

Introductory Course Mathematics

Winter Semester 2010/11
Silke Möser

27 September – 8 October 2010



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Mathematik



Title Picture by Prof. Dr. K. H. Hofmann

Introduction

These lecture notes are for the introductory course for beginning students of mathematics at TU Darmstadt.

The goal of this introductory course is to bring all students to a common level of knowledge, to repeat some of the more important contents you probably learned in school and to give you a first impression about what studying math is like. Moreover, since the course language for this course is English, the course aims to make you familiar with the English terminology. And because of all this, not only freshmen of the bilingual study programmes can benefit from this course but everyone else is also cordially invited to participate. (Even if one does not plan to do a bilingual programme, it might still be a good idea to gain some familiarity with the English vocabulary.) Therefore, I will, in addition to the English terms, also give German translations for most of the expressions. They will appear in brackets after the English term; for example [*Beispiel*].

Chapters 1 to 9 of these notes are based on the lecture notes originally written by Dr (AUS) Werner Nickel for the MCS introductory course and some modifications applied by Max Horn and Dennis Frisch.

If you find any mistakes in this text or have other suggestions, comments, remarks, questions, ... of any sort, please feel free to contact me under:

`smoeser@mathematik.tu-darmstadt.de`

Finally, I would like to thank Prof. Dr. K. H. Hofmann for giving permission to use his wonderful drawing of the old main building on the title page of these lecture notes.

*Silke Möser
21 September, 2010*

Contents

Introduction	1
1 Numbers	3
1.1 <i>The Natural Numbers</i>	3
1.1.1 <i>Prime numbers</i>	4
1.1.2 <i>Counting</i>	5
1.2 <i>The Integers</i>	9
1.3 <i>The Rational Numbers</i>	9
1.4 <i>The Real Numbers</i>	10
1.5 <i>The Complex Numbers</i>	12
2 Propositional Logic	16
2.1 <i>Logical operators</i>	16
2.2 <i>Quantifiers</i>	18
2.3 <i>Negation of propositions</i>	18
2.4 <i>The order of quantifiers</i>	19
3 Proof Techniques	20
3.1 <i>Direct proof</i>	20
3.2 <i>Proof by contradiction</i>	20
3.3 <i>Proof by contraposition</i>	20
3.4 <i>Proof by induction</i>	21
3.5 <i>Proof strategies</i>	22
3.6 <i>The pigeon hole principle</i>	23
Index	25

Lecture 1 — Numbers

1.1 The Natural Numbers

The natural numbers [natürliche Zahlen] count objects, e.g. 3 eggs, 160 students, about 10^{70} atoms in the universe.

The set of natural numbers is denoted by \mathbb{N} . Two natural numbers can be added and multiplied:

$$3 + 5 = 8 \quad 12 \cdot 11 = 132 \quad 7^2 = 49.$$

There are many interesting subsets of \mathbb{N} , three of them are

2, 4, 6, 8, 10, ... the even numbers [gerade Zahlen]
1, 3, 5, 7, 9, 11, ... the odd numbers [ungerade Zahlen]
1, 4, 9, 16, 25, ... the perfect squares [Quadratzahlen].

Any two natural numbers can be compared and they are either equal or one is smaller than the other. I.e., for any two natural numbers m and n we have that

$m < n$ m is less than n [m ist kleiner als n],
 $m > n$ m is greater than n [m ist grösser als n], or
 $m = n$ m is equal to n [m ist gleich n].

We thus say that the natural numbers are equipped with a total order [totale Ordnung].

Furthermore, if $a < b$ and $m < n$, then $a + m < b + n$ and $a \cdot m < b \cdot n$.

The elements of any subset of \mathbb{N} can be put in increasing order starting with the smallest element. Each non-empty subset of \mathbb{N} has a unique smallest element.

However, subsets of \mathbb{N} need not have a largest element.

Exercise 1.1.1. Find an example of a subset of \mathbb{N} that does not have a largest element. Describe all subsets of \mathbb{N} that do have a largest element!

Definition 1.1.2. We say that a natural number n is divisible [teilbar] by a natural number d if there exists a natural number m in \mathbb{N} such that

$$d \cdot m = n.$$

If this is the case, we also say that d divides [teilt] n and write $d|n$. A natural number d that divides n is also called a divisor [Teiler] of n . Vice versa, n is a multiple [Vielfaches] of d .

Example 1.1.3.

- The number 12 is divisible by 4.

Proof: We need to use the definition above. Here we have that $n = 12$ and $d = 4$. We have to find a natural number m such that $12 = 4 \cdot m$. This is easy since $m = 3$ is such a number (in fact the only one).

- The number 12 is not divisible by 7.

Proof: We need to show that there is no number m such that $7 \cdot m = 12$. (If there was such an m , then 7 would divide 12). In other words, we need to show that no multiple of 7 is equal to 12. The first few multiples of 7 are 7, 14, 21 which shows that 12 is not a multiple of 7.

Exercise 1.1.4.

- Prove: If d is a divisor of n , then $d = n$ or $d < n$.
- List all divisors of 12, 140 and 1001. Prove for 12 that there are no other divisors.
- Show that 7 is not a divisor of 100.
- Show that each natural number n is divisible by 1 and by n .
- Prove: If d divides m and n , then d also divides $m + n$ and $m - n$ and d^2 divides mn .

1.1.1 Prime numbers

Definition 1.1.5. A natural number different from 1 that is divisible by 1 and itself only is called a *prime number* [Primzahl].

Examples of primes are: 2, 3, 5, 7, 2003, $2^{13} - 1$.

The definition of primes raises the question how one can find primes. This is a difficult problem in general. There is an algorithm which, in principle, can find all the primes, although it is impractical for large prime numbers.

The sieve of Eratosthenes

This procedure finds all primes up to a given bound. It works as follows: Choose a number N , e.g. $N = 20$. List the natural numbers up to N beginning with 2:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

We iterate the following procedure: The next number which is not crossed out is a prime. We record it and cross out all its multiples:

So, 2 is a prime. Cross out its multiples, the even numbers:

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

The next prime is 3. Cross out all multiples of 3:

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~.

The next prime is 5. At this point we notice that all multiples of 5 have already been crossed out. The same is true for 7 and all the remaining numbers. Therefore, all the remaining numbers are primes.

Trial division

How does one check if a natural number n is a prime? One way is to try if it is divisible by any smaller number. To do that one has to carry out $n - 2$ divisions if n is a prime.

The following theorem helps in reducing the number of trial divisions because it shows that one only has to do trial divisions with smaller prime numbers. We have already used this fact in Eratosthenes' Sieve because we have declared a number a prime if it was not a multiple of any smaller prime.

Theorem 1.1.6. Any natural number n is divisible by a prime.

Proof. Consider all divisors of n different from 1. There is a smallest element q among these. Let m be a natural number such that $q \cdot m = n$.

We will show that q is a prime. Suppose that q is not a prime. Then q has a divisor $1 < d < q$ and $q = d \cdot m'$. We get

$$n = q \cdot m = (d \cdot m') \cdot m = d \cdot (m' \cdot m).$$

We see that d is a divisor of n . But d is smaller than q , which contradicts the choice of q . Therefore, it is impossible that q has a proper divisor. Hence, q is a prime. \square

Theorem 1.1.7 (without a proof). Each natural number is a product of primes. This product is unique up to permuting the factors.

Theorem 1.1.8. There are infinitely many primes.

Proof. We assume that there are only finitely many primes and show that this assumption leads to a contradiction.

Let k be the number of primes and let $p_1, p_2, p_3, \dots, p_k$ be the finitely many primes. Consider $M := p_1 p_2 p_3 \dots p_k + 1$. Clearly, p_j divides $p_1 p_2 p_3 \dots p_k$. If p_j divides M , then p_j also divides $M - p_1 p_2 p_3 \dots p_k = 1$. But no prime is a divisor of 1. Therefore, M is not divisible by any of the k primes above. This contradicts Theorem 1.1.6. \square

We will now leave the prime numbers and turn our attention back to using natural numbers for counting.

1.1.2 Counting

Example 1.1.9. Consider the five vowels A E I O U. Here are all three-letter arrangements (without repetition of letters) of these:

AEI AEO AEU AIE AIO AIU AOE AOI AOU AUE AUI AUO EAI EAO EAU
EIA EIO EIU EOA EOI EOU EUA EUI EUO IAE IAO IAU IEA IEO IEU
IOA IOE IOU IUA IUE IUO OAE OAI OAU OEA OEI OEU OIA OIE OIU
OUA OUE OUI UAE UAI UAO UEA UEI UEO UIA UIE UIO UOA UOE UOI

If we want to write down all three-letter words, then we have 5 choices for the first letter. Once the first letter is fixed we have 4 choices for the second letter and after that 3 choices for the last letter. This gives $5 \cdot 4 \cdot 3 = 60$ different choices, each of which produces a different word.

The general argument goes like this: For the first object we have n choices. For the second object we have $n - 1$ choices. As each choice of the first object can be combined with each

choice of the second object, this gives $n(n-1)$ possibilities. For the third choice we have $n-2$ possibilities. Therefore there are $n(n-1)(n-2)$ possibilities to place 3 objects out of n objects in a row. In general, there are $n(n-1)(n-2)\dots(n-(k-1))$ possibilities to place k out of n objects in a row.

If $k = n$, then this gives $n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1$ possibilities to arrange n different objects in a row. We denote the number

$$n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1 =: n!,$$

which is pronounced *n factorial* [*n Fakultät*]. We also set $0! := 1$. This can be interpreted as saying that there is one way to arrange no objects.

Example 1.1.10. The four symbols $+ - \cdot /$ can be arranged in $24 = 4 \cdot 3 \cdot 2 \cdot 1$ ways:

$$\begin{array}{cccccccc} + - \cdot / & + - / \cdot & + \cdot - / & + \cdot / - & + / - \cdot & + / \cdot - & - + \cdot / & - + / \cdot \\ - \cdot + / & - \cdot / + & - / + \cdot & - / \cdot + & \cdot + - / & \cdot + / - & \cdot - + / & \cdot - / + \\ \cdot / + - & \cdot / - + & / + - \cdot & / + \cdot - & / - + \cdot & / - \cdot + & / \cdot + - & / \cdot - + \end{array}$$

With the factorial notation we can write the number $n(n-1)(n-2)\dots(n-(k-1))$ as

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

This counts the number of arrangements of k objects out of n objects.

If we were interested in the number of ways there are to choose k objects out of n objects, then the order in which objects are chosen would be unimportant. The words AEI and EIA consist of the same letters and would not be considered different choices of three vowels.

Example 1.1.11. There are 10 ways to choose 3 vowels from A E I O U:

$$\text{AEI AEO AEU AIO AIU AOU EIO EIU EOU IOU}$$

In general, we need to take the number $\frac{n!}{(n-k)!}$ and divide by the number of arrangements of k objects. This gives

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

This expression is abbreviated by

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

which is pronounced as *n choose k* [*n über k*]. Note that $\binom{n}{0} = 1$. This means that there is one way to choose no object out of n .

Exercise 1.1.12.

- Show that $\binom{n}{k} = \binom{n}{n-k}$.

- Show that $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

The last property can be used to compute these numbers in a systematic way, known as Pascal's Triangle [Pascalsches Dreieck]:

						1												
					1		1											
				1		2		1										
			1		3		3		1									
		1		4		6		4		1								
		1	5		10		10		5		1							
	1		6		15		20		15		6		1					
	1	7		21		35		35		21		7		1				
	1	8		28		56		70		56		28		8		1		
1		9		36		84		126		126		84		36		9		1

Each number is the sum of the two numbers above. The number $\binom{n}{k}$ is the k -th element in row n (counted from top to bottom), where we start counting from 0.

The numbers $\binom{n}{k}$ are called binomial coefficients [Binomialkoeffizient]. The reason for this name becomes clear from the following: Consider the powers of the expression $x + y$. The first few are:

n	$(x + y)^n$
1	$x + y$
2	$x^2 + 2xy + y^2$
3	$x^3 + 3x^2y + 3xy^2 + y^3$
4	$x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

Notation 1.1.13 (The Sigma Sign). The following notation is a useful shorthand to concisely write sums and ubiquitous throughout mathematics.

Let's do an example: Consider the sum $1^2 + 2^2 + 3^2 + \dots + k^2$. Here we simply used the dots and hoped that everyone would guess correctly what we mean by them. This is where the sigma notation comes in:

$$1^2 + 2^2 + 3^2 + \dots + k^2 =: \sum_{i=1}^k i^2.$$

The expressions below and above the sigma sign specify the index variable (i in that case), and all the values that i takes in the expression behind the sigma sign (all numbers between 1 and k).

Comparing the numbers in the expressions above with the numbers in Pascal's Triangle reveals the following connection:

Theorem 1.1.14 (Binomial Theorem [Binomischer Lehrsatz]). For each natural number n we have the following equality:

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

The expression on the right hand side is the abbreviation of the sum

$$\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \dots + \binom{n}{n-1}xy^{(n-1)} + \binom{n}{n}y^n.$$

We will give two proofs of this theorem:

Proof 1. We consider the coefficient of the expression $x^{n-k}y^k$ and how it arises from the product

$$\underbrace{(x+y)(x+y)\dots(x+y)(x+y)}_{n\text{-times}}.$$

Expanding the brackets, we have to multiply each occurrence of x or y with each other occurrence of x or y . To obtain $x^{n-k}y^k$ we have to choose y exactly k -times. Since we are choosing k times y out of n occurrences of y , we can do this in $\binom{n}{k}$ ways. Therefore, the term $x^{n-k}y^k$ occurs $\binom{n}{k}$ times. \square

Proof 2. We do a proof by induction [Induktion].

First, we show that the theorem is true for $n = 1$:

$$(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y.$$

Now we show that the statement of the theorem is true for $n+1$ if it is true for a natural number n .

$$\begin{aligned} (x+y)^{n+1} &= (x+y)(x+y)^n \\ &= (x+y) \cdot \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \\ &= \sum_{k=0}^n \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^n \binom{n}{k} x^{n-k} y^{k+1} \\ &= \sum_{k=0}^n \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^{n+1} \binom{n}{k-1} x^{n+1-k} y^k \\ &= x^{n+1} + \sum_{k=1}^n \binom{n}{k} x^{n+1-k} y^k + \sum_{k=1}^n \binom{n}{k-1} x^{n+1-k} y^k + y^{n+1} \\ &= x^{n+1} + \sum_{k=1}^n \left(\binom{n}{k} + \binom{n}{k-1} \right) x^{n+1-k} y^k + y^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k \end{aligned} \quad \square$$

1.2 The Integers

The set \mathbb{N} is closed [abgeschlossen] under taking sums and products of natural numbers. I.e., sums and products of natural are again natural numbers.

However the difference of two natural numbers need not be a natural number: $7 - 13 = ?$ In other words, there is no solution to the equation $7 = x + 13$ in the set of natural numbers.

Thus, one defines the set \mathbb{Z} of integers [ganze Zahlen]:

$$\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots$$

The integers are closed under taking sums, products and differences.

The notions of order, divisibility and primes defined above can be extended to the set of integers in a natural way with little changes:

Theorem 1.2.1 (without proof). Each integer is a product of primes and ± 1 . This product is unique up to permuting the factors.

1.3 The Rational Numbers

The quotient of two integers need not be an integer. In fact, the quotient of an integer m and an integer d is an integer if and only if m is divisible by d . In other words, for integers m and n the equation $m \cdot x = n$ need not have a solution for x in the set of integers.

Again, we define a new set to sort out this problem, the set \mathbb{Q} of rational numbers [rationale Zahlen]. It consists of all fractions [Brüche] $\frac{a}{b}$ where a is an integer and b a non-zero integer. The integer a is called the numerator [Zähler] and b is called the denominator [Nenner]. The rationals are closed under addition, subtraction, multiplication and division.

A set of numbers in which those four arithmetic operations can be performed is called a field [Körper]; \mathbb{Q} is called the field of rational numbers [Körper der rationalen Zahlen].

Arithmetic of rational numbers

Definition 1.3.1. Let a, b, c and d be integers with b and d not 0.

- **Addition** Two fractions are added by finding a common denominator (you may want to look for their smallest common denominator):

$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}.$$

- **Multiplication** Two fractions are multiplied by multiplying numerators and denominators:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

- **Division** A fraction is divided by another fraction by multiplying with the reciprocal [Kehrwert] of the second fraction ($c \neq 0$):

$$\frac{a}{b} : \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}.$$

- Between any two different rational numbers lie infinitely many rational numbers. For this it is enough to show that there is always a rational number lying strictly between any pair of different rational numbers. For example, a rational number lying between the rational numbers x and y is the number $\frac{x+y}{2}$.

- **Equality** Two fractions $\frac{a}{b}$ and $\frac{c}{d}$ are equal if and only if $ad = bc$.

This definition implies that canceling common factors in the numerator and denominator of a fraction does not change the value of the fraction: Let a , b and c be integers with b and c different from 0. Then

$$\frac{ac}{bc} = \frac{a}{b} \quad \text{because} \quad ac \cdot b = bc \cdot a.$$

However, certain equations do not have a solutions in the set of rational numbers. For example, the equation $x^2 = 2$.

Theorem 1.3.2. A solution of the equation $x^2 = 2$ is not a rational number.

Proof. Let $\frac{a}{b}$ be a rational number with $\left(\frac{a}{b}\right)^2 = 2$. We may assume that a and b have no common factor.

Then $a^2 = 2b^2$. Therefore a^2 is an even number. The square of an integer is even if and only if the integer is even. Therefore, a is even and can be written as $a = 2d$. This gives $2b^2 = 4d^2$ and dividing by two gives $b^2 = 2d^2$. By the same reasoning as above, b is even. Hence a and b contain the common factor 2, contrary to our assumption. \square

Exercise 1.3.3.

- Let n be a natural number. Show that n^2 is even if and only if n is even.
- Show that $x^2 = 6$ does not have a rational solution.
- Show that $1 + \sqrt{2}$ is not a rational number.
- Show that $x^3 = 2$ does not have a rational solution.

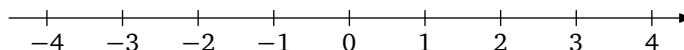
1.4 The Real Numbers

The set of real numbers [reelle Zahlen], denoted by \mathbb{R} is an extension of the rational numbers containing all limits [Grenzwerte] of rational sequences [Folgen] such as

$$\begin{aligned} \sqrt{2} &= 1,4142135623730950488016887242096980785696718753769480731766797379907324784621\dots \\ e &= 2.7182818284590452353602874713526624977572470936999595749669676277240766303535\dots \\ \pi &= 3.1415926535897932384626433832795028841971693993751058209749445923078164062862\dots \end{aligned}$$

and the solutions to equations of the form $x^5 + x + 1 = 0$ and many more. The real numbers are much more complicated than the rational numbers. Most real numbers cannot be written down explicitly.

However, one important feature of the reals is that they – just as the rationals – form a field. The set of real numbers is often visualised by a line, called the real line [reelle Zahlengerade].



Definition 1.4.1. Let a be a non-negative real number and n a natural number. The n -th root [n-te Wurzel] of a is a non-negative real number r such that $r^n = a$.

Note that in general the n -th root is only defined for non-negative real numbers. Also the n -th root of a non-negative real number is always a non-negative real number. Taking the root of a positive number is the inverse operation to raising a real number to the n -th power.

If x is a negative number, then taking the square root is not the inverse operation of squaring x because the square root is positive: $x \neq \sqrt{x^2} = -x$. The same is true for all even powers n . If n is an odd number, however, then the n -th root is declared for all real numbers x , e.g.

$$\sqrt[3]{-8} = -2.$$

Definition 1.4.2. Let a be a real number. We define the following function:

$$|a| = \begin{cases} a & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -a & \text{if } a < 0. \end{cases}$$

The non-negative real number $|a|$ is called the *absolute value* [Betrag] of a .

Exercise 1.4.3. Let a , b and c be real numbers and ε a positive real number.

- Show that $|a| \leq c$ is the same as saying $-c \leq a \leq c$.
- Show that $a \leq |a|$ and $-|a| \leq a$.
- Prove the triangle inequality: $|a + b| \leq |a| + |b|$. *Hint:* Use the previous two inequalities.
- Prove the inequality $|a| - |b| \leq |a - b|$.
- Show that $|x - a| \leq \varepsilon$ is the same as saying $a - \varepsilon \leq x \leq a + \varepsilon$. Interpret this geometrically! What is the set of all x satisfying this condition?
- Determine the solutions of the inequalities $|4 - 3x| > 2x + 10$ and $|2x - 10| \leq x$.

1.5 The Complex Numbers

The real numbers allow us to solve many more equations than the rational numbers, which in turn allow solving more equations than the integers. Still, there are some simple equations we cannot solve. In particular, the equation $x^2 + 1 = 0$ has no solution over the reals. A solution to this would be $\sqrt{-1}$ if it were defined.

When faced with the problem of not being able to divide by arbitrary non-zero numbers, we simply introduced new symbols (namely fractions). We do the same with the square root of -1 by defining the symbol i (the imaginary unit) such that

$$i^2 = -1.$$

This leads to the set \mathbb{C} of complex numbers [komplexe Zahlen]. It consists of all terms of the form $z = a + bi$, where a and b are real numbers. We call a the real part [Realteil], and b the imaginary part [Imaginär Teil] of z . The complex numbers form a field with the real numbers naturally embedded in them. Unlike the number sets we saw so far, the complex numbers do not permit a natural total order.

Arithmetic of complex numbers

Definition 1.5.1. Let $a, b, c, d \in \mathbb{R}$.

- **Equality** Two complex numbers $a + bi$ and $c + di$ are equal if and only if their real and imaginary parts are equal, i.e., if $a = c$ and $b = d$.
- **Addition** Two complex numbers are added as one might expect:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

- **Multiplication** Two complex numbers are multiplied by following the normal rules of multiplication, treating i like a variable and using that $i^2 = -1$:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

- **Division** A complex number is divided by another (non-zero) complex number by multiplying with the *inverse* [Inverse] of the second number. The inverse is computed as follows:

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i.$$

Exercise 1.5.2. Verify that the inversion formula in Definition 1.5.1 is correct.

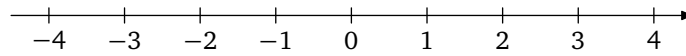
We define the *complex conjugate* [komplex konjugierte] of the complex number $z = a + bi$ as $\bar{z} := a - bi$. We now define the *absolute value* for a complex number z as

$$|z| := \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}.$$

Note that over the real numbers this coincides with the previous definition of absolute value. Using these notations, we can write z^{-1} as $\frac{\bar{z}}{|z|^2}$.

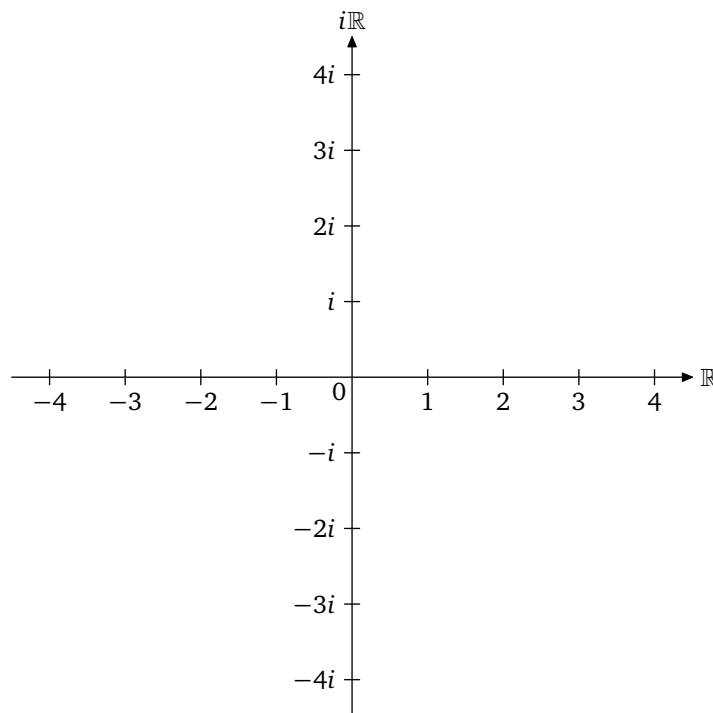
Complex numbers from a geometric point of view

When introducing the real numbers, we also introduced the real line.



The real line is a geometric way to visualise the real numbers. So let's try and find out how the arithmetic operations are reflected in this geometric setting. We can easily see that addition is a translation and multiplication is a dilation. If the number we multiply with is negative, then the dilation also changes the direction.

We can view the complex numbers as a product of two real lines, one for the real part and one for the imaginary part. We can visualise complex numbers in a coordinate system:



Now we can view the field of complex numbers as a two dimensional plane, the so called complex plane [komplexe Zahlenebene].

There is another possibility to describe complex numbers:

Proposition 1.5.3. Each complex number $z = a + bi$ can be expressed as

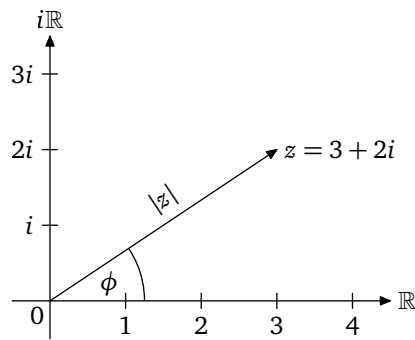
$$z = |z|(\cos \phi + i \sin \phi),$$

where ϕ is a real number called the argument [Argument] of z and

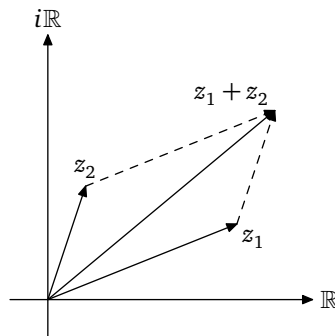
$$|z| := \sqrt{a^2 + b^2}$$

is the absolute value of z . If we take $-\pi < \phi \leq \pi$, then ϕ is uniquely determined.

Moreover, if we draw z as a vector in the complex plane, then $|z|$ is its length and ϕ is the angle between the vector and the real axis.

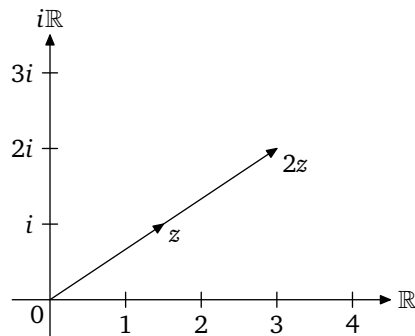


We know from above that adding a real number to a real number is a translation. This is still true for complex numbers.



Looking at the multiplication, we saw that multiplying a real number with a real number is a dilation.

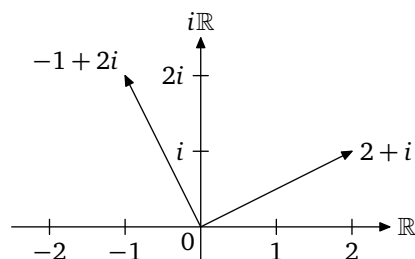
This is still correct, if we multiply a complex number with a real number.



Now consider a complex number with non-zero imaginary part:

Let $z := 2 + i$. If we multiply with i we get $(2 + i) \cdot i = 2i + i^2 = -1 + 2i$.

We see that $|2 + i| = |-1 + 2i|$ and in the complex plane we see that a multiplication with i results in a rotation about 90 degrees counterclockwise.



In general, if we multiply two complex numbers z_1 and z_2 , we multiply the lengths and add the angles.

Proposition 1.5.4. *Let $z_1 = |z_1|(\cos \phi_1 + i \sin \phi_1)$, $z_2 = |z_2|(\cos \phi_2 + i \sin \phi_2)$, then*

$$z_1 \cdot z_2 = |z_1| |z_2| (\cos(\phi_1 + \phi_2) + i \sin(\phi_1 + \phi_2)).$$

Lecture 2 — Propositional Logic

Examples of propositions: 5 is not a number. Darmstadt is in Germany. Mathematics is a science. 7 divides 12.

A proposition [Aussage] is a grammatically correct statement which it can be decided of whether it is true or false.

More interesting than deciding whether one proposition is true or false is to decide whether a proposition is true under certain circumstances. This process is fundamental in mathematics.

We now have a look at how to combine given propositions to new propositions and under which circumstances the new proposition is true.

2.1 Logical operators

Whenever we construct a new proposition from other propositions we can use a truth table [Wahrheitstabelle] to describe the newly constructed proposition. We simply write down the value of the new one for all combinations of values of the old ones. This section gives several examples for truth tables.

Negation: The negation [Verneinung] of a proposition A is false when A is true and vice versa (written $\neg A$):

A	$\neg A$
t	f
f	t

And (Conjunction): Two propositions A and B can be combined by “and” to give a new proposition $A \wedge B$ (the conjunction [Konjunktion] of A and B) which is true precisely when both A and B are true:

A	B	$A \wedge B$
t	t	t
t	f	f
f	t	f
f	f	f

Or (Disjunction): Two propositions A and B can be combined by “or” to give a new proposition $A \vee B$ (the disjunction [Disjunktion] of A and B) which is true precisely when at least one of A and B is true:

A	B	$A \vee B$
t	t	t
t	f	t
f	t	t
f	f	f

Implication: If a proposition B is true whenever another proposition A is true, then A implies [impliziert] B . We write $A \Rightarrow B$ and call this statement an implication [Implikation]:

A	B	$A \Rightarrow B$
t	t	t
t	f	f
f	t	t
f	f	t

Equivalence: A proposition A is equivalent [äquivalent] to a proposition B (written $A \Leftrightarrow B$) if A is true precisely when B is true and A is false precisely when B is false (also written A iff B , which means A is true if and only if B is true).

A	B	$A \Leftrightarrow B$
t	t	t
t	f	f
f	t	f
f	f	t

We give another characterisation for equivalence. And we take this as an example for a typical proof of such logical propositional statements:

Theorem 2.1.1. Let A and B be two propositions. Then the following are equivalent:

- (i) $((A \Rightarrow B) \wedge (B \Rightarrow A))$
- (ii) $(A \Leftrightarrow B)$

Proof.

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
t	t	t	t	t
t	f	f	t	f
f	t	t	f	f
f	f	t	t	t

□

Implications that are not equivalences

Here are some examples for implications which are only true “in one direction”, i.e., they are no equivalences:

- For all $x \in \mathbb{R}$: $x > 0 \Rightarrow x^2 > 0$.
- If x and y are negative real numbers, then $x \cdot y > 0$.

Now let us have a look at the converses [Umkehrung] of the above propositions:

- For all $x \in \mathbb{R}$: $x^2 > 0 \Rightarrow x > 0$.
- If $x \cdot y > 0$ then x and y are negative real numbers.

In both cases we easily find a counterexample to refute these propositions.

2.2 Quantifiers

Another important feature of propositional logic are the quantifiers [Quantoren]:

All quantifier [All-Quantor]: If for each element e of a set S a proposition $A(e)$ is given then

$$\forall e \in S : A(e)$$

is a proposition which is true iff $A(e)$ is true for each $e \in S$. (Read: For all e in S , $A(e)$ is true.)

Existence quantifier [Existenz-Quantor]: If for each element e of a set S a proposition $A(e)$ is given then

$$\exists e \in S : A(e)$$

is a proposition which is true iff $A(e)$ is true for at least one $e \in S$. (Read: It exists an element e such that $A(e)$ is true.)

2.3 Negation of propositions

Consider the following examples:

- All sheep are black.
- It exists a male student at the TU Darmstadt.
- An animal is a lion or a duck.
- A real number is positive and negative.

Now consider the negations of the above:

- If all sheep are black, then there is no sheep with another colour. So the negation is: There exists a sheep which is not black.
- This proposition is true if at least one student at the TU Darmstadt is male. So the negation is: All students at the TU Darmstadt are not male.
- To be true, each animal has to be a duck or a lion. So the negation is: There is an animal which is neither a duck nor a lion.
- The proposition is true if all real numbers are both positive and negative. So the negation is: There is a real number which is not negative or not positive.

We summarise these insights using quantifier symbols:

Proposition 2.3.1.

- $\neg(\forall e \in S : A(e)) \iff \exists e \in S : \neg A(e)$
- $\neg(\exists e \in S : A(e)) \iff \forall e \in S : \neg A(e)$
- $\neg(A \vee B) \iff \neg A \wedge \neg B$
- $\neg(A \wedge B) \iff \neg A \vee \neg B$

As a rule of thumb you can keep in mind that a negation moving to and fro inside a proposition flips every quantifier it passes.

2.4 The order of quantifiers

It is very important to understand that we cannot change the order of the quantifiers in a proposition. E.g. let $A(x, y)$ be a proposition defined for each x and y . Then the proposition $(\forall x)(\exists y) : A(x, y)$ is not equivalent to the proposition $(\exists y)(\forall x) : A(x, y)$.

This is immediately evident if you consider the following everyday example:

Example 2.4.1. Consider the following proposition:

$$(\forall p \in \text{people})(\exists m \in \text{people}) : m \text{ is mother of } p,$$

where *people* denotes the set of all people in the world (living or dead).

Then the assertion of this proposition is that every person possesses a mother, which is clearly true.

Now assume we exchange the order of the quantifiers involved to get the proposition

$$(\exists m \in \text{people})(\forall p \in \text{people}) : m \text{ is mother of } p.$$

Then this proposition asserts that there is one person in the world who is the mother of every person in the world (including herself), which is just as clearly false.

Lecture 3 — Proof Techniques

A *proof* is a convincing demonstration (within the accepted standards of the field) that some mathematical statement is necessarily true. Proofs are obtained from deductive reasoning, rather than from inductive or empirical arguments. That is, a proof must demonstrate that a statement is true in all cases, without a single exception.

In this chapter we will take a look at the most common and expedient proof techniques and give examples to illustrate them.

3.1 Direct proof

A *direct proof* [direkter Beweis] is straightforward. The conclusion is established by logically combining the axioms, definitions, and earlier theorems. Thus, you start out with the assumptions A and try to directly conclude proposition B . I.e., we want to show $A \implies B$.

Example 3.1.1.

- The sum of two even integers is even.
- If a divides b and a divides c then a divides $b + c$.

3.2 Proof by contradiction

A *proof by contradiction* [Beweis durch Widerspruch] (also known as *reductio ad absurdum*) uses the fact that a proposition can only be either true or false.

It is shown that if some statement (namely, the negation of what we aim to prove) were true, then a logical contradiction would have to occur.

Example 3.2.1.

- $\sqrt{3}$ is irrational.
- There is no smallest positive (i.e., > 0) rational number.

3.3 Proof by contraposition

A *proof by contraposition* [Beweis durch Kontraposition] uses

$$(A \implies B) \iff (\neg B \implies \neg A).$$

In other words, it establishes the conclusion “if A then B ” by proving the equivalent contrapositive statement “if not B then not A ”.

Example 3.3.1. If n^2 is even, then n is even.

3.4 Proof by induction

A proof by induction [Beweis durch vollständige Induktion] is a useful tool to prove a proposition $B(n)$ which is stated for all natural numbers n (or for all natural numbers greater than a given number $k \in \mathbb{N}$).

A proof by induction consists of two parts:

- (i) *Induction beginning* [Induktionsanfang]: Prove $B(1)$ (or $B(k)$).
- (ii) *Induction step* [Induktionsschritt]: Assume that $B(n)$ is true and show that $B(n + 1)$ is true (making use of the fact that $B(n)$ is true).

Imagine a domino chain. The induction step assures that a domino (here $n + 1$) falls if domino n falls.

Look at this example:

Example 3.4.1. A typical example for a proof by induction is the following:

Proposition: $\sum_{k=1}^n k = \frac{n(n+1)}{2}$.

Proof. We do a proof by induction.

Induction beginning: For $n = 1$, the claim is

$$\sum_{k=1}^1 k = 1 = \frac{1 \cdot 2}{2},$$

which is quite obviously true.

Induction step: Now we assume that the proposition is true for n . That means

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}$$

is true. With the help of this assumption we try to prove the proposition

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2},$$

which is the proposition for $n + 1$. We get

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \sum_{k=1}^n k + (n+1) \\ &\stackrel{\text{assumption}}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

□

To see that both steps (beginning and induction) are essential for the proof to be valid, consider the following:

Example 3.4.2. Consider the proposition: $1 + n > 2 + n$ for all $n \in \mathbb{N}$.

This is obviously wrong, but still it is easy to do the induction step:

Assume that the proposition is true for n . So

$$\begin{aligned}n + 1 &> n + 2 \\ \iff n + 1 + 1 &> n + 2 + 1 \\ \iff (n + 1) + 1 &> (n + 1) + 2.\end{aligned}$$

But we cannot do the induction beginning because there is no smallest natural number satisfying $n + 1 > n + 2$.

A fake induction proof

Some proofs look good at the first glance, but sometimes a subtle error is inside. Look at this “proof”:

Theorem: All sheep have the same colour.

Proof. We proof inductively that any set of sheep consists of only sheep of a single colour, i.e., is equicolored.

Induction start: A set containing one sheep is obviously equicolored.

Induction step: Assume that any set of n sheep is equicolored. Now consider a set of $n + 1$ sheep. The set formed by the first n sheep is equicolored. But so is the set formed by the last n sheep. Hence the whole set must be equicolored. \square

What is wrong here?

3.5 Proof strategies

In mathematics, you often state the existence of a certain object. For example:

Theorem 3.5.1. Any two natural numbers a and b have a greatest common divisor [größter gemeinsamer Teiler].

We will first consider two different proofs of Theorem 3.5.1.

Existence proof

Like the name promises, an existence proof [Existenzbeweis] proves the existence of something. Let's look at Theorem 3.5.1:

Proof. A divisor of a natural number has to be less or equal to the number. Since there are only finitely many natural numbers which are less than or equal to a and b , respectively, only finitely many divisors can exist.

Take 1: it is a natural number and divides both a and b . So 1 is a common divisor. Since there are only finitely many other divisors, a greatest common divisor exists. \square

At the end of the proof, we know that the theorem holds but we cannot say what the greatest common divisor is.

Constructive proof

A constructive proof [konstruktiver Beweis] is a proof which also delivers a solution. Again we look at Theorem 3.5.1:

Proof. For each prime number p denote by $e_a(p), e_b(p)$ its exponent in the (unique!) prime factor decompositions of a , respectively b . (Note that in either case only finitely many of the $e_a(p), e_b(p)$ are larger than zero.)

Then

$$d := \prod_{p \text{ prime}} p^{\min(e_a(p), e_b(p))}$$

is the greatest common divisor of a and b . □

Uniqueness proof

Once we know about the existence of a solution, we might be interested in its uniqueness. Then we have to maintain a uniqueness proof [Eindeutigkeitsbeweis].

Consider the following theorem, which is stronger than Theorem 3.5.1.

Theorem 3.5.2. Any two natural numbers a and b have a unique greatest common divisor.

Proof. Assume that there are two different greatest common divisors c and d of a and b . Since c and d are common divisors and c is the greatest common divisor, this leads to $c \geq d$. The same is true for d leading to $d \geq c$ and so $c = d$. □

3.6 The pigeon hole principle

The following – surprisingly simple – theorem can very often be applied in proofs:

Theorem 3.6.1 (The pigeon hole principle [Schubfachprinzip]). Assume we are given $n + 1$ balls and n boxes and are asked to distribute the balls among the boxes. Then there exists one box which contains more than one ball.

There is nothing to prove.

Now let us apply the pigeon hole principle to prove the following:

Proposition 3.6.2. Let $n \in \mathbb{N}$ with $2 \nmid n$, $5 \nmid n$. Then there is a number $N \in \mathbb{N}$ whose decimal representation is $N = 111 \dots 111$ such that $n|N$.

Proof. Denote by N_1, N_2, \dots, N_{n+1} the first $n + 1$ numbers of the form $111 \dots 111$, i.e.,

$$N_i = \underbrace{111 \dots 111}_{i \text{ ones}}$$

Moreover, denote by R_i the remainder of N_i on division by n . Then $0 \leq R_i \leq n - 1$. Thus, there are only n different possible values for R_i and by the pigeon hole principle (Theorem 3.6.1) there are $i \neq j$ such that $R_i = R_j$. Without loss of generality assume that $i > j$. Then $n|(N_i - N_j)$ and

$$N_i - N_j = \underbrace{111 \dots 111}_{i-j \text{ many}} \underbrace{000 \dots 000}_{j \text{ many}} = \underbrace{111 \dots 111}_{i-j \text{ many}} \cdot 10^j = N_{i-j} \cdot 10^j.$$

Since n is relatively prime to 10^j , we must have $n|N_{i-j}$. □

Index

- absolute value, 11
- all quantifier, *see* quantifier
- argument, 13

- binomial coefficient, 6
- binomial coefficients, 7
- Binomial Theorem, 7

- closed, 9
- complex conjugate, 12
- complex numbers, 12
- complex plane, 13
- conjunction, 16
- constructive proof, 23
- converse
 - of a proposition, 17

- denominator, 9
- direct proof, 20
- disjunction, 16
- divide, *see* divisible
- divisible, 3, 9
- divisor, 3

- equivalent, 17
- even numbers, 3
- existence proof, 22
- existence quantifier, *see* quantifier

- factorial, 6
- field, 9
 - of complex numbers, 12
 - of rational numbers, 9
 - of real numbers, 11
- fraction, 9

- greatest common divisor, 22

- imaginary part, 12
- implication, 17
- implies, 17
- induction, 8, 21, 22
- induction beginning, 21

- induction step, 21
- integer, 9
- inverse, 12

- limit, 10

- multiple, 3

- n choose k , *see* binomial coefficient
- n -th root, 11
- natural numbers, 3
- negation, 16
- numerator, 9

- odd numbers, 3

- Pascal's Triangle, 7
- pigeon hole principle, 23
- prime number, 4, 5
- proof by contradiction, 20
- proof by contraposition, 20
- proof by induction, *see* induction
- proposition, 16

- quantifiers, 18

- rational numbers, 9
- real line, 11
- real numbers, 10
- real part, 12
- reciprocal, 9

- sequence, 10
- squares, 3

- total order, 3
- truth table, 16

- uniqueness proof, 23