0 Fundamentals of Mathematics

$(\mathbb{N}, +, \cdot), (\mathbb{Z}, \oplus, \odot), (\mathbb{Q}, \boxplus, \boxdot)$
Algebraic structures
Maps & relations
Set theory
Proofs
Logics

Instead of lots of repetition, we try to say it once, and say it right, since

$$8 \text{ years of school } \mathrel{\widehat{=}} \ 4 \text{ lectures}$$

1 Logic

We will be discussing **classical logic**, steps:

- Propositional logic
- Predicate logic

Definition 1.1. A **proposition** can take the values T and F (true and false), no other.

Remark. It is not in the purview of the propositional logic to study the interior structure of a proposition. One can define new propositions in terms of given ones.

1.1 Logical operators

- Unary operators: 'takes' one proposition and makes a new one.

p	$\neg p$	$\mathrm{id}(p)$	T_p	$\bot_p$
T	F	T	T	F
F	T	F	T	F

These are ALL unary operators, actually. Exhausted all cases, no other ones possible.

- Binary operators: 'takes' two propositions and make a new one. A few important ones:

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$	$p \implies q$	$p \iff q$
T	T	T	T	F	T	T
T	F	T	F	T	F	F
F	T	T	F	T	T	F
F	F	F	F	F	T	T

If you had a half-decent high-school teacher, you would've known about logical implication (lol). For logical implication: **ex falso quod libet**.

Theorem 1.1. $(p \implies q) \iff (\neg q) \implies (\neg p)$

Proof. Looking at the truth table, we can see the last two columns are equivalent for all cases, therefore the theorem holds.

p	q	$\neg p$	$\neg q$	$(\neg q) \implies (\neg p)$	$p \implies q$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

□

Remark. This theorem is kind of like the 'license' to perform proofs by way of contradiction. Other logic systems exist where proofs by way of contradiction do not 'work' in a sense.

Remark. $(\neg q) \implies (\neg p)$ is called the **contrapositive** of $p \implies q$.

1.2 Notational convention

We agree that the 'binding strength' of the following operators strictly decreases:

$$\neg \wedge \vee \implies \iff$$

1.3 N-ary operators

An N-ary operator is just a more general case of the types of operators we have seen before, they 'take' N propositions and produce a single new one. There are exactly 2^{2^N} (whatever that means) N-ary operators for all $N \in \mathbb{N}$.

Theorem 1.2. *Every N-ary operator operator can be expressed solely in terms of one particular binary operator, namely NAND, or the not-and, or the symbol 'Sheffer stroke', $p \mid q$. Its truth table:*

p	q	$p \mid q$
T	T	F
T	F	T
F	T	T
F	F	T

No proof, sadly.

Example. $\neg p :\iff p \mid p$

Remark. The : symbol 'defines' the left hand side of the equivalence in terms of the right hand side, for example, $:\iff$ and $:=$.

1.4 Predicate Logic

'Refines' propositional logic, **instead** of propositions, predicate logic uses the following:

- objects, commonly referred to by capital letters (A, B, C), further unspecified, because again, predicate logic theory does not study the interior structure of its objects,
- predicates (P, Q, R), which 'operate' on objects.

Each predicate is assigned a valence, e.g. the valence of a predicate P is $\text{val}(P)$ (technically the valence is a natural number, but those are not properly defined yet). (continuing) objects and predicates play together such that any **evaluation** of a predicate P on $\text{val}(P)$ many objects $X_1, X_1, \ldots, X_{\text{val}(P)}$, namely $P(X_1, X_1, \ldots, X_{\text{val}(P)})$ is a proposition. (this is kind of the definition of a predicate but you cannot properly write it nicely as a definition in this form)

Remark. A predicate P such that $\text{val}(P) = 0$ is a proposition.

1.4.1 Examples

Example. Let P be a predicate of valence 1 such that

$$P(X) :\iff X^2 = X$$

This would be a nice, intuitive, didactically approved example, but we lack the required mathematical structures to make sense of it.

Example. Let E be a predicate of valence 2 such that

$$E(X, Y) :\iff X \in Y$$

Same problem again, what is the $\in$ operator even?

Example. Let P be a predicate of valence 1 and let R be a predicate of valence 2, then define a predicate Q of valence 2 such that

$$Q(X, Y, Z) :\iff P(X) \wedge Y(Z, Z)$$

1.5 Quantification

Definition 1.2. Let P be a predicate such that $\mathrm{val}(P) = 1$, then define the proposition (called 'universal quantification')

$$\forall X : P(X) :\iff \begin{cases} T & \text{if } P(X) \text{ is true indenpendent of } X, \\ F & \text{otherwise.} \end{cases}$$

Read this as 'For all X, P(X) (is true)'.

Definition 1.3. Let P be a predicate such that $\mathrm{val}(P) = 1$, then define the proposition (called 'there exists')

$$\exists X : P(X) :\iff \neg(\forall X : \neg P(X))$$

Theorem 1.3. *Let P be a predicate of valence one. Then:*

$$\forall X : P(X) \implies P(Y)$$

Proof. Suppose the left hand side of the implication is true. Then P is true and independent of X, so the theorem holds. If the left hand side of the implication is false, then the proposition still holds because of ex falso quod libet. □

Remark. The following

$$\forall X : \exists Y : R(X, Y)$$

is generically not equivalent to

$$\exists Y : \forall X : R(X, Y)$$

1.6 Proofs and axiomatic systems

Definition 1.4. An axiomatic system is given by a finite list of propositions, $a_1, a_2, \ldots, a_N$, called axioms.

Definition 1.5. A proof for a proposition P under a set of assumptions $S_1, S_2, \ldots, S_N$ (which are propositions), and withing an axiomatic system, is a finite list $q_1, q_2, \ldots, q_{F-1}, P$ (think 'proof steps') with the following property: for every j with $1 \leq j < F$, one of the following conditions must be true:

- q_j is an axiom,
- q_j is an assumption,
- q_j is a tautology,
- $\exists m, n : q_m \wedge q_n \implies q_j$ and $1 \leq m, n < j$.

2 Set theory

Set theory is built on predicate logic. There are 2 further stipulations we need to make:

- there are **objects** that satisfy a set of additional conditions (axioms of set theory), and thus qualify as 'sets';
- there is a particular valence two predicate $\in$ (element of, epsilon, etc.) which is defined for objects that happen to be sets. In other words, if A and B are sets, then $\in(A, B)$ is a proposition.

This is the general idea of set theory.
There are two 'ways' to set theory, starting with:

2.1 Naive set theory

Basic idea: sets are collections (bags) of objects, where the selection of which object belongs to a particular set is made by a valence one predicate, S. More precisely, we have the one and only axiom of naive set theory:

Axiom 2.1. (G) ***Axiom of General comprehension****: Let S be a predicate of valence one, then there is a naive set denoted*

$$\{X \mid S(X)\}$$

which is defined by

$$E \in \{X \mid S(X)\} :\iff S(E)$$

Definition 2.1. Let A and B be sets. Then

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

Definition 2.2. Let A and B be sets. Then

$$A \subseteq B :\iff \forall E : (E \in A \implies E \in B)$$

Thus, we have further defined two valence two predicates, $=, \subseteq$, in terms of $\in$.

Remark. Notational convention:

$$A \in B :\iff \in(A, B)$$
$$A \subseteq B :\iff \subseteq(A, B)$$
$$A = B :\iff =(A, B)$$

The general comprehension axiom wonderfully allows to construct any set one needs in order to enact all of modern mathematics.

Example. Consider a set $\varnothing := \{X \mid S(X)\}$, and let $S(X)$ be a valence one predicate such that

$$S(X) :\iff F$$

By general comprehension, this is a (naive) set, called the 'empty set'.
Justification for terminology:

$$E \in \varnothing \iff S(E) \iff F$$

Therefore, $\varnothing$ 'has no elements'.

Example. Let A and B be naive sets. Then

$$A \cup B := \{X \mid X \in A \vee X \in B\}$$

By (G), $E \in A \cup B \iff X \in A \vee X \in B$. Similarly:

$$A \cap B := \{X \mid X \in A \wedge X \in B\}$$

$$A \setminus B := \{X \mid X \in A \wedge X \notin B\}$$

Example. Let A be a naive set. Then

$$\mathcal{P}(A) := \{X \mid X \subseteq A\}$$

2.2 Trouble in (general comprehension) paradise

Let $u := \{X \mid \underbrace{X \notin X}_{S(X)}\}$, then u by Ⓖ is a naive set. Let us consider whether $u \in u$, by exhausting all cases.

Case 1: $u \in u \underbrace{\iff}_{\text{by } S(X)} u \notin u$, contradiction.

Case 2: $u \notin u \underbrace{\iff}_{\text{by } S(X)} u \in u$, contradiction.

2.3 Zermelo-Fraenkel set theory

Formulation of set theory on which modern mathematics is formed. Overview: we should repair Ⓖ, weakened to Ⓜ. The following axioms shall be defined at some point:

$$\overbrace{\underbrace{\text{Ⓔ}\,\text{Ⓜ}}_{\text{restricted comprehension}}\quad\text{Ⓟ}}^{\text{doublet sets}}\ \text{Ⓤ}\ \text{Ⓘ}\ \text{Ⓕ}(\text{Ⓒ})$$

Axiom 2.2. Ⓔ ***Axiom of empty set existence****: There is a set E such that*

$$\forall X : X \notin E$$

Remark. Terminology: any such set is called 'an empty set'.

Theorem 2.1. *Let E and $\tilde{E}$ be empty sets. Then $E = \tilde{E}$*

Proof. E is empty, so by definition, for all X, $X \in E$ is false, and by ex falso quod libet, the statement '$X \in E \implies X \in \tilde{E}$' is true. Analogously, $\tilde{E}$ is empty, so by definition, $X \in \tilde{E}$ is false, and by ex falso quod libet, the statement '$X \in \tilde{E} \implies X \in E$' is true. Therefore, $\forall X : X \in \tilde{E} \iff X \in E$, and by definition of set equality, $E = \tilde{E}$. □

This proves that there is only a single empty set, so we can assign it its symbol again, $\varnothing$. In order to state Ⓜ, we need a preceding definition:

Definition 2.3. A valence two predicate F is called a **mapping** if and only if

$$\forall X : \exists! Y : F(X, Y)$$

Axiom 2.3. Ⓜ ***Axiom of mapped sets****: Let A be a ZFC set, and F a mapping. Then there is a set (denoted* $\underbrace{\operatorname{im}_F(A)}_{\textit{image set of } A \textit{ under } F}$ *) defined by*

$$Y \in \operatorname{im}_F(A) :\iff \exists X : [X \in A \wedge F(X, Y)]$$

Combining Ⓔ and Ⓜ, one finds as an implication the most used theorem of mathematics[1]:

Theorem 2.2. ***Principle of restricted comprehension****: Let A be a ZFC set, let S be a valence one predicate. Then the set denoted by* $\left\{ X \underbrace{\in A}_{new} \mid S(X) \right\}$ *and defined through*

$$E \in \{X \in A \mid S(X)\} :\iff E \in A \wedge S(E)$$

is a ZFC set.

[1] Citation needed

Proof. Consider the following two cases:
Case 1: Suppose there exists no E such that $E \in A \land S(E)$. Then we define $\{X \in A \mid S(X)\} := \varnothing$.
Case 2: Suppose such an E does exist. Then define the following predicate of valence two:

$$F(X,Y) :\iff S(X) \land (Y = X) \lor \neg S(X) \land (Y = E)$$

F is by definition a mapping. By (M), $\mathrm{im}_F(A)$ is a ZFC set. For notational purposes we then define $\{X \in A \mid S(X)\} := \mathrm{im}_F(A)$ □

Axiom 2.4. (P) ***Powerset axiom***: *For every ZFC set A, there exists the set denoted $\mathcal{P}(A)$, defined by*

$$X \in \mathcal{P}(A) :\iff X \subseteq A$$

Remark. Recall that in naive set theory we define $\mathcal{P}(A)$ through general comprehension.

Example. $\varnothing$ is a ZFC set due to (E). Therefore, we can ask the question whether $\varnothing \subseteq \varnothing$. Well, by definition:

$$\varnothing \subseteq \varnothing \iff \forall X : X \in \varnothing \implies X \in \varnothing$$

which, because $X \in \varnothing$ is always false, is true, independent of X, therefore $\varnothing \in \mathcal{P}(\varnothing)$

Combining (E), (M) and (P), one finds as an implication the most used theorem of kindergarten mathematics[2]:

Theorem 2.3. *Let A and B be sets. Then there is a set denoted $\{A, B\}$ such that*

$$X \in \{A, B\} \iff X = A \lor X = B$$

Proof. First, let us consider what $\mathcal{P}(\varnothing)$ is. By (P),

$$X \in \mathcal{P}(\varnothing) \iff X \subseteq \varnothing \iff \forall Y : (Y \in X \implies Y \in \varnothing)$$

But $Y \in \varnothing$ is false, therefore $\forall Y : Y \notin X$. Only one such set by (E) exists, namely $\varnothing$. So $\varnothing \in \mathcal{P}(\varnothing)$. Next, let us then consider $\mathcal{P}(\mathcal{P}(\varnothing))$. Well,

$$X \in \mathcal{P}(\mathcal{P}(\varnothing)) \iff X \subseteq \mathcal{P}(\varnothing) \iff \forall Y : (Y \in X \implies Y \in \mathcal{P}(\varnothing))$$

We can consider the case where $Y \notin \mathcal{P}(\varnothing)$, in which case $X = \varnothing$, and we can consider the case where $Y \in \mathcal{P}(\varnothing)$, and there exists as shown at least one such Y, namely $\varnothing$. Thus $\varnothing, \mathcal{P}(\varnothing) \in \mathcal{P}(\mathcal{P}(\varnothing))$. Then define the following mapping F:

$$F(X,Y) :\iff (X = \varnothing) \land (Y = A) \lor (X \neq \varnothing) \land (Y = B)$$

Then, by (M), $\mathrm{im}_F(\mathcal{P}(\mathcal{P}(\varnothing)))$ is a ZFC set, so we define

$$\{A, B\} := \mathrm{im}_F(\mathcal{P}(\mathcal{P}(\varnothing)))$$

Again by (M), $X \in \{A, B\} \iff \exists X : [X \in \mathcal{P}(\mathcal{P}(\varnothing)) \land F(X,Y)]$. There exists only two cases for which $F(X,Y)$ is true, by the definition of F, namely A and B. Hence we have shown $X \in \{A, B\} \implies X = A \lor X = B$. Let us now evaluate F on A and B in order to show that the implication in the other direction is true as well. $F(X, A) \iff X = \varnothing$, and since such an $X \in \mathcal{P}(\mathcal{P}(\varnothing))$ exists, we have proven $A \in \{A, B\}$. Now check $F(X, B) \iff X \neq \varnothing$, and such an element also exists in $\mathcal{P}(\mathcal{P}(\varnothing))$, hence $B \in \{A, B\}$. □

Axiom 2.5. (U) ***Axiom of union***: *Let C be a set. Then there is a set denoted by* $\underbrace{\bigcup C}_{union\ set}$ *defined by*

$$X \in \bigcup C :\iff \exists S : (S \in C \land X \in S)$$

[2] Again, citation needed

Definition 2.4. Let $A_1, A_2, \ldots$ be sets. Then A_1, A_2 is a set by the principle of doublet sets. Let us first define a **singleton set**:

$$\{A_1\} := \{A_1, A_1\}$$

which is a ZFC set by doublet sets. Similarly:

$$\begin{aligned}
\{A_1, A_2, A_3\} &:= \bigcup\{\{A_1, A_2\}, \{A_3\}\} \\
\{A_1, A_2, A_3, A_4\} &:= \bigcup\{\{A_1, A_2, A_3\}, \{A_4\}\} \\
&\vdots \\
\{A_1, \ldots, A_N\} &:= \bigcup\{\{A_1, \ldots, A_{N-1}\}, \{A_N\}\}
\end{aligned}$$

This way, any finite set can now be constructed.

Axiom 2.6. (I) ***Axiom of infinity***: *There exists a set* $\mathbb{N}$ *such that* $\varnothing \in \mathbb{N}$ *and*

$$\forall X : (X \in \mathbb{N} \implies \{X\} \in \mathbb{N})$$

Remark. $\varnothing \in \mathbb{N}$, $\{\varnothing\} \in \mathbb{N}$, $\{\{\varnothing\}\} \in \mathbb{N}$, etc. We gave them nicknames!

$$\begin{aligned}
0 &:= \varnothing \\
1 &:= \{\varnothing\} \\
2 &:= \{\{\varnothing\}\}
\end{aligned}$$

3 Relations and maps

3.1 Order from disorder

Sets have no order: $\{A, B\} = \{B, A\}$. There is no order that a set imposes on its elements.

Definition 3.1. Let A and B be sets. Define the **ordered pair**:

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

Observation.

$$(b, a) = \{\{b\}, \{a, b\}\} \neq \{\{a\}, \{a, b\}\} = (a, b)$$

Observation.

$$(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$$

Therefore we cannot 'extract' the first entry by looking which set is the singleton set.

Theorem 3.1. *The first entry of* (a, b) *is* $\bigcup\bigcap(a, b)$*, and the second entry is*

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

Proof. For the first element:

$$\begin{aligned}
\bigcup\bigcap(a, b) &= \bigcup\bigcap\{\{a\}, \{a, b\}\} \\
&= \bigcup\{a\} \\
&= a
\end{aligned}$$

For the second element:

- **Case 1**: Assume $\bigcup(a,b) = \bigcap(a,b)$. This means that $\{a,b\} = \{a\}$, therefore, $b = a$. Then, the definition is equivalent to the definition of the first element, and the first element is equal to the second element, hence proven.
- **Case 2**: Now assume $\bigcup(a,b) = \bigcap(a,b)$, therefore $b \neq a$. Then

$$\begin{aligned}\bigcup\Big(\bigcup(a,b) \setminus \bigcap(a,b)\Big) &= \bigcup\Big(\{a,b\} \setminus \{a\}\Big)\\ &= \bigcup\{b\}\\ &= b\end{aligned}$$

□

Definition 3.2. Let A and B be sets. Then the **cartesian product** of A and B is denoted by $A \times B$ and defined by

$$A \times B := \left\{(a,b) \in \mathcal{P}\Big(\mathcal{P}\Big(\bigcup\{A,B\}\Big)\Big) \;\middle|\; a \in A \wedge b \in B\right\}$$

Remark. This definition can be extended to $A \times B \times C := (A \times B) \times C$, and then by using certain notational choices, we will be able to define n-tuples $(a_1, \ldots, a_n)$.

3.2 Relations

Definition 3.3. A **relation** R between a set A and a set B is a subset of $A \times B$.

Remark. Notation: Having chosen a relation R, we write

$$aRb :\Longleftrightarrow (a,b) \in R$$

Additionally, a relation 'on a set A' means a relation between set A and itself.

Example. Define the following relation on $\mathbb{N}$:

$$< :\Longleftrightarrow \left\{\begin{array}{cccc}(0,1), & (0,2), & (0,3), & \ldots\\ & (1,2), & (1,3), & \ldots\\ & & (2,3), & \ldots\\ \vdots & \vdots & \vdots & \ddots\end{array}\right\}$$

Now, $(1,2) \in < \iff 1 < 2$, and $(2,1) \notin < \iff 2 < 1$.

3.3 Maps

Definition 3.4. 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**.

Remark. Notation:

$$f : A \to B$$

$$a \mapsto f(a) = b$$

means the same as 'Let F be a map from A to B, then $(a,b) \in f :\Longleftrightarrow \ldots$.', since by definition $f(a) = b :\Longleftrightarrow (a,b) \in f$. A is the **domain**, B is the **codomain**, $f(a) = b$ is the **function prescription**.

Remark. **Bad talk**: 'Consider the function $f(x) = x^2$'. **Correct**: 'Consider the map

$$f : \mathbb{R}_0^+ \to \mathbb{R}$$

,

Example. Consider the map (called the **successor map**)

$$S : \mathbb{N} \to \underbrace{\mathbb{N}^*}_{\mathbb{N} \text{ without } 0}$$

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

For example, $S(1) = S(\{\varnothing\}) = \{\{\varnothing\}\} = 2$.

Example. Consider the map (called the **predecessor map**)

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

$$\{n\} \mapsto n$$

For example, $P(7) = P(\{6\}) = 6$.

Definition 3.5. Let $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$ be maps. Then, we define the **composite map** as follows:

$$g \circ f : A \to C$$

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

(read the $\circ$ symbol as 'composed with' or 'after')

Theorem 3.2. *Composition is associative: let $A \xrightarrow{f} B$, $B \xrightarrow{g} C$ and $C \xrightarrow{h} D$ be maps. Then*

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

Proof. For all $a \in A$,

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

Hence both sides of the identity are equal for all a, therefore the maps are equal. □

Definition 3.6. Let $f : A \to A$ be a map. Then define f^n as follows:

- $F^0 := \mathrm{id}_A$
- $F^n := F^{P(n)} \circ f$

Theorem 3.3. *Let $f : A \to B$ be a map. Then $\mathrm{id}_A \circ f = f$.*

Proof. For all $a \in A$, $(\mathrm{id}_A \circ f)(a) = \mathrm{id}_A(f(a)) = f(a)$, therefore $\mathrm{id}_A \circ f = f$. □

Example.

$$\begin{aligned} f^3 &= f^{P(3)} \circ F = F^2 \circ f \\ &= f^{P(2)} \circ f \circ f \\ &= f^1 \circ f \circ f \\ &= f^{P(1)} \circ f \circ f \circ f \\ &= f^0 \circ f \circ f \circ f \\ &= \mathrm{id}_A \circ f \circ f \circ f \\ &= f \circ f \circ f \end{aligned}$$

which shows why f^n is equivalent to composing f with itself n times.

Remark. Consider a map $f : A \to B$ such that $A = M \times N$ and M, N are sets. Now, $(m, n) \mapsto f((m, n)) =: f(m, n)$. This way, we can do multivariable functions as well.

Definition 3.7. Define

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(a, b) \mapsto S^b(a)$$

Remark. Notational shorthand: $a + b := +((a, b))$. Also, $+ \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N}$. From now on, we assume we can figure out associativity, commutativity, distributivity, etc. of the plus operator, and we assume we have defined times, and its rules.
To give an idea, you might want to define multiplication according to

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(a, b) \mapsto \begin{cases} 0 & \text{if } b = 0 \\ \cdot((a, P(b))) + a & \text{otherwise} \end{cases}$$

Definition 3.8. A map $f : A \to B$ is

- **injective** if $f(a) = f(a') \implies a = a'$;
- **surjective** if $\forall b \in B : \exists a \in A : b = f(a)$;
- **bijective** if the map is injective and surjective. In this case, the map is called an **isomorphism**.

Definition 3.9. 2 sets A, B are called **isomorphic** if there exists an isomorphism $\phi : A \to B$.

3.4 Equivalence relations

A relation $\sim$ on a set A is called an **equivalence relation** if and only if it satisfies the following conditions:

- Reflexivity: for all $a \quad , \quad a \sim a$
- Symmetry: for all $a, b \quad , \quad a \sim b \implies b \sim a$
- Transitivity: for all $a, b, c \quad , \quad a \sim b \wedge b \sim c \implies a \sim c$

Definition 3.10. Let $\sim$ be an equivalence relation on A. Then for any $a \in A$, one defines the set

$$[a]_\sim := \{m \in A \mid m \sim a\}$$

called the **equivalence class** of a with respect to $\sim$.

Theorem 3.4. *Let A be a set and let $\sim$ be an equivalence relation on A. Let $a, b \in A$. For any two equivalence classes $[a]_\sim, [b] \sim$,*

$$[a] = [b] \vee [a] \cap [b] = \varnothing$$

Proof. **Case 1**: $a \sim b$. Since $E \in [a] \implies E \in A \wedge E \sim a$, $[a] = [b]$, since by the transitivity of $\sim$, $E \sim a \iff E \sim b$ and therefore $E \in [a] \iff E \in [b]$;
Case 2: $\neg(a \sim b)$. By the same argument as case 1, we know that $E \in [a] \iff E \notin [b]$. The predicate $E \in [a] \wedge E \in [b]$ is always false. Therefore by the principle of restricted comprehension and the definition of set intersection, $\forall E : E \notin [a] \cup [b]$. This set, by $\textcircled{E}$, is an/the empty set. □

Definition 3.11. Define the set of all equivalence classes (called the **quotient set** of A with respect to $\sim$)

$$A/_\sim := \{[a] \in \mathcal{P}(A) \mid a \in A\}$$

Theorem 3.5. *Let A be a set, let $\sim$ be an equivalence relation on A. Then*

$$\bigcup A/_\sim = A$$

4 Ring of $\mathbb{Z}$ & field of $\mathbb{Q}$

To start out, we assume we already know $(\mathbb{N}, +, \cdot)$.

4.1 Construction of $\mathbb{Z}$

Definition 4.1. Define the relation

$$\sim \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$$

$$\forall a, b, c, d \in \mathbb{N} : (a, b) \sim (c, d) :\iff a + d = b + c$$

Motivation, morally $a - b = c - d$, therefore the ordered pair (a, b) represents $a - b$.

Claim 4.1. *$\sim$ is an equivalence relation.*

Proof. (This will be my version of the proof, by no means this is necessarily right) We need to show reflexivity, symmetry and transitivity:

- $\sim$ is reflexive $\iff \forall a, b \in \mathbb{N} : (a, b) \sim (a, b) \iff a + b = a + b$ which is obviously true;
- $\sim$ is symmetric $\iff \forall a, b, c, d \in \mathbb{N} : (a, b) \sim (c, d) \implies (c, d) \sim (a, b) \iff a + d = b + c \implies c + b = a + d$ which is obviously true;
- $\sim$ is transitive $\iff \forall a, b, c, d, e, f \in \mathbb{N} :$

$$\begin{aligned} & (a, b) \sim (c, d) \land (c, d) \sim (e, f) \implies (a, b) \sim (e, f) \\ \iff\ & a + d = b + c \land c + f = d + e \implies a + f = b + e \\ \iff\ & a + d + c + f = b + c + d + e \implies a + f = b + e \\ \iff\ & a + f = b + e \implies a + f = b + e \end{aligned}$$

  which is a tautology. Hence proven.

□

Intuition: we make from the problem of not having a natural number that represents $2 - 3$ (for example) the solution by introducing these ordered pairs under the equivalence relation $\sim$ such that '$2 - 3 = 6 - 7$'. Formally:

$$(2, 3) \sim (6, 7) \iff 2 + 7 = 3 + 6$$

which is provably true of course. Therefore, it makes sense to not consider these ordered pairs to be integers, but rather **all of the equivalent representations**, does that ring a bell?

Definition 4.2. Let $\mathbb{Z}$ be a set (called the **integers**) such that $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_\sim$. In other words, integers are equivalence classes of ordered pairs of natural numbers under $\sim$.

Definition 4.3. Let

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

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

be a map, called **integer addition**.

Morally again, $a - b + c - d = a + c - (b + d)$, kind of like having a positive and a negative part, so to speak.

Definition 4.4. Let

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

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

be a map, called **integer multiplication**.

Morally, $(a - c)(b - d) = ab + cd - bc - ad$ which justifies the definition. For these definitions, we are using quotient sets (set of all equivalence classes) in the domain and codomain of the map. In order to be of value, it would make sense that those operations produce the same result for any two equivalence classes, independent of the representative elements. If a map satisfies this property, it is called **well-defined**, and the inverse, **ill-defined**.

Claim 4.2. *The map $\oplus$ is well-defined.*

Proof. Let $a, b, c, d, a', b', c', d'$ be natural numbers. Assume that $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$. This implies that $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. These statements imply $a + b' = a' + b$ and $c + d' = c' + d$, respectively. Consider $[(a, b)] \oplus [(c, d)] = [(a + c, b + d)]$ and $[(a', b')] \oplus [(c', d')] = [(a' + c', b' + d')]$. To show that $\oplus$ is well-defined, it would be sufficient to show that these two expressions are equal.

$$\begin{aligned}
[(a' + c', b' + d')] &= [(a' + c' + b, b' + d' + b)] \\
&= [(a + c' + b', b' + d' + b)] \\
&= [(a + c', d' + b)] \\
&= [(a + c' + d, d' + b + d)] \\
&= [(a + c + d', d' + b + d)] \\
&= [(a + c, b + d)]
\end{aligned}$$

Therefore, $[(a + c, b + d)] = [(a' + c', b' + d')]$. Thus for any two pairs of representatives, such that the first and second integer of each pair is equal to the other pair's first and last element, respectively, $\oplus$ maps to an equivalence class of an identical representative, and thus $\oplus$ is well-defined. □

Remark. Checking well-definedness is really important on an exam. Whenever you declare a map that incorporates quotient sets, you should always prove well-definedness.

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

Definition 4.5. A set and two operations, $(A, +_A, \cdot_A)$, is a structure called a **ring** if and only if it satisfies the following laws (denoting $+_A$ and $\cdot_A$ as simply $+$ and $\cdot$ for clarity):

- C^+: $\forall x, y \in A : x + y = y + x$
- A^+: $\forall x, y, z \in A : (x + y) + z = x + (y + z)$
- N^+: $\exists 0_A \in A : \forall x \in A : x + 0_A = x$
- I^+: $\forall x \in A : \exists (-x) \in A : x + (-x) = 0_A$
- $C^\cdot$: $\forall x, y \in A : x \cdot y = y \cdot x$
- $A^\cdot$: $\forall x, y, z \in A : (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $N^\cdot$: $\exists 1_A \in A : \forall x \in A : x \cdot 1_A = x$
- $D^{+,\cdot}$: $\forall x, y, z \in \mathbb{Z} : x \cdot (y + z) = x \cdot y + x \cdot z$

Meaning of the symbols for the laws:

- Commutativity
- Associativity
- Neutral element
- Inverse elements
- Distributivity

Theorem 4.1. *$(\mathbb{Z}, \oplus, \odot)$ is a ring, where $0_\mathbb{Z} = [(0, 0)]$, $1_\mathbb{Z} = [(1, 0)]$, $(-x) := [(0, x)]$.*

Proof. Proving all laws:

- $C^{\oplus}$: Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, $x := [(a,b)]$ and $y := [(c,d)]$. Starting with a tautology, we find

$$\begin{aligned}
&\iff [(a \oplus c, b \oplus d)] = [(a \oplus c, b \oplus d)] \\
&\iff [(a \oplus c, b \oplus d)] = [(c \oplus a, d \oplus b)] \\
&\iff [(a,b)] \oplus [(c,d)] = [(c,d)] \oplus [(a,b)] \\
&\iff x \oplus y = y \oplus x
\end{aligned}$$

- $A^{\oplus}$: Let $x, y, z \in \mathbb{Z}$, $x := [(a,b)]$, $y := [(c,d)]$ and $z := [(e,f)]$. On one hand,

$$(x \oplus y) \oplus z = [(a+c, b+d)] \oplus z = [(a+c+e, b+d+f)]$$

  On the other hand,

$$x \oplus (y \oplus z) = x \oplus [(c+e, d+f)] = [(a+c+e, b+d+f)]$$

  which are equal;

- $N^{\oplus}$: For all $x \in \mathbb{Z}$ such that $x = [(a,b)]$, $x + 0 = [(a,b)] + [0,0] = [(a+0, b+0)]$, and by definition of addition in $\mathbb{N}$, that is equal to $[(a,b)] = x$;

- $I^{\oplus}$: Let $-[(a,b)] = [(b,a)]$. Then, their sum is $[(b+a, a+b)]$ and by associativity $[(a+b, a+b)] = [(0,0)] = 0_{\mathbb{Z}}$;

- $C^{\odot}$: Let $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, $x := [(a,b)]$ and $y := [(c,d)]$. Starting with a tautology, we find

$$\begin{aligned}
&\iff [(ac+bd, ad+bc)] = [(ac+bd, bc+ad)] \\
&\iff [(ac+bd, ad+bc)] = [(ca+db, cb+da)] \\
&\iff [(a,b)] \odot [(c,d)] = [(c,d)] \odot [(a,b)] \\
&\iff x \odot y = y \odot x
\end{aligned}$$

- $A^{\odot}$: Let $x, y, z \in \mathbb{Z}$, $x := [(a,b)]$, $y := [(c,d)]$ and $z := [(e,f)]$. On one hand,

$$\begin{aligned}
(x \odot y) \odot z &= [(ac+bd, ad+bc)] \odot z \\
&= [((ac+bd) \cdot e + (ad+bc) \cdot f, (ac+bd) \cdot f + (ad+bc) \cdot e)] \\
&= [(ace + bde + adf + bcf, acf + bdf + ade + bce)]
\end{aligned}$$

  On the other hand,

$$\begin{aligned}
x \odot (y \odot z) &= x \odot [(ce+df, cf+de)] \\
&= [(a \cdot (ce+df) + b \cdot (cf+de), a \cdot (cf+de) + b \cdot (ce+df))] \\
&= [(ace + adf + bcf + bde, acf + ade + bce + bdf)] \\
&= [(ace + bde + adf + bcf, acf + bdf + ade + bce)]
\end{aligned}$$

  Thus $(x \odot y) \odot z = x \odot (y \odot z)$;

- $N^{\odot}$: Let $[(a,b)] \in \mathbb{Z}$, then

$$\begin{aligned}
[(a,b)] \cdot 1_{\mathbb{Z}} &= [(a,b)] \cdot [(1,0)] \\
&= [(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)] \\
&= [(a+0, 0+b)] \\
&= [(a,b)]
\end{aligned}$$

- $D^{+,\odot}$: Let $x, y, z \in \mathbb{Z}$, $x := [(a, b)]$, $y := [(c, d)]$ and $z := [(e, f)]$.

$$\begin{aligned} x \odot (y + z) &= [(a, b)] \odot [(c + e, d + f)] \\ &= [(a \cdot (c + e) + b \cdot (d + f), a \cdot (d + f) + b \cdot (c + e))] \\ &= [(ac + ae + bd + bf, ad + af + bc + be))] \\ &= [(ac + bd + ae + bf, ad + bc + af + be)] \\ &= [(ac + bd, ad + bc)] \oplus [(ae + bf, af + be)] \\ &= x \odot y \oplus x \odot z \end{aligned}$$

Hence all laws hold under the imposed conditions. □

Remark. You have been lied to in elementary/high school (again). Rather obviously, $\mathbb{N} \subseteq \mathbb{Z}$ is false. For example, $2 \in \mathbb{N}$, and $2 := \{\{\varnothing\}\}$. Similarly, $[(2, 0)] \in \mathbb{Z}$, and $[(2, 0)]$ is an infinite set of all natural number pairs (a, b) such that $a - b = 2$. Elements of $\mathbb{Z}$ have no resemblance whatsoever to elements of $\mathbb{N}$.

4.3 Embedding of N into Z

Definition 4.6. Let the following be a map:

$$\begin{aligned} \text{int} : \mathbb{N} &\to \mathbb{Z} \\ n &\mapsto [(n, 0)] \end{aligned}$$

Claim 4.3. int *is injective.*

Proof. Let $a, a' \in \mathbb{N}$. Suppose $\text{int}(a) = \text{int}(a')$. This implies that $[(a, 0)] = [(a', 0)]$. By definition of the equivalence of integers, $a + 0 = 0 + a'$. By associativity and the definition of addition on the naturals, $a = a'$. Thus int is injective. □

Theorem 4.2. int *is an* ***embedding*** *of* $(\mathbb{N}, +, \cdot)$ *into* $(\mathbb{Z}, \oplus, \odot)$. *That is, the following conditions must hold:*

- $\forall n, m \in \mathbb{N} : \text{int}(n + m) = \text{int}(n) \oplus \text{int}(m)$
- $\forall n, m \in \mathbb{N} : \text{int}(n \cdot m) = \text{int}(n) \odot \text{int}(m)$
- $\text{int}(0) = 0_{\mathbb{Z}}$
- $\text{int}(1) = 1_{\mathbb{Z}}$

Proof. Let $n, m \in \mathbb{N}$. Then:

- $\text{int}(n + m) = [(n + m, 0)] = [(n, 0)] \oplus [(m, 0)] = \text{int}(n) \oplus \text{int}(m)$;
- Similarly,

$$\begin{aligned} \text{int}(n \cdot m) &= [(nm, 0)] \\ &= [(nm + 0 \cdot 0, n \cdot 0 + 0 \cdot m)] \\ &= [(n, 0)] \odot [(m, 0)] \\ &= \text{int}(n) \odot \text{int}(m) \end{aligned}$$

- $\text{int}(0) = [(0, 0)] = 0_{\mathbb{Z}}$;
- $\text{int}(1) = [(1, 0)] = 1_{\mathbb{Z}}$.

□

For that reason, morally you can think $\mathbb{N} \subseteq \mathbb{Z}$.

Example. Traditional notation: let $n \in \mathbb{N}$, then $\text{int}(n) = [(n,0)]$, $-\text{int}(n) = [(0,n)]$. That way, any integer $[(a,b)]$ can be written as

$$\begin{cases} [(n,0)] & \text{if } a \geq b \iff \exists m \in \mathbb{N} : a = b + m \\ [(0,n)] & \text{if } a < b \iff \exists m \in \mathbb{N}^* : b = a + m \end{cases}$$

(this fact can be very trivially shown). Hence proven that any integer can be written as '$\text{int}(n)$' or '$-\text{int}(n)$' where n is a natural number. Now, in order to arrive at the traditional notation, we leave out the int in order to save chalk, I suppose. Now, it 'makes sense' to write $5 + (-7)$.

4.4 Construction of $\mathbb{Q}$

Definition 4.7. Define the following relation:

$$\approx \subseteq (Z \times Z^*) \times (Z \times Z^*)$$

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

Morally, $\frac{a}{b} = \frac{c}{d} \iff ad = bc$.

Claim 4.4. *$\approx$ is an equivalence relation.*

Proof. We need to show all properties of an equivalence relation:

- reflexivity: $(a,b) \approx (a,b) \iff ab = ba$ which is true;
- symmetry: $(a,b) \approx (c,d) \iff ad = bc \iff cb = da \iff (c,d) \approx (a,b)$;
- transitivity: Given $(a,b) \approx (c,d) \wedge (c,d) \approx (e,f)$, we can deduce that $ad = bc$ and $cf = de$. Equivalently, $ade = bce$ and $acf = ade$, respectively. Then, $bce = acf$ and $af = be$, which is equivalent to $(a,b) \approx (e,f)$.

□

Definition 4.8. $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^*)/_{\approx}$

This relates to the traditional notation, e.g. $\frac{a}{b} := [(a,b)]_{\approx}$.

4.5 Addition and multiplication on $\mathbb{Q}$

Definition 4.9. Define the following map:

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

$$[(a,b)] \boxplus [(c,d)] := [(ad \oplus bc, bd)]$$

This is again morally related to fractions as we know them already:

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

Definition 4.10. Define the following map:

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

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

Claim 4.5. *$\boxplus$ and $\boxdot$ are well-defined.*

Proof. Let $[(a,b)],[(c,d)],[(a',b')],[(c',d')] \in \mathbb{Q}$. Assume $(a,b) \approx (a',b')$ and $(c,d) \approx (c',d')$, i.e. they belong to the same equivalence classes. From these statements it clearly follows that $a \odot b' = a' \odot b$ and $c \odot d' = c' \odot d$ (for clarity I will now omit the $\odot$, just know that it is there).
Let us first prove that $\boxplus$ is well-defined. We start with a tautology:

$$\begin{aligned}
&[(ad \oplus bc, bd)] = [(ad \oplus bc, bd)] \\
\iff &[(ad \oplus bc, bd)] = [(adb'c' \oplus b'c'bc, b'dbc')] \\
\iff &[(ad \oplus bc, bd)] = [(a'd'bc \oplus b'c'bc, b'd'bc)] \\
\iff &[(ad \oplus bc, bd)] = [(a'd' \oplus b'c', b'd')] \\
\iff &[(a,b)] \boxplus [(c,d)] = [(a',b')] \boxplus [(c',d']
\end{aligned}$$

Let us now prove that $\boxdot$ is well-defined. We again start with a tautology:

$$\begin{aligned}
&\iff acb'd' = acb'd' \\
&\iff acb'd' = a'c'bd \\
&\iff (ac, bd) \approx (a'c', b'd') \\
&\iff [(ac, bd)] = [(a'c', b'd')] \\
&\iff [(a,b)] \boxdot [(c,d)] = [(a',b')] = [(c',d')]
\end{aligned}$$

□

The following definition is not from lecture, but from the finger practice.

Definition 4.11. Define the map

$$\begin{aligned}
(\,)^{-1} &: \mathbb{Q}^* \times \mathbb{Q}^* \\
[(a,b)]^{-1} &:= (b,a)^{-1}
\end{aligned}$$

Claim 4.6. $(\,)^{-1}$ *is well-defined.*

Proof. Take $x = [(a,b)]$ and $x' = [(a',b')]$, and assume $x = x'$. In other words, $(a,b) \approx (a',b')$. Equivalently, $ab' = a'b$. To show well-definedness we want to show that these assumptions imply that $x^{-1} = x'^{-1}$. We start with a tautology:

$$\begin{aligned}
&a'b = a'b \\
\iff &ba' = ab' \\
\iff &(b,a) \approx (b',a') \\
\iff &[(b,a)] = [(b',a')] \\
\iff &[(a,b)]^{-1} = [(a',b')]^{[} - 1] \\
\iff &x^{-1} = x'^{-1}
\end{aligned}$$

□

Theorem 4.3. *For all* $x \in \mathbb{Q}$, $x \boxdot x{-}1 = 1_{\mathbb{Q}}$ *(where* $1_{\mathbb{Q}} = [(1,1)]$*).*

Proof. Let $a \in \mathbb{Z}$, $b \in Z^*$ and $x = [(a,b)]$. Then

$$\begin{aligned}
x \boxdot x^{-1} &= [(a,b)] \boxdot [(a,b)]^{-1} \\
&= [(a,b)] \boxdot [(b,a)] \\
&= [(ab, ba)] \\
&= [(1,1)]
\end{aligned}$$

The last step should probably be more justified: $(ab, ab) \approx (1,1) \iff ab \odot 1 = ab \odot 1$ which is a tautology. This also morally shows that the map $(\,)^{-1}$ produces a multiplicative inverse, which is a property of a field. □