Chapter 2

The Ring $\mathbb{Z}$ of Integers

The next step in constructing the rational numbers from $\mathbb{N}$ is the construction of $\mathbb{Z}$, that is, of the (ring of) integers.

2.1 Equivalence Classes and Definition of Integers

Before we can do that, let us say a few words about equivalence relations. Given a set S, a relation $\sim$ is –mathematically speaking – a subset $E \subseteq S \times S$, and we write $s \sim t$ for $s, t \in S$ if and only if $(s, t) \in E$.

For example, if $S = \{A, B, C\}$ and $E = \{(A, B), (B, C)\}$, then $A \sim B$ and $B \sim C$, but $A \not\sim C$.

An equivalence relation is a relation having the following properties:

- reflexitivity: $s \sim s$ for all $s \in S$;
- symmetry: if $s \sim t$ for $s, t \in S$, then $t \sim s$;
- transitivity: if $s \sim t$ and $t \sim u$ for $s, t, u \in S$, then $s \sim u$.

In terms of the subset E, these properties can be stated as follows:

- reflexitivity: $(s, s) \in E$ for all $s \in S$;
- symmetry: if $(s, t) \in E$ for $s, t \in S$, then $(t, s) \in E$;
- transitivity: if $(s, t)(t, u) \in E$ for $s, t, u \in S$, then $(s, u) \in E$.

The relation defined on the set $\{A, B, C\}$ above is not an equivalence relation (why?). For any equivalence relation on a set S we can define the equivalence class of $s \in S$ as the set of all elements to which s is equivalent:

$$[s] = \{t \in S : t \sim s\}.$$

Lemma 2.1. *Equivalence classes are either disjoint or they coincide.*

Proof. Assume that $[s] \cap [t]$ is nonempty; then there is an element $x \in S$ such that $x \in [s]$ and $x \in [t]$. By definition, this implies $x \sim s$ and and $x \sim t$. Since $\sim$ is an equivalence relation, we deduce $s \sim x$ and $x \sim t$, hence $s \sim t$, so $t \in [s]$ and $s \in [t]$. But then $[s] \subseteq [t]$: $y \in [s]$ implies $y \sim s$, which together with $s \sim t$ gives $y \sim t$, hence $y \in [t]$. By symmetry, we also have $[t] \subseteq [s]$, hence $[s] = [t]$. □

Here's how to do create integers. We can represent every natural number n as a difference of two natural numbers in many ways, e.g. $2 = 3 - 1 = 4 - 2 = 5 - 3 = \ldots$. Thus we can represent 2 by the pairs $(2, 0)$, $(3, 1)$, $(4, 2)$, etc. of natural numbers. If we already knew negative numbers, then of course $-2 = 1 - 3 = 2 - 4 = \ldots$ would be represented by the pairs $(0, 2)$, $(1, 3)$, $(2, 4)$, etc. The idea is now to turn everything around and create negative integers using pairs (m, n) of natural numbers.

We define an equivalence relation on the set

$$W = \{(m, n) : m, n \in \mathbb{N}\}$$

of such pairs by putting $(m, n) = (m', n')$ if $m + n' = m' + n$. This is indeed an equivalence relation because it is

- reflexive: $(m, n) \sim (m, n)$;
- symmetric: $(m, n) \sim (m', n') \Longrightarrow (n', m') \sim (m, n)$;
- transitive: $(n, m) \sim (n', m')$ and $(n', m') \sim (n'', m'') \Longrightarrow (n, m) \sim (n'', m'')$.

For example, $(m, n) \sim (m, n)$ holds because $m + n = n + m$ for $m, n \in \mathbb{N}$.

Now let $[m, n] = \{(x, y) : (x, y) \sim (m, n)\}$ denote the equivalence class of (m, n), and let $\mathbb{Z} = \{[m, n] : m, n \in \mathbb{N}\}$ denote the set of all equivalence classes.

We can make $\mathbb{N}$ into a subset of $\mathbb{Z}$ by identifying a natural number n with the equivalence class $[n, 0]$. Moreover, we shall simply write $-n$ for the class $[0, n]$ and put $0 = [0, 0]$ (this is a generally accepted abuse of notation: the neutral element in any additive group is usually denoted by 0).

This 'identification' can be given a precise mathematical formulation by introducing the map $\iota : \mathbb{N} \longrightarrow \mathbb{Z}$ that identifies $\mathbb{N}$ with a subset of $\mathbb{Z}$: we put $\iota(n) = [n, 0]$. Now we only are able to 'identify' $\mathbb{N}$ with its image $\iota(\mathbb{N}) \subseteq \mathbb{Z}$ if ι does not map two natural numbers to the same integer, that is, if ι is injective. Let's check this: assume that $\iota(m) = \iota(n)$, i.e., that $[m, 0] = [n, 0]$. By definition of these equivalence classes this means that $(m, 0) \sim (n, 0)$, that is, $m+0 = n+0$. This implies $m = n$, hence ι is injective.

We remark that

$$\mathbb{Z} = \{\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

To see this, we have to prove that every $(m, n) \in W$ is equivalent to exactly one element in $\{-2, -1, 0, 1, 2, \ldots\}$. This follows from the Trichotomy Law: for

example, if $m > n$, then $m = n + z$ for some nonzero $z \in \mathbb{N}$, hence $[m, n] = [n + z, n] = [z, 0]$ etc.

We now show that we can define addition, multiplication and an order $<$ on $\mathbb{Z}$ in such a way that the properties of $\mathbb{N}$ proved in Chapter 1 continue to hold.

2.2 Addition

We start by defining addition $\oplus$ on $\mathbb{Z}$. We have to say what $[r, s] \oplus [t, u]$ is supposed to be. Clearly we would like to have $[r, s] = r - s$, $[t, u] = t - u$, so the sum should be $r - s + t - u = r + t - (s + u) = [r + t, s + u]$. With this idea in mind we now define

$$[r, s] \oplus [t, u] = [r + t, s + u], \tag{2.1}$$

where the addition inside the brackets is the addition in $\mathbb{N}$.

Now there's some work to do. First we have to prove that this addition is well defined (this is something that comes up whenever we define something on equivalence classes). What this means is: assume that $[r, s] = [r', s']$ and $[t, u] = [t', u']$. On the one hand, we have

$$[r, s] \oplus [t, u] = [r + t, s + u].$$

If we replace the left hand side by $[r', s'] \oplus [t', u']$, then we clearly get

$$[r', s'] \oplus [t', u'] = [r' + t', s' + u'].$$

But if our addition is to make any sense, then the right hand sides should be equal because, after all, the left hand sides are. Thus we want to show that

$$[r' + t', s' + u'] = [r + t, s + t]. \tag{2.2}$$

We know that $[r, s] = [r', s']$, which by definition means $(r, s) \sim (r', s')$, that is, $r + s' = s + r'$. Similarly, $[t, u] = [t', u']$ implies $t + u' = u + t'$. Adding these equations and using commutativity and associativity for natural numbers we get $r + t + s' + u' = s + u + r' + t'$, which in turn is equivalent to (2.2).

Next we have to show that the two additions agree on $\mathbb{N}$; after all, we are using the very same symbols for natural numbers 1, 2, ... and their images 1, 2, ... under ι in $\mathbb{Z}$. This can only work if, for natural numbers m, n, the sum $m + n$ is the same whether evaluated in $\mathbb{N}$ or in $\mathbb{Z}$. In other words: we want to be sure that

$$\iota(m + n) = \iota(m) \oplus \iota(n).$$

This is a straight forward computation:

$$\begin{array}{rcll} \iota(m) \oplus \iota(n) & = & [m, 0] \oplus [n, 0] & \text{by definition of } \iota \\ & = & [m + n, 0] & \text{by (2.1)} \\ & = & \iota(m + n) & \text{by definition of } \iota \end{array}$$

Now that there is no need to distinguish between the two types of addition anymore, we shall often write $+$ instead of $\oplus$ for the addition on $\mathbb{Z}$.

Of course we have prove that associativity and commutativity also hold for our addition in $\mathbb{Z}$. So why is $(x+y)+z = x+(y+z)$ for all $x, y, z \in \mathbb{Z}$? Write $x = [r,s]$, $y = [t,u]$ and $z = [v,w]$ with $r,s,t,u,v,w \in \mathbb{N}$. Then $(x+y)+z = [r+t, s+u] + [v,w] = [(r+t)+v, (s+u)+w]$, and similarly $x+(y+z) = [r+(t+v), s+(u+w)]$. Because addition in $\mathbb{N}$ is associative, so is addition in $\mathbb{Z}$ (again, observe that there's no need for invoking induction here).

Exercise. Prove that addition on $\mathbb{Z}$ is commutative.

For defining subtraction $x - y$ in $\mathbb{Z}$, we write $x = [r,s]$ and $y = [t,u]$; we cannot put $x - y = [r-t, s-u]$ because $r-t$ and $s-u$ might not be natural numbers; but if they were, we would have $[r-t, s-u] = [r+u, s+t]$, and nothing prevents us from defining

$$[r,s] \ominus [t,u] = [r,s] \oplus [u,t] = [r+u, s+t]. \tag{2.3}$$

Note that $\ominus$ is well defined because the right hand side is. Now it is easy to prove that $\mathbb{Z}$ is a group with respect to addition, and that $0 = [0,0]$ is the neutral element.

What does that mean? A group is a set G of elements together with a composition, that is, a map $+ : G \times G \longrightarrow G$ that maps a pair of elements $(g, g') \in G \times G$ to another element $g + g' \in G$; we also demand that this composition satisfy the following rules:

G1 there is a neutral element $0 \in G$ such that $g + 0 = g$ for all $g \in G$;

G2 for every $g \in G$ there is an element $g' \in G$ such that $g + g' = 0$ (we shall write $g' = -g$);

G3 the composition is associative: we have $(g + g') + g'' = g + (g' + g'')$ for all $g, g', g'' \in G$.

If the group also satisfies the condition

G4 $g + g' = g' + g$ for all $g, g' \in G$;

then we say that G is commutative (abelian).

The set $\mathbb{N}$ of natural numbers is not a group with respect to $+$: there is a composition $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, but the element $1 \in \mathbb{N}$ has no inverse. In fact, if $n+1 = 0$ were solvable in $\mathbb{N}$, then 0 would be the successor of n in contradiction to Peano's axiom N3.

The set $\mathbb{Z}$ of integers, on the other hand, is a group with respect to $+$. In fact, $\mathbb{Z}$ is not only a group, it also carries the structure of a ring. But in order to see this, we have to define multiplication in $\mathbb{Z}$ first.

2.3 Multiplication

In order to define multiplication on $\mathbb{Z}$, let us think of $[r,s]$ as the 'integer' $r-s$; then we want $[r,s]\odot[t,u]\simeq(r-s)(t-u)=rt+su-ru-st\simeq[rt+su,ru+st]$, and this suggests the definition

$$[r,s]\odot[t,u]=[rt+su,ru+st]. \tag{2.4}$$

Once more we have to show that the multiplication (2.4) is well defined and that it agrees with multiplication in $\mathbb{N}$ (actually we have defined it in such a way that it must; what we have to check here is that $\iota(m)\odot\iota(n)=\iota(mn)$). Then one generalizes distributivity, commutativity, associativity and the cancellation law to integers in $\mathbb{Z}$.

Let us just note in passing that

$$\begin{array}{rcll}(-1)\cdot(-1) & = & [0,1]\odot[0,1] & \text{by our identification}\\ & = & [1,0] & \text{by (2.4)}\\ & = & +1 & \text{since } \iota(1)=[2,1]\end{array}$$

More generally, for $m,n\in\mathbb{Z}$ we now can prove that

$$\begin{aligned}(-m)\cdot\ \ n &= -mn,\\ m\cdot(-n) &= -mn,\\ (-m)\cdot(-n) &= \ \ mn.\end{aligned}$$

Thus the rules for multiplying signs come out naturally from our definition of multiplication on $\mathbb{Z}$.

Now we are ready to state that $\mathbb{Z}$ is a ring. A ring R is a set on which two kinds of compositions are defined; they are usually denoted by $+$ (addition) and $\cdot$ (multiplication). Of course, these compositions are to satisfy certain conditions; first of all, $r+s$ and $r\cdot s$ should be elements of R whenever r and s are. Moreover, we demand

R1 R is an abelian group with respect to $+$;

R2 (associativity): $r(st)=(rs)t$ for $r,s,t\in R$;

R3 (distributivity): we have $r(s+t)=rs+rt$ and $(r+s)t=rt+st$ for $r,s,t\in R$.

R4 R contains a unit element $e\neq 0$ satisfying $er=re=r$ for all $r\in R$;

The element e in $R4$ is usually denoted by 1. Note that every ring has at least two elements since $1\neq 0$ by R4.

If R also satisfies $rs=sr$ for all $r,s\in R$, then we say that R is commutative. Finally, a ring R is called an integral domain if $xy=0$ implies $x=0$ or $y=0$.

In any ring we have $0x=0$: in fact,

$$\begin{array}{rcll}0x & = & (0+0)x & \text{since 0 neutral element of } +\\ & = & 0x+0x & \text{by distributivity,}\end{array}$$

so substracting $0x$ from both sides gives $0=0x$.

Theorem 2.2. *The integers $\mathbb{Z}$ form a commutative integral domain with respect to addition and multiplication.*

Let us prove that $\mathbb{Z}$ is indeed an integral domain.

Assume that $xy = 0$ for $x, y \in \mathbb{Z}$. Write $x = [r, s]$ and $y = [t, u]$. Then $[0, 0] = 0 = xy = [r, s] \odot [t, u] = [rt + su, ru + st]$ by assumption, hence $rt + su = ru + st$.

Now assume that $x \neq 0$; then $r + m = s$ or $r = s + m$ for some $m \in \mathbb{N}$ by the Trichotomy Law for Addition. In the first case, $r + m = s$ for some $m \in \mathbb{N}$. Then $rt + (r + m)u = rt + su = ru + st = ru + (r + m)t$, hence $mu = mt$ and so $u = t$, that is, $y = 0$. The case $r > s$ is treated similarly.

2.4 $\mathbb{Z}$ as an ordered domain

Last not least we have to extend the relation $<$ to $\mathbb{Z}$. We put

$$[r, s] < [t, u] \quad \text{if} \quad r + u < t + s. \tag{2.5}$$

This is well defined and agrees with the ordering on $\mathbb{N}$.

For showing that the relation is well defined, we have to assume that $(r, s) \sim (r', s')$ and $(t, u) \sim (t', u')$, and then show that $r+u < t+s$ implies $r'+u' < t'+s'$.

For showing that the order just defined agrees with the one we know from $\mathbb{N}$ we have to prove that $n < m$ if and only if $\iota(n) < \iota(m)$.

Proposition 2.3. *The set $\mathbb{Z}$ is simply ordered with respect to $<$.*

An ordered domain is a domain R together with an order $<$ such that
OD1 R is simply ordered with respect to $<$.
OD2 If $x < y$, then $x + z < y + z$ for $x, y, z \in R$.
OD3 If $x < y$ and $0 < z$, then $xz < yz$.

Proposition 2.4. *$\mathbb{Z}$ is an ordered domain with respect to $<$.*

Proof. Write $x = [r, s]$ and $y = [t, u]$. If $z \in \mathbb{N}$, then we may put $z = [v, 0]$. By definition, $x < y$ means $r + u < t + s$, and $xz < yz$ is equivalent to $(r + u)v < (t + s)v$. Since $v \in \mathbb{N}$, this is clear.

The rest is left as an exercise. □

Proposition 2.5. *In any ordered domain R, the following assertions are true:*

1. *If $x < 0$, then $-x > 0$.*
2. *If $x < y$ and $z < 0$, then $xz > yz$.*
3. *We have $x^2 \geq 0$ for all $x \in R$, with equality if and only if $x = 0$.*

Proof. 1. If $x < 0$, then $x + (-x) < 0 + (-x)$ by OD2, and so $0 < -x$.

2. We have $0 < -z$, hence $-xz = x \cdot (-x) < y \cdot (-z) = -yz$, hence $xz > yz$.

3. If $x \geq 0$, then multiplying through by $x \geq 0$ gives $x^2 \geq= 0$; if $x \leq 0$, then multiplying through by $x \leq 0$ gives $x^2 \geq 0$.

□

We now introduce absolute values in any ordered domain by putting

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

Here are a few simple properties of absolute values:

Lemma 2.6. *In any ordered domain R, the absolute value $|\cdot|$ has the following properties.*

1. $|x| \geq 0$.
2. $|xy| = |x| \cdot |y|$.
3. *If $s \geq 0$ and $-s \leq r \leq s$, then $|r| \leq s$.*

Proof. 1. is clear if $x \geq 0$; if $x < 0$, multiply through by $-1 < 0$.

2. Just consider the four possible cases: a) if $x > 0$, $y > 0$, then $xy > 0$, so the claim is $xy = xy$, which obviously holds; b) if $x > 0$ and $y < 0$, then $xy < 0$, hence the claim is $-xy = x \cdot (-y)$. The other two cases are treated similarly.

3. In fact, it is sufficient to prove that $r \leq s$ and $-r \leq s$. The first one is true by assumption, the second one follows from multiplying $-s \leq r$ through by -1. □

The following inequality is important:

Proposition 2.7 (Triangle Inequality)**.** *For all x, y in an ordered domain, we have $|x + y| \leq |x| + |y|$.*

Proof. By adding $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$ we obtain $-(|x| + |y|) \leq x + y \leq |x| + |y|$. Now apply Lemma 2.6.3 to $r = x + y$ and $s = |x| + |y|$. □

Division with Remainder

The following property of the integers is the basis for the arithmetic of $\mathbb{Z}$:

Theorem 2.8. *For every pair $a, b \in Z$ with $b > 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. The proof that q and r are unique is the same as in the proof of the analogous result in $\mathbb{N}$. This result also takes care of the existence of q and r if $a \geq 0$. Assume therefore that $a < 0$; then there exist q', r' such that $-a = bq' + r'$ with $0 \leq r' < b$. Thus $a = b(-q') + (-r')$, and we may take $q = -q'$, $r = -r'$ if $r' = 0$, and $q = -q' - 1$ and $r = -r' + b$ if $r' < 0$. □

2.5 Historical Remarks

Already Diophantus had discovered rules like $(a-b)(c-d) = ac - bc - ad + bd$ for positive rational numbers $a > b$ and $c > d$, but his books do not contain any negative numbers. Negative numbers were, just as 0, invented by the Hindus (around 600 AD or earlier) and the Chinese (before 1100 AD). Although their positional system found its way into the Arabic world, negative numbers did not: they were not accepted as valid solutions by the Arabs. Leonardo di Pisa (also known by his nickname Fibonacci, which he was given by a mathematician of the 19th century, and which stuck), son of a merchant travelling around the Mediterranean, made Arabic numbers known in Europe; his books even contain some negative numbers (which are interpreted as debt), but they were not accepted as useful. Thus when Italian mathematicians discovered the solution of the cubic, they treated $x^3 + 3x + 1 =$ and $x^3 + 3x = 1$ etc. as being different kind of cubics, and therefore had to distinguish a lot of cases. After Fermat and Descartes had started analytic geometry, negative numbers became 'visible' as solutions e.g. to quadratic equations that simply were to the left of the y-axis, yet negative solutions were called 'false solutions'. Newton was one of the first who used negative numbers freely in analytic geometry.

Here are some bits and pieces from the history of negative numbers:

- Nicolas Chuquet (1445–1488) wrote *Triparty en la science des nombres*, in which he worked with equations having negative numbers as coefficients; this book was, however, lost for a long time and was published only in 1880.
- Michael Stifel's (1487–1567) book *arithmetica integra* explains how to work with negative numbers, which he calls 'numeri absurdi' or 'numeri ficti infra nihil'.
- Cardano allows negative numbers as solutions if they can be interpreted as debt. In his theory of cubics, he does not allow negative coefficients.
- Simon Stevin (1548–1620) accepts negative numbers.
- René Descartes (1596–1650) called negative solutions of polynomial equations false roots.
- Thomas Harriot (1560–1621) claimed that equations do not have negative solutions; rather the negative solutions of $f(x) = 0$ are the positive solutions of $f(-x) = 0$.
- John Wallis claimed that negatives do not exist, but that they are useful to work with.
- Leibniz stumbled over the following problem in 1712: he observed that $\frac{1}{-1} = \frac{-1}{1}$ and claimed that this shows that $-1 < 0$ is false; otherwise the numerator on the left is bigger than the denominator, on the right it's the other way round, yet the two fractions are equal.

- Auguste de Morgan in 1831:

> It is astonishing that the human intellect should ever have tolerated such an absurdity as the idea of a quantity less than nothing, above all, that the notion should have outlived the belief in judicial astronomy and the existence of witches, either of which is ten thousand times more probable.

Here's another one:

> The imaginary expression $\sqrt{-a}$ and the negative expression $-b$, have this resemblance, that either of them occurring as the solution of a problem indicates some inconsistency or absurdity. As far as real meaning is concerned, both are imaginary, since $0 - a$ is as inconceivable as $\sqrt{-a}$.

His father-in-law William Frend had this to say about negative numbers in 1796:

> (A number) submits to be taken away from a number greater than itself, but to take it away from a number less than itself is ridiculous. Yet this is attempted by algebraists who talk of a number less than nothing; of multiplying a negative number into a negative number and thus producing a positive number; of a number being imaginary. ... This is all jargon, at which common sense recoils; but, from its having been once adopted, like many other figments, it finds the most strenuous supporters among those who love to take things upon trust and hate the colour of serious thought.

Exercises

2.1 Show that $[r, s] * [t, u] = [rt, su]$ is not well defined on $\mathbb{Z}$.

2.2 Prove the following rules for $n, m \in \mathbb{Z}$:

1. $-(n + m) = -n - m$;
2. $-(n - m) = m - n$;
3. $-(-n) = n$.

2.3 Show that if $a < b$ and $c < d$, then $a + c < b + d$.