Foundations of mathematics

Foundations of mathematics

Advanced ↑	numbers
	Algebraic structures
	Maps & relations
	Set theory
	proofs
basic ↓	logics

(Classical) Logic

1. Propositional logic

⇒ **Definition**: a proposition (logical statement) can take the values true (T) or false (F), no other.

⇒ **Remark**: It is not in the purview of propositional logic to study the 'interior structure' of a proposition.

⇒ One can define new propositions in terms of given ones with logical operators

Logical operators

a) **unary operators**: only 1 variable

	Poss. 1	Poss. 2	
P	T	F	P : either T or F
¬P	F	T	¬P : not P
ID P	T	T	ID : same as P
T P	T	T	**T** P : always T
⊥ P	F	F	**⊥** P : never T

b) **binary operators**: 2 variables

	P	q	P∨q	P∧q	P⇒q	P⇔q
poss. 1	T	T	T	T	T	T
poss. 2	T	F	T	T	F	F
poss. 3	F	T	T	T	T	F
poss. 4	F	F	F	F	T	T

$p \vee q$: true when at least p or q is true
$p \not\vee q$: only true when p or q is true and the other one false
$p \Rightarrow q$: only from true to false is false
$p \Leftrightarrow q$: true when p and q have the same value

⇒ Theorem: $(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$

p	q	¬p	¬q	p ⇒ q	(¬q) ⇒ (¬p)
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

These are the same, so ⇔

↳ Remark: This logical theorem is essentially the license to conduct proofs by the way of contradiction.
↳ Remark: There are other logics than classical logic where proofs by contradiction are not possible.

⇒ Convention about the notation
↳ We agree that the 'binding strenght' of the following operators strictly decreases:
$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$
↳ Example: $(p \Rightarrow q) \Leftrightarrow ((\neg q) \Rightarrow (\neg p))$ can now be written as: $p \Rightarrow q \Leftrightarrow \neg q \Rightarrow \neg p$

c) N-ary operators: n variables
⇒ Theorem: Every n-ary operator can be expressed solely in terms of one binary operator.

p	q	p|q
T	T	F
T	F	T
F	T	T
F	F	T

p|q: not both p and q can't be true

↳ example a) $\neg p :\Leftrightarrow p|p$
b) $p \wedge q :\Leftrightarrow (p|q)|(p|q)$

LHS of this equivalence is defined in terms of the RHS

2. Predicate logic

⇒ Refines propositional logic

⇒ Instead of propositions, predicate logic uses:
1) (not further specified) objects x, y, z
2) Predicates $P, Q, R, \dots$
↳ where each predicate is assigned a so called vallence (e.g. $val(P) = 1$, could be any non negative integer) who play together such that any evaluation of a predicate P on $val(p)$-many objects $x_1, \dots x_{val(p)}$
↳ $P(x_1, x_2, \dots x_{val(p)})$
Predicate objects
evaluation of P on $x_1, \dots x_{val(p)}$ is a proposition

⇒ Remark: A vallence of zero means predicate M is a proposition

⇒ Examples:
a) - let P be of valence 1
- let R be of valence 2
then
$Q(x,y,z) :\Leftrightarrow P(x) \wedge R(z,z)$
defines a predicate Q of valence 3 ?

b) - R is above
$S(x) :\Leftrightarrow R(x,x)$?

Quantification

⇒ universal quantifier: $\forall x : P(x)$
↳ definition: 'For all x, x is p (or P is true)'
↳ $\forall x : P(x) :\Leftrightarrow$ { True if $P(x)$ is independent of x / False else

⇒ Existential quantifier: $\exists x : P(x)$
↳ definition: 'For some x, x is p (or p is true)
↳ $\exists x : P(x) :\Leftrightarrow \neg(\forall x : \neg(p(x)))$

⇒ Theorem: $\forall x: P(x) \Rightarrow P(y)$?

⇒ non theorem: $\forall x: \exists y: R(x,y)$ is generically (for any choice of what it can be) not equivalent to $\exists y: \forall x: R(x,y)$

3. Axiomatic systems & Proofs

⇒ **Definition**: An axiomatic system is given by a finite list of prepositions $a_1, \ldots a_N$, called the axioms (statement assumed true without proof)

⇒ **Definition**: A formal proof for preposition P under assumptions $S_1, \ldots S_n$ (all props) whithin an axiositic system is a finite list $q_1, q_2, \ldots q_{T-1}$. P of proposition with the following propoties: for every J with $1 \leq J < T$ one of the following constitin applies:
(A) q_j is one of the axioms
(S) q_j is one of the assumptions
(T) q_j is a tautology (e.g. $q_j :\Leftrightarrow p \vee \neg p$)
(m) $\exists m,n$ with $1 \leq m,n < j$ (previous steps) $q_m \wedge q_n \Rightarrow q_j$

Set theory

⇒ Set theory is built on predicate logic. There are two further types of stipulations:
1) There are objects that satisfy a set of additional conditions (called axioms) and then qualify as sets.
2) There is a particular valence-two predicate $\in$, which is defined on objects that happen to be sets. In other words, if A and B are sets, then $\in(A,B)$
⇒ Remark: notation correction $A \in B :\Leftrightarrow \in(A,B)$

1. Naive set theory

⇒ Basic idea: sets are collections of objects, where the selection of which objects belongs to a particular set is made by a valence-one predicate S, the so-called sellection predicate

↳ More precisely: the one and only axiom of MST is

(a) Axiom of general comprehension

⇒ let S be a predicate of valence one. Then there is a (naive) set denotes $\{x|S(x)\}$, which is defined by

$E \in \{x|S(x)\} :\Leftrightarrow S(E)$

⇒ **Definition:** Let A and B be (the same) sets. Then

$A = B :\Leftrightarrow \forall E : (E \in A \Leftrightarrow E \in B)$

↳ = means are the same sets

↳ Subset: $A \subseteq B :\Leftrightarrow \forall E : (E \in A \Rightarrow E \in B)$

A is a subset of B (a)

Thus we have defined two futher valence-two predicates $=, \subseteq$ in terms of the given $\in$.

The general comprehension axiom wonderfully allows to conduct any set one needs in order to erect all of the modern mathematics on the basis of naive set theory

⇒ Examples: Empty set (i) $\emptyset := \{x|S(x)\}$ where $S(x) :\Leftrightarrow \mathcal{F}$

Justification of terminology

↳ $E \in \emptyset \Leftrightarrow \mathcal{F}$ ($\emptyset$ has no elements)

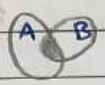
↳ $\emptyset \in \emptyset \Leftrightarrow \mathcal{F}$

Let A,B be naive sets and form a union:

$A \cup B := \{x|x \in A \vee x \in B\}$ by @ $E \in A \cup B \Leftrightarrow E \in A \vee E \in B$

$A \cap B := \{x|x \in A \wedge x \in B\}$

$A \setminus B := \{x|x \in A \wedge \underbrace{\neg(x \in B)}_{x \notin B}\}$

$A \cup B$  $A \cap B$  $A \setminus B$ 

⇒ **Powerset**: the powerset $\mathcal{P}(A)$ includes all the subsets from set A
↳ $\mathcal{P}(A) := \{x \mid x \subseteq A\}$

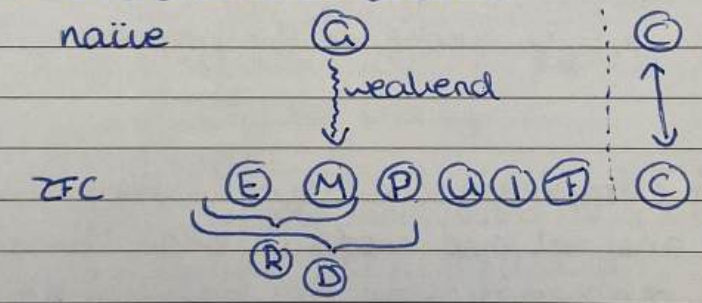
⇒ **Trouble**:
naïve set $u := \{x \mid \underbrace{\neg(x \in x)}_{S(x)}\}$ by general comprehension

1) $u \in u \Rightarrow u \notin u$
2) $u \notin u \Rightarrow u \in u$
} Contradiction

2. Zermelo-Fraenkel set theory

⇒ Formulation of set theory in which modern maths is founded.

⇒ Overview of axioms



(E) Axioms of empty set existence

⇒ There is a set E such that $\forall X : \neg(X \in E)$
↳ Terminology: any such set is called an empty set.

⇒ Theory: Let E and $\tilde{E}$ be empty sets, then $E = \tilde{E}$
↳ Proof: E empty, thus $X \in E$ is false, but then $\underbrace{X \in E}_{F} \Rightarrow \underbrace{X \in \tilde{E}}_{T}$

Analogously: $\tilde{E}$ empty $\Rightarrow X \in \tilde{E}$ is false, thus $\underbrace{X \in \tilde{E} \Rightarrow X \in E}_{\text{True}}$

Thus $X \in E \Leftrightarrow X \in \tilde{E}$
Thus $E = \tilde{E}$ by def. of $\in$ QED

⇒ In order to state axiom (M) we need a preceding definition

⇒ **Definition**: A valence-two predicate F is called a mapping with the property $\forall x: \exists! y: F(x,y)$

↳ $\exists!$ means there is a unique

(M) Axiom on mapped sets

⇒ Let A be a (ZFC) set and F a mapping. Then there is a set which we denote $\text{im}_F(A)$ (the image set of A under mapping F) and which is defined by $y \in \text{im}_F(A) :\Leftrightarrow \exists x: [x \in A \wedge F(x,y)]$

(R) Combing (E) and (M)

⇒ One finds as an implication to most heavily used theorem of mathematics

⇒ **Theorem: The principle of restricted comprehension**

↳ Let A be a (ZFC) set and let S be a valence-one, then the set denoted by $\{x \in A \mid S(x)\}$ and defined by $E \in \{x \in A \mid S(x)\} :\Leftrightarrow E \in A \wedge S(E)$ is (already) a set of ZFC set theory

↳ Proof:

i) Suppose there exists no E such that $E \in A \wedge S(E)$. Then define $\{x \in A \mid S(x)\} := \emptyset$

ii) Suppose there exists a E such that $E \in A \wedge S(E)$. Then define a predicate F of valence two through

$F(x,y) :\Leftrightarrow S(x) \wedge (y = x) \vee \neg S(x) \wedge (y = E)$

Then we define $\{x \in A \mid S(x)\} := \text{im}_F(A)$

In both cases the element Y results in the property $y \in A \wedge S(y)$ QED

(D) Doublet sets (combining (M) (E) (P)

⇒ **Theorem**: Let A and B be (ZFC) sets. Then there is a (ZFC) set $\{A,B\}$ such that $X \in \{A,B\} \Leftrightarrow X = A \cup X = B$

⇒ **Remark/Definition**: $\{x\} := \{x,x\}$

↳ Proof: $\{x,y\} \stackrel{?}{=} \{y,x\}$

$a \in \{x,y\} \Rightarrow a \in \{y,x\}$

$a \in \{y,x\} \Rightarrow a \in \{x,y\}$

$\Rightarrow \{x,y\} \subseteq \{y,x\}$, $\{y,x\} \subseteq \{x,y\}$ $\Big\} \{x,y\} = \{y,x\}$

ⓤ Axiom on unions

⇒ Let C be a (ZFC) set. Then there is a set denoted UC defined by $x \in UC :\Leftrightarrow \exists S : (S \in C \wedge x \in S)$ called the union set.

⇒ Observation/definition: Let $A_1, A_2, A_3, \ldots$ be (ZFC) sets.

$\{A_1, A_2\}$ is a (ZFC) set by ⓓ

$\{A\} := \{A,A\}$ is a (ZFC) set

$\{A_1, A_2, A_3\} := \bigcup \{\{A_1, A_2\}, \{A_3\}\}$

Ⓘ Axiom of infinity

⇒ There exists a set N such that $\emptyset \in N$ and $\forall x (x \in N \Rightarrow \{x\} \in N)$

⇒ Remark:

N	N	N	.....
↓	↓	↓	
$\emptyset$	$\{\emptyset\}$	$\{\{\emptyset\}\}$	.....
nicknames: 0	1	2	.....

Relations & maps

1. Order from disorder

⇒ In sets there is no order $\{A,B\} = \{B,A\}$, $\{A,B,C\} = \{C,B,A\}, \ldots$

⇒ Definition: Let a,b be sets. Define the ordered pair $(a,b) \neq (b,a)$

↳ $(a,b) := \{\{a\}, \{a,b\}\}$

⇒ Observation : i) $(b,a) = \{\{b\},\{b,a\}\}$ is not the same set as above
ii) $(a,a) = \{\{a\},\{a,a\}\} = \{\{a\}\{a\}\} = \{\{a\}\}$

⇒ Theorem: first entry of (a,b) is $\underbrace{\bigcup \underbrace{\bigcap (a,b)}_{\{a\}}}_{a}$

Secondsentry of (a,b) is $\begin{cases} \bigcup\bigcap(a,b) & \text{if } \bigcup(a,b) = \bigcap(a,b) \\ \bigcup(\bigcup(a,b) \setminus \bigcap(a,b)) & \text{otherwise} \end{cases}$

⇒ Definition: let A and B be (ZFC) sets. Then the Cartesian product of A and B is
$A \times B :\overset{\text{R}}{=} \{(a,b) \in \mathcal{P}(\mathcal{P}(\bigcup\{A,B\})) \mid a \in A \wedge b \in B\}$

⇒ Remark: Can be extended to $A \times B \times C := (A \times B) \times C$ with notation choices (TOC) ⇝ N-tuples $(a_1, \dots, a_N)$

2. Relations

⇒ Definition: A relation R between a set A and a set B is $R \subseteq A \times B$

⇒ Remark: notation, having chosen an R, we write
$aRb :\Leftrightarrow (a,b) \in R$

⇒ Example: define the following relation on $\mathbb{N}$ (between $\mathbb{N}$ and $\mathbb{N}$)

$$\begin{aligned} < := \{ & \cancel{(0,0)}, (0,1), (0,2), (0,3), \dots \\ & \cancel{(1,0)}, \cancel{(1,1)}, (1,2), (1,3), \dots \\ & \cancel{(2,0)}, \cancel{(2,1)}, \cancel{(2,2)}, (2,3), \dots \} \subseteq \mathbb{N} \times \mathbb{N} \end{aligned}$$

↳ $1<2 \Leftrightarrow (1,2) \in <$ true

↳ $2<1 \Leftrightarrow (2,1) \in <$ false

3. Maps

⇒ **Definition**: A relation f between A and B for which $\forall a \in A \exists! b \in B : (a,b) \in f$ is called a **map**.

⇒ Notation: $f : A \to B$ (function; domain; to; co-domain)

$a \mapsto f(a) = b$ ($\mapsto$: maps to; $f(a)=b$: function prescription)

⇒ Bad talk: consider the function $f(x) = x^2$

↳ Correct would be: Consider $f : \mathbb{R}_0^+ \to \mathbb{R}$

$x \mapsto f(x) = x^2$

⇒ Examples: a) $S : \mathbb{N} \to \mathbb{N}^* := \mathbb{N} \setminus \{0\}$

$n \mapsto S(n) := \{n\}$

$S(0) = 1$, $S(1) = 2$, $S(S(1)) = 3$, $S(S(S(1))) = 4 \ldots$

b) $P : \mathbb{N}^* \to \mathbb{N}$

$\{n\} \mapsto n$

$P(7) = \ldots = 6$

⇒ **Definition**: let $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ be maps. Then we define the **composite map**

↳ $g \circ f : A \to C$ (g after f)

$a \mapsto (g \circ f)(a) := g(f(a))$

⇒ Theorem: $\circ$ is associative, let $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} d$ be maps.

Then $h \circ (g \circ f) = (h \circ g) \circ f$

↳ **Definition**: associative means that the operation can be done multiple times where order of the elements doesn't matter

↳ Proof: $(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$

$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$ QED

⇒ **Definition**: let $f: A \to A$ be a map. Then define

$f^n := f^{p(n)} \circ f$ for all $n \in \mathbb{N}^*$

$f^0 := id_A$

↳ $id_A : A \to A$

$a \mapsto a$

⇒ **Example**: $f^3 = f^{p(3)} \circ f = f^2 \circ f = (f^{p(2)} \circ f) \circ f = (f^1 \circ f) \circ f$

$= ((f^{p(1)} \circ f) \circ f) \circ f = ((f^0 \circ f) \circ f) \circ f$

$= ((id_A \circ f) \circ f) \circ f = (f \circ f) \circ f = f \circ (f \circ f) = f \circ f \circ f$

$\uparrow$

$(id_A \circ f)(a) = id_A(f(a)) = fa$

⇒ **Remark**: consider a map $f: A \to B$

$M \times N$

$(m,n) \mapsto f(\underbrace{(m,n)}_{\text{one variable}})$

$=$

$f(m,n)$

⇒ **Definition**: $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$(a,b) \mapsto s^b(a)$

↳ notation: $3+2 := +((3,2))$

↳ Example: $+(3,2) = s^2(3) = (s \circ s)(3) = (s \circ s)(\{\{\{\emptyset\}\}\})$

$= s(s(\{\{\{\emptyset\}\}\}) = s(\{\{\{\{\emptyset\}\}\}\})$

$= \{\{\{\{\{\emptyset\}\}\}\}\} = 5$

⇒ **Definition**: A map $f: A \to B$ is:

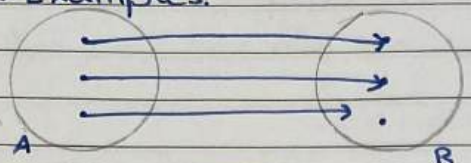
a) injective if $f(a) = f(\bar{a}) \Rightarrow a = \bar{a}$

b) surjective if $\forall b \in B \; \exists a \in A : b = f(a)$

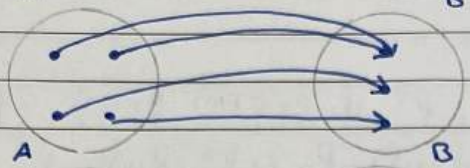
c) bijective/isomorphin if it is injective & surjective

↳ **Definition**: Two sets are called isomorphic if there exist an isomorphic $f: A \to B$

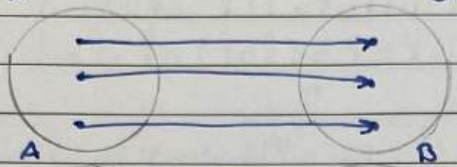
=> Examples:



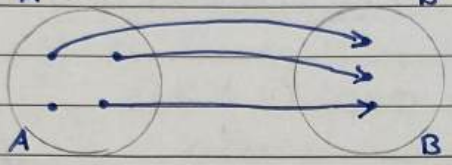
injective, not surjective



surjective, not injective



bijective



not a map ☹

4. Equivalence relations ~

=> Definition: A relation $\sim$ on a set A is called an equivalence $\sim \subseteq A \times A$

↳ 3 conditions: $(a,a) \in \sim$

1) reflexibility: $a \sim a$ for all $a \in A$
2) Symmetry: $a \sim b \Rightarrow b \sim a$ for all $a, b \in A$
3) transcibility: $a \sim b \wedge b \sim c = a \sim c$

=> Examples: a) $a \sim b :\Leftrightarrow$ a is a sibling of b ~~reflexibility~~

b) $a \sim b :\Leftrightarrow$ a is in love with b ~~reflexibility~~ ~~symmetry~~ ~~transcibility~~

c) $a \sim b :\Leftrightarrow$ a votes as the same party as b

Equivalence

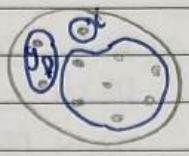
⇒ **Definition**: Let $\sim$ be a equivalent relation on A. Then for any $a \in A$ one defines $[a] := \{m \in A \mid m \sim a\} \subseteq A$

Equivalence class of a with respect to $\sim$ = subset ↖ is equivalent to

⇒ Example:

$[f] = [g] = \{f, g\}$

$[i] = \{i\}$



equivalent classes can't overlap

⇒ **Theorem**: either two equivalence classes are $[a] = [b]$ (the same) or $[a] \cap [b] = \emptyset$ (have no overlap)

↳ proof: Given $a, b \in A$

i) $a \sim b$

$m \in [a] \Rightarrow m \sim a$

$\Rightarrow m \sim b \Rightarrow m \in [b]$ (by transibility)

$[a] \subseteq [b]$

doing the same by a,b swapped $\Rightarrow [a] \supseteq [b]$] $[a] = [b]$

ii) $a \not\sim b$

$m \in [a] \Rightarrow m \sim a$

Assume $m \in [b] \Rightarrow m \sim b$] by trans, sym $\Rightarrow a \sim b$ ↯ $\Rightarrow m \notin [b]$

$\Rightarrow (\forall m \in [a] \Rightarrow m \notin [b])$

$\Rightarrow [a] \cap [b] = \emptyset$

⇒ **Theorem**: $\bigcup A_\lambda = A$

Ring of integers & Field of rationals

⇒ $\mathbb{N}$: natural numbers $(\mathbb{N}, +, \cdot)$

⇒ $\mathbb{Z}$: integers $(\mathbb{Z}, \oplus, \odot)$, 8 properties

⇒ $\mathbb{Q}$: rationals $(\mathbb{Q}, \boxplus, \boxdot)$, 9 properties

⇒ **Properties of $\mathbb{N}$**

↳ C^+: $a+b = b+a$

↳ A^+: $(a+b)+c = a+(b+c)$

↳ N^+: $\exists 0 \forall a : a+0 = a$

↳ $N^\cdot$: $\exists 1 \forall a : a \cdot 1 = a$

↳ $D^{+,\cdot}$: $a \cdot (b+c) = a \cdot b + a \cdot c$

1. Construction of the set $\mathbb{Z}$

=> **Definition:** $\sim \subseteq (\mathbb{N}\times\mathbb{N})\times(\mathbb{N}\times\mathbb{N})$

$$(a,b)\sim(c,d) :\Leftrightarrow a+d=b+c$$

=> Claim: $\sim$ is a equivalence relation

↳ proof: (i) $(a,b)\sim(a,b) :\Leftrightarrow a+b=b+a$

$\Rightarrow \sim$ refexive $\quad c^{+}$

(ii) $(a,b)\sim(c,d) \Leftrightarrow a+d=b+c$

$\Updownarrow \qquad \Updownarrow \; c^{+}, c^{+}, =$

$(c,d)\sim(a,b) \Leftrightarrow c+b=d+a$ $\quad$ = or - ?

$\Rightarrow \sim$ is symmetric

(iii) $(a,b)\sim(c,d)$ and $(c,d)\sim(e,f)$

$a+d=b+c \qquad c+f=d+e$

$$a+d+c+f=b+c+d+e$$

$$a+f=b+e$$

$$\Updownarrow$$

$$(a,b)\sim(e,f)$$

$\Rightarrow \sim$ is transitive $\qquad$ QED

=> Example: $-1 := 2-3 \qquad (2,3)$

$\qquad\qquad\quad \wr \qquad\qquad\quad \wr \qquad -1 := [(2,3)]$

$\qquad\quad -1 := 6-7 \qquad (6,7)$

=> **Definition:** $\mathbb{Z} := (\mathbb{N}\times\mathbb{N})/\sim$

2. Addition & multiplication on $\mathbb{Z}$

$\oplus : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} := \{[(a,b)]_\sim \mid (a,b)\in\mathbb{N}\times\mathbb{N}\}$

$$[(a,b)]_\sim \oplus [(c,d)] := [(a+c,\, b+d)]$$

$\nwarrow\nearrow$ $\sim$

$\odot : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$

$$[(a,b)] \odot [(c,d)] := [(ac+bd,\, ad+bc)]$$

$[(a+n, b+n)] \qquad [(c+m, d+m)]$

=> Well and ill definedness

↳ $IQ([a]) := IQ(a)$

$[f] \quad IQ[f]$

$IQ([a]) = IQ([f])$

True → well defined

False → ill defined

=> proof: show well-definedness of the $\oplus$ map

If $[(a,b)] = [(\tilde{a},\tilde{b})] \Leftrightarrow (a,b) \sim (\tilde{a},\tilde{b}) \Leftrightarrow a+\tilde{b} = \tilde{a}+b$

$[(c,d)] = [(\tilde{c},\tilde{d})] \Leftrightarrow (c,d) \sim (\tilde{c},\tilde{d}) \Leftrightarrow c+\tilde{d} = \tilde{c}+d$

$[(a,b)] \oplus [(c,d)] \overset{?}{=} [(\tilde{a},\tilde{b})] \oplus [(\tilde{c},\tilde{d})]$

$[(a+c, b+d)]$

$[(\tilde{a}+\tilde{c}, \tilde{b}+\tilde{d})]$

$[(\tilde{a}+\tilde{c}+n, \tilde{b}+\tilde{d}+n)]$

$[(\tilde{a}+\tilde{c}+b, \tilde{b}+\tilde{d}+b)]$

$[(a+\tilde{b}+\tilde{c}, \tilde{b}+\tilde{d}+b)]$

$[(a+\tilde{c}, b+\tilde{d})]$

$[(a+\tilde{c}+d, b+\tilde{d}+d)]$

$[(a+c+\tilde{d}, b+\tilde{d}+d)]$

$[(a+c, b+d)]$

↳ $\oplus$ is a well defined map, similarly for $\odot$

=> Example $[(2,3)] \oplus [(5,1)] = [(7,8)] \oplus [(4,0)]$

3. Ring structure of $(\mathbb{Z}, \oplus, \odot)$

=> Theorem: $(\mathbb{Z}, \oplus, \odot)$ is a ring. That means:

$C^{\oplus}$: $\forall x,y \in \mathbb{Z} : x \oplus y = y \oplus x$

$A^{\oplus}$: $\forall x,y,z \in \mathbb{Z} : (x \oplus y) \oplus z = x \oplus (y \oplus z)$

$N^{\oplus}$: $\exists 0_{\mathbb{Z}} \in \mathbb{Z}$ (incl $\wedge$) $\forall x \in \mathbb{Z} : x \oplus 0_{\mathbb{Z}} = x$

$i^{\oplus}$: $\forall x \in \mathbb{Z}\ \exists (-x) \in \mathbb{Z} : x \oplus (-x) = 0_{\mathbb{Z}}$

$C^{\odot}$: $\forall x,y \in \mathbb{Z} : x \odot y = y \odot x$

$A^{\odot}$: $\forall x,y,z \in \mathbb{Z} : (x \odot y) \odot z = x \odot (y \odot z)$

$N^{\odot}$: $\exists 1_{\mathbb{Z}} \in \mathbb{Z} : \forall x \in \mathbb{Z} : x \odot 1_{\mathbb{Z}} = x$

$i^{\odot}$: does only exists in fields

$D^{\odot,\odot}$: $\forall x,y,z \in \mathbb{Z} : x \odot (y \oplus z) = x \odot y \oplus x \odot z$

⇒ Remark: elementary school claims

$\mathbb{N} \subseteq \mathbb{Z} :\Leftrightarrow n \in \mathbb{N} \not\Rightarrow n \in \mathbb{Z}$

↓

$2 = \{\{\emptyset\}\}$ ↘ $[(0,0)]_\sim$

$(0,0) = \{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots\}$

4. Embedding of $\mathbb{N}$ into $\mathbb{Z}$ & traditional notation

⇒ Definition: $\text{int}\ \mathbb{N} \hookrightarrow \mathbb{Z}$

$n \mapsto [(n,0)]$

↳ $\hookrightarrow$: injective (hits everything only ones)

↳ Claim: int is injective

⇒ Theorem: int is an "embedding" of $(\mathbb{N},+,\cdot)$ into $(\mathbb{Z},\oplus,\odot)$

1) $\text{int}(n+m) = \text{int}(n) \oplus \text{int}(m)$
2) $\text{int}(n \cdot m) = \text{int}(n) \odot \text{int}(m)$
3) $\text{int}(0) = 0_{\mathbb{Z}}$
4) $\text{int}(1) = 1_{\mathbb{Z}}$

⇒ Traditional notation: $n \in \mathbb{N}$

$\text{int}(n) = [(n,0)] = [(a,b)]$ $a \geq b \Leftrightarrow \exists n \in \mathbb{N} : a = b+n$

$-\text{int}(n) = [(0,n)] = [(a,b)]$ $a < b \Leftrightarrow \exists m \in \mathbb{N}^* : b = a+m$

↳ Any $z \in \mathbb{Z}$ can be written either as $\text{int}(n)$ or $-\text{int}(m)$

=

$[(a,b)]$

5. Construction of $\mathbb{Q}$

⇒ Definition: $\approx \subseteq (\mathbb{Z} \times \mathbb{Z}^*) \times (\mathbb{Z} \times \mathbb{Z}^*)$

$(a,b) \approx (c,d) :\Leftrightarrow a \odot d = c \odot b$

↳ claim: $\approx$ is an equivalent relation

↳ proof:

⇒ Definition: $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z}^*)/\approx$

↳ Traditional notation: $\frac{a}{b} := [(a,b)]_\approx$

$a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$

6. Adding & multiplication on $\mathbb{Q}$

$\Rightarrow$ Definition: $\boxplus : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$

$$[(a,b)] \boxplus [(c,d)] := [(a \odot d \oplus c \odot b, b \odot d)]$$

$\boxdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$

$$[(a,b)] \boxdot [(c,b)] := [(a \odot c, b \odot d)]$$

$\Rightarrow$ Fact: $\boxplus$ and $\boxdot$ are well-defined

↳ proof:

$\Rightarrow$ It's fun to study the idiots addition on $\mathbb{Q}$:

$\oplus : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$

$[(a,b)] \oplus [(c,d)] := [(a \oplus c, b \oplus d)]$

$\oplus$ is ill-defined: $\frac{2}{3} \oplus \frac{3}{5} = \frac{5}{8}$

$$\begin{array}{ccccc} \frac{2}{3} & \oplus & \frac{3}{5} & = & \frac{5}{8} \\ \| & & \| & & \nparallel \\ \frac{4}{6} & \oplus & \frac{9}{15} & = & \frac{13}{21} \end{array}$$

Some important summaries

$\Rightarrow$ natural numbers: $(\mathbb{N}, +, \cdot)$

↳ $\mathbb{N} := \{..\{\emptyset\}...\}$ $\quad a, b$

$\Rightarrow$ integers: $(\mathbb{Z}, \oplus, \odot)$ "morally"

↳ $\mathbb{Z} :=$ "$[(\mathbb{N}-\mathbb{N})]_\sim$" $\quad a-b$ (ring)

$\Rightarrow$ rational numbers: $(\mathbb{Q}, \boxplus, \boxdot)$ (field)

↳ $\mathbb{Q} :=$ "$[(\mathbb{Z} : \mathbb{Z}^*)]_\approx$" $\quad \frac{a}{b}$

$\Rightarrow$ "implies", "follows from"

$\Leftrightarrow$ "if and only if", "is equivalent to"

$:=$ "is defined by" (equality by definition)

$:\Leftrightarrow$ "is defined by"

Axioms

(E) empty set: $\forall x : \neg(x \in E)$

(M) mapped sets: $y \in im_F(A) :\Leftrightarrow \exists x : [x \in A \wedge F(x,y)$

(R) restricted comprehension: $E \in \{x \in A \mid S(x)\} :\Leftrightarrow E \in A \wedge S(E)$
(D) Doublet sets: $x \in \{A, B\} x = A \vee x = B$
(U) union set: $x \in UC :\Leftrightarrow \exists S: (S \in C \wedge x \in S)$
(I) infinity: $\emptyset \in N \wedge \forall x: (x \in N \Rightarrow \{x\} \in N)$

$C^+: a+b=b+a$ $\quad C^\cdot: a \cdot b = b \cdot a$
$A^+: (a+b)+c = a+(b+c)$ $\quad A^\cdot: (a \cdot b) \cdot c = a \cdot (b \cdot c)$
$N^+: a+0=0$ $\quad N^\cdot: a \cdot 1 = 0$
$i^+: a+(-a)=0$ $\quad i^\cdot:$
$D^{+,\cdot}: a \cdot (b+c) = a \cdot b + a \cdot c$

$\Rightarrow$ Associative: $(a+b)+c = a+(b+c)$
$\Rightarrow$ Commutative: $a+b = b+y$

Check well-definedness of a map wenn the domain includes a quotionset