product” of f and g is a function fg sending x to $f(g(x))$ for every $x \in \mathbb{R}$. This product satisfies the left distributivity, (17.11.1), but not the right one, (17.11.2). Therefore, S is not a ring.

Fields.

We say that a commutative ring R is a field if every nonzero element of R has a multiplicative inverse, i.e.

$$\forall a \in R, a \neq 0 \quad \exists b \in R \quad a \cdot b = 1.$$

\mathbb{Q} and \mathbb{R} are examples of fields. On the other hand \mathbb{Z} is not a field since 2 has no multiplicative inverse. Similarly $\mathbb{Z}/6$ is not a field, since $2 \cdot x \neq 1$ for every $x \in \mathbb{Z}/6$.

Lemma 17.13. If a is a zero divisor in a commutative ring then a does not have a multiplicative inverse in \mathbb{Z} .

Proof. Since a is a zero divisor, $a \cdot b = 0$ for some $b \neq 0$, $b \in R$. If a has a multiplicative inverse $c \in R$ then $a \cdot c = 1$. Hence

$$0 = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot (c \cdot b) = (a \cdot c) \cdot b = b.$$

Contradiction. □

Theorem 17.14. \mathbb{Z}/n is a field iff n is prime.

Proof. in class. □

For example $\mathbb{Z}/3, \mathbb{Z}/11$ are fields. Fields \mathbb{Z}/n for n prime share many algebraic properties with the fields of rational and real numbers. There are two big differences are: (a) the sum of n ones in \mathbb{Z}/n is zero! (e.g. $1 + 1 + 1 = 0$ in $\mathbb{Z}/3$), and (b) inequalities do not make sense in \mathbb{Z}/n . For example, if $1 < 2$ in $\mathbb{Z}/3$ then $1 + 1 > 2 + 2$ in $\mathbb{Z}/3$.

PROBLEMS 17.

Problem 17.1. Prove that S in Example 17.12, does not satisfy the right distributivity law. Therefore S is not a ring.

Problem 17.2. A person defined a new operation on $\mathbb{Z}/13$ called “a square root” by declaring that

$$\sqrt{[a]} = \begin{cases} [\sqrt{a}] & \text{if } \sqrt{a} \text{ is an integer} \\ 0 & \text{otherwise.} \end{cases}$$

Is this operation well defined?

Problem 17.3. Find all zero divisors in \mathbb{R}^3 in Example 17.9.

Problem 17.4. Give an example of a zero divisor in $M_2(\mathbb{R})$.

Problem 17.5. (a) What $f \in C(X)$ is the multiplicative identity in Example 17.6?

(b) Find a zero divisor in $C(\mathbb{R})$ or prove that they do not exist.

Problem 17.6. (a) If $x = \pm 1$ then x is its own multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$. Find an element $x \neq \pm 1$ in $\mathbb{Z}[\sqrt{2}]$ which has a multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$.

(b) Find an element $x \neq 0$ in $\mathbb{Z}[\sqrt{2}]$ which does not have a multiplicative inverse in $\mathbb{Z}[\sqrt{2}]$.

(c) Is $\mathbb{Z}[\sqrt{2}]$ a field?

18. COMPLEX NUMBERS

Consider \mathbb{R}^2 with the addition operation,

$$(18.0.1) \quad (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

and multiplication operation

$$(18.0.2) \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1).$$

Clearly, the addition is additive, associative and $(0, 0)$ is the zero element.

Lemma 18.1. *This multiplication is commutative, associative, and distributive over addition. Furthermore, $(1, 0)$ is the identity element.*

Proof. (1) The multiplication is commutative, since

$$(a_2, b_2) \cdot (a_1, b_1) = (a_2a_1 - b_2b_1, a_2b_1 + a_1b_2) = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1) = (a_1, b_1) \cdot (a_2, b_2).$$

(2) Proof of associativity is left as HW.

(3) Proof of distributivity is skipped.

(4) Proof of $(1, 0)$ being the identity element is left as HW. □

Since $(-a, -b)$ the additive inverse of (a, b) , \mathbb{R}^2 with addition and multiplication defined above is a ring!

Proposition 18.2. *For every $(a, b) \neq (0, 0)$, $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b) .*

Proof.

$$(a, b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(a \cdot \frac{a}{a^2+b^2} - b \cdot \frac{-b}{a^2+b^2}, a \cdot \frac{-b}{a^2+b^2} + b \cdot \frac{a}{a^2+b^2}\right) = (1, 0).$$

□

Hence, we have proved that \mathbb{R}^2 (with the above addition and multiplication) is a field! We call it the field of complex numbers and denote it by \mathbb{C} . With each real number r we can associate an element $(r, 0) \in \mathbb{C}$. Note that these elements add and multiply as real numbers do, i.e. $(r, 0) + (s, 0) = (r + s, 0)$ and $(r, 0) \cdot (s, 0) = (rs, 0)$. Hence we can identify an element of the form $(r, 0)$ in \mathbb{C} with the real number $r \in \mathbb{R}$. As we have observed already, $0 = (0, 0)$ is the zero in \mathbb{C} and $1 = (1, 0)$ is the identity in \mathbb{C} . Denote $(0, 1)$ by i . Then

$$i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1.$$

Lemma 18.3. *For every $a, b \in \mathbb{R}$, $(a, b) = (a, 0) + (0, b) = a + i \cdot b$*

Proof. $i \cdot b = (0, 1) \cdot (b, 0) = (0, b)$ □

Therefore, every complex number is of the form $a + bi$, for some $a, b \in \mathbb{R}$. You do not need to use the equation (18.0.2) to multiply complex numbers, as long as you remember that $i^2 = -1$. For example, $(1 + 2i)(-1 + 3i) = \dots$

If $z = x + yi$ then $\bar{z} = x - yi$ is called the conjugate of z . Note that $z \cdot \bar{z} = a^2 + b^2$. This is always a non-negative real number and its square root, $\sqrt{a^2 + b^2}$, is called the norm or modulus of z and it is denoted by $|z|$. Geometrically, every complex number represents a point on the xy -plane and $|z|$ is the distance of this point to the origin.

Theorem 18.4 (Triangle Inequality). $|x + y| \leq |x| + |y|$ for all complex numbers x, y .

The points $0, z_1, z_1 + z_2$ form a triangle in the complex plane, with sides of length $l(0, z_1) = |z_1|$, $l(z_1, z_1 + z_2) = |z_2|$ and $l(z_1 + z_2, 0) = |z_1 + z_2|$. Hence, geometrically, the triangle inequality says that a side of a triangle is no longer than the sum of lengths of the two other sides. That is the motivation for its name. You may be asked for a rigorous proof of that inequality in HW.

Since $z\bar{z} = |z|^2$, we have $z^{-1} = \frac{\bar{z}}{|z|^2}$ for $z \neq 0$. Note that this formula coincides with the one of Proposition 18.2.

For a non-zero $z \in \mathbb{C}$, the argument of z , denoted by $\arg z$ is an angle between the positive real axis and the vector representing z . To remove any ambiguity, the angle is positive and measured counterclockwise. Hence $\arg z \in [0, 2\pi)$ (although some mathematicians define it as an element in $(-\pi, \pi]$).

More formally, $\arg z$ is equal $\phi \in [0, 2\pi)$ such that

$$z = |z|(\cos\phi + i \cdot \sin\phi).$$

One can easily prove that ϕ exists and, since we assume that $z \neq 0$, that it is unique.

Theorem 18.5 (Fundamental Theorem of Algebra). *Every polynomial with complex coefficients of degree ≥ 1 has a complex root, i.e. for every $c_0, c_1, \dots, c_n \in \mathbb{C}$, $n \geq 1$, there is $z \in \mathbb{C}$ such that $c_n z^n + \dots + c_1 z + c_0 = 0$.*

The proof is difficult. (In fact, this is the first Theorem in this course, whose proof is too difficult to be discussed here.) Note that an analogous theorem does not hold for real numbers. For example, $x^2 + 1 = 0$ has no roots.

Theorem 18.6 (An alternative version of Fundamental Theorem of Algebra). *Every polynomial with complex coefficients is a product of linear factors. More specifically, for every $c_0, \dots, c_n \in \mathbb{C}$ there exist $z_1, \dots, z_n \in \mathbb{C}$ such that*

$$c_n z^n + \dots + c_1 z + c_0 = c_n (z - z_1) \cdot \dots \cdot (z - z_n)$$

for all $z \in \mathbb{C}$.

Clearly the above statement implies Theorem 18.5. One can prove the opposite implication as well by induction on n .

PROBLEMS 18.

Problem 18.1. Prove the Triangle Inequality, Thm 18.4. Hint: Represent x and y by $a_1 + b_1 i$ and $a_2 + b_2 i$, respectively and then prove the corresponding inequality involving real numbers a_1, b_1, a_2, b_2 .

Problem 18.2. Prove that $|x - y| \geq |x| - |y|$ for arbitrary complex numbers x, y .

Problem 18.3. Write a formula expressing $\arg z_1 z_2$ in terms of $\arg z_1$ and $\arg z_2$, for any complex numbers z_1, z_2 .

Problem 18.4. (1) We say that $x \in \mathbb{C}$ is a square root of $z \in \mathbb{C}$ if $x^2 = z$. Does every complex number have a square root? How many? (Notice that unlike for z real we cannot not require that the square root is non-negative.)

(2) Write a formula expressing $\arg \sqrt{z}$ in terms of $\arg z$.

(3) Find square roots of i and of $1 + i$.

19. APPLICATION OF COMPLEX NUMBERS: FRACTALS

An infinite sequence a_1, a_2, \dots of complex numbers is bounded if there is $B \in (0, \infty)$ such that $|a_n| \leq B$ for all n .

Let us consider this notion for sequences defined recursively as follows:

Fix $a, c \in \mathbb{C}$. Let $a_1 = a$, and $a_{n+1} = a_n^2 + c$ for all $n = 1, 2, \dots$

Example 19.1. *If $a = 1, c = -1$ then $a_1 = 1, a_2 = 0, a_3 = -1, a_4 = 0$, and so on. It is easy to prove by induction that $a_n \in \{-1, 0, 1\}$ for all n and, hence, a_n is bounded, for example by $B = 1$.*

Example 19.2. *If $a = 2, c = -1$ then $a_1 = 2, a_2 = 3, a_3 = 8, a_4 = 63$, and so on. It is easy to prove by induction that $a_n > n$ for all n and, hence, it is unbounded.*

Given $c \in \mathbb{C}$, let J_c be the set of those complex numbers a such that the sequence $a_1 = a, a_{n+1} = a_n^2 + c$ defined above is bounded.

J_c is called the filled Julia set (for a given c .) When visualized as a subset of the complex plane, this set is a “fractal” whose shape depends on c . Pictures of Julia sets at the bottom of http://en.wikipedia.org/wiki/Julia_set The set of those values c for which J_c is “connected” (i.e. it is not a union of disjoint pieces) is called the Mandelbrot set.

Computer experimentation:

1. Have a look at <http://math.bu.edu/DYSYS/applets/Quadr.html> There is Julia set, J_{-1} , on the left and the Mandelbrot set on the right.

2. Enter $c = -1.3 + 0i$ and click “Compute”. Note that the shape of the Julia set have changed. The white point on the right shows the position of c on the complex plane. Since the Julia set is connected, the point is inside of the Mandelbrot set.

3. Click at a “red” point outside (but near) Mandelbrot set in the right window and then press “Compute”. See the Julia set now. It should be disconnected.

4. Click on a point inside of the Julia set in the left window. This point represents our complex number “ a ”, called the “seed” in this applet. Check its value in the “seed” window. Press “orbit”. You should be able to see that the numbers a_1, a_2, \dots in the sequence are “small”. (That does not prove anything, but it gives an indication that the sequence is bounded.)

5. Click on a point outside the Julia set. Press “orbit”. You should be able to see that the absolute values of a_1, a_2, \dots are growing. (An indication that this sequence is unbounded.)

PROBLEMS 19.

Problem 19.1. Prove that if $|a| \geq 2 + \frac{|c|}{2}$ then $|a^2 + c| \geq 2|a|$. (Use the inequality $|x - y| \geq |x| - |y|$ of HW Sec. 18.)

Problem 19.2. Use the previous problem, to prove that for every $c \in \mathbb{C}$ all elements of J_c have absolute value less than $2 + \frac{|c|}{2}$. (Hence, J_c is a bounded set.)

20. EQUIVALENCE OF SETS

Definition 20.1 (Correspondence). A function $f: A \rightarrow B$ is a bijection or a 1-1 correspondence if f is 1-1 and onto.

Note the difference between 1-1 function and 1-1 correspondence: the first one does not have to be onto.

Definition 20.2 (Equivalent sets, Cardinality). Sets A and B are equivalent, written $A \sim B$, if there exists a 1-1 correspondence $f: A \rightarrow B$. We also say in this situation that A and B have the same cardinality.

Remark 20.3. *To prove that A is equivalent with B it is enough to find a function $f: A \rightarrow B$ and to verify that it is 1-1 and onto. For example, \mathbb{Z} is equivalent with the set of odd integers $O = \{\dots, -3, -1, 1, 3, \dots\}$ via a function $f: \mathbb{Z} \rightarrow O$, $f(n) = 2n + 1$. However, there are many other functions which work here, eg. $f(n) = -2n + 3$. In this section we will consider many interesting equivalences of sets where an appropriate f is much harder to find.*

Proposition 20.4. *Equivalence of sets is:*

- (1) *reflexive* ($A \sim A$)
- (2) *symmetric* ($A \sim B$ implies $B \sim A$)
- (3) *transitive* ($A \sim B$ and $B \sim C$ implies $A \sim C$).

Remark 20.5. \sim is “like” an equivalence relation. Formally speaking though, it is not a relation, since by definition a relation is a property of pairs of elements of a certain set. By the Russell’s paradox discussed earlier in this class though, there is no such thing as the set of all sets!

Definition 20.6. (1) A set A has cardinality n , where $n \in \mathbb{N}$, (or, equivalently, A has n elements) if A is equivalent to the set $\{1, \dots, n\}$. We write then $|A| = n$.

(2) A is finite if it has n elements for some $n \in \mathbb{N}$ or $A = \emptyset$ (in this case it has zero elements).

(3) A set is infinite (or, equivalently, it has infinitely many elements) if it is not finite.

Below we summarize some obvious properties of finite and infinite sets.

Proposition 20.7. (1) *Two finite sets are equivalent if and only if they have equal number of elements.*

(2) *If A and B are finite sets, then $A \cup B$ is finite.*

(3) *If A and B are equivalent sets, then that the power sets, 2^A and 2^B , are equivalent as well.*

(4) *\mathbb{N} is infinite.*

We have observed already that two finite sets are equivalent if and only if they have the same numbers of elements. On the other hand, equivalences of infinite sets are a much more interesting subject. We are going to see soon that not all infinite sets are equivalent.

Definition 20.8 (Countable Sets).

(1) A set equivalent to \mathbb{N} is called countably infinite.

(2) A set is countable if either finite or countably infinite.

(3) A set which is not countable is uncountable.

Observe that a set A is infinite countable if every element of A is labeled by a unique natural number, such that different elements of A have different labels and all natural numbers are utilized.

Proposition 20.9. *Every subset of \mathbb{N} is countable.*

Proof. If $A \subset \mathbb{N}$ is finite then it is countable by definition. Assume hence that A is infinite. We define $f: \mathbb{N} \rightarrow A$ inductively as follows:

Base step: Let $f(1)$ be the smallest element of A . (This element exists by the well-ordering principle, Theorem 6.13.)

Inductive step: Suppose that $f(1), \dots, f(n) \in A$ are defined already. We define $f(n+1)$ to be the smallest element of $A - \{f(1), \dots, f(n)\}$. (Since A is infinite, $A - \{f(1), \dots, f(n)\}$ is a non-empty subset of \mathbb{N} and, therefore, it contains its smallest element by the well-ordering principle.)

To complete the proof we need to show that f is an equivalence. We start with the following:

Lemma 20.10. (1) $f : \mathbb{N} \rightarrow \mathbb{N}$ is an increasing function.

(2) $f(n) \geq n$ for every $n \in \mathbb{N}$.

Proof. (1) if $n < m$ then $f(m) \in A - \{f(1), \dots, f(m-1)\}$ and, hence, $f(m) \neq f(n)$.

(2) By induction on n : Base step is obvious, since $f(1) \geq 1$. Assume that $f(n) \geq n$. Since f is increasing, $f(n+1) > f(n)$ and, hence, $f(n+1) \geq n+1$. □

Completion of the proof of Proposition 20.9: Since f is increasing, f is 1-1. We are going to prove that f is onto, by contradiction: suppose that $f(\mathbb{N}) \subsetneq A$. Then $A - f(\mathbb{N})$ is a non-empty subset of \mathbb{N} and, hence, by well-ordering principle, $A - f(\mathbb{N})$ has its smallest element n . (In other words, n is the smallest natural number not in the image of f .) Since $f(n)$ is the smallest element of $\mathbb{N} - \{f(1), \dots, f(n-1)\}$ and n is in this set, $f(n) \leq n$. On the other hand, $f(n) \geq n$ by Lemma 20.10(2). Therefore $f(n) = n$. This contradicts the assumption that n is not in the image of f . □

Corollary 20.11. For every set A the following are equivalent:

(1) A is countable

(2) there is a 1-1 function $f : A \rightarrow \mathbb{N}$

(3) A is equivalent to a subset of \mathbb{N} .

Remark 20.12. (1) The words “the following are equivalent” are often denoted by the acronym *TFAE*.

(2) The statement claims that $(i) \Rightarrow (j)$ for all $i, j \in \{1, 2, 3\}$. To prove it, it is enough to show implications:

$$(1) \Rightarrow (2), \quad (2) \Rightarrow (3), \quad (3) \Rightarrow (1).$$

All other implications will then follow. For example, $(3) \Rightarrow (1)$ and $(1) \Rightarrow (2)$ imply

$(3) \Rightarrow (2)$.

Proof of Cor. 20.11:

(1) \Rightarrow (2): If A is finite then there is a 1-1 correspondence $f : A \rightarrow \{1, 2, \dots, n\}$. In particular, f is a 1-1 function into \mathbb{N} .

If A is infinite countable then, by definition, there is a 1-1 function $f : A \rightarrow \mathbb{N}$.

(2) \Rightarrow (3): If f is 1-1 then f is a 1-1 correspondence between A and $f(A)$. The latter set is a subset of \mathbb{N} .

(3) \Rightarrow (1) by Proposition 20.9. □

Corollary 20.13. A subset of a countable set is countable.

Proof. Let A be a subset of a countable set B . If B is finite then A is finite as well and, hence, countable. If A is infinite countable then there is a 1-1 correspondence $f : A \rightarrow \mathbb{N}$. This 1-1 correspondence restricted to B is a 1-1 function from B into \mathbb{N} . Hence B is countable by Proposition 20.9. □

Remark 20.14. f sending

$$1, 2, 3, 4, 5, 6, 7, 8 \dots \text{ to } 0, -1, 1, -2, 2, -3, 3, -4 \dots$$

is a 1-1 correspondence between \mathbb{N} and \mathbb{Z} .

The above statement may look surprising since there seems to be “much more” integers than natural numbers. Here is an even more surprising result:

Proposition 20.15. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ (i.e. $\mathbb{N} \times \mathbb{N}$ is infinite countable).

Proof. requires a picture. Was presented in class. □

More generally, we have

Theorem 20.16. *If A_1, A_2, \dots, A_n are countable then $A_1 \times \dots \times A_n$ is countable.*

Proof. By Corollary 20.11, there are 1-1 functions $f_1 : A_1 \rightarrow \mathbb{N}, \dots, f_n : A_n \rightarrow \mathbb{N}$. By the same corollary, it is enough to prove that there is a 1-1 function $f : A_1 \times \dots \times A_n \rightarrow \mathbb{N}$. We define it as follows: Let $p_1 = 2, p_2 = 3, p_3 = 5, \dots$ be the sequence of all primes. For $(a_1, a_2, \dots, a_n) \in A_1 \times \dots \times A_n$ we define

$$f(a_1, a_2, \dots, a_n) = p_1^{f_1(a_1)} \dots p_n^{f_n(a_n)} \in \mathbb{N}.$$

We claim that f is 1-1. Indeed, if $(a_1, a_2, \dots, a_n) \neq (b_1, b_2, \dots, b_n)$ then $a_i \neq b_i$ for at least one i . Then $f_i(a_i) \neq f_i(b_i)$ (since f_i is 1-1) and, consequently, the numbers $f(a_1, a_2, \dots, a_n)$ and $f(b_1, b_2, \dots, b_n)$ have different prime factorizations. By uniqueness of prime factorization (Theorem 9.6), $f(a_1, a_2, \dots, a_n) \neq f(b_1, b_2, \dots, b_n)$. □

Corollary 20.17. *The set \mathbb{Q} of rational numbers is countable.*

Proof. For every $x \in \mathbb{Q}, x \neq 0$, there is unique $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that $x = p/q, p \neq 0$ and p, q are relatively prime. (Note that the sign of p coincides with the sign of x .) Consider the function $f : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{N}$ sending x to (p, q) defined above, and sending 0 to $(0, 1)$. This function is 1-1, since $f(x) = (p, q) = f(y)$ implies $x = p/q = y$. By Remark 20.14 and Theorem 20.16, $\mathbb{Z} \times \mathbb{N}$ is countable and, therefore, by Corollary 20.13, \mathbb{Q} is countable as well. □

Further properties of countable sets:

Proposition 20.18. (1) *If A and B are countable sets then $A \cup B$ is countable.*

(2) *Furthermore, if A_1, A_2, A_3, \dots are countable $\bigcup_{i=1}^{\infty} A_i$ is countable as well.*

Theorem 20.19. *The interval $(0, 1)$ is uncountable.*

Proof. Consider an arbitrary function $f : \mathbb{N} \rightarrow [0, 1)$. We are going to prove that f cannot be onto. By Theorem 16.5, every number in $[0, 1)$ has a unique decimal expansion $0.a_1a_2\dots$ without repeating 9. Consider a number $x_0 = 0.b_1b_2\dots \in [0, 1)$ constructed as follows: For every n , let b_n be not equal the n -th digit in $f(n) \in [0, 1)$. (For example, we can define b_n to be the n -th digit of $f(n)$ plus 1 mod 10.) By its definition, $x_0 \neq f(n)$ for any n . (Indeed, these two numbers disagree on the n -th digit.) Therefore, x_0 does not belong to the image of f in $[0, 1)$ and f is not onto. This is Cantor's famous "diagonal argument". □

Proposition 20.20. (1) *$f(x) = x/(1 - x^2)$ is a 1-1 correspondence between $(-1, 1)$ and \mathbb{R} .*

(2) *There is a 1-1 correspondence between $(0, 1)$ and $(-1, 1)$. Therefore, $(0, 1), (-1, 1)$, and \mathbb{R} are all equivalent.*

Proof. (1) Since f is differentiable and $f'(x) > 0$ for all x , f is increasing. Therefore f is 1-1 one. To prove that f is onto, observe that

$$\lim_{x \rightarrow -1} f(x) = -\infty, \quad \text{and} \quad \lim_{x \rightarrow 1} f(x) = \infty.$$

Therefore f takes arbitrarily large and small values. (This does not imply yet that f takes all values.) The remainder of the proof is left as HW.

(2) left as HW. □

Corollary 20.21. \mathbb{R} are uncountable.

Corollary 20.22. *The set of irrational numbers is uncountable.*

Proof. Left as HW. □

PROBLEMS 20.

Problem 20.1. Prove Proposition 20.4.

Problem 20.2. Prove that the following sets have the same cardinality:

- (1) The open intervals $(0, 2)$ and $(0, 11)$.
- (2) Any two open intervals (a, b) and (c, d) where $a < b, c < d$ and a, b, c, d are all (finite) real numbers.

Problem 20.3. Complete the proof of Proposition 20.20(1) and (2).

Problem 20.4. Describe a 1-1 correspondence f between \mathbb{N} and $\mathbb{N} \times \mathbb{N}$. Write down the values of $f(1), \dots, f(10)$. *Hint:* Such 1-1 correspondence was discussed in class, c.f. Proposition 20.15.

Problem 20.5. Is it true that $A_1 \times B \sim A_2 \times B$ for some sets A_1, A_2, B implies that $A_1 \sim A_2$?

Problem 20.6. Prove that $[0, 1]$ is uncountable.

Problem 20.7. Prove Corollary 20.22.

Problem 20.8. (a) Find a 1-1 function $f : (0, 1) \times (0, 1) \rightarrow (0, 1)$. *Hint:* use decimal expansions of numbers in $(0, 1)$.

(b) Is your f onto?

Motivation: We will prove later that $(0, 1) \times (0, 1) \sim (0, 1)$. However, it is not easy to find an explicit 1-1 correspondence between these sets.

Problem 20.9. Find a 1-1 correspondence between \mathbb{R} and $\mathbb{Z} \times [0, 1)$.

Problem 20.10. Prove that the intervals $(0, 1)$ and $[0, 1]$ are equivalent. *Hint:* Let $B_1 = \{1/2, 1/3, 1/4, \dots\}$. Let $A_1 = A_2 = (0, 1) - B_1$. Let $B_2 = \{0, 1\} \cup B_1$. Check that $(0, 1) = A_1 \cup B_1$ and that $[0, 1] = A_2 \cup B_2$. Construct a 1-1 correspondence between $(0, 1)$ and $[0, 1]$ sending A_1 to A_2 and B_1 to B_2 .

21. ALGEBRAIC NUMBERS

Definition 21.1. A complex number x is algebraic if it is a root of a non-zero polynomial with rational coefficients, i.e.

$$(21.1.1) \quad c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 = 0$$

for some $c_0, c_1, \dots, c_n \in \mathbb{Q}$. The smallest such $n \in \mathbb{N}$ is called the degree of x .

(2) A number which is not algebraic is called transcendental.

Remark 21.2. (1) Since every $a \in \mathbb{Q}$ is the root of the polynomial $x - a$ it is an algebraic of degree 1. Conversely, every algebraic number of degree 1 is rational.

(2) Being a root of $x^2 - 2$, $\sqrt{2}$ is algebraic. Since $\sqrt{2}$ is irrational (Theorem 12.1), its degree is 2.

(3) Ferdinand von Lindemann proved in 1882 that π is transcendental. (That is a very difficult result).

(4) Charles Hermite proved in 1873 that the Euler's number $e = 2.7182\dots$ is transcendental as well. (In particular, both π and e are irrational.)

We denote the set of all algebraic numbers by $\overline{\mathbb{Q}}$. (This notation will become clear once you take a graduate level algebra course.)

Theorem 21.3. $\overline{\mathbb{Q}}$ is a field. In particular, if x, y are algebraic numbers, then $x + y, x - y, xy, x/y$ are algebraic as well. (In the last case, we need $y \neq 0$.)

Proof. is too difficult to be presented here. □

Example 21.4. Let us prove that $x = \sqrt{2} + \sqrt{3}$ is algebraic. Since $x^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + 2\sqrt{6}$, we have $(x^2 - 5)^2 = 4 \cdot 6 = 24$. Hence x is a root of $x^4 - 10x^2 + 1 = 0$.

Proposition 21.5. The set of all complex algebraic numbers is countable.

Proof. Denote the set of all algebraic numbers of degree n by A_n .

(1) We are going to prove first that A_n is countable. Let $x \in A_n$. Then equation (21.1.1) is satisfied and one can show that $c_1, \dots, c_n \in \mathbb{Q}$ are unique. Label all solutions of that equation by $1, 2, \dots, k$. We have $k \leq n$. ($k = n$ if there are no repeating solutions.) In this way each algebraic number x is uniquely determined by numbers c_0, c_1, \dots, c_n, i where i is the label of x as a solution of (21.1.1). Hence we have constructed a 1-1 function

$$f : A_n \rightarrow B_n = \mathbb{N}^n \times \{0, \dots, n\}.$$

B_n is countable by Theorem 20.16. Therefore, A_n is countable by Corollary 20.13.

(2) Since the set of all algebraic numbers is a union $A = \bigcup_{i=1}^{\infty} A_i$, it is countable by Proposition 20.18. □

Corollary 21.6. The set of transcendental numbers is uncountable.

This corollary stay in sharp contrast with the fact that we know only a few transcendental numbers! The following famous conjecture was formulated by Steven Schanuel, a professor at SUNY Buffalo:

Conjecture 21.7 (A basic form of Schanuel's Conjecture). For every $a, b \in \mathbb{Q}$, e^{a+bi} is not algebraic.

For example the conjecture claims that $e^i = \cos(1) + i\sin(1)$ is not algebraic. Indeed, the only known algebraic values of $\cos(\alpha)$ and $\sin(\alpha)$ are for α being a rational multiple of π .

PROBLEMS 21.

Problem 21.1. Let x be an algebraic number and let y be rational. Theorem 21.3 implies that $x \cdot y$ and $x + y$ are algebraic. Prove that without assuming Theorem 21.3.

Problem 21.2. Prove that $\sqrt{1 + \sqrt{2}}$ is algebraic.

Problem 21.3. Prove that the following numbers are transcendental: (a) π^2 , (b) $\sqrt{\pi}$, (c) $\pi + 1$.
(Hint: Use the definition and Thm 21.3.)

22. CARDINAL NUMBERS

For each set A one defines its cardinality, denoted by $|A|$. For example, if A is a set of n elements, we write $|A| = n$.

If A is infinite countable, we write $|A| = \aleph_0$. (“Aleph”, \aleph , is the first letter of Hebrew alphabet.) We denote the cardinality of \mathbb{R} by $|\mathbb{R}| = \mathfrak{c}$. This Gothic “ \mathfrak{c} ” stands for “continuum”.

Since the proper definition of cardinality is bit involved, we will not formulate it here. Imprecisely speaking, $|A|$ is the equivalence class of all sets equivalent to A . Hence we write $|A| = |B|$ iff A and B are equivalent.

Furthermore, we will write $|A| \leq |B|$ if A is equivalent to a subset of B . The following statement shows that this notation is justified:

Theorem 22.1. $|A| = |B|$ iff $|A| \leq |B|$ and $|B| \leq |A|$.

Proof. \Rightarrow obvious.

\Leftarrow skipped. (More difficult.) □

We say that A is of smaller cardinality than B and B has larger cardinality than A if $|A| \leq |B|$ and $|A| \neq |B|$. We write $|A| < |B|$ then.

Corollary 22.2. For every sets A, B either $|A| < |B|$ or $|A| = |B|$ or $|A| > |B|$.

Proposition 22.3. $|A| < |B|$ iff no function $f : A \rightarrow B$ is onto.

Proof. left as HW. □

By Corollary 20.21, $\aleph_0 \neq \mathfrak{c}$. Furthermore, we have

Corollary 22.4. $\aleph_0 < \mathfrak{c}$.

Proof. The proof of Theorem 20.19 shows that there is no epimorphism $\mathbb{N} \rightarrow (0, 1)$. The cardinality of $(0, 1)$ is \mathfrak{c} , by Problem 20.2. Now the statement follows from Proposition 22.3. □

Recall that 2^A denotes the set of all subsets of A .

Theorem 22.5. $2^{\aleph_0} = \mathfrak{c}$.

Proof. in class. □

In 1877, Georg Cantor stated the following famous

Conjecture 22.6 (Continuum Hypothesis (CH)). *There is no set A such that $\aleph_0 < |A| < \mathfrak{c}$.*

Kurt Gödel showed that CH cannot be disproved on the basis of Peano Axioms. Paul Cohen showed that CH cannot be proven from these axioms either! Therefore, we can assume that CH holds or that it does not hold without any contradiction. For that reason we say that the system of Peano Axioms is incomplete. One could resolve that conundrum by adding the statement of Continuum Hypothesis (or its negation) to Peano axioms. However, that systems of axioms will be incomplete as well:

Theorem 22.7 (Gödel Incompleteness Theorem). *No finite system of axioms is capable of proving all facts about the natural numbers.*

It is natural to ask whether there are sets of cardinality higher than \mathfrak{c} .

Theorem 22.8. *For every nonempty set A , 2^A has higher cardinality than A .*

Note that this statement is obvious for finite but not for infinite sets.

Proof. Since $f : A \rightarrow 2^A$ sending a to the one element subset $\{a\}$ is 1-1, the cardinality of 2^A is either larger or equal to the cardinality of A . Therefore, it is enough to prove that the cardinalities of A and of 2^A differ. We are going to prove that by showing that there is no onto function $f : A \rightarrow 2^A$.

Proof by contradiction. Suppose that $f : A \rightarrow 2^A$ is onto. We will say for the sake of the proof, that $a \in A$ is “self-included under f ” if $a \in f(a)$. E.g. If $A = \{1, 2, 3\}$ and $f(1) = \emptyset$, $f(2) = \{2, 3\}$, $f(3) = \{3\}$ then 2 and 3 are self-included. Let $S = \{a \in A \mid a \text{ not self-included under } f\}$. Since $S \in 2^A$ and $f : A \rightarrow 2^A$ is onto, $S = f(s)$ for some $s \in S$. Does s belong to S ? If it does then $s \in f(s) = S$. Hence s self-included and $s \notin S$. Contradiction. If it does not then $s \notin f(s)$ and, hence, s is not self-included. Therefore $s \in S$. Also a contradiction. \square

It is convenient to write the cardinality of 2^A using power notation, $|2^A| = 2^{|A|}$. Therefore, by Theorem 22.8, $2^{\aleph_0} > \aleph_0$.

Theorem 22.8 implies that there are infinitely many types of infinity. Indeed, for every set there is another one of strictly greater cardinality!

PROBLEMS 22.

Problem 22.1. Prove Proposition 22.3.

Problem 22.2. Prove that $(0, 1) \sim (0, 1) \times (0, 1)$. *Hint:* Use Theorem 22.1 and the 1-1 function $f : (0, 1) \rightarrow (0, 1) \times (0, 1)$ which you found in Problem 20.8.

Problem 22.3. Prove that $\mathbb{R} \sim \mathbb{R} \times \mathbb{R}$ (or, equivalently, that $\mathbb{R} \sim \mathbb{C}$).