6. Integers and rationals

Having discussed a full set-theoretical construction of the naturals, we will now take a somewhat lighter approach to the construction of the integers and rationals. For more abstract approaches we refer the reader to standard textbooks in set theory.

6.1 The integers.

Recall that, for $m, n \in \mathbb{N}$ the relation $m \leqslant n$ is equivalent to the existence of a natural $r \in \mathbb{N}$ such that $n = m + r$. We will call that r the *difference* between m and n with the notation $r = n - m$. Unfortunately, the existence of the symbol $n - m$ is restricted to the pairs $(m, n) \in \mathbb{N}$ with $m \leqslant n$. To eliminate this restriction, we enlarge the naturals (4.1) into the set of the *integers* that, informally, takes the form

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}. \tag{6.1}$$

This is again too vague due to the usage of the dots and so we have to proceed more formally. First introduce a relation $\overset{+}{\sim}$ on $\mathbb{N} \times \mathbb{N}$ by setting

$$(m, n) \overset{+}{\sim} (m', n') := \; m + n' = n + m'. \tag{6.2}$$

for any $m, n, m', n' \in \mathbb{N}$. We then observe:

Lemma 6.1 *$\overset{+}{\sim}$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Proof. Reflexivity and symmetry are immediate from the definition so we just have to prove transitivity. Suppose $m, n, m', n' \in \mathbb{N}$ are such that

$$(m, n) \overset{+}{\sim} (m', n') \;\wedge\; (m', n') \overset{+}{\sim} (m'', n''). \tag{6.3}$$

Then we have

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

Using the associative and commutative law of the addition, from here we get

$$m + n'' + n' \overset{(1)}{=} m' + n + n'' \overset{(2)}{=} m'' + n + n'. \tag{6.4}$$

Lemma 5.5 then gives $m + n'' = m'' + n$ and so $(m, n) \overset{+}{\sim} (m'', n'')$. □

Roughly speaking, the equivalence $(m, n) \overset{+}{\sim} (m', n')$ means that $m - n$ represents the same integer as $m' - n'$. To factor out all possible representations of one integer as the difference of two naturals, we recall the concept of a equivalence class $[x]$ represented by element x defined in (3.9) and set

$$\mathbb{Z} := \big\{[(m, n)] \colon m, n \in \mathbb{N}\big\}. \tag{6.5}$$

We will call the elements of $\mathbb{Z}$ *integers*. Informally, the equivalence class $[(m, n)]$ represents an integer "$m - n$" with "positive part" m and "negative part" n; the equivalence ensures that adding any natural to both parts simultaneously does not change the result. This in fact characterizes equivalent pairs:

Lemma 6.2 *For each $m, n, m', n' \in \mathbb{N}$:*

$$\big((m, n) \overset{+}{\sim} (m', n') \;\wedge\; m \leqslant m'\big) \Leftrightarrow \big(\exists k \in \mathbb{N} \colon m' = m + k \;\wedge\; n' = n + k\big) \tag{6.6}$$

Proof. The direction $\Leftarrow$ was noted before the statement. For $\Rightarrow$ we use that $m' \leqslant m$ implies $m = m' + k$ for some $k \in \mathbb{N}$. The equivalence $(m,n) \overset{+}{\sim} (m',n')$ then implies

$$m + n' = m' + n = m + k + n \tag{6.7}$$

The injectivity of addition (Lemma 5.5) allows us to "cancel" m on both sides, thus showing $n' = n + k$ as desired. □

With the integers defined, we define the unary operation of (taking a) negative as well as the binary operations of addition, subtraction and multiplication by

$$\begin{aligned} -[(m,n)] &:= [(n,m)] \\ [(m,n)] + [(m',n')] &:= [(m+m', n+n')], \\ [(m,n)] - [(m',n')] &:= [(m+n', n+m')], \\ [(m,n)] \cdot [(m',n')] &:= [(m \cdot m' + n \cdot n', m \cdot n' + m' \cdot n)]. \end{aligned} \tag{6.8}$$

These will not be meaningful (as operations on equivalence classes) until we check:

Lemma 6.3 *The integers on the right-hand side of* (6.8) *are the same for any choice of the representatives of* $[(m,n)]$ *and* $[(m',n')]$.

Proof. We will only deal with multiplication as that is the hardest case of all. Suppose $(\widetilde{m},\widetilde{n}) \in [(m,n)]$. Then also $(m,n) \in [(\widetilde{m},\widetilde{n})]$. The fact that $\leqslant$ is a total ordering implies that either $m \leqslant \widetilde{m}$ or $\widetilde{m} \leqslant m$. By symmetry, we may thus assume that $m \leqslant \widetilde{m}$. Lemma 6.2 then gives $k \in \mathbb{N}$ such that $\widetilde{m} = m + k$ and $\widetilde{n} = n + k$. The laws of addition and multiplication on $\mathbb{N}$ then give

$$\begin{aligned} &\Big(\widetilde{m} \cdot m' + \widetilde{n} \cdot n', \widetilde{m} \cdot n' + m \cdot \widetilde{n}\Big) \\ &\qquad = \Big(m \cdot m' + n \cdot n' + k \cdot (m' + n'),\ m \cdot n' + m' \cdot n + k \cdot (m' + n')\Big) \\ &\qquad\qquad \overset{+}{\sim} \big(m \cdot m' + n \cdot n', m \cdot n' + m' \cdot n\big) \end{aligned} \tag{6.9}$$

Hence, the equivalence class on the right of the third line of (6.8) is independent of the choice of the representative of $[(m,n)]$. The other cases are handled analogously. □

It it interesting to note that that the set

$$\big\{[(m,0)] \colon m \in \mathbb{N}\big\} \tag{6.10}$$

is in a bijective correspondence with $\mathbb{N}$ and the addition and multiplication defined above then matches the two operations on $\mathbb{N}$. The naturals $\mathbb{N}$ are thus *naturally embedded* into (our model of) $\mathbb{Z}$. A key novelty of the integers is that subtraction acts as the inverse to addition. This is seen from

$$\begin{aligned} [(m',n')] + \big([(m,n)] - [(m',n')]\big) &= [(m',n')] + [(m+n', n+m')] \\ &= [(m+m'+n', n+m'+n')] = [(m,n)]. \end{aligned} \tag{6.11}$$

The element $[(0,0)]$ is a zero element under addition and $[(1,0)]$ is the unit element under multiplication. Abandoning the cumbersome notation of equivalence classes, similarly we also verify all other properties listed in:

Lemma 6.4 *The commutative, associative and distributive laws hold for addition and multiplication on $\mathbb{Z}$. Moreover, we have:*

(1) *(Zero element)* $\exists 0 \in \mathbb{Z}\, \forall a \in \mathbb{Z}\colon a + 0 = a$
(2) *(Negative element)* $\forall a \in \mathbb{Z}\, \exists (-a) \in \mathbb{Z}\colon a + (-a) = 0$
(3) *(Unit element)* $\exists 1 \in \mathbb{Z}\, \forall a \in \mathbb{Z}\colon 1 \cdot a = a$
(4) *(Injectivity of multiplication)* $\forall a, b, c \in \mathbb{Z}\colon a \cdot b = a \cdot c \,\wedge\, a \neq 0 \,\Rightarrow\, b = c$

We leave the proof of this lemma to the reader. Note that, by associativity of addition, the zero and negative elements (a.k.a. the additive inverse element) are necessarily unique. For similar reasons, also the unit element under multiplication is unique.

The stated properties show $\mathbb{Z}$ has the structure of a commutative ring. Note however, that the properties do not necessarily characterize $\mathbb{Z}$ — indeed, the rationals will satisfy these as well. We will eventually articulate conditions under which the rationals are unique but we will not attempt to do this for the integers.

The integers also admit a natural extension of the ordering relation $\leqslant$ via

$$[(m,n)] \leqslant [(m',n')] \quad \Leftrightarrow \quad m + n' \leqslant m' + n \tag{6.12}$$

Here the independence of the choice of a representative is quite apparent as well as the fact that the restriction of this relation to $\{[(m,0)]\colon m \in \mathbb{N}\}$ reproduces $\leqslant$ on $\mathbb{N}$. The total ordering of $\mathbb{N}$ by $\leqslant$ implies the total ordering of $\mathbb{Z}$ by $\leqslant$ as well.

6.2 The rationals.

As a consequence of expanding $\mathbb{N}$ to $\mathbb{Z}$, the equation $n = m + r$ now can be solved for $r \in \mathbb{Z}$ for all $m, n \in \mathbb{Z}$. This is, however, not true for the equation $n = m \cdot r$. This motivates us to further expand $\mathbb{Z}$. We will proceed just as before. Indeed, we start by introducing a relation on $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$ by

$$(p,q) \overset{\bullet}{\sim} (p',q') \;\Leftrightarrow\; p \cdot q' = p' \cdot q. \tag{6.13}$$

for all $(p,q), (p',q') \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$. We had to exclude zero from the allowed values in the second component in order to ensure, via part (4) of Lemma 6.4, that

$$(p,q) \overset{\bullet}{\sim} (p',q) \;\Leftrightarrow\; p = p'. \tag{6.14}$$

Lemma 3.8 then shows that $\overset{\bullet}{\sim}$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$. This permits us to set

$$\mathbb{Q} := \Big\{[(p,q)]\colon (p,q) \in \mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})\Big\} \tag{6.15}$$

Informally, the pair (p,q) stands for the fraction $\frac{p}{q}$; the equivalence relation then ensures that for any $m \in \mathbb{Z} \smallsetminus \{0\}$, the rational $\frac{pm}{qm}$ coincides with $\frac{p}{q}$.

As before, we introduce the operations of addition, subtraction, multiplication on $\mathbb{Q}$ via the formulas

$$\begin{aligned} [(p,q)] + [(p',q')] &:= \big[(p \cdot q' + q \cdot p', q \cdot q')\big] \\ [(p,q)] - [(p',q')] &:= \big[(p \cdot q' - q \cdot p', q \cdot q')\big] \\ [(p,q)] \cdot [(p',q')] &:= \big[(p \cdot p', q \cdot q')\big] \end{aligned} \tag{6.16}$$

and, assuming $[(p',q')] \neq 0$ which entails $p' \neq 0$, also the operation of *division* via

$$[(p,q)] \div [(p',q')] := \big[(p \cdot q', q \cdot p')\big]. \tag{6.17}$$

In all of these we first need to check:

Lemma 6.5 *The rationals on the right-hand side of (6.16–6.17) are the same for any choice of the representatives of* $[(p,q)]$ *and* $[(p',q')]$.

Proof (sketch). As a demonstration how the proof works, let us deal with the hardest case, which is addition. Take (p,q) and $(\tilde p,\tilde q)$ and first prove that $(p,q) \overset{\cdot}{\sim} (\tilde p,\tilde q)$ is equivalent to $\exists k,\ell \in \mathbb{Z} \smallsetminus \{0\}\colon (\tilde p\cdot\ell,\tilde q\cdot\ell) = (p\cdot k, q\cdot k)$. Then note the latter property gives

$$\begin{aligned}(\tilde p\cdot q' + \tilde q\cdot p', \tilde q\cdot q') &\overset{\cdot}{\sim} \bigl((\tilde p\cdot q' + \tilde q\cdot p')\cdot\ell, (\tilde q\cdot q')\cdot\ell\bigr)\\ &= \bigl((p\cdot q' + q\cdot p')\cdot k, (q\cdot q')\cdot k\bigr) \overset{\cdot}{\sim} (p\cdot q' + q\cdot p', q\cdot q') \qquad (6.18)\end{aligned}$$

as desired. □

The operation of division is relative to multiplication as subtraction is to addition: Indeed, assuming $[(p',q')] \neq 0$, we have

$$[(p',q')]\cdot\Bigl([(p,q)] \div [(p',q')]\Bigr) = [(p,q)] \qquad (6.19)$$

Abandoning the equivalence class notation, we then check:

Theorem 6.6 *The operations of addition and multiplication defined via (6.16–6.17) satisfy the commutative, associative and distributive laws. In addition, we have:*

(1) *(Zero element)* $\forall a \in \mathbb{Q}\colon 0 + a = a \wedge 0\cdot a = 0$,
(2) *(Unit element)* $\forall a \in \mathbb{Q}\colon 1\cdot a = a$,
(3) *(Additive inverse)* $\forall a \in \mathbb{Q}\ \exists(-a) \in \mathbb{Q}\colon a + (-a) = 0$,
(4) *(Multiplicative inverse)* $\forall a \in \mathbb{Q}\smallsetminus\{0\}\ \exists a^{-1} \in \mathbb{Q}\colon a\cdot a^{-1} = 1$.

As it turns out, the above is what gives $\mathbb{Q}$ an algebraic structure called a *field*. (We will give a definition of what it means for a set to be a field in the next lecture.) In our construction, the inverse elements in (3) and (4) are supplied by

$$-[(p,q)] = [(-p,q)] \quad\text{and}\quad [(p,q)]^{-1} = [(q,p)] \qquad (6.20)$$

while, as noted above, $0 := [(0,1)]$ and $1 := [(1,1)]$. Note also that the integers (and thus naturals) are represented inside $\mathbb{Q}$ by

$$\bigl\{[(p,1)]\colon p \in \mathbb{Z}\bigr\} \qquad (6.21)$$

The rationals admit also an extension of the relation $\leqslant$ by setting:

$$[(p,q)] \leqslant [(p',q')] \quad\Leftrightarrow\quad \begin{cases} p\cdot q' \leqslant p'\cdot q, & \text{if } q\cdot q' \geqslant 0,\\ p'\cdot q \leqslant p\cdot q', & \text{else,}\end{cases} \qquad (6.22)$$

We again readily check that the relation does not depend on the representatives of $[(p,q)]$ and $[(p',q')]$ and that it faithfully reproduces the corresponding relation on $\mathbb{Z}$. With $\leqslant$ in place, the rationals have the structure of an *ordered field* (again, to be defined next).

An inquisitive reader may wonder whether other constructions of the integers and rationals exist that would give us intrinsically different objects from those constructed above. The answer to this is negative: the set of the rationals, viewed as an ordered field, is determined uniquely up to an isomorphism — i.e., a bijection reproducing all stated structures. We will discuss this in more detail in the next lecture.