12 Multiplication

We would like to develop multiplication in a way that follows addition as closely as possible. In that case, Example 11.9 and Lemma 11.16 showed respectively that the extension of the Moore operation is well defined and that it preserves locatedness. The first of these tasks is complicated for multiplication by negation and intervals, so we shall not attempt to prove Lemma 12.4 for back-to-front intervals *à la* Kaucher (Remark 2.19).

Even the definition for *positive* real numbers is more difficult, because we used subtraction in Example 11.9, but we did not include division in the assumptions about Q. In any place-value representation, such as binary floating point, division may be performed as accurately as required, by first shifting the divisor by sufficiently many (n) places and then dividing to give an *integer* quotient. Proposition 12.2 is the same idea in abstract form; in the next section we shall show that this is enough to provide genuine division in R.

Lemma 12.1 Any linearly ordered ring Q is an ***integral domain***, admitting cancellation:

$$\text{if}\quad q>0\quad\text{then}\quad bq=cq \iff b=c\quad\text{and}\quad bq<cq\iff b<c. \qquad \square$$

Proposition 12.2 Q has ***approximate division***, for $a,q,z:Q$,

$$(a<z)\ \wedge\ (q>0)\ \Rightarrow\ \exists m{:}Q.\ (a<mq<z).$$

Proof Either $0<4q<z-a$ or $0<z-a<8q$.

In the first case, we may apply the Archimedean principle directly with the given q:

$$\text{for some } k,k':\mathbb{Z},\quad q(k-1)<a<q(k+1)\quad\text{and}\quad q(k'-1)<z<q(k'+1).$$

Then $4q<z-a<q(k'+1)-q(k-1)$, so $k<k'-2$ by the previous lemma. Hence $m\equiv k+1<k'-1$, where $m:\mathbb{Z}\subset Q$, has the required property.

In the second case, the Archimedean principle for $8q$ (as p) and $z-a$ (as q) provides $k:\mathbb{Z}$ with $8q<2n(z-a)$, and then $0<k<2^n$ for some $n:\mathbb{N}$. Let h satisfy $0<h+h<1$ (Lemma 11.4). Then

$$4q'\equiv 4qh^n<kh^n(z-a)<(2h)^n(z-a)<(z-a),$$

for which the first case gives $a<m'q'=m'qh^n<z$, so $m\equiv m'h^n$ is the required approximate quotient. $\square$

The next result is similar to Lemma 9.1, but that was for the *continuum* R: here we work with the *discrete* object Q, in which we may use case analysis for $q<0$, $q=0$ and $q>0$. The next two lemmas can actually be proved using the constructive formulation of a linear order (with $0<q$ or $q<1$, Definition 6.1), but it is more complicated.

Lemma 12.3 In Q, $\quad(a<cq<z)\iff\exists bd.\,(b<c<d)\ \wedge\ (a<bq<z)\ \wedge\ (a<dq<z)$.

Proof For $q>0$, Lemma 12.1 gives $bq<cq<dq\Leftrightarrow b<c<d$, where we obtain b and d from $a<cq<z$ by approximate division. The case $q<0$ is similar, with $a<dq<cq<bq<z$, whilst for $q=0$ both sides are $a<0<z$ for any $b<c<d$. $\square$

Lemma 12.4 Let $d\le u$, $e\le t$ and $a,z:Q$. Then

$$\begin{aligned}&a<\mathsf{min}(de,dt,ue,ut)\ \wedge\ \mathsf{max}(de,dt,ue,ut)<z\\ \iff\ &\exists d'<d.\,\exists u'>u.\ \ a<\mathsf{min}(d'e,d't,u'e,u't)\ \wedge\ \mathsf{max}(d'e,d't,u'e,u't)<z.\end{aligned}$$

Proof First recall that the inequalities $a<\mathsf{min}$ and $\mathsf{max}<z$ are equivalent to

$$a<de<z\quad\wedge\quad a<dt<z\quad\wedge\quad a<ue<z\quad\wedge\quad a<ut<z.$$

Using (⇒) of the previous lemma on each of these conjuncts, we have some $d'', d''' < d$ and $u < u'', u'''$ such that

$$a < d''e < z \quad \wedge \quad a < d'''t < z \quad \wedge \quad a < u''e < z \quad \wedge \quad a < u'''t < z,$$

but by (⇐) of the previous lemma, we may replace them by d', u', where $\mathsf{max}(d'', d''') < d' < d$ and $u < u' < \mathsf{min}(u'', u''')$, while still satisfying the constraints.

For the converse we need to assume that $d \leq u$ and $e \leq t$. Then if $d' < d$,

$$\begin{array}{rcl} e \leq t \leq 0 & \vdash & \mathsf{min}' = \mathsf{min}(ue, ut) = \mathsf{min} \\ e \leq 0 \leq t & \vdash & \mathsf{min}' = \mathsf{min}(ue, d't) \leq \mathsf{min}(ue, dt) = \mathsf{min} \\ 0 \leq e \leq t & \vdash & \mathsf{min}' = \mathsf{min}(d'e, d't) \leq \mathsf{min}(de, dt) = \mathsf{min}, \end{array}$$

so $a < \mathsf{min}' \Rightarrow a < \mathsf{min}$, and similarly for $\mathsf{max} < z$ and $u < u'$. □

Corollary 12.5 Moore multiplication ⊗ (Remark 2.2) is rounded, satisfying Proposition 7.12 in the restricted form. It therefore extends to general intervals, *i.e.* rounded, bounded and disjoint pseudo-cuts, $\otimes : IR \times IR \to IR$. It is also defined as a map $(\Sigma^Q \times \Sigma^Q)^{\mathbf{2}} \to (\Sigma^Q \times \Sigma^Q)$ as required for Remarks 11.5 and 11.8(a). □

Exercise 12.6 Use the argument so far to show that R is a Q-module, *cf.* [Joh77, §6.6]. □

The other task is to show that products are located, *cf.* Lemma 11.16. Let's look at this from a programmer's perspective again:

Remark 12.7 If we are asked to calculate xy to precision $0 < p < 1$, we need to decide how precisely to compute the factors x and y. For addition, $p/2$ is fine (Exercise 11.17(b)), but for multiplication,

(a) if x and y are both small in magnitude, *i.e.* $|x|, |y| < 1$, then it suffices to find each of them to within p; but

(b) if x is large (legally, if $0 < M < |x|$, but we're thinking of the situation where M is in the millions), we need to find y correspondingly more precisely, to within p/M [[?]];

(c) similarly, if y is large then we need to know x more precisely.

Curiously, whereas we needed to strengthen the notion of locatedness in Proposition 11.15 in order to define addition, we do *not* need to do so (or apply the Archimedean principle) again for multiplication.

Lemma 12.8 Any additively located positive cut $(\delta, \upsilon) : R$ is ***multiplicatively located***:

$$(0 < a < z) \wedge \delta 0 \;\Rightarrow\; \exists du{:}Q.\ (0 < d < u) \wedge \delta d \wedge \upsilon u \wedge (ua < dz),$$

where the last conjunct corresponds to $u - d < p$ in Proposition 11.15.

Proof By roundedness of δ, let $0 < r : Q$ with δr. By approximate division in Q, let $0 < p : Q$ with $0 < zp < r(z - a)$. By additive locatedness, let $0 < d < u : Q$ with $\delta d \wedge \upsilon u \wedge (u - d < p)$. Since we have $\delta r \wedge \upsilon u$, disjointness of (δ, υ) gives $r < u$, so $z(u - d) < zp < r(z - a) < u(z - a)$. Hence $ua < zd$ as required. □

Lemma 12.9 The product of a positive cut (δ, υ), *i.e.* such that $\delta 0$, with any cut (ϵ, τ) is another cut (α, σ), *cf.* Lemma 11.16.

Proof Suppose first that $0 < a < z$. By multiplicative locatedness of (δ, υ), there are $0 < d < u$ with $\delta d \wedge \upsilon u \wedge (ua < dz)$. Then, using approximate division by du, there are e, t with

$$au < due < dut < zd.$$

So $a < de$, $e < t$ and $ut < z$ by Lemma 12.1, whilst $\epsilon e \vee \tau t$ by order-locatedness. Hence

$$(\exists de.\, a < de \wedge \delta d \wedge \epsilon e) \;\vee\; (\exists ut.\, ut < z \wedge \upsilon u \wedge \tau t) \;\equiv\; \alpha a \vee \sigma z.$$

More generally, given $a < z$, either

- $0 < z$, in which case there is some a' with $0, a \leq \mathsf{max}(0, a) < a' < z$, so $\alpha a' \vee \sigma z$ by the foregoing argument, and hence $\alpha a \vee \sigma z$ since α is lower;
- or $a < 0$, where we apply the previous case to $-z < -a$, $\ominus(\epsilon, \tau)$ and $\ominus(\alpha, \sigma)$. □

It only remains to prove locatedness of the product of two numbers that are both small. Note that we can bound a product *away* from zero iff we can do so for both factors, and in that case the previous result applies. The point of the fifth case below is therefore to constrain the product to be *near* to zero.

Lemma 12.10 The product of any two real numbers (cuts) $x, y : R$ is another cut.
Proof If $a < z$ then $a < 0 \vee 0 < z$, so $0 < m \equiv \mathsf{max}(z, -a)$ and

$$(x > 0) \;\vee\; (x < 0) \;\vee\; (y > 0) \;\vee\; (y < 0) \;\vee\; (|\,x\,| < 1 \;\wedge\; |\,y\,| < m).$$

It only remains to consider the last of these five cases, which is itself a disjunction because of the definition of $< \mathsf{max}$ (Proposition 9.8). Then essentially

$$|\,x\,| < 1 \;\wedge\; |\,y\,| < m \quad\Longrightarrow\quad a < -|\,y\,| < xy \quad\vee\quad xy < |\,y\,| < z.$$

We need to explain these inequalities in terms of cuts $x \equiv (\delta, \upsilon)$ and $y \equiv (\epsilon, \tau)$:

$$\begin{array}{lcl} |\,x\,| < 1 & \equiv & -1 < x < +1 \;\equiv\; \delta d \wedge \upsilon u, \qquad \text{where} \quad d \equiv -1, \quad u \equiv +1 \\ a < -|\,y\,| & \equiv & \exists et.\, \epsilon e \wedge \tau t \;\wedge\; (a < e) \wedge (a < -t) \\ a < xy & \equiv & \exists duet.\, \delta d \wedge \upsilon u \wedge \epsilon e \wedge \tau t \;\wedge\; a < \mathsf{min}(de, dt, ue, ut). \end{array}$$

□

Proposition 12.11 R is an ordered commutative ring. □

We shall use division to prove that R is Archimedean, but let us consider very briefly the necessity of that hypothesis on Q.

Remark 12.12 There are *Cauchy*-complete ordered fields with infinitesimals but, classically, any *Dedekind*-complete Abelian group must be Archimedean. This is because the sets

$$D \equiv \{d \mid \exists n{:}\mathbb{N}.\ d < n\} \quad \text{and} \quad U \equiv \{u \mid \forall n{:}\mathbb{N}.\ n < u\}$$

form a Dedekind cut that is located only in the weaker order-theoretic sense: since every $u - d$ is infinite, (D, U) is not additively located.

The significance of the Archimedean principle in Greek mathematics was recognised by Otto Stolz [Sto83]. He coined the name because, although the principle had been used implicitly by Eudoxus and Euclid, Archimedes stated it explicitly. (He also made far deeper use of it, in his *Method*, but Stolz was writing before the discovery of the most important Archimedes codex.)

Stolz also gave the argument above that Dedekind completeness implies the Archimedean principle [*loc. cit.*, p. 509]. His result was disputed by his contemporaries [**?**, **?**, **?**] and historians [**?**], possibly because of its context in the debate at the time over the axiomatics of Euclid. However, we consider that his proof is valid, because it includes the two key points, namely the construction of the limit of an increasing sequence as the cut (D, U), and the problem with the value $(D, U) - 1$. He even uses the *constructive* least upper bound principle.

Remark 12.13 What does this argument say about Conway's number system? Recall that it is a proper class. Although the class D is equivalent as a left cut to the set $\mathbb{N}$, the class U cannot be expressed as a right cut, so $\{D \mid U\}$ is not a legitimate Conway Number — he calls it a *gap* [Con76, p. 37].

The argument also fails in ASD, for an analogous reason: U is not *definable* in the calculus as an open subspace. The point is really that the space D of *finite* numbers is *overt*, as it is given by an existential quantifier, or as the numbers for which repeated decrementation *terminates.* On the other hand, U consists of *infinite* or *non-terminating* numbers, which is the canonical example of a non-overt subspace in recursion theory.

We do not know whether there is in fact a Dedekind-complete but non-Archimedean "real line" in ASD. This is a difficult but intriguing problem in recursion theory. Careful study of John Conway's construction may yield a recursive analogue (when this conjecture was put to him, he considered it plausible). The principal difficulty arises from the alternating quantifiers in the definition of $<$, as the arithmetic operations are clearly constructive [Ros01]. Even if such a model exists, Stolz's argument would still show that the sequence $0,\ 1,\ \ldots,$ has no limit: any infinite element ω is "inaccessible" from finite values.

Such an object could, of course, be rather useful to develop differential calculus in a "non-standard" way ⟦refs for SDG and non-standard analysis⟧. It would also illustrate the importance of overtness very clearly. Here we have simply "left the door open" to such a possibility, by using approximate division and additive locatedness in the proof, instead of the Archimedean principle itself.

Theorem 12.14 Let Q be any linearly ordered field (or commutative ring with approximate division) for which every Dedekind cut is additively located. Then these cuts form a commutative ring. □