MT241P FINITE MATHEMATICS

1. Natural Numbers, Integers and Rational Numbers

Definition 1.1. *A* **Ring** *is a set R together with two operations of addition $+$ and multiplication $\cdot$, where the following rules hold, for $a, b, c \in R$:*

(R1) $a + b = b + a$ *(addition is commutative);*
(R2) $a + (b + c) = (a + b) + c$ *(addition is associative);*
(R3) $a + 0 = a = 0 + a$ *(0 is the additive identity);*
(R4) *there exists an integer x such that $a + x = 0 = x + a$. We denote x by $-a$ (existence of additive inverses);*
(R5) $a \cdot b = b \cdot a$ *(multiplication is commutative);*
(R6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *(multiplication is associative);*
(R7) $a \cdot 1 = a = 1 \cdot a$ *(1 is the multiplicative identity);*
(R8) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$ *(multiplication distributes over addition);*

Remark 1.2. (Natural Numbers)

In the following we want to define the natural numbers using the five **Peano Axioms**. *To this end let X be a set such that :*

(PA1) $0 \in X$*, that is, X has at least one element*
(PA2) *there is a function $S : X \to X$, called the* **successor function**,
(PA3) *there is no $x \in X$ such that $S(x) = 0$,*
(PA4) *if $S(x) = S(y)$, then $x = y$,*
(PA5) *(Axiom of Induction) If K is a subset of X such that*
(a) $0 \in K$ and
(b) if $x \in K$ then $S(x) \in K$,
then $K = X$.

By (PA1) there is an element $0 \in X$. (PA2) implies that $S(0)$ exists and it differs from 0, by (PA3). Now, by (PA2), an element $S(S(0))$ exists, which differs from 0, by (PA3), and differs from $S(0)$, by (PA4). Going on like this we get a sequence of distinct elements

$$(\star) \quad 0, S(0), S(S(0)), S(S(S(0))), \ldots$$

This alone will not describe the natural numbers as we know them, because so far all of this also holds true for instance for the interval $[0, \infty)$ of real *numbers, where* 0 *is the real number zero and* $S(x) = x + 1$*. However, (PA5) ensures that every element in* X *is the successor of another element. Because let* K *be the list* $(\star)$ *of elements. Then* K *satisfies conditions (PA5a) and (PA5b), and therefore* $K = X$*. In particular* X *is restricted to only elements on the list and therefore cannot be* $[0, \infty)$*.*

We agree to the following notation:

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

and we denote X *by* $\mathbb{N}$ *and call it the* **natural numbers***. In particular* $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$*.*

We define an addition (+) and a multiplication $(\cdot)$ *on* $\mathbb{N}$*. For all* $m, n \in \mathbb{N}$*:*

$$(A1)\ m + 0 := m \qquad (M1)\ m \cdot 0 := 0$$

$$(A2)\ m + S(n) := S(m + n) \qquad (M2)\ m \cdot S(n) := m + (m \cdot n)$$

One can show that $(\mathbb{N}, +, \cdot)$ *satisfies all ring properties except for (R4).*

Remark 1.3. (Integers)

For two $m, n \in \mathbb{N}$ *the equation* $m + x = n$ *may or may not have a solution for* x *in* $\mathbb{N}$*. Let the pair* $(n, m) \in \mathbb{N} \times \mathbb{N}$ *represent the equation. Then we say two equations* $(n_1, m_1), (n_2, m_2)$ *are* **equivalent** *if* $n_1 + m_2 = n_2 + m_1$*. One can show that the elements*

$$X := \{(0, 0), (1, 0), (0, 1), (2, 0), (0, 2), (3, 0), (0, 3), \ldots\}$$

are all non-equivalent, but every element $(n, m) \in \mathbb{N} \times \mathbb{N}$ *is equivalent to precisely one of them. Furthermore we define an addition and multiplication on* $\mathbb{N} \times \mathbb{N}$ *as follows:*

(Addition) $(n_1, m_1) + (n_2, m_2) := (n_1 + n_2, m_1 + m_2)$

(Multiplication) $(n_1, m_1) \cdot (n_2, m_2) := (n_1 \cdot n_2 + m_1 \cdot m_2, n_1 \cdot m_2 + n_2 \cdot m_1)$*, for all* $n_1, n_2, m_1, m_2 \in \mathbb{N}$*.*

If we identify each (n, m) *with its equivalence companion in* X*, then one can show that* $(X, +, \cdot)$ *is a ring. If we identify the element* $(n, 0)$ *with* $n \in \mathbb{N}$*, then* X *contains* $\mathbb{N}$*. Furthermore* $(0, n)$ *is the additive inverse of* $(n, 0)$ *and thus can be written as* $-n$*. Overall we denote the set* X *by* $\mathbb{Z}$ *and call it the* **integers***. In particular we have*

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

There is an **order** *on* $\mathbb{Z}$*. For* $a, b \in \mathbb{Z}$ *we write* $a < b$ *if there is an* $x \in \mathbb{N} \setminus \{0\}$ *such that* $a + x = b$*, or in other words* $(-a) + b \in \mathbb{N} \setminus \{0\}$*.*

If $(-a) + b \notin \mathbb{N} \setminus \{0\}$*, then either* $(-a) + b = 0$*, that is,* $a = b$*, or* $(-a) + b = -c$*, for some* $c \in \mathbb{N} \setminus \{0\}$*. The latter gives* $b + c = a$ *and therefore* $b < a$*. Thus* *precisely one of the following is true:*

$$a < b, \quad a = b, \quad b < a.$$

Furthermore we write $a \leq b$ *if* $a < b$ *or* $a = b$*, we write* $a > b$*, if* $b < a$ *and we write* $a \geq b$ *if* $b \leq a$*.*

Next note that for every $a \in \mathbb{Z}$ *we have* $0 < a$ *if and only if* $a \in \mathbb{N} \setminus \{0\}$ *and we call those integers* **positive***. Moreover* $a < 0$ *if and only* $a \in \mathbb{Z} \setminus \mathbb{N}$ *and we call those integers* **negative***.*

Remark 1.4. (Rational Numbers) *Observe that the equation* $3 \cdot x = 4$ *has no solution in* $\mathbb{Z}$*. We identify the equation* $b \cdot x = a$*, where* $a, b \in \mathbb{Z}, b \neq 0$ *with the pair* (a, b) *and we say two such pairs* (a, b) *and* (c, d) *are equivalent if* $a \cdot d = b \cdot c$*. Set*

$$X := \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\},$$

where we understand equivalent elements as the same element. Then X *forms a ring under the operations*

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

The additive identity is $(0, 1)$ *(which equals* $(0, x)$*, for any integer* $x \neq 0$*) and the multiplicative identity is* $(1, 1)$ *(which equals* (x, x)*, for any* $x \neq 0$*). Overall we denote the set* X *by* $\mathbb{Q}$ *and call it the* **rational numbers***. Furthermore we denote the pair* (a, b)*, by the fraction* $\frac{a}{b}$*. Overall we get that*

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

In addition, the rationals are ordered by

$$\frac{a}{b} < \frac{c}{d} \quad \text{if and only if} \quad a \cdot d < b \cdot c.$$

We can identify $\mathbb{Z}$ *as the subset* $\{\frac{a}{1} \mid a \in \mathbb{Z}\}$ *of* $\mathbb{Q}$*. Note that then the above operations and order are an extension of the operations and order on* $\mathbb{Z}$*.*