This text is an ai-translation of my man-made german teaching material, pls notify me if there are any mistakes, made by the ai or me. Thanks

Bernd Kirchheim kirchheim@math.uni-leipzig.de (once it runs again)

1. Real Numbers

These are the analyst's bread and butter. For the construction of the real numbers see W. Rudin's book 'Analysis'; here we simply assume their existence. Then the real numbers are a set $\mathbb{R}$ with

- two arithmetic operations which assign to every pair $(x, y) \in \mathbb{R} \times \mathbb{R}$ of two real numbers an element $x + y \in \mathbb{R}$ and $x \cdot y \in \mathbb{R}$ respectively, and
- an order (or comparison) relation $<$

such that the 13 axioms gradually discussed below hold. In the process we also derive most of the rules for equations and inequalities familiar from school, i.e. we reduce them to our few axioms.

I. Field axioms

There are 9 of these, and they concern only the arithmetic operations

	Addition		Multiplication	
(AA)	$(x+y)+z = x+(y+z)$	(MA)	$(x\cdot y)\cdot z = x\cdot(y\cdot z)$	$\forall x,y,z \in \mathbb{R}$ associative law
(AK)	$x+y = y+x$	(MK)	$x\cdot y = y\cdot x$	$\forall x,y \in \mathbb{R}$ commutative law
(AN)	$\exists 0 \in \mathbb{R}\, \forall x \in \mathbb{R}:\ 0+x = x$	(MN)	$\exists 1 \in \mathbb{R} : (1 \neq 0\ \&\ \forall x \in \mathbb{R} : 1\cdot x = x)$	neutral element
(AI)	$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R} : x+y = 0$	(MI)	$\forall x \in \mathbb{R}$ with $x \neq 0\, \exists y \in \mathbb{R} : x\cdot y = 1$	inverse element
(DG)	$x\cdot(y+z) = (x\cdot y)+(x\cdot z)$			$\forall x,y,z \in \mathbb{R}$ distributive law

Remark 1.1. The neutral elements in (AN),(MN) are unique as a consequence of the axioms – without this being explicitly assumed; however, it has to be proved! In any case, it makes the right-hand sides in (AI),(MI) well defined. The neutral element of addition is called zero, the neutral element of multiplication one.

Here we prove only the uniqueness of zero, so let us consider 0_I and 0_{II} in $\mathbb{R}$ such that

$$\text{by (AN) we have:}\quad \forall x \in \mathbb{R} : 0_I + x = x \text{ and } \forall y \in \mathbb{R} : 0_{II} + y = y.$$

Then it follows that

$$0_{II} \overset{(AN) \text{ with } x=0_{II}}{=} = 0_I + 0_{II} \overset{(AK)}{=} 0_{II} + 0_I \overset{(AN) \text{ with } y=0_I}{=} = 0_I,$$

so indeed $0_I = 0_{II}$, as claimed. The uniqueness of one follows analogously.

Remark 1.2. We see that without the distributive law, addition and multiplication would be almost equivalent ('isomorphic') operations; note, however, the exclusion of zero in (MI). Only this ninth axiom breaks the far-reaching symmetry between the two.

Remark 1.3. Inverse elements in (AI),(MI) are unique for given x, see Theorem 2.6 for a more general statement. We write $-x$ and x^{-1} for the additive and multiplicative inverse respectively.

Remark 1.4. The 9 field axioms do not yet characterise $\mathbb{R}$; there are other fields (still to be discussed) which also satisfy them. See, e.g., $\mathbb{Q}$ or Example 2.12. A completely trivial field is $\{0\}$ with the operations $0 + 0 = 0 = 0 \cdot 0$. To exclude this example, we **always** require $0 \neq 1$ in what follows.

Lemma 1.5. *For all $x, y \in \mathbb{R}$ and $s \in \mathbb{R}$, $f \in \mathbb{R} \setminus \{0\}$ we have*

$$x = y \Leftrightarrow x + s = y + s \quad \text{and} \quad x = y \Leftrightarrow x \cdot f = y \cdot f.$$

We show only the second part

Theorem 1.6. *Unique solvability of equations*

a) $\forall x, y \in \mathbb{R}\, \exists z \in \mathbb{R} : x + z = y$. This z is unique and given by $z = y + (-x)$.
b) $\forall x, y \in \mathbb{R}$ with $x \neq 0\, \exists z \in \mathbb{R} : xz = y$. This z is unique and given by $z = y(x^{-1})$.

We write $z = y - x$ for the solution in a) and $z = y/x$ for the solution in b).

We show only the second part

Theorem 1.7. $\forall x \in \mathbb{R} : 0 \cdot x = 0$. *('Being neutral for + forces being a terminator for $\cdot$.')*

Corollary 1.8. $\forall x \in \mathbb{R} : (-1) \cdot x = -x$.

Theorem 1.9. $\forall x, y \in \mathbb{R} : xy = 0 \Leftrightarrow (x = 0 \text{ } \textit{or } y = 0)$.
Algebraists phrase this as: no 'zero divisors' in $\mathbb{R}$*, or in a field/ integral domain.*

Proof e.g. by the case distinction $x = 0$ versus $x \neq 0$ and Lemma 2.5.

Lemma 1.10.

a) $\forall x \in \mathbb{R} : -(-x) = x$
b) $\forall x \in \mathbb{R}$ with $x \neq 0 : (x^{-1} \neq 0 \ \& \ (x^{-1})^{-1} = x)$

We show only the second part.

Example 1.11. $z^2 = 1 \Leftrightarrow (z = 1 \text{ or } z = -1)$, *or more generally* $\forall z, x \in \mathbb{R} : z^2 = x^2 \Leftrightarrow (z = x \vee z = -x)$.

This follows from the binomial formula and Theorem 2.9

Example 1.12. A finite field
$GF(3) = \{0, 1, 2\}$ *with the following rules of calculation ('residue classes modulo 3' – for experts).*

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

so $2^{-1} = 2$ *and* $2 = -1$ *here.*

Checking the nine field axioms by hand is possible but tedious. (This is simpler e.g. for $GF(2) = \{0, 1\}$ *with the corresponding rules of calculation, of which only* $1 + 1 = 0$ *does not follow directly from (AN),(MN) or Theorem 1.5). It turns out that for every prime number* p *there exists a field* $GF(p)$ *with* p *elements, and the validity of the field axioms (AA),(MA),(AK),(MK),(AN),(MN) and (DG) follows easily from similar statements for the natural numbers, without tediously trying out all individual cases.)*

Remark 1.13. *In the proofs so far, the conclusions could each be derived easily from the axioms. We did not yet need finer methods such as indirect proof (proof by contradiction). This will change in what follows.*

The field axioms defined so far enable calculation with equations; for calculating with inequalities we need the notion of order(ing). (compare Chapter 3 in O. Forster's book) First and foremost one has to specify which numbers are 'positive', i.e. greater than zero. These numbers must then have the properties listed below:

II. Order axioms

There is a set $\mathbb{P}$ of real numbers (i.e. $\mathbb{P} \subset \mathbb{R}$) such that

(O.1) $\forall x \in \mathbb{R}$ *exactly* one of the statements holds: $x \in \mathbb{P}$, $x = 0$, $-x \in \mathbb{P}$ 'trichotomy'

(O.2) If $x \in \mathbb{P}$ & $y \in \mathbb{P}$ then $x + y \in \mathbb{P}$ 'closure under addition'

(O.3) If $x \in \mathbb{P}$ & $y \in \mathbb{P}$ then $xy \in \mathbb{P}$ 'closure under multiplication'

Definition 1.14. We say

$0 < x$ (i.e. x is *positive*) iff $x \in \mathbb{P}$; $0 > x$ (i.e. x is negative) iff $-x \in \mathbb{P}$
$x < y$ (i.e. x less than y) iff $0 < y - x$; $x > y$ (i.e. x greater than y) iff $0 > y - x$
$x \leq y$ iff ($x < y$ or $x = y$); $x \geq y$ iff ($x > y$ or $x = y$)

Remark 1.15. a) *every* $x \in \mathbb{R}$ *is positive, negative or zero*
b) *by Theorem 1.5,* $x = y \Leftrightarrow 0 = y - x$, *so* $\forall x, y \in \mathbb{R} : x < y$ or $x > y$ or $x = y$
c) $x < y \Leftrightarrow -(x - y) = y - x \in \mathbb{P} \Leftrightarrow 0 > x - y \Leftrightarrow y > x$, *so* x *is less than* y *if and only if* y *is greater than* x.
d) $x \leq y \Leftrightarrow y - x \in \mathbb{P}_0 = \mathbb{P} \cup \{0\}$, *the non-negative numbers*

Theorem 1.16. *Transitivity of the order* $\forall x, y, z \in \mathbb{R} : (x < y \ \& \ y < z) \Rightarrow x < z$

Proof uses only $\mathbb{P} + \mathbb{P} \subset \mathbb{P}$, see in-class exercise W2.

Remark 1.17. *So* $(x \leq y \ \& \ y \leq z) \Rightarrow x \leq z$*, with* $x < z$ *if in addition* $x < y$ *or* $y < z$*, see also in-class exercise W2.*

Lemma 1.18. *Translation invariance* $\forall x, y, z \in \mathbb{R} : x < y \Leftrightarrow x + z < y + z$*, cf. L.2.5.*

Proof

Lemma 1.19. Addition of inequalities

$$\forall x, y, u, v \in \mathbb{R} : (x < y \ \& \ u < v) \Rightarrow x + u < y + v.$$

Proof uses only $\mathbb{P} + \mathbb{P} \subset \mathbb{P}$, see in-class exercise W2.

Proposition 1.20. *Reflection* $\forall x, y \in \mathbb{R} : x < y \Leftrightarrow -y < -x$

Proof 2 possibilities: add $-(x + y)$ and use 2.18, or directly Def. 2.14

Lemma 1.21. $\forall x, y, z \in \mathbb{R}$ *with* $x < y : (0 < z \Rightarrow zx < zy), (0 > z \Rightarrow zx > zy)$

Proof uses $\mathbb{P} \cdot \mathbb{P} \subset \mathbb{P}$ if $z > 0$, then P.2.20 if $z < 0$.

Corollary 1.22. $\forall x, y, u, v \in \mathbb{R} : (0 \leq x < y \ \& \ 0 \leq u < v) \Rightarrow xu < yv$

Proof

Theorem 1.23. $\forall x \in \mathbb{R} : x \neq 0 \Rightarrow 0 < x \cdot x = x^2$

Proof CD (= case distinction): $x > 0 \vee (-x) > 0$.

Corollary 1.24. $0 < 1$, *since* $1 = 1 \cdot 1 = 1^2$*!*

Although $1 > 0$ and also the somewhat more general inequality $0 < x^2$, $x \neq 0$, seem very natural, they are central to the further development of analysis! Because $1 + 1 + 1 = 0$ in GF(3), see Example 2.12, no suitable set $\mathbb{P}$ of 'positive' elements can be found in this field.

In the next section we shall show that, conversely, every positive real number is also the square of a real number. This will need yet another (last) axiom.

Proposition 1.25. $\forall x, y \in \mathbb{R}$:

a) $x > 0 \Leftrightarrow x^{-1} > 0$
b) $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$ *('reflection in 1')*

Proof (In a) a proof by contradiction of $\neg(x^{-1} < 0)$ is also possible)
a) If $x > 0$, then $x \neq 0$ and $x^{-1} \neq 0$ (Lemma 2.10.b)). Hence $0 < x^{-1}x^{-1}$ by Theorem 2.23. Since $x > 0$, Lemma 2.21 shows that

$$0 = x \cdot 0 < x(x^{-1} \cdot x^{-1}) = (x \cdot x^{-1})x^{-1} = 1 \cdot x^{-1} = x^{-1}.$$

Conversely, since $(x^{-1})^{-1} = x$, the reverse implication follows from what has just been shown.
b) Since $0 < x, y$, part a) gives $0 < x^{-1}, y^{-1}$ and hence $0 < x^{-1}y^{-1}$. Now we use Lemma 2.21 again to conclude

$$0 = 0(x^{-1}y^{-1}) < y^{-1} = x(x^{-1}y^{-1}) < x^{-1} = y(x^{-1}y^{-1}).$$

Example 1.26. *Let* $x, y \in \mathbb{R}$ *with* $x > 0$ *and* $y > 0$*. Then* $x < y$ *if and only if* $x^2 < y^2$*.*

Proof Compare Ex. 2.11.

Example 1.27. *If* $x, y \in \mathbb{R}$*, then* $x^2 + y^2 = 0$ *implies* $x = y = 0$*.*

Proof Uses Theorem 2.23, Remark 2.17 and Theorem 2.9.

Example 1.28. *Let $0 < x < y$ and suppose $\sqrt{xy}$ exists (i.e. a positive number whose square is xy). Then the AM–GM inequality (between the arithmetic and geometric mean) holds:*

$$y > \frac{x+y}{2} > \sqrt{xy} > x.$$

Proof The first $>$ uses L.2.18 and L.2.21, the other two also Th. 2.23 and Ex. 2.26.

Definition 1.29. *Let $x, y \in \mathbb{R}$ be given; we then define*

$$\min(x,y) = \begin{cases} x & \text{if } x \le y \\ y & \text{if } x > y \end{cases}, \text{ and } \max(x,y) = \begin{cases} y & \text{if } x \le y \\ x & \text{if } x > y \end{cases}.$$

By means of $\max(x,y,z) = \max(x, \max(y,z))$ etc., the maximum and analogously the minimum are defined for arbitrary 'finite' sets M of real numbers (not yet precisely defined!; in any case it works by induction – this will be done properly later – for all $\{x_1, \ldots, x_n\}$). These greatest and smallest elements of a set no longer exist if, as in what follows, we consider general infinite sets.

Example 1.30. *$M = \{x \in \mathbb{R} : x > 0\}$ has no minimum.*

Proof indirect; $\frac{1}{2} \cdot \min(M)$ yields a contradiction if $\min(M)$ exists.

Definition 1.31. *Let $M \subset \mathbb{R}$ be arbitrary*

a) *$s \in \mathbb{R}$ is $\max M$, the maximum of the set M, if $s \in M$ and $\forall x \in M : x \le s$.*
$s \in \mathbb{R}$ is $\min M$, the minimum of the set M, if $s \in M$ and $\forall x \in M : x \ge s$

b) *$s \in \mathbb{R}$ is an upper bound* (**UB**) *for M if $\forall x \in M : x \le s$, $s \in \mathbb{R}$ is a lower bound* (**LB**) *for M if $\forall x \in M : x \ge s$*

- *$s \in \mathbb{R}$ is the* **supremum** *of M ($s = \sup M$) if s is the least of all upper bounds of M, i.e.*
$$(\forall x \in M : x \le s) \ \& \ (\forall t \text{ UB of } M : t \ge s).$$
- *$s \in \mathbb{R}$ is the* **infimum** *of M ($s = \inf M$) if s is the greatest of all lower bounds of M, i.e.*
$$(\forall x \in M : x \ge s) \ \& \ (\forall t \text{ LB of } M : t \le s).$$
- *M is bounded above (resp. below) if there is an upper (resp. lower) bound for M. M is bounded if it is bounded below and above.*

Example 1.30. *(continued)* $M = \{x \in \mathbb{R} : x > 0\}$ *has no UB;* s *is a LB iff* $s \leq 0$*, so* $\inf M = 0$ *but* $\sup M$ *does not exist.*

Proof

The existence of inf and sup whenever there are corresponding bounds holds not only for such simple sets as this M (an interval), but in general. This distinguishes $\mathbb{R}$ from other fields and is formulated in the last axiom still needed:

III. Completeness axiom

(VA) For every non-empty set $M \subset \mathbb{R}$ that is bounded above, the supremum $\sup M$ exists.

Lemma 1.32. *Let* M *be a set of real numbers; then* $(\exists \max M \Leftrightarrow \sup M \in M)$

Proof

Proposition 1.33. *Let* $M \subset \mathbb{R}$ *be non-empty and bounded above,* $s \in \mathbb{R}$*. Then*

a) $s \geq \sup M \Leftrightarrow \forall m \in M : m \leq s$

b) $s = \sup M \Leftrightarrow (\forall m \in M : m \leq s \;\&\; \forall \varepsilon > 0\; \exists m \in M : s - \varepsilon < m)$

Approximation principle*, does not need VA!*

Proof

Lemma 1.34. *Let $M, N \subset \mathbb{R}$ be non-empty and bounded above. Then*

a) $\inf(-M) = -\sup M$,

b) $\sup(M+N) = \sup M + \sup N$,

where $-M = \{-m : m \in M\}$ is the 'reflection' of M, and $M+N = \{m+n : m \in M \,\&\, n \in N\}$ is the 'Minkowski' sum of the two sets.

Proof a) follows directly from the definition of sup and inf; we show only b), using the approximation principle and the $\frac{\varepsilon}{2}$ trick. In particular, we motivated the latter in the lecture by introducing a further quantity, $\delta > 0$, still to be determined, which is used in the approximation property for M and N.

Now the first surprising and important consequence of the completeness axiom.

Theorem 1.35. *For all positive real x there exists a unique $w > 0$ such that $w^2 = x$.*

We write $w = \sqrt{x}$ for this number and call it the root of x.

Proof The key idea is to show that $w^2 = x$, where $w = \sup(M)$ and $M = \{y > 0 : y^2 < x\}$. With the first binomial formula we can refute both $w^2 > x$ and $w^2 < x$.

A few more details on the procedure Central is Ex. 2.26: if $x, y > 0$ then $(x < y \Leftrightarrow x^2 < y^2)$. Having shown the existence of w (see lecture), we exclude $w^2 \neq x$ by a case distinction. In both cases we shall show and then exploit that the inequalities $w^2 < 2$ and $w^2 > 2$ remain true if w is replaced by $w + \Delta$, with Δ sufficiently close to zero. For this we use the binomial formula $(w+\Delta)^2 = w^2 + 2w\Delta + \Delta^2$.

First case $w^2 > x$: we want to show that there is an $\varepsilon > 0$ such that still $(w-\varepsilon)^2 > x$, i.e. $\Delta = -\varepsilon < 0$. So we consider the quadratic inequality $w^2 - 2w\varepsilon + \varepsilon^2 > x$. We cannot solve it exactly, since this would use a formula involving roots, whose existence we are only just trying to show. Therefore we simplify the quadratic inequality by replacing ε^2 by the constant 0, i.e. we make an estimate from below. In doing so we may lose solutions, but we only need one (positive and smaller than w). Indeed, if $0 < \varepsilon < w$ and $x < w^2 - 2w\varepsilon$, then the quadratic inequality also holds. The linear inequality requires precisely $\varepsilon < \frac{x-w^2}{2w}$, and so $\varepsilon = \frac{\min}{(} w, \frac{x-w^2}{2w})$ is an admissible choice with $0 < w - \varepsilon$ and $x < w^2$; from Ex. 2.26 it follows that $y < w - \varepsilon$ if $y \in M$, so $\sup(M) \leq w - \varepsilon$, a contradiction.

In the second case we analogously look for $\varepsilon > 0$ with $(w + \varepsilon^2) < x$; then $\sup(M) < w + \varepsilon \in M$, a contradiction. We simplify the resulting quadratic inequality to a linear one by the upper estimate $\varepsilon^2 < \varepsilon$ if $\varepsilon \in (0, 1)$ and then proceed analogously to the first case.

Absolute value, maximum and minimum

Definition 1.36. *Let $x \in \mathbb{R}$; we define the absolute value of x as*

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

Remark 1.37. i) *important geometric meaning: $|x-y|$ is the distance from x to y*
ii) *from the definition (with a* **c***ase* **d***istinction $x >, =, < 0$) it follows easily that $|x| = |-x|$ and hence $|x| \geq 0$ with '$=$' iff $x = 0$, and thus $x \leq |x|$.*

Lemma 1.38. *For all $x, y \in \mathbb{R}$ we have:*
a) $-|x| \leq x \leq |x|$, $x^2 = |x|^2$ *and thus* $|x| \in \{-x, x\}$.
b) $|x| \leq y \Leftrightarrow -y \leq x \leq y$ *(and then $y \geq 0$),*

Proof: a) By 2.37.ii) $x \leq |x|$ and $-x \leq |-x| = |x|$, hence also $x = -(-x) \geq -|x|$. If $x \geq 0$ then $x = |x|$ and so $|x|^2 = x^2$; otherwise $-x > 0$, so $|x|^2 = |-x|^2 = (-x)^2 = x^2$. By Ex. 2.11 we thus have $|x| = x \vee |x| = -x$.

For b): Since by Prop. 2.20 $-y \leq x \leq y \Leftrightarrow -y \leq -x \leq y$ and because $|x| = |-x|$, we may assume wlog (without loss of generality) that $0 \leq x$. Then

$$|x| \leq y \Leftrightarrow x \leq y \Leftrightarrow 0 \leq x \leq y \Leftrightarrow -y \leq x \leq y \Leftrightarrow -y \leq |x| \leq y.$$

Definition 1.39. *Let $x \in \mathbb{R}$; we define the signum (corresponds to the sign) of x as*

$$\operatorname{sgn}(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \end{cases}$$

Remark 1.40. $\operatorname{sgn}(0)$ *is generally, and in this lecture course, defined as* 1*; -1 is also possible, and* $\operatorname{sgn}(0) = 0$ *is likewise occasionally used in the literature. In every case, as e.g. an easy CD shows,*

$$\forall x \in \mathbb{R} \ : \quad |x| = \operatorname{sgn}(x) \cdot x \text{ and } x = \operatorname{sgn}(x) \cdot |x|.$$

This often helps to save tedious, more complicated CDs.

Theorem 1.41. *For all $x, y \in \mathbb{R}$*
a) $|xy| = |x||y|$ *multiplicativity*
b) $|x+y| \leq |x| + |y|$ *triangle inequality!*

Proof: a) By (MK) and 2.38.a) we have $|x|^2|y|^2 = x^2y^2 = |xy|^2$, so Ex. 2.26 yields the claim. To show b), add the inequality from 2.38.a) for x and for y to obtain

$$-(|x| + |y|) \leq x + y \leq |x| + |y|;$$

now 2.38.b) gives the claim.

Lemma 1.42. *For all* $x, y \in \mathbb{R}$

$$\max(x, y) = \frac{x + y}{2} + \frac{|x - y|}{2}.$$

Proof CD; or it suffices to consider the case $x \geq y$ and then to use the symmetry of both sides (LHS because of 2.37.ii)) under interchanging x and y.

The geometric meaning of this formula is clear: starting from the midpoint $\frac{x+y}{2}$ between two numbers x, y, go half the distance $\frac{|x-y|}{2}$ between the two numbers in the positive direction and arrive at the larger of the two numbers. The analogous formula holds for $\min(x, y)$.

Number systems

Having introduced all the basic axioms for $\mathbb{R}$ and seen first applications, we now name some important subsets of $\mathbb{R}$ – such as the natural numbers, the integers and the rational numbers.

Definition 1.43. *$M \subset \mathbb{R}$ is called* inductive *if $1 \in M$ and $\forall n \in \mathbb{R} : n \in M \Rightarrow n+1 \in M$.*

Theorem 1.44. *There is a* smallest *inductive set, i.e. it is a subset of every inductive set.*

Proof Idea: as in linear algebra, the intersection of the family of all inductive sets is inductive. More precisely: we denote

$$\mathbb{N} = \{x \in \mathbb{R} : \text{ if } M \subset \mathbb{R} \text{ is inductive, then } x \in M\}.$$

Now we prove that $\mathbb{N}$ is inductive and is contained in every inductive subset of $\mathbb{R}$.

This smallest inductive set is unique; it is denoted by $\mathbb{N}$ and its elements are called natural numbers.

Remark 1.45. *There are undoubtedly many inductive subsets of $\mathbb{R}$, e.g. $\mathbb{R}, [-2, \infty)$ or $\mathbb{Z}$. The set $[3, \infty)$ is not inductive, since $1 \notin [3, \infty)$.*

Since $M = \{1\} \cup [2, \infty)$, where $2 = 1+1$, is inductive, we have $(1, 2) \cap \mathbb{N} = \emptyset$. Analogously one shows $(1, 3) \cap \mathbb{N} = \{2\}$.

Corollary 1.46. *(Weak) principle of induction: M inductive $\Rightarrow \mathbb{N} \subset M$. So if P is a mathematical predicate such that $P(1)$ is true and, for all $n \in \mathbb{N}$, $P(n)$ true implies $P(n+1)$ true, then $P(n)$ holds for all $n \in \mathbb{N}$.*

Proof Idea: to show that the set M of all $n \in \mathbb{N}$ for which $P(n)$ holds is inductive. But what is needed for this is exactly what the assumption about P says. □

Remark $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; then $0 \in M$ and $(n \in M \Rightarrow n+1 \in M)$ implies $\mathbb{N}_0 \subset M$, since M is inductive and hence $\mathbb{N} \subset M$. So if P is a mathematical statement such that $P(0)$ and $\forall n \in \mathbb{N}_0 : P(n) \Rightarrow P(n+1)$, then $P(n)$ holds for all $n \in \mathbb{N}_0$.

Example 1.47. *We want to prove that*

$$\forall n \in \mathbb{N} : \quad \sum_{k=1}^{n}(2k-1) := 1+3+\ldots+(2n-1) = n^2,$$

(the precise definition of the summation symbol is given in the following Def. 2.48.)

For the proof we denote by $P(n)$ the statement that, for $n \in \mathbb{N}$, the (second) equality in the formula above holds. Then $P(1)$ is true, since $1 = 1^2$. Now suppose $P(n)$ holds, i.e. $\sum_{k=1}^{n}(2k-1) = n$ is true; we call this (IA), the induction assumption. Then, as required, we obtain

$$\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + (2(n+1)-1) \overset{(IA)}{=} n^2 + (2n+2-1) = n^2+2n+1 = (n+1)^2.$$

So $P(n)$ always implies $P(n+1)$; by the principle of induction $P(n)$ holds for all natural numbers.

Definition 1.48. Summation and product symbols *For $n, m, k \in \mathbb{N}_0$ we set*

$$\sum_{k=n}^{n-1} a_k = 0 \text{ (empty sum)} \,, \forall m \geq n-1 : \sum_{k=n}^{m+1} a_k = \left(\sum_{k=n}^{m} a_k\right) + a_{m+1}$$

$$\prod_{k=n}^{n-1} a_k = 1 \text{ (empty product)} \,, \forall m \geq n-1 : \prod_{k=n}^{m+1} a_k = \left(\prod_{k=n}^{m} a_k\right) \cdot a_{m+1}$$

$$a^n = \prod_{k=1}^{n} a, \text{ power } \quad (a^0 = 1 \text{ if } a \neq 0), n! = \prod_{k=1}^{n} k, \text{ factorial } \quad (0! = 1)$$

Theorem 1.49. *Bernoulli's inequality: $\forall n \in \mathbb{N} \forall x \in \mathbb{R}$ with $x \geq -1 : (1+x)^n \geq 1+nx$. Moreover*

$$\forall n \in \mathbb{N} \forall x \in \mathbb{R} \text{ if } n \geq 2 (= 1+1) \text{ and } (x \geq -1 \;\&\; x \neq 0) \text{ then } (1+x)^n > 1+nx.$$

Proof Idea: induction on n.

Proposition 1.50. *For $n \in N$ let $a_n = \left(1 + \frac{1}{n}\right)^n$. Then $\forall n \in \mathbb{N} : a_n < a_{n+1}$.*

Proof Idea: e.g. prove $\frac{a_{n+1}}{a_n} > 1$ using Bernoulli's inequality; the calculation becomes simpler if we consider $\frac{a_n}{a_{n-1}}$, $n > 2$.

Definition 1.51. *For $n, k \in \mathbb{N}_0$ the binomial coefficient is defined by*

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} \left(= \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k(k-1)\cdot\ldots\cdot 1}\right) & \text{for } 0 \le k \le n \\ 0 & \text{if } k > n. \end{cases}$$

$$\text{e.g. } \binom{n}{0} = \binom{n}{n} = 1, \binom{n}{1} = n \text{ if } n > 0, \binom{n}{k} = \binom{n}{n-k}, 0 \le k \le n.$$

Lemma 1.52.

$$\forall n \in \mathbb{N}_0 \forall k \in \mathbb{N} : \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Proof If $k > n$ (i.e. $k = n+1 \vee k > n+1$) use the definition directly, otherwise calculate with fractions.

Theorem 1.53. Binomial theorem *With the convention $0^0 = 1$ we have*

$$\forall x, y \in \mathbb{R} \; \forall n \in \mathbb{N}_0 \; : \; (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Proof Idea: induction on n using Lemma 2.52.

Although we defined $\mathbb{N}$ via the property of being an inductive set, as a number system it allows us to carry out the arithmetic operations as we are used to from elementary mathematics. As one would expect, we can prove this by induction.

Lemma 1.54.

$$\forall n, m \in \mathbb{N} : \ n + m \in \mathbb{N} \ \& \ n \cdot m \in \mathbb{N}.$$

Proof: Idea – by induction: first, for arbitrary but fixed m, do induction on n for addition; this relies on axiom (AA). We then use this, again for arbitrary but fixed m, to do induction on n for multiplication.

Lemma 1.55.

$$\forall n \in \mathbb{N} : \ n = 1 \ \textit{or} \ (n > 1 \ \& \ n - 1 \in \mathbb{N}).$$

In particular $1 = \min \mathbb{N}$.

Proof by induction on n; in fact we already have $\forall n \in \mathbb{N} : \ (n \geq 1 \Rightarrow P(n+1))$.

Theorem 1.56.

$$\forall n \in \mathbb{N} \, \forall m \in \mathbb{N} : \quad n \leq m \ \textit{or} \ n - m \in \mathbb{N}.$$

Proof Idea: for fixed n, induction on m, using Lemma 2.55 for $k = n - m$ where necessary.

So we have shown: $n < m$ in $\mathbb{N} \Rightarrow n \leq m - 1$, since $m - n \in \mathbb{N}$ and so $m - n \geq 1$.

Definition 1.57. $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ *are the integers.*

By Theorem 2.56 we have $\mathbb{Z} = \mathbb{N} - \mathbb{N} = \{n - m \,:\, n, n \in \mathbb{N}\}$, in particular $\mathbb{Z} \supset \mathbb{N} - \mathbb{N}$.

Corollary 1.58. $\forall x, y \in \mathbb{Z} : x + y, x - y, x \cdot y \in \mathbb{Z}$.

Proof Idea: use $\mathbb{Z} = \mathbb{N} - \mathbb{N}$ and rearrange terms according to sign.

Definition 1.59. $\mathbb{Q} = \{\frac{p}{q} \,:\, p \in \mathbb{Z} \;\&\; q \in \mathbb{N}\}$ *are the rational numbers. So* $q \neq 0$*!*

Clearly $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$; use $q = 1$.

Remark 1.60. $(\mathbb{Q}, +_{\mathbb{R}}, \cdot_{\mathbb{R}})$ *with* $\mathbb{P}_{\mathbb{Q}} = \mathbb{P} \cap \mathbb{Q}$ *satisfies the 9 field axioms and the 3 order axioms; this is easy to check:*

(1) *since* $\frac{p}{q}\frac{m}{n} = \frac{pm}{qn}$ *and* $\frac{p}{q} + \frac{m}{n} = \frac{pn+qm}{qn}$*, the operations* $+, \cdot$ *lead from* $\mathbb{Q} \times \mathbb{Q}$ *back into* $\mathbb{Q}$

(2) $-\frac{p}{q} = \frac{-p}{q}$ *and* $(\frac{p}{q})^{-1} = \frac{q}{p}$ *for* $p > 0$*,* $(\frac{p}{q})^{-1} = \frac{-q}{-p}$ *for* $p < 0$ *shows the existence of inverses in* $\mathbb{Q}$*.*

Strong induction

Theorem 1.61. WELL-ORDERING OF THE NATURAL NUMBERS *Let $M \subset \mathbb{N}$ be non-empty; then* $\min M$ *exists.*

Proof Idea – by induction, i.e. show using Corollary 1.46:

$$\forall n \in \mathbb{N} : ((\exists m \in M \subset \mathbb{N} \,\&\, m \leq n) \Rightarrow \exists \min M).$$

Corollary 1.62. STRONG PRINCIPLE OF INDUCTION *Let P be a mathematical statement such that $P(1)$ and $\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : k \leq n \Rightarrow P(k)) \Rightarrow P(n+1)$. Then $P(n)$ holds for every $n \in \mathbb{N}$.*

Proof Idea: consider $M = \{n \in \mathbb{N} \ : \ P(n) \text{ false }\}$; if $M \neq \emptyset$ then, because $1 \notin M$, there is a contradiction for $n = \min(M) - 1$.

Remarks

- also known as the principle of 'least criminals', meaning the smallest/first 'villains' in the sense of minimal counterexamples. It is often easier to rule out the existence of these than the existence of general counterexamples.
- why it is called the *strong* principle of induction: in order to prove the crucial $P(n+1)$, we may now assume $P(1), P(2), \ldots, P(n)$. Previously we could only assume $P(n)$, and so we now have a 'stronger' method of proof, which allows us to prove more and 'stronger' statements.
- a simpler formulation, which however deviates from the familiar formulation $\Rightarrow P(n+1)$, is the following. Let P be a mathematical predicate such that for every

$n \in \mathbb{N}$ the statement $P(n)$ holds if $\forall k \in \mathbb{N} : k < n \Rightarrow P(k)$. Then $P(n)$ holds for all $n \in \mathbb{N}$. (Hidden in this formulation is, e.g., that $P(1)$ holds, since there is no $k < 1$ in $\mathbb{N}$.)

Definition 1.63. *We say p is a prime number if $p \in \mathbb{N}$, $p > 1$ and*
$$(p = n \cdot m, \text{ with } n, m \in \mathbb{N}) \Rightarrow (n = 1 \text{ or } m = 1)).$$
Claim: *Every $n \in \mathbb{N}$ with $n > 1$ is a product (possibly with a single factor) of finitely many prime numbers. (The uniqueness of the product representation is much deeper! See possibly DS)*

Proof: By strong induction.

Lemma 1.64. *$\forall n \in \mathbb{N} : (\exists k \in \mathbb{N} : n = 2k$ or $\exists l \in \mathbb{N} : n = 2l - 1)$, and only one of the cases occurs.*

Proof: Induction; use a contradiction to $1 = \min \mathbb{N}$ for the uniqueness of the case.

Theorem 1.65. *(The classic) $\sqrt{2} \notin \mathbb{Q}$, i.e. the diagonal of the unit square is irrational.*

Proof: Idea: by ↯; consider a fractional representation with smallest denominator.

Rational versus real

Since not all real numbers are rational, we must study the relationship between $\mathbb{Q}$ and $\mathbb{R}$. We begin with the following statement, which is attributed to Archimedes, although he mentions Eudoxus of Cnidus as its originator. The name 'axiom' is customary in the literature for historical reasons, but in the theory of the real numbers it is unjustified, since this is a consequence of our 13 axioms.

Theorem 1.66. (Archimedean 'axiom') *The set* $\mathbb{N}$ *of natural numbers is not bounded above in* $\mathbb{R}$*.*

Proof: Idea: by $\lightning$; to do so consider $\sup \mathbb{N}$ and the approximation principle.

Corollary 1.67. (Eudoxus) $\forall x \in \mathbb{R} : x > 0 \Rightarrow \exists n \in \mathbb{N} : \frac{1}{n} < x$

Proof: Idea: follows directly from the Archimedean axiom.

We can now show that, although not all numbers are rational, the rational numbers can at least approximate all numbers well.

Theorem 1.68. (The rational numbers are dense) *For all real* $x < y$ *there exists* $z \in \mathbb{Q}$ *satisfying* $x < z < y$*.*

Proof: Idea: first shift into $\mathbb{R}_+$. Now small steps lead to the goal!

The complex numbers

As the last field we introduce the complex numbers; in this field the equation $x^2+1=0$, which is unsolvable in $\mathbb{R}$, is easily solvable.

Definition 1.69. *We consider* $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a,b) : a,b \in \mathbb{R}\}$ *with the operations*

$$(a,b)+(c,d) = (a+c, b+d), (a,b)\cdot(c,d) = (ac-bd, ad+bc).$$

Then $\mathbb{C}$ is a field with zero element $(0,0)$ (neutral for '+') and unit element $(1,0)$ (neutral for '$\cdot$').

Remark 1.70.

- *only the axioms (MA), (MK) and (DG) require some work*
- *for* $(a,b) \neq (0,0)$, $(a/(a^2+b^2), -b/(a^2+b^2))$ *is the multiplicative inverse!!*
- $\mathbb{R} \equiv \mathbb{R} \times \{0\} \subset \mathbb{C}$, *i.e.* $x \to (x,0)$ *gives* $\mathbb{R}$ *as a subfield of* $\mathbb{C}$ – *we have* $x+y \to (x,0)+(y,0)$ *and* $x \cdot y \to (x,0)\cdot(y,0)$
- $(0,1)^2 = (-1,0)$**!!** *We write* i *for* $(0,1)$ *and* $a+bi$ *for* (a,b). *Thus* $i^2 = -1$ *and* $\mathbb{C}$ *can* not *be ordered, i.e. there is no* $\mathbb{P} \subset \mathbb{C}$ *satisfying (O.1), (O.2) and (O.3).*

Definition 1.71. *For* $z = a+bi = (a,b) \in \mathbb{C}$ *we define*

$Re(z) = a, Im(z) = b, |z| = \sqrt{a^2+b^2}$ *the real part, imaginary part and modulus of* z

as well as

$$\bar{z} = a - bi \text{ the complex conjugate of } z.$$

As in $\mathbb{R}$, $|z|$ is the distance from z to the origin ($\mathbb{C}$ is identified with the Euclidean plane $\mathbb{R}^2$).

Lemma 1.72. $\forall z, w \in \mathbb{C}$

a) $\overline{z+w} = \overline{z} + \overline{w}, \overline{z \cdot w} = \overline{z} \cdot \overline{w}$ *!*

b) $\overline{\bar{z}} = z, |z| = \sqrt{z \cdot \bar{z}} = |\bar{z}|, Re(z) = (z+\bar{z})/2, Im(z) = (z-\bar{z})/2i.$

Proof: The second part of the claim in a) is indeed crucial.

Theorem 1.73. *For all* $z, w \in \mathbb{C}$

a) $|Re(z)| \leq |z|, |Im(z)| \leq |z|$ *and* $|Re(z)| = |z| \Leftrightarrow Im(z) = 0 \Leftrightarrow z \in \mathbb{R}$

b) $|z| \geq 0, |z| = 0 \Leftrightarrow z = 0$ *(as in* $\mathbb{R}$*)*

c) $|z \cdot w| = |z| \cdot |w|$ *multiplicativity* *(as in* $\mathbb{R}$*)*

d) $|z + w| \leq |z| + |w|$ Δ*-inequality* *(as in* $\mathbb{R}$*)*

Proof:

Proposition 1.74. Complex square roots *For given* $c \in \mathbb{C}$ *we look for* all *(since no 'positive' one is distinguished)* $w \in \mathbb{C}$ *with* $w^2 = c$.

Here $w^2 = 0 \Leftrightarrow w = 0$, *and if* $c \neq 0$ *then*

$$w_1 = \sqrt{\frac{|c| + Re(c)}{2}} + \sigma\sqrt{\frac{|c| - Re(c)}{2}}i \text{ where } \sigma = \begin{cases} 1 & \text{for } Im(c) \geq 0 \\ -1 & \text{for } Im(c) < 0 \end{cases}$$

is a solution; the only other solution is $w_2 = -w_1$.

$$0 = z^2 + az + b = (z + \frac{a}{2})^2 - (\frac{a^2}{4} - b) = (z + \frac{a}{2} + w)(z + \frac{a}{2} - w)$$

where $w^2 = \frac{a^2}{4} - b$ *can thus be solved in* $\mathbb{C}$.

Proof:

In connection with the exponential function and Euler's formula we shall soon find a more geometric approach to the complex numbers $\mathbb{C}$, which interprets them as a plane and the arithmetic operations as geometric translations and rotational dilations.

Appendix A. Notation

The terms and symbols collected here will each be introduced in the lectures as they are needed; this chapter therefore serves as a summary for reference.

Definition A.1. Set *(intuitive definition due to G. Cantor)* is a collection of objects (elements) which share a certain property ("the mathematical statement $P(x)$ holds").

We write $x \in M$ if x is an element of M, i.e. belongs to M, and $x \notin M$ otherwise.

Typically we study $\{x \in X \,:\, P(x)\}$, i.e. the set of all x from a (large, fixed "universal") set X for which the (mathematical) statement $P(x)$ is true.

We say M is a subset of N (notation $M \subset N$) if all elements of M also belong to N; two sets are equal if they have exactly the same elements. (Instead of "M is a subset of N" we often say "M is smaller than (or smaller than or equal to) N".) Analogously to the order relation for real numbers, $M \subset N$ is equivalent to $N \supset M$. We write $M \subsetneq N$ if $M \subset N$ and $M \neq N$, and say M is *strictly* smaller than N.

From given sets M, N we construct

- $M \cap N = \{x \,:\, x \in M \;\&\; x \in N\}$ the intersection of M and N
- $M \cup N = \{x \,:\, x \in M \text{ or } x \in N\}$ the union
- $M \setminus N = \{x \,:\, x \in M \;\&\; x \notin N\}$ the set difference
- $M \times N = \{(x, y) \,:\, x \in M \;\&\; y \in N\}$ the Cartesian product, where $(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$ – ordered pairs. These can also be represented as sets, e.g. $(x, y) = \{\{x\}, \{x, y\}\}$.
- $\mathfrak{P}(M) = \{N \,:\, N \subset M\}$ the power set of M

Special notation is reserved for

- $\emptyset$ the empty set, which contains *no* element
- $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$ the natural numbers
- $\mathbb{Z} = \{\dots, -3, -2 - 1, 0, 1, 2, 3, \dots\}$ the integers
- $\mathbb{Q} = \{\frac{m}{n} \,:\, m \in \mathbb{Z} \;\&\; n \in \mathbb{N}\}$ the rational numbers
- $\mathbb{R}$ the real numbers
- $\mathbb{C}$ the complex numbers

Warning: $\{\emptyset\} \neq \emptyset$!

Furthermore, we denote intervals of integers or real numbers by the usual notation (which will later be handled more flexibly):

- $\{k, \dots, m\} = \{l \in \mathbb{Z} \,:\, k \leq l \leq m\}$ if $k, m \in \mathbb{Z}$; this is a subset of $\mathbb{N}_0$ or $\mathbb{N}$ if $k \in \mathbb{N}_0$ or $k \in \mathbb{N}$ respectively,
- $[a, b] = \{x \in \mathbb{R} \,:\, a \leq x \leq b\}$ closed interval for $a, b \in \mathbb{R}$,
- $(a, b) = \{x \in \mathbb{R} \,:\, a < x < b\}$ open interval for $a \in \{-\infty\} \cup \mathbb{R}$ and $b \in \mathbb{R} \cup \{\infty\}$, where we cannot regard $\pm\infty$ as part of the (algebraic) field $\mathbb{R}$, but assume that $\forall x \in \mathbb{R} \,:\, -\infty < x < \infty$.
- $[a, b) = \{x \in \mathbb{R} \,:\, a \leq x < b\}$ right-open (half-open) interval for $a \in \mathbb{R}$ and $b \in \mathbb{R} \cup \{\infty\}$
- $(a, b] = \{x \in \mathbb{R} \,:\, a < x \leq b\}$ left-open (half-open) interval for $a \in \{-\infty\} \cup \mathbb{R}$ and $b \in \mathbb{R}$.

Definition A.2. Quantifiers We use the abbreviations

- $\forall x \ldots$ means "for all x it holds that $\ldots$"
- $\exists x \ldots$ means "there exists an x such that $\ldots$"

Further symbols (logical ones (connectives) and others):

- $\&$ for "and"
- $\Rightarrow$ for "implies", and also $\curvearrowright$ in the very similar sense of "hence"
- $\Leftrightarrow$ for "if and only if"
- $\lightning$for "contradiction" (reached)
- # for cardinality, i.e. the number of elements of a set
- ☺,□ for q.e.d., i.e. end of proof
-  for warning

A map F maps a set X into a set Y if

$$F \subset M \times N, \quad \forall x \in X \exists y \in Y : (x, y) \in F \text{ and } \forall (x, y), (x, y') \in F : y = y'.$$

If $(x, y) \in F$ then we write $y = F(x)$. We thus identify the map $F = \{(x, F(x)) \ : \ x \in X\}$ with its "graph". If $Y = \mathbb{R}, \mathbb{C}$ (or $\mathbb{R}^n$) we often call F a function and like to use lower-case letters $f, g, h, \ldots$.

A map $F : X \to Y$ is called

- injective (also called $1-1$) if $F(x) = F(x') \Rightarrow x = x'$,
- surjective (maps *onto* Y) if $\forall y \in Y \exists x \in X : F(x) = y$,
- bijective if F is both injective and surjective.