arith.1 Ordered Rings and Fields

sfr:arith:check:sec

Throughout this chapter, we claimed that certain definitions behave "as they ought". In this technical appendix, we will spell out what we mean, and (sketch how to) show that the definitions do behave "correctly".

In **??**, we defined addition and multiplication on $\mathbb{Z}$. We want to show that, as defined, they endow $\mathbb{Z}$ with the structure we "would want" it to have. In particular, the structure in question is that of a commutative ring.

Definition arith.1. A *commutative ring* is a set S, equipped with specific elements 0 and 1 and operations $+$ and $\times$, satisfying these eight formulas:[1]

Associativity	$a + (b + c) = (a + b) + c$	$(a \times b) \times c = a \times (b \times c)$
Commutativity	$a + b = b + a$	$a \times b = b \times a$
Identities	$a + 0 = a$	$a \times 1 = a$
Additive Inverse	$(\exists b \in S) 0 = a + b$	
Distributivity	$a \times (b + c) = (a \times b) + (a \times c)$	

So, to check that the integers form a commutative ring, we just need to check that we meet these eight conditions. None of the conditions is difficult to establish, but this is a bit laborious. For example, here is how to prove *Associativity*, in the case of addition:

Proof. Fix $i, j, k \in \mathbb{Z}$. So there are $m_1, n_1, m_2, n_2, m_3, n_3 \in \mathbb{N}$ such that $i = [m_1, n_1]$ and $j = [m_2, n_2]$ and $k = [m_3, n_3]$. (For legibility, we write "$[x, y]$" rather than "$[x, y]_\sim$"; we'll do this throughout this section.) Now:

$$\begin{aligned} i + (j + k) &= [m_1, n_1] + ([m_2, n_2] + [m_3, n_3]) \\ &= [m_1, n_1] + [m_2 + m_3, n_2 + n_3] \\ &= [m_1 + (m_2 + m_3), n_1 + (n_2 + n_3)] \\ &= [(m_1 + m_2) + m_3, (n_1 + n_2) + n_3] \\ &= [m_1 + m_2, n_1 + n_2] + [m_3, n_3] \\ &= ([m_1, n_1] + [m_2, n_2]) + [m_3, n_3] \\ &= (i + j) + k \end{aligned}$$

helping ourselves freely to the behavior of addition on $\mathbb{N}$. □

Equally, here is how to prove *Additive Inverse*:

Proof. Fix $i \in \mathbb{Z}$, so that $i = [m, n]$ for some $m, n \in \mathbb{N}$. Let $j = [n, m] \in \mathbb{Z}$. Helping myself to the behaviour of the naturals, $(m+n)+0 = 0+(n+m)$, so that $\langle m + n, n + m\rangle \sim_{\mathbb{Z}} \langle 0, 0\rangle$ by definition, and hence $[m + n, n + m] = [0, 0] = 0_{\mathbb{Z}}$. So now $i + j = [m, n] + [n, m] = [m + n, n + m] = [0, 0] = 0_{\mathbb{Z}}$. □

[1] Implicitly, these are all bound with universal quantifiers restricted to S. Thus the first principle, more explicitly, is: $(\forall a, b, c \in S) a+(b+c) = (a+b)+c$. And note that the elements 0 and 1 here need not be the natural numbers with the same name.

And here is a proof of *Distributivity*:

Proof. As above, fix $i = [m_1, n_1]$ and $j = [m_2, n_2]$ and $k = [m_3, n_3]$. Now:

$$\begin{aligned}
i \times (j + k) &= [m_1, n_1] \times ([m_2, n_2] + [m_3, n_3]) \\
&= [m_1, n_1] \times [m_2 + m_3, n_2 + n_3] \\
&= [m_1(m_2 + m_3) + n_1(n_2 + n_3), m_1(n_2 + n_3) + n_1(m_2 + m_3)] \\
&= [m_1m_2 + m_1m_3 + n_1n_2 + n_1n_3, m_1n_2 + m_1n_3 + m_2n_1 + m_3n_1] \\
&= [m_1m_2 + n_1n_2, m_1n_2 + m_2n_1] + [m_1m_3 + n_1n_3, m_1n_3 + m_3n_1] \\
&= ([m_1, n_1] \times [m_2, n_2]) + ([m_1, n_1] \times [m_3, n_3]) \\
&= (i \times j) + (i \times k)
\end{aligned}$$

□

We leave it as an exercise to prove the remaining five conditions. Having done that, we have shown that $\mathbb{Z}$ constitutes a commutative ring, i.e., that addition and multiplication (as defined) behave as they should.

Problem arith.1. Prove that $\mathbb{Z}$ is a commutative ring.

But our task is not over. As well as defining addition and multiplication over $\mathbb{Z}$, we defined an ordering relation, $\leq$, and we must check that this behaves as it should. In more detail, we must show that $\mathbb{Z}$ constitutes an *ordered* ring.

Definition arith.2. An *ordered ring* is a commutative ring which is also equipped with a total ordering relation, $\leq$, such that:[2]

$$\begin{aligned}
a \leq b &\to a + c \leq b + c \\
(a \leq b \wedge 0 \leq c) &\to a \times c \leq b \times c
\end{aligned}$$

Problem arith.2. Prove that $\mathbb{Z}$ is an ordered ring.

As before, it is laborious but routine to show that $\mathbb{Z}$, as constructed, is an ordered ring. We will leave that to you.

This takes care of the integers. But now we need to show very similar things of the rationals. In particular, we now need to show that the rationals form an ordered *field*, under our given definitions of $+$, $\times$, and $\leq$:

Definition arith.3. An *ordered field* is an ordered ring which also satisfies: sfr:arith:check:orderedfield

$$\textit{Multiplicative Inverse} \qquad (\forall a \in S \setminus \{0\})(\exists b \in S) a \times b = 1$$

Once you have shown that $\mathbb{Z}$ constitutes an ordered ring, it is easy but laborious to show that $\mathbb{Q}$ constitutes an ordered field.

Problem arith.3. Prove that $\mathbb{Q}$ is an ordered field.

[2] Recall from **??** that a total ordering is a relation which is reflexive, transitive, and connected. In the context of order relations, connectedness is sometimes called *trichotomy*, since for any a and b we have $a \leq b \vee a = b \vee a \geq b$.

Having dealt with the integers and the rationals, it only remains to deal with the reals. In particular, we need to show that $\mathbb{R}$ constitutes a *complete* ordered field, i.e., an ordered field with the Completeness Property. Now, **??** established that $\mathbb{R}$ has the Completeness Property. However, it remains to run through the (tedious) of checking that $\mathbb{R}$ is an ordered field.

Before tearing off into *that* laborious exercise, we need to check some more "immediate" things. For example, we need a guarantee that $\alpha + \beta$, as defined, is indeed a *cut*, for any cuts α and β. Here is a proof of that fact:

Proof. Since α and β are both cuts, $\alpha + \beta = \{p + q : p \in \alpha \wedge q \in \beta\}$ is a non-empty proper subset of $\mathbb{Q}$. Now suppose $x < p + q$ for some $p < \alpha$ and $q < \beta$. Then $x - p < q$, so $x - p \in \beta$, and $x = p + (x - p) \in \alpha + \beta$. So $\alpha + \beta$ is an initial segment of $\mathbb{Q}$. Finally, for any $p + q \in \alpha + \beta$, since α and β are both cuts, there are $p_1 \in \alpha$ and $q_1 \in \beta$ such that $p < p_1$ and $q < q_1$; so $p + q < p_1 + q_1 \in \alpha + \beta$; so $\alpha + \beta$ has no maximum. □

Similar efforts will allow you to check that $\alpha - \beta$ and $\alpha \times \beta$ and $\alpha \div \beta$ are cuts (in the last case, ignoring the case where β is the zero-cut). Again, though, we will simply leave this to you.

Problem arith.4. Prove that $\mathbb{R}$ is an ordered field.

But here is a small loose end to tidy up. In **??**, we suggest that we can take $\sqrt{2} = \{p \in \mathbb{Q} : p < 0 \text{ or } p^2 < 2\}$. But we do need to show that this set is a *cut*. Here is a proof of that fact:

Proof. Clearly this is a nonempty proper initial segment of the rationals; so it suffices to show that it has no maximum. In particular, it suffices to show that, where p is a positive rational with $p^2 < 2$ and $q = \frac{2p+2}{p+2}$, both $p < q$ and $q^2 < 2$. To see that $p < q$, just note:

$$\begin{aligned} p^2 &< 2 \\ p^2 + 2p &< 2 + 2p \\ p(p+2) &< 2 + 2p \\ p &< \tfrac{2+2p}{p+2} = q \end{aligned}$$

To see that $q^2 < 2$, just note:

$$\begin{aligned} p^2 &< 2 \\ 2p^2 + 4p + 2 &< p^2 + 4p + 4 \\ 4p^2 + 8p + 4 &< 2(p^2 + 4p + 4) \\ (2p+2)^2 &< 2(p+2)^2 \\ \tfrac{(2p+2)^2}{(p+2)^2} &< 2 \\ q^2 &< 2 \end{aligned}$$

□

Photo Credits

Bibliography