Partial Solutions for Exercises in Where do Numbers Come From? DRAFT C

T. W. Körner

When I was young, I used to be surprised when the answer in the back of the book was wrong. I could not believe that the wise and gifted people who wrote textbooks could possibly make mistakes. I am no longer surprised.

Here are what I believe to be sketch solutions to the bulk of the exercises. They may be considered proof that the chef has tasted the dishes he supplied. However the reader should note the following warnings.

(1) Much less care has been put into writing and checking the sketch solutions than into writing and checking the main book.

(2) There is substantial variation in the amount of detail supplied. These are sketch solutions — not model solutions.

(3) There are often several ways of proving a result. If your proof differs greatly from the one supplied, try to understand why the two proofs differ, but do not ask if one is 'better' than the other.

I would appreciate the opportunity to remedy problems. Please tell me of any errors, unbridgeable gaps, misnumberings etc. I welcome suggestions for additions.

ALL COMMENTS AND CORRECTIONS GRATEFULLY RECEIVED.

If you can, please use LaTeX 2_ε or its relatives for mathematics. If not, please use plain text. My e-mail is **twk@dpmms.cam.ac.uk**. You may safely assume that I am both lazy and stupid, so that a message saying 'Presumably you have already realised the mistake in Exercise Z' is less useful than one which says 'I think you have made a mistake in Exercise Z because you have assumed that the sum is necessarily larger than the integral. One way round this problem is to assume that f is decreasing.'

It may be easiest to navigate this document by using the table of contents which follow on the next few pages. To avoid disappointment, observe that those exercises marked ★ have no solution given.

CONTENTS

Exercise 1.1.1

Using commutativity, the distribution law and commutativity again,

$$(b + c) \times a = a \times (b + c) = (a \times b) + (a \times c) = (b \times a) + (c \times a).$$

Exercise 1.1.2

(i) We have

$$a \boxplus b = 2 \times (a + b) = 2 \times (b + a) = b \boxplus a.$$

(ii) We have

$$\begin{aligned} a \times (b \boxplus c) &= a \times (2 \times (b + c)) = (a \times 2) \times (b + c) = (2 \times a) \times (b + c) \\ &= ((2 \times a) \times b) + ((2 \times a) \times c) = (2 \times (a \times b)) + (2 \times (a \times c)) \\ &= (a \times b) \boxplus (a \times c). \end{aligned}$$

(iii) Take $a = 1$, $b = 2$, $c = 3$. We have

$$1 \boxplus (2 \boxplus 3) = 1 \boxplus 10 = 22,$$

but

$$(1 \boxplus 2) \boxplus 3 = 6 \boxplus 3 = 18.$$

Exercise 1.2.1

(i) We have

α	β	γ
45	103	
22	206	103
11	412	
5	824	412
2	1648	824
1	3296	

We have $3296 + 824 + 412 + 103 = 4635$.

(ii) See Exercise 4.3.15.

Exercise 1.2.2★

See Exercise 4.3.14.

Exercise 1.3.1

The commutative law of multiplication and the equation labelled ‘One is a unit’ give
$$a \times 1 = 1 \times a = a.$$

Exercise 1.3.2

(Note that this is a special case of Theorem 5.1.13 with $p = 2$.)

Commutative laws $a + b = b + a$, $a \times b = b \times a$ by inspection.

Associative law of addition,
$$a + (b + c) = \begin{cases} 1 & \text{if odd number of } a, b, c \text{ take value } 1, \\ \theta & \text{otherwise,} \end{cases}$$
$$(a + b) + c = \begin{cases} 1 & \text{if odd number of } a, b, c \text{ take value } 1, \\ \theta & \text{otherwise,} \end{cases}$$
so $a + (b + c) = (a + b) + c$.

Associative law of multiplication, $a \times (b \times c) = \theta = (a \times b) \times c$ unless $a = b = c = 1$, but then $a \times (b \times c) = 1 = (a \times b) \times c$.

1 is a multiplicative unit.

Distributive law
$$\theta \times (b + c) = \theta = \theta + \theta = (\theta \times b) + (\theta \times c)$$
$$1 \times (b + c) = b + c = (1 \times b) + (1 \times c)$$

Exercise 1.3.5

$\theta = \theta + \theta$, so $\theta \circledgtr \theta$.

$1 = \theta + 1$, so $1 \circledgtr \theta$.

$\theta = 1 + 1$, so $\theta \circledgtr 1$.

$1 = 1 + \theta$, so $1 \circledgtr 1$.

Exercise 1.3.6

Suppose (i) and (ii) hold.

(1) If $a \geq b$ and $b \geq a$ and $a \neq b$, then $a > b$ and $b > a$ which is is impossible by (i).

(2) If $a \geq b$ and $b \geq c$, then, if $a = b$, we have $a \geq c$ and, if $b = c$, we have $a \geq c$. If $a \neq b$ and $b \neq c$, then $a > b$ and $b > c$ so, by (ii), $a > c$ whence $a \geq c$.

(3) By trichotomy (that is to say, by (ii)), $a > b$ so $a \geq b$, or $a = b$, so $a \geq b$ or $b > a$, so $b \geq a$.

(4) Follows from trichotomy.

Suppose (1), (2), (3) and (4) hold.

(i) If $a > b$ and $b > c$, then, certainly, $a \geq b$ and $b \geq c$ so $a \geq c$. If $a = c$, then $a \geq b$ and $b \geq a$ so $a = b$, by (1), which is excluded by the condition $a > b$. Thus $a > c$.

(ii) By (3), we know that at least one of the three conditions $a > b$, $a = b$ or $b > a$ holds.

By (4), the two conditions $a > b$ and $a = b$ cannot hold together and the two conditions $b > a$ and $a = b$ cannot hold together. If $a > b$ and $b > a$, then $a \geq b$ and $b \geq a$ so, by (1), $a = b$ and we know, by (4), that the two conditions $a > b$, $a = b$ cannot hold together. Thus at most one of the three conditions $a > b$, $a = b$ or $b > a$ holds

Exercise 1.3.7

By trichotomy, exactly one of the following is true
$$a = b \text{ or } a > b \text{ or } b > a.$$
If $a = b$ or $a > b$, set $\max\{a, b\} = a$, $\min\{a, b\} = b$. Otherwise, set $\max\{a, b\} = b$, $\min\{a, b\} = a$.

We now observe that, if $a = b$ or $a > b$,
$$\max\{a, b\} + \min\{a, b\} = a + b$$
and, otherwise,
$$\max\{a, b\} + \min\{a, b\} = b + a = a + b$$
(using the commutative law of addition).

Exercise 1.3.10

(ii) If $a > b$, then $a \times c > b \times c$ and, by trichotomy, $a \times c \neq b \times c$. Similarly, if $b > a$, then $b \times c > a \times c$ and, by trichotomy, $a \times c \neq b \times c$. Since $a \times c = b \times c$, trichotomy tells us that $a = b$.

(iii) If $a = b$, then $a + c = b + c$ which is impossible by trichotomy. If $b > a$, then $b + c > a + c$ which is impossible by trichotomy. Thus, by trichotomy, $a > b$.

(iv) If $a = b$, then $a \times c = a \times b$ which is impossible by trichotomy. If $b > a$, then $b \times c > a \times c$ which is impossible by trichotomy. Thus, by trichotomy, $a > b$.

Exercise 2.1.1

$$\begin{array}{cccccc}
9 & 7 & 3 & & & \\
5 & 6 & 2 & \times & & \\
\hline
5 & 9 & 8 & 1 & & \\
 & 4 & 7 & 2 & 2 & \\
 & & 8 & 5 & 7 & \\
\hline
5 & 3 & 4 & 0 & 0 & 1
\end{array}$$

One hundred thousand four hundred and thirty five. (Please pass the aspirin.)

Exercise 2.1.2

Two quadrillion, one hundred and forty trillion, six hundred and seventy six billion, nine hundred and twelve million, nine hundred and twenty six thousand nine hundred and twenty seven.

Perhaps:- Count the number of digits. If your expression is $(3 \times r) + k$ digits long with $3 \geq k \geq 0$, group it as

$$A_r A_{r-1} \dots A_0$$

where the group A_r is k digits long and each other group is 3 digits long. Translate A_s into words as B_s where we suppress initial zeros unless all the entries are zeros in which case we omit the words entirely. Now say 'B_r r-illion, B_{r-1} $r-1$-illion, $\dots B_2$ million, B_1 thousand and B_0'.

I am sure the reader can to better.

Exercise 2.1.3

(i) In octal, $153 + 672 = 1045$, $53 \times 72 = 4676$.

(ii) 104 in decimal is 110100 in binary.
10011 in binary is 35 in decimal.

Exercise 2.1.4★

Exercise 2.1.5★

Exercise 2.2.1

$=$ is reflexive, symmetric and transitive.

$\geq$ is reflexive and transitive, but not symmetric ($3 \geq 2$, but $2 \ngeq 3$).

$>$ is not reflexive ($1 \ngtr 1$) and not symmetric ($3 > 2$, but $2 \ngtr 3$), but is transitive.

Exercise 2.2.2

(i) Not reflexive ($x \nsim x$), not symmetric ($x \sim y$, but $y \nsim x$), not transitive ($x \sim y$ and $y \sim z$, but $x \nsim z$).

(ii) Reflexive, not symmetric ($x \sim y$, but $y \nsim x$), not transitive ($x \sim y$ and $y \sim z$, but $x \nsim z$).

(iii) Not reflexive ($x \nsim x$), symmetric, not transitive ($x \sim y$ and $y \sim x$, but $x \nsim x$).

(iv) Not reflexive ($x \nsim x$), not symmetric ($x \sim y$, but $y \nsim x$), but transitive.

(v) Not reflexive ($z \nsim z$), but symmetric and transitive.

(vi) Reflexive, not symmetric ($x \sim y$ but $y \nsim x$), transitive.

(vii) Reflexive and symmetric, but not transitive ($x \sim y$ and $y \sim z$, but $x \nsim z$),

(viii) Reflexive, symmetric and transitive.

Exercise 2.2.3

If $x \in X$, we can find a $y \in X$ such that $x \sim y$. Since the relation is symmetric, $y \sim x$. By transitivity $x \sim x$.

Exercise 2.2.8

$$
\begin{aligned}
(d\times(a\times f))\times c &= ((d\times a)\times f)\times c && \text{(associative law multiplication)}\\
&= (d\times a)\times(f\times c) && \text{(associative law multiplication)}\\
&= (a\times d)\times(c\times f) && \text{(commutative law multiplication)}\\
&= (b\times c)\times(e\times d) && \text{(substitution)}\\
&= b\times(c\times(e\times d)) && \text{(associative law multiplication)}\\
&= b\times((e\times d)\times c) && \text{(commutative law multiplication)}\\
&= (b\times(e\times d))\times c && \text{(associative law multiplication)}\\
&= ((b\times(d\times e))\times c && \text{(commutative law multiplication)}\\
&= ((b\times d)\times e))\times c && \text{(associative law multiplication)}\\
&= ((d\times b)\times e))\times c && \text{(commutative law multiplication)}\\
&= (d\times(b\times e))\times c && \text{(associative law multiplication)}
\end{aligned}
$$

Exercise 2.2.9

We write $\underset{A}{=}$ when we use the associative law and $\underset{C}{=}$ when we use the commutative law.

$$\begin{aligned}((a \times b) \times c) \times d &\underset{A}{=} (a \times b) \times (c \times d) \underset{C}{=} (a \times b) \times (d \times c) \underset{A}{=} ((a \times b) \times d) \times c)\\
&\underset{A}{=} (a \times (b \times d)) \times c \underset{C}{=} (a \times (d \times b)) \times c \underset{A}{=} ((a \times d) \times b)) \times c\\
&\underset{A}{=} ((d \times a) \times b)) \times c \underset{A}{=} (d \times a) \times (b \times c) \underset{C}{=} (d \times a) \times (c \times b)\\
&\underset{A}{=} ((d \times a) \times c) \times b \underset{A}{=} (d \times (a \times c)) \times b \underset{C}{=} (d \times (c \times a)) \times b\\
&\underset{A}{=} ((d \times c) \times a) \times b \underset{A}{=} (d \times c) \times (a \times b) \underset{C}{=} (d \times c) \times (b \times a)\\
&\underset{A}{=} ((d \times c) \times b) \times a\end{aligned}$$

Exercise 2.2.10

$1 \times 4 = 2 \times 2$, so $[(1, 2)] = [(2, 4)]$. However

$$[(1 + 1, 2 + 1)] = [(2, 3)] \text{ and } \big[((1 + 2), (2 + 4))\big] = [(3, 6)],$$

whilst $2 \times 6 = 12 \neq 9 = 3 \times 3$ so

$$[(1 + 1, 2 + 1)]) \neq \big[((1 + 2), (2 + 4))\big].$$

Exercise 2.2.12

Using the commutative law of multiplication together with the symmetry of $\sim$ and ★

$$\begin{aligned}\big((a \times m') + (b \times n'), b \times m'\big) &= ((m' \times a) + (n' \times b), m' \times b)\\
&= ((m' \times a') + (n' \times b'), m' \times b')\\
&= ((a' \times m') + (b' \times n'), b' \times m').\end{aligned}$$

EXERCISE 2.2.13

Suppose that $(a,b) \sim (a',b')$ and $(n,m) \sim (n',m')$ so $a \times b' = a' \times b$ and $n \times m' = m \times n'$

Then, using the associative and commutative laws of multiplication,

$$\begin{aligned}
(a \times n') \times (b \times m) &= a \times \big(n' \times (b \times m)\big) && \text{(associative law)}\\
&= a \times \big((b \times m) \times n')\big) && \text{(commutative law)}\\
&= a \times \big(b \times (m \times n')\big) && \text{(associative law)}\\
&= a \times \big(b \times (n \times m')\big) && \text{(substitution)}\\
&= a \times \big((n \times m') \times b)\big) && \text{(commutative law)}\\
&= a \times \big(n \times (m' \times b)\big) && \text{(associative law)}\\
&= (a \times n) \times (m' \times b) && \text{(associative law)}\\
&= (a \times n) \times (b \times m') && \text{(commutative law)}
\end{aligned}$$

Thus

$$(a \times n, b \times m) \sim (a \times n', b \times m').$$

Similarly (or using commutativity),

$$(a \times n', b \times m') \sim (a' \times n', b' \times m')$$

so, by the transitivity of $\sim$,

$$(a \times n, b \times m) \sim (a' \times n', b' \times m').$$

Thus we may define

$$[(a,b)] \otimes [(n,m)] = [(a \times n, b \times m)]$$

unambiguously.

We are thinking of

$$\frac{a}{a'} \times bb' = \frac{ab}{a'b'}.$$

EXERCISE 2.2.15

$$
\begin{aligned}
(b \times m') \times a &= b \times (a \times m') \\
&> b \times (a' \times m) \qquad (1) \\
&= (a' \times b) \times m \\
&= (a \times b') \times m \qquad (2) \\
&= (b' \times m) \times a.
\end{aligned}
$$

(Step (1) uses the multiplication law for inequalities from lemma 1.3.8. Step (2) uses the fact that $(a, a') \sim (b, b')$. The remaining steps use the associative and commutative laws of multiplication, sometimes condensing several steps into one.) The cancellation law for multiplication (see Lemma 1.3.9) now gives

$$b \times m' > b' \times m$$

as required.

Exercise 2.3.2

(i) We have, using the commutative laws of addition and multiplication for $\mathbb{N}^{+}$,

$$\begin{aligned}\mathbf{a} \oplus \mathbf{b} &= [(a \times b') + (b \times a'), a' \times b']\\ &= [(b' \times a) + (a' \times b), b' \times a']\\ &= [(a' \times b) + (b' \times a), b' \times a']\\ &= \mathbf{b} \oplus \mathbf{a}.\end{aligned}$$

(ii) We have, using the associative laws of addition and multiplication for $\mathbb{N}^{+}$, together with the left handed and right handed versions of the distributive law

$$\begin{aligned}\mathbf{a} \oplus (\mathbf{b} \oplus \mathbf{c}) &= [a, a'] \oplus [(b \times c') + (c \times b'), b' \times c']\\ &= [(a \times (b' \times c')) + (a' \times ((b \times c') + (c \times b'))), a' \times (b' \times c')]\\ &= [(a \times (b' \times c')) + ((a' \times (b \times c')) + (a' \times (c \times b'))), a' \times (b' \times c')]\\ &= [((a \times (b' \times c') + (a' \times (b \times c'))) + (a' \times (c \times b')), a' \times (b' \times c')]\\ &= [(((a \times b') \times c') + ((a' \times b) \times c'))) + ((a' \times c) \times b'), (a' \times b') \times c')]\\ &= (\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{c}.\end{aligned}$$

(iii) We have, using the commutative law of multiplication for $\mathbb{N}^{+}$,

$$\mathbf{a} \otimes \mathbf{b} = [a \times b, a' \times b'] = [b \times a, b' \times a'] = \mathbf{b} \otimes \mathbf{a}.$$

(iv) We have, using the associative law of multiplication for $\mathbb{N}^{+}$,

$$\begin{aligned}\mathbf{a} \otimes (\mathbf{b} \otimes \mathbf{c}) &= \mathbf{a} \otimes [b \times c, b' \times c'] = [a \times (b \times c), a' \times (b' \times c')]\\ &= [(a \times b) \times c, (a' \times b') \times c'] = [a \times b, a' \times b'] \otimes \mathbf{c}\\ &= (\mathbf{a} \otimes \mathbf{b}) \otimes \mathbf{c}\end{aligned}$$

(ix) By trichotomy for $\mathbb{N}^{+}$, exactly one of the following will occur

$$a \times b' > a' \times b,\ a' \times b > a \times b' \text{ or } a \times b' = a' \times b.$$

In other words, exactly one of the following conditions holds: $\mathbf{a} \ogreaterthan \mathbf{b}$ or $\mathbf{b} \ogreaterthan \mathbf{a}$ or $\mathbf{a} = \mathbf{b}$.

Exercise 2.3.3

Just a word for word copy of the lemmas mentioned in the hint (except for (b)).

(ix) If $\mathbf{a} \ogreaterthan \mathbf{b}$ and $\mathbf{b} \ogreaterthan \mathbf{c}$ then, by definition, we can find $\mathbf{u}$ and $\mathbf{v}$ such that $\mathbf{a} = \mathbf{b} + \mathbf{u}$, $\mathbf{b} = \mathbf{c} + \mathbf{v}$. Using the associative law of addition we have

$$\mathbf{a} = \mathbf{b} + \mathbf{u} = (\mathbf{c} + \mathbf{v}) + \mathbf{u} = \mathbf{c} + (\mathbf{v} + \mathbf{u}),$$

so $\mathbf{a} \ogreaterthan \mathbf{c}$.

(x) If $\mathbf{a} \ogreaterthan \mathbf{b}$, then we can find a $\mathbf{u}$ such that $\mathbf{a} = \mathbf{b} + \mathbf{u}$. By the associative and commutative laws of addition,

$$\mathbf{a} \oplus \mathbf{c} = (\mathbf{b} \oplus \mathbf{u}) \oplus \mathbf{c} = \mathbf{b} \oplus (\mathbf{u} \oplus \mathbf{c}) = \mathbf{b} \oplus (\mathbf{c} \oplus \mathbf{u}) = (\mathbf{b} \oplus \mathbf{c}) \oplus \mathbf{u}$$

so $\mathbf{a} \oplus \mathbf{c} \ogreaterthan \mathbf{b} \oplus \mathbf{c}$.

(xi) If $\mathbf{a} \ogreaterthan \mathbf{b}$, then we can find a $\mathbf{u}$ such that $\mathbf{a} = \mathbf{b} \oplus \mathbf{u}$. By the distributive law and the commutative law of multiplication

$$\mathbf{a} \otimes \mathbf{c} = (\mathbf{b} \oplus \mathbf{u}) \otimes \mathbf{c} = \mathbf{c} \otimes (\mathbf{b} \oplus \mathbf{u}) = (\mathbf{c} \otimes \mathbf{b}) \oplus (\mathbf{c} \otimes \mathbf{u}) = (\mathbf{b} \otimes \mathbf{c}) \oplus (\mathbf{b} \otimes \mathbf{u})$$

so $\mathbf{a} \otimes \mathbf{c} \ogreaterthan \mathbf{b} \otimes \mathbf{c}$.

(a) By trichotomy we know that exactly one of the following holds: $\mathbf{a} \ogreaterthan \mathbf{b}$, $\mathbf{b} \ogreaterthan \mathbf{a}$ or $\mathbf{b} = \mathbf{a}$. If $\mathbf{a} \ogreaterthan \mathbf{b}$, then $\mathbf{a} \oplus \mathbf{c} \ogreaterthan \mathbf{b} \oplus \mathbf{c}$ and (by trichotomy again) $\mathbf{a} \oplus \mathbf{c} \neq \mathbf{b} \oplus \mathbf{c}$. If $\mathbf{b} > \mathbf{a}$, then $\mathbf{b} \oplus \mathbf{c} > \mathbf{a} \oplus \mathbf{c}$ and $\mathbf{a} \oplus \mathbf{c} \neq \mathbf{b} \oplus \mathbf{c}$. Thus, if $\mathbf{a} \oplus \mathbf{c} = \mathbf{b} \oplus \mathbf{c}$, we have $\mathbf{a} = \mathbf{b}$.

(b) If $\mathbf{a} \otimes \mathbf{c} \ogreaterthan \mathbf{b} \otimes \mathbf{c}$ then

$$\mathbf{a} = (\mathbf{a} \otimes \mathbf{c}) \times \mathbf{c}^{-1} \ogreaterthan (\mathbf{b} \otimes \mathbf{c}) \times \mathbf{c}^{-1} = \mathbf{b}.$$

Exercise 3.1.1

In modern notation, the first four girls took

$$\frac{2}{7} + \frac{1}{12} + \frac{1}{6} + \frac{1}{3} = \frac{73}{84}$$

of the nuts leaving $11/84$ of the original quantity. But there are

$$20 + 12 + 11 + 1 = 44$$

nuts left over, so the original quantity is

$$\frac{84}{11} \times 44 = 336.$$

There were 336 nuts originally.

Exercise 3.1.2

In modern notation, we must solve

$$n^2 - 64n + 12 \times 64 = 0$$

and, using the standard formula,

$$n = \frac{64 \pm \sqrt{64^2 - 48 \times 64}}{2} = \frac{64 \pm 8\sqrt{64 - 48}}{2} = 32 \pm 4\sqrt{16} = 32 \pm 16$$

There were 16 or 48 monkeys in the troop.

Exercise 3.1.3

(i) It is harder than it looks to make up amusing stories, but the quadratic $(n + 1)(n - 2) = n^2 - n - 2$ associated with the equation $n^2 = n + 2$ has one positive and one negative solution. 'The square of the troop is the same as the size of the troop joined by two monkeys'.

(ii) The quadratic $(n+1)(n+2) = n^2+3n+2$ associated with the equation $n^2 + 4n + 4 = n + 2$ has two negative solutions. Perhaps 'if two monkeys leave the square of the troop of monkeys joined with two more monkeys then the new troop is the same size as the old'.

Exercise 3.1.4

In modern notation, we must solve

$$n = 1 + (n/5 - 3)^2,$$

that is to say,

$$25n = 25 + (n - 15)^2$$

which yields

$$n^2 - 55n + 10 \times 5^2 = 0.$$

Using the standard formula,

$$n = \frac{55 \pm \sqrt{55^2 - 40 \times 5^2}}{2} = \frac{55 \pm 5\sqrt{11^2 - 40}}{2} = \frac{55 \pm 45}{2},$$

so $n = 50$ or $n = 5$.

Exercise 3.1.5

In modern notation, we must solve

$$8 + 7\sqrt{n} = n$$

so

$$7\sqrt{n} = n - 8 \qquad \bigstar$$

and

$$49n = n^2 - 16n + 64 \qquad \bigstar\bigstar$$

so

$$n^2 - 65n + 64 = 0.$$

Using the standard formula, so $n = 1$ or $n = 64$.

However, although ★★ follows from ★, it is not true that ★ follows from ★★. Thus the only possible solutions to our initial problem are so $n = 1$ or $n = 64$. By substitution we check that $n = 1$ is not a solution but $n = 64$ is.

Looking at thing in different way, we must solve

$$8 + 7\sqrt{n} = n,$$

so $n = 1$ is only a solution to our initial problem if we allow negative square roots that is to say $\sqrt{1} = -1$.

Exercise 3.2.1

Reflexive $a + b = a + b$, so $(a, b) \sim (a, b)$.

Symmetric If $(a, b) \sim (c, d)$, then, using the commutative law of addition,

$$c + b = b + c = a + d = d + a$$

and $(c, d) \sim (a, b)$.

Transitive If $(a, b) \sim (c, d)$ and $(c, d) \sim (u, v)$, then $a + d = c + b$, $c + v = d + u$ so, using the commutative and associative laws of addition,

$$\begin{aligned}(a + v) + c &= a + (v + c) = a + (c + v) = a + (d + u)\\ &= (a + d) + u = (c + b) + u = (b + c) + u = b + (c + u)\\ &= b + (u + c) = (b + u) + c.\end{aligned}$$

The cancellation law now gives $a + v = b + u$, so $(a, b) \sim (u, v)$.

Exercise 3.2.2

If $(a, a') \sim (b, b')$ and $(c, d) \sim (c', d')$, then

$$a + b' = a' + b, \text{ and } c + d' = c' + d$$

so, using the commutative and associative laws of addition repeatedly,

$$(a + c) + (b' + d') = (a + b') + (c + d') = (a' + b) + (c' + d) = (a' + c') + (b + d)$$

Thus

$$(a + c, a' + c') \sim (b + d, b' + d')$$

and we may define

$$[(a, a')] \oplus [(b, b')] = [(a + b, a' + b')]$$

unambiguously.

EXERCISE 3.2.4

Using the commutative laws of multiplication and addition and the result already obtained,

$$
\begin{aligned}
((a \times d) + (a' \times d'),&(a \times d') + (a' \times d)) \\
&= ((d \times a) + (d' \times a'), (d' \times a) + (a' \times d)) \\
&= ((d \times b) + (d' \times b'), (d' \times b) + (b' \times d)) \\
&= ((b \times d) + (b' \times d'), (b \times d') + (d \times b')) \\
&= ((b \times d) + (b' \times d'), (d \times b') + (b \times d'))
\end{aligned}
$$

so

$$((a\times d)+(a'\times d'), (a\times d')+(a'\times d)) \sim ((b\times d)+(b'\times d'), (b\times d')+(b'\times d)).$$

EXERCISE 3.2.5

Suppose $(a, a') \sim (c, c')$ and $a + b' > a' + b$. Then, since $a + c' = a' + c$, we have, using associativity, commutativity and the addition inequality law (Lemma 1.3.8 (i), if $x > y$, then $x + z > y + z$),

$$
\begin{aligned}
(b' + c) + a &= (c + b') + a = c + (b' + a) \\
&= c + (a + b') > c + (a' + b) \\
&= (c + a') + b = (a' + c) + b \\
&= (a + c') + b = a + (c' + b) \\
&= (c' + b) + a = (b + c') + a
\end{aligned}
$$

We now use Lemma 1.3.9 (iii) to obtain $b + c' > b' + c$

A similar calculation shows that, if $(b, b') \sim (d, d')$ and $b+c' > b'+c$, then $c + d' > c' + d$. Thus, if $(a, a') \sim (c, c')$, $(b, b') \sim (d, d')$ and $a + b' > a' + b$, then $c + d' > c' + d$.

It follows that the definition,

$$[(a, a')] \circledgtr [(b, b')]$$

if and only if $a + b' > a' + b$, is unambiguous.

Exercise 3.2.6

(i) $a + 1 = a + 1$ so $(a, a) \sim (1, 1)$ and $[a, a] = [1, 1]$.

Using the associative law of addition, $(a + 1) + 1 = a + (1 + 1)$. Thus $(a + 1, a) \sim (1 + 1, 1)$ and $[a + 1, a] = [1 + 1, 1]$.

(ii) Using the commutative law of addition,

$$\begin{aligned}[a, a'] \otimes [b, b'] &= [(a \times b) + (a' \times b'), (a \times b') + (a' \times b)] \\ &= [(a' \times b') + (a \times b), (a' \times b) + (a \times b')] = [a', a] \otimes [b', b].\end{aligned}$$

Exercise 3.2.8

Using the distributive law (together with the remark of Exercise 1.3.1), the rule $1 \times d = d \times 1 = d$, and making repeated use of the commutative and associative laws of addition,

$$\begin{aligned}\big((1 + c) \times (1 + c^{-1})\big) &= \big(1 \times (1 + c^{-1})\big) + \big(c \times (1 + c^{-1})\big) \\ &= (1 + c^{-1}) + \big((c \times 1) + (c \times c^{-1})\big) \\ &= (c^{-1} + 1) + (c + 1) = (1 + 1) + (c + c^{-1}).\end{aligned}$$

Thus, again making use the rule $1 \times d = d \times 1 = d$, and then making repeated use of the commutative and associative laws of addition,

$$\big((1 + c) \times (1 + c^{-1})\big) + (1 \times 1) = (1 + 1) + \big(1 + (c + c^{-1})\big).$$

The commutative and associative laws of addition give

$$(c + 1) + (c^{-1} + 1) = 1 + \big(1 + (c + c^{-1})\big),$$

so ★ follows.

EXERCISE 3.2.9

(i) $\mathbf{a} \oplus \mathbf{b} = [a + b, a' + b'] = [b + a, b' + a'] = \mathbf{b} \oplus \mathbf{a}$.

(ii) We have

$$\begin{aligned}\mathbf{a} \oplus (\mathbf{b} \oplus \mathbf{c}) &= \mathbf{a} \oplus [b + c, b' + c'] = [a + (b + c), a' + (b' + c')]\\ &= [(a + b) + c, (a' + b') + c'] = [a + b, a' + b'] + \mathbf{c}\\ &= (\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{c}.\end{aligned}$$

(iii) $(a + 1) + a' = a + (1 + a') = a + (a' + 1)$, so

$$\mathbf{0} \oplus \mathbf{a} = [1, 1] \oplus [a, a'] = [1 + a, 1 + a'] = [a + 1, a' + 1] = [a, a'] = \mathbf{a}.$$

(v) We have

$$\begin{aligned}\mathbf{a} \otimes \mathbf{b} &= [(a \times b) + (a' \times b'), (a' \times b) + (a \times b')]\\ &= [(a \times b) + (a' \times b'), (a \times b') + (a' \times b)]\\ &= [(b \times a) + (b' \times a'), (b' \times a) + (b \times a')] = \mathbf{b} \otimes \mathbf{a}.\end{aligned}$$

(vi) Making use of the distributive law at the beginning and the distributive law together with the commutative law of multiplication at the end and making free use of the associative and commutative laws of addition and multiplication, we have

$$\begin{aligned}&\mathbf{a} \otimes (\mathbf{b} \otimes \mathbf{c}) = \mathbf{a} \otimes [(b \times c) + (b' \times c'), (b \times c') + (b' \times c)]\\ &\quad = [(a \times ((b \times c) + (b' \times c'))) + (a' \times ((b' \times c) + (b \times c')),\\ &\qquad\qquad (a' \times ((b \times c) + (b' \times c'))) + (a \times ((b' \times c) + (b \times c')))]\\ &\quad = [((a \times (b \times c)) + (a \times (b' \times c')) + ((a' \times (b' \times c)) + (a' \times (b \times c')),\\ &\qquad\qquad ((a' \times (b \times c)) + (a' \times (b' \times c')) + ((a \times (b' \times c)) + (a \times (b \times c'))]\\ &\quad = [((a \times b) \times c) + ((a \times b') \times c')) + ((a' \times b') \times c) + ((a' \times b) \times c')),\\ &\qquad\qquad ((a' \times b) \times c) + ((a' \times b') \times c') + ((a \times b') \times c)) + ((a \times b) \times c'))]\\ &\quad = [((a \times b) \times c) + ((a' \times b') \times c)) + ((a' \times b) \times c') + ((a \times b') \times c')),\\ &\qquad\qquad ((a' \times b) \times c) + (a \times b') \times c)) + ((a' \times b') \times c') + ((a \times b) \times c'))]\\ &\quad = [((a \times b) + (a' \times b')) \times c) + (((a' \times b) + (a \times b')) \times c')),\\ &\qquad\qquad (((a' \times b) + (a \times b')) \times c)) + (((a' \times b') + ((a \times b)) \times c'))]\\ &\quad = (\mathbf{a} \otimes \mathbf{b}) \otimes \mathbf{c}\end{aligned}$$

(vii) We have

$$\begin{aligned}\mathbf{1} \otimes \mathbf{a} &= [((1 + 1) \times a) + 1 \times a', ((1 + 1) \times a') + 1 \times a]\\ &= [(a + a) + a', (a' + a') + a] = [a + (a + a'), a' + (a' + a)]\\ &= [a + (a + a'), a' + (a + a')] = [a, a'] = \mathbf{a}\end{aligned}$$

(ix) We have, making use of the distributive law and free use of the associative and commutative laws of addition for $\mathbb{Q}^+$,

$$
\begin{aligned}
\mathbf{a} \otimes (\mathbf{b} + \mathbf{c}) &= \mathbf{a} \otimes [b + c, b' + c'] \\
&= [(a \times (b + c)) + (a' \times (b' + c')), (a' \times (b + c)) + (a \times (b' + c'))] \\
&= [((a \times b) + (a \times c)) + ((a' \times b') + (a' \times c')), \\
&\qquad ((a' \times b) + (a' \times c)) + ((a \times b') + (a \times c'))] \\
&= [((a \times b) + (a' \times b')) + ((a \times c) + (a' \times c')), \\
&\qquad ((a' \times b) + (a \times b')) + ((a \times c') + (a' \times c))] \\
&= [(a \times b) + (a' \times b'), (a \times b') + (a' \times b)] \\
&\qquad + [(a \times c) + (a' \times c'), (a \times c') + (a' \times c)] \\
&= (\mathbf{a} \otimes \mathbf{b}) \oplus (\mathbf{a} \otimes \mathbf{c})
\end{aligned}
$$

(x) If $\mathbf{a} \ogreaterthan \mathbf{b}$ and $\mathbf{b} \ogreaterthan \mathbf{c}$, then $a + b' > a' + b$, $b + c' > b' + c$. Thus

$$
\begin{aligned}
(a + c') + (b + b') &= ((a + c') + b) + b' = (a + (c' + b)) + b' \\
&= (a + (b + c')) + b' = a + ((b + c') + b') \\
&= a + (b' + (b + c')) = (a + b') + (b + c') \\
&> (a + b') + (b' + c) = (b' + c) + (a + b') \\
&> (b' + c) + (a' + b) = (a' + c) + (b + b')
\end{aligned}
$$

and, by the cancellation law of Lemma 1.3.9 (iii), $a + c' > a' + c$, whence $\mathbf{a} \ogreaterthan \mathbf{c}$.

(xi) By trichotomy for $\mathbb{Q}^+$, exactly one of the following is true

$$a + b' > a' + b, \; a + b' = a' + b, \text{ or } a' + b > a + b',$$

so exactly one of the corresponding results $\mathbf{a} \ogreaterthan \mathbf{b}$ or $\mathbf{a} = \mathbf{b}$ or $\mathbf{b} \ogreaterthan \mathbf{a}$ is true.

(xii) If $\mathbf{a} \ogreaterthan \mathbf{b}$, then $a + b' > a' + b$, so

$$
\begin{aligned}
(a + c) + (b' + c') &= ((a + c) + b') + c') = (a + (c + b')) + c' \\
&= (a + (b' + c)) + c' = ((a + b') + c) + c' \\
&= (a + b') + (c + c') > (a' + b) + (c + c') \\
&= (a' + c') + (b + c)
\end{aligned}
$$

and $\mathbf{a} \oplus \mathbf{c} \ogreaterthan \mathbf{b} \oplus \mathbf{c}$.

(xiv) By the order rule stated as part (viii) Theorem 2.3.1 we have

$$(1 + 1) + 1 > 1 + 1$$

so $\mathbf{1} \ogreaterthan \mathbf{0}$ and, by trichotomy, $\mathbf{1} \neq \mathbf{0}$.

EXERCISE 3.2.10

Secretly we know that $1 > 0$, but $(-1) \times 1 \not> (-1)$.

In the language of the theorem (repeating our proof of (xiv))

$$(1 + 1) + 1 > 1 + 1 \text{ so } \mathbf{1} = [1 + 1, 1] \oslash [1, 1] = \mathbf{0}.$$

However

$$(-\mathbf{1}) \otimes \mathbf{1} = -\mathbf{1}$$

and

$$\begin{aligned}(-\mathbf{1}) \otimes \mathbf{0} &= [1, 1 + 1] \otimes [1, 1] \\ &= [(1 \times 1) + ((1 + 1) \times 1), (1 \times 1) + ((1 + 1) \times 1] = [1, 1] = \mathbf{0}\end{aligned}$$

whilst $1 \times 1 = 1 \not> 1 + 1 = 1 \times (1 + 1)$ so

$$(-\mathbf{1}) \otimes \mathbf{0} \oslash (-\mathbf{1}) \otimes \mathbf{1}.$$

EXERCISE 3.2.11

(i) Using commutativity of addition for A,

$$\tilde{\mathbf{0}} = \tilde{\mathbf{0}} \oplus \mathbf{0} = \mathbf{0} \oplus \tilde{\mathbf{0}} = \mathbf{0}.$$

(ii) Using commutativity and associativity for addition,

$$\begin{aligned}\mathbf{a}^{\bullet} &= \mathbf{a}^{\bullet} \oplus \mathbf{0} = \mathbf{a}^{\bullet} \oplus (\mathbf{a} \oplus (-\mathbf{a})) \\ &= (\mathbf{a}^{\bullet} \oplus \mathbf{a}) \oplus (-\mathbf{a}) = (\mathbf{a} \oplus \mathbf{a}^{\bullet}) \oplus (-\mathbf{a}) \\ &= \mathbf{0} \oplus (-\mathbf{a}) = (-\mathbf{a}) \oplus \mathbf{0} = -\mathbf{a}\end{aligned}$$

(iii) Using commutativity of multiplication for A,

$$\tilde{\mathbf{1}} = \tilde{\mathbf{1}} \otimes \mathbf{1} = \mathbf{1} \otimes \tilde{\mathbf{1}} = \mathbf{1}.$$

(iv) Using commutativity and associativity for multiplication,

$$\begin{aligned}\mathbf{a}^{\star} &= \mathbf{a}^{\star} \otimes \mathbf{1} = \mathbf{a}^{\star} \otimes (\mathbf{a} \otimes \mathbf{a}^{-1}) \\ &= (\mathbf{a}^{\star} \otimes \mathbf{a}) \otimes \mathbf{a}^{-1} = (\mathbf{a} \otimes \mathbf{a}^{\star}) \otimes \mathbf{a}^{-1} \\ &= \mathbf{1} \otimes \mathbf{a}^{-1} = \mathbf{a}^{-1} \otimes \mathbf{1} = \mathbf{a}^{-1}.\end{aligned}$$

EXERCISE 3.2.12

(i) If $\mathbf{a} \oplus \mathbf{c} = \mathbf{b} \oplus \mathbf{c}$, then

$$\begin{aligned}\mathbf{a} &= \mathbf{0} \oplus \mathbf{a} = \mathbf{a} \oplus \mathbf{0}\\ &= \mathbf{a} \oplus (\mathbf{c} \oplus (-\mathbf{c})) = (\mathbf{a} \oplus \mathbf{c}) \oplus (-\mathbf{c})\\ &= (\mathbf{b} \oplus \mathbf{c}) \oplus (-\mathbf{c}) = \mathbf{b} \oplus (\mathbf{c} \oplus (-\mathbf{c}))\\ &= \mathbf{b} \oplus \mathbf{0} = \mathbf{0} \oplus \mathbf{b} = \mathbf{b}\end{aligned}$$

as required.

(ii) If $\mathbf{a} \otimes \mathbf{c} = \mathbf{b} \otimes \mathbf{c}$ and $\mathbf{c} \neq \mathbf{0}$, then

$$\begin{aligned}\mathbf{a} &= \mathbf{1} \otimes \mathbf{a} = \mathbf{a} \otimes \mathbf{1}\\ &= \mathbf{a} \otimes (\mathbf{c} \otimes \mathbf{c}^{-1}) = (\mathbf{a} \otimes \mathbf{c}) \otimes \mathbf{c}^{-1}\\ &= (\mathbf{b} \otimes \mathbf{c}) \otimes \mathbf{c}^{-1} = \mathbf{b} \otimes (\mathbf{c} \otimes \mathbf{c}^{-1})\\ &= \mathbf{b} \otimes \mathbf{1} = \mathbf{1} \otimes \mathbf{b} = \mathbf{b}\end{aligned}$$

as required.

(iii) If $\mathbf{c} = (-\mathbf{a}) \oplus \mathbf{b}$, then

$$\begin{aligned}\mathbf{a} \oplus \mathbf{c} &= \mathbf{a} \oplus ((-\mathbf{a}) \oplus \mathbf{b}) = (\mathbf{a} \oplus (-\mathbf{a})) \oplus \mathbf{b}\\ &= ((-\mathbf{a}) \oplus \mathbf{a}) \oplus \mathbf{b} = \mathbf{0} \oplus \mathbf{b} = \mathbf{b}.\end{aligned}$$

(iv) If $\mathbf{c} = \mathbf{a}^{-1} \otimes \mathbf{b}$, then

$$\begin{aligned}\mathbf{a} \otimes \mathbf{c} &= \mathbf{a} \otimes (\mathbf{a}^{-1} \otimes \mathbf{b}) = (\mathbf{a} \otimes \mathbf{a}^{-1}) \otimes \mathbf{b}\\ &= (\mathbf{a}^{-1} \otimes \mathbf{a}) \otimes \mathbf{b} = \mathbf{1} \otimes \mathbf{b} = \mathbf{b}.\end{aligned}$$

EXERCISE 3.2.13

By trichotomy, exactly one of these three things must be true:-

$$\mathbf{0} \ogreaterthan -\mathbf{a} \text{ or } -\mathbf{a} = \mathbf{0} \text{ or } -\mathbf{a} \ogreaterthan \mathbf{0}.$$

If $-\mathbf{a} \ogreaterthan \mathbf{0}$ or $-\mathbf{a} = \mathbf{0}$, then

$$\mathbf{0} = \mathbf{a} \oplus (-\mathbf{a}) \ogreaterthan \mathbf{0}.$$

Thus the only possibility is $\mathbf{0} \ogreaterthan -\mathbf{a}$.

The second part follows by a similar argument.

EXERCISE 3.2.14

(i) We have

$$(-\mathbf{a}) \oplus \mathbf{a} = \mathbf{a} \oplus (-\mathbf{a}) = \mathbf{0},$$

so, by the uniqueness result of Exercise 3.2.11 (ii), $-(-\mathbf{a}) = \mathbf{a}$.

(ii) We have

$$\begin{aligned}\mathbf{a} &= \mathbf{1} \otimes \mathbf{a} = \mathbf{a} \otimes \mathbf{1}\\ &= \mathbf{a} \otimes (\mathbf{1} \oplus \mathbf{0}) = (\mathbf{a} \otimes \mathbf{1}) \oplus (\mathbf{a} \otimes \mathbf{0})\\ &= (\mathbf{1} \otimes \mathbf{a}) \oplus (\mathbf{0} \otimes \mathbf{a}) = \mathbf{a} \oplus (\mathbf{0} \otimes \mathbf{a})\end{aligned}$$

Thus, using the associative and commutative laws of addition,

$$\begin{aligned}\mathbf{0} &= \mathbf{a} \oplus (-\mathbf{a}) = \big(\mathbf{a} \oplus (\mathbf{0} \otimes \mathbf{a})\big) \oplus (-\mathbf{a})\\ &= (\mathbf{a} \oplus (-\mathbf{a})) \oplus (\mathbf{0} \otimes \mathbf{a}) = \mathbf{0} \oplus (\mathbf{0} \otimes \mathbf{a})\\ &= (\mathbf{0} \otimes \mathbf{a}) \oplus \mathbf{0} = \mathbf{0} \otimes \mathbf{a} = \mathbf{a} \otimes \mathbf{0}\end{aligned}$$

(iii) We have

$$\begin{aligned}\mathbf{0} &= \mathbf{b} \otimes \mathbf{0} = \mathbf{b} \otimes (\mathbf{a} \oplus (-\mathbf{a}))\\ &= (\mathbf{b} \otimes \mathbf{a}) \oplus (\mathbf{b} \otimes (-\mathbf{a})) = (\mathbf{a} \otimes \mathbf{b}) \oplus ((-\mathbf{a}) \otimes \mathbf{b})\end{aligned}$$

so, by the uniqueness result of Exercise 3.2.11 (ii), $(-\mathbf{a}) \otimes \mathbf{b} = -(\mathbf{a} \otimes \mathbf{b})$.

(iv) We have

$$\begin{aligned}(-\mathbf{a}) \otimes (-\mathbf{b}) &= -\big(\mathbf{a} \otimes (-\mathbf{b})\big) = -\big((-\mathbf{b}) \otimes \mathbf{a}\big)\\ &= -\big(-(\mathbf{b} \otimes \mathbf{a})\big) = \mathbf{b} \otimes \mathbf{a} = \mathbf{a} \otimes \mathbf{b}.\end{aligned}$$

EXERCISE 3.2.15

(i) Using the commutative and associative laws for addition.

$$(\mathbf{a} \oplus \mathbf{b}) \oplus (-\mathbf{a}) \oplus (-\mathbf{b}) = (\mathbf{a} \oplus (-\mathbf{a})) \oplus (\mathbf{b}) \oplus (-\mathbf{b})) = \mathbf{0} \oplus \mathbf{0} = \mathbf{0}$$

so by uniqueness of additive inverses (see Exercise 3.2.11).

(ii) Using the commutative and associative laws for multiplication

$$(\mathbf{a} \otimes \mathbf{b}) \otimes (\mathbf{a}^{-1} \otimes \mathbf{b}^{-1}) = (\mathbf{a} \otimes \mathbf{a}^{-1}) \otimes (\mathbf{b}) \otimes \mathbf{b}^{-1}) = \mathbf{1} \otimes \mathbf{1} = \mathbf{1}$$

so $\mathbf{a} \otimes \mathbf{b} \neq \mathbf{0}$ and, by uniqueness of multiplicative inverses, (see Exercise 3.2.11) $(\mathbf{a} \otimes \mathbf{b})^{-1} = \mathbf{a}^{-1} \otimes \mathbf{b}^{-1}$.

Using the distributive law, the commutative laws for addition and multiplication and the associative law of addition freely together with part (i) of this question and parts (ii) and (iv) of the previous question, we have

$$\begin{aligned}
(\mathbf{a} \oplus (-\mathbf{a}')) \otimes (\mathbf{b} \oplus (-\mathbf{b}')) &= ((\mathbf{a} \oplus (-\mathbf{a}')) \otimes \mathbf{b}) \oplus ((\mathbf{a} \oplus (-\mathbf{a}')) \otimes (-\mathbf{b}')) \\
&= ((\mathbf{a} \otimes \mathbf{b}) \oplus ((-\mathbf{a}') \otimes \mathbf{b})) \oplus ((\mathbf{a} \otimes -\mathbf{b}) \oplus ((-\mathbf{a}') \otimes -\mathbf{b})) \\
&= ((\mathbf{a} \otimes \mathbf{b}) \oplus (-(\mathbf{a}' \otimes \mathbf{b})) \oplus ((-(\mathbf{a} \otimes \mathbf{b})) \oplus (\mathbf{a}' \otimes \mathbf{b}')) \\
&= ((\mathbf{a} \otimes \mathbf{b}) \oplus (\mathbf{a}' \otimes \mathbf{b}')) \oplus ((-(\mathbf{a}' \otimes \mathbf{b}) \oplus (-(\mathbf{a} \otimes \mathbf{b}')) \\
&= ((\mathbf{a} \otimes \mathbf{b}) \oplus (\mathbf{a}' \otimes \mathbf{b}')) \oplus (-((\mathbf{a}' \otimes \mathbf{b}) \oplus (\mathbf{a} \otimes \mathbf{b}'))).
\end{aligned}$$

EXERCISE 3.2.16

(i) $(-\mathbf{1}) \otimes (-\mathbf{1}) = \mathbf{1} \otimes \mathbf{1} = \mathbf{1}$.

(ii) Apply condition (xiii) of Theorem 3.2.7 with $\mathbf{c} = \mathbf{a}$ and $\mathbf{b} = \mathbf{0}$.

(iii) If $\mathbf{a} \oslash 0$ we use (ii). If not, $\mathbf{0} \oslash \mathbf{a}$ and using condition (xii) from Theorem 3.2.7, we have

$$-\mathbf{a} = \mathbf{0} \oplus (-\mathbf{a}) \oslash \mathbf{a} \oplus (-\mathbf{a}) = \mathbf{0}$$

(iv) We note that, if we consider $\mathbb{Q}$, then $\mathbf{1} \otimes \mathbf{0} = \mathbf{0} = \mathbf{0} \otimes \mathbf{0}$ yet $\mathbf{1} \neq \mathbf{0}$.

(v) We have

$$\mathbf{1} = \mathbf{1} \otimes \mathbf{1} \oslash \mathbf{0}$$

so

$$\mathbf{0} = \mathbf{1} \oplus (-\mathbf{1}) = (-\mathbf{1}) \oplus \mathbf{1} \oslash (-\mathbf{1}) \oplus \mathbf{0} = -\mathbf{1}.$$

(vi) $\mathbf{0} \otimes \mathbf{0} = \mathbf{0}$ and, if $\mathbf{a} \neq \mathbf{0}$, then

$$\mathbf{a} \otimes \mathbf{a} \oslash \mathbf{0}.$$

Part (v) and trichotomy tell us that

$$\mathbf{a} \otimes \mathbf{a} \neq -\mathbf{1}.$$

Exercise 3.2.17

If we define $f : \mathbb{Q}^+ \to B/\sim$ by $f(a) = [a+1, 1]$, then, if $f(a) = f(b)$, we have

$$a + (1 + 1) = (a + 1) + 1 = (b + 1) + 1 = b + (1 + 1)$$

so, by the cancellation law for addition, $a = b$. Thus f is injective.

Further

$$\begin{aligned} f(a) \oplus f(b) &= [a+1, 1] \oplus [b+1, 1] = [(a+1) + (b+1), 1+1] \\ &= [((a+b)+1)+1, 1+1] = [a+b+1, 1] = f(a+b) \end{aligned}$$

and, using the distributive, commutative and associative laws and multiplicative property of 1,

$$\begin{aligned} f(a \times b) &= [a+1, 1] \otimes [b+1, 1] \\ &= \big[(a+1) \times (b+1) + (1 \times 1), ((a+1) \times 1) + (1 \times (b+1))\big] \\ &= \big[(a \times b) + (((a + (b+1)) + 1), (a+1) + (b+1)\big] \\ &= \big[((a \times b) + 1) + ((a+b)+1), 1 + ((a+b)+1)\big] \\ &= \big[(a \times b) + 1, 1\big] = f(a) \otimes f(b) \end{aligned}$$

Finally, if $a > b$, then $a + 1 > b + 1$ and $(a+1) + 1 > (b+1) + 1$, so $f(a) = [a+1, 1] \ogreaterthan [b+1, 1] = f(b)$.

Exercise 3.2.20

(i) If $a \in \mathbb{N}^+$, then $a = (a+1) - 1 \in \mathbb{Z}$.

(ii) If a, $b \in \mathbb{Z}$, then $a = a_1 - a_2$, $b = b_1 - b_2$ with a_j, $b_j \in \mathbb{N}^+$ $[j = 1,\ 2]$. Thus

$$\begin{aligned} a + b &= (a_1 + b_1) - (a_2 + b_2) \in \mathbb{Z}, \\ a \times b &= (a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1) \in \mathbb{Z}, \\ -a &= a_2 - a_1 \in \mathbb{Z}. \end{aligned}$$

Exercise 3.2.21

(i) $2 - 1 = 1 \neq -1 = 1 - 2$.

(ii) $2 \div 1 = 1 \neq 1/2 = 1 \div 2$.

(iii) $3 - (2 - 1) = 2 \neq 0 = (3 - 2) - 1$.

(iv) $12 \div (6 \div 2) = 4 \neq 1 = (12 \div 6) \div 2$.

Exercise 3.4.3

The first paragraph of the exercise is a simple (but therefore long) modification of Section 3.2.

Consider the collection X of ordered pairs (n, n') with $n,\ n' \in \mathbb{N}^+$. We say that $(n, n') \sim (m, m')$ if $n + m' = n' + m$.

(a) We observe that, since $n + n = n + n$, we have $(n, n) \sim (n, n)$.

(b) If $(n, n') \sim (m, m')$, then $m + n' = n' + m = n + m' = m' + n$ and so $(m, m') \sim (n, n')$.

(c) If $(n, n') \sim (m, m')$, $(m, m') \sim (p, p')$, then, making free use of the commutative and associative laws of addition,

$$(n+p')+(m+m') = (n+m')+(m+p') = (n'+m)+(m'+p) = (n'+p)+(m+m'),$$

so, using the cancellation law, $n + p' = n' + p$. Thus $(n, n') \sim (p, p')$.

Thus $\sim$ is an equivalence relation and we may consider $X/{\sim}$.

Observe that if $(n, n') \sim (m, m')$ and $(u, u') \sim (v, v')$ we have, making free use of the commutative and associative laws of addition,

$$(n+u)+(m'+u') = (n+m')+(u+u') = (n'+m)+(u+u') = (n'+u')+(m+u)$$

so $(n+u, n'+u') \sim (m+u, m'+u')$. Similarly $(m+u, m'+u') \sim (m+v, m'+v')$, so, by transitivity, $(n + u, n' + u') \sim (m + v, m' + v')$. Thus we may define

$$[(n, n')] \oplus [(m, m')] = [(n + m, n' + m')]$$

unambiguously.

Now suppose $(a, a') \sim (b, b')$ and $(c, c') \sim (d, d')$.

$$\begin{aligned}
&((a \times c) + (a' \times c')) + ((a \times d') + (a' \times d)) \\
&\qquad = ((a \times c) + (a \times d')) + ((a' \times c') + (a' \times d')) \\
&\qquad = ((a \times (c + d'))) + ((a' \times (c' + d))) &(1)\\
&\qquad = ((a \times (c' + d))) + ((a' \times (c + d'))) \\
&\qquad = ((a \times c') + (a \times d)) + ((a' \times c) + (a' \times d')) &(2)\\
&\qquad = ((a \times d) + (a' \times d')) + ((a \times c') + (a' \times c))
\end{aligned}$$

as required. (In addition to the commutative and associative laws of addition and multiplication, we used the distributive law for $\mathbb{N}^+$ at steps (1) and (2).)

A similar calculation now shows that

$$((a\times d)+(a'\times d'), (a\times d')+(a'\times d)) \sim ((b\times d)+(b'\times d'), (b\times d')+(b'\times d))$$

so

$$((a\times c)+(a'\times c'), (a\times c')+(a'\times c)) \sim ((b\times d)+(b'\times d'), (b\times d')+(b'\times d)).$$

Thus we may define

$$[(a,a')] \otimes [(c,c')] = [((a \times c) + (a' \times c'), (a \times c') + (a' \times c))]$$

unambiguously

Suppose $(a,a') \sim (c,c')$ and $a + b' > a' + b$. Then, since $a + c' = a' + c$ we have, using associativity commutativity and the addition inequality law (if $x > y$ then $x + z > y + z$),

$$\begin{aligned}(c + b') + a &= c + (b' + a) = c + (a + b') \\ &> c + (a' + b) = (c + a') + b \\ &= (a + c') + b = a + (c' + b) \\ &= (c' + b) + a = (b + c') + a\end{aligned}$$

We now use Lemma 1.3.9 (iii) to obtain $b + c' > b' + c$

A similar calculation shows that, if $(b,b') \sim (d,d')$ and $b+c' > b'+c$, then $c + d' > c' + d$. Thus, if $(a,a') \sim (c,c')$, $(b,b') \sim (d,d')$ and $a + b' > a' + b$, then $c + d' > c' + d$.

It follows that the definition

$$[(a,a')] \circledcirc [(b,b')] \text{ if and only if } a + b' > a' + b$$

is unambiguous.

The statements and proofs of Theorem 3.2.7 supplemented by Exercise 3.2.9 go over without change, except for Theorem 3.2.7 (viii) which must be replaced by a cancellation law.

If $\mathbf{b} \neq 0$ *and* $\mathbf{a} \otimes \mathbf{b} = \mathbf{0}$ *then* $\mathbf{a} = \mathbf{0}$. (Multiplicative cancellation)

To prove this, suppose $\mathbf{b} \neq \mathbf{0}$. and $\mathbf{a} \otimes \mathbf{b} = \mathbf{0}$. This means that $b \neq b'$ but $(a \times b) + (a' \times b') = (a' \times b) + (a \times b')$. Trichotomy tells us that either $b > b'$ or $b' > b$. Suppose that $b' > b$. Then we know by the rules for $\mathbb{N}^+$ that we can find a $c \in \mathbb{N}^+$ such that $b' = b + c$.

Thus

$$(a \times b) + (a' \times (b + c)) = (a' \times b) + (a \times (b + c))$$

so, using the distributive law,

$$(a \times b) + ((a' \times b) + (a' \times c)) = (a' \times b) + ((a \times b) + (a \times c)).$$

Thus, using the associative and commutative laws of addition freely,

$$(a \times c) + ((a \times b) + (a' \times b)) = (a' \times c) + ((a \times b) + (a' \times b))$$

so, by the cancellation law for addition in $\mathbb{N}^+$,

$$a \times c = a' \times c$$

so, by the cancellation law for multiplication in $\mathbb{N}^+$, $a = a'$ and $\mathbf{a} = \mathbf{0}$. A similar argument applies if $b > b'$.

The verification of the laws for an ordered integral domain (see Definitions 10.4.1 and 10.4.7) follow very closely the verifications we made for Theorem 3.2.7 with one exception.

The construction of an ordered field from an integral domain undertaken in Section 10.4 (Exercises 10.4.11, 10.4.13 and 10.4.15, all of which have written out solutions in these notes) will produce $\mathbb{Q}$ from $\mathbb{N}$.

Exercise 3.4.4

We write out the winning plays (in increasing order within a game).

1	5	9
1	6	8
2	4	9
2	5	8
2	6	7
3	4	8
3	5	7
4	5	6

These are the reordered horizontal, vertical and diagonal lines of the magic square.

6	1	8
7	5	3
2	9	4

If the first player puts an X on any number she chooses and the second player puts a O on any number she chooses, we recover 'Noughts and Crosses'.

Exercise 3.4.8

(i) Not injective, $f_1(1) = f_1(2)$. Not surjective, $f_1(x) \neq 2$ for all $x \in X$. Therefore not bijective.

(ii) Injective, surjective, so bijective from definition.

(iii) Injective since $f_3(1) \neq f_3(2)$. Not surjective, $f_3(x) \neq 3$ for all $x \in X$. Therefore not bijective.

(iv) Surjective, since $f_4(1) = 1$, $f_4(2) = 2$. Not injective, since $f_4(1) = f_4(3)$. So not bijective.

Exercise 3.4.9

(i) Injective since $f_1(r) = f_1(s)$ implies $2 \times r = 2 \times s$ and so (considering $\mathbb{Z}$ as embedded in $\mathbb{Q}$) $r = s$. Not surjective, since $f_1(r) \neq 1$ for all $r \in \mathbb{Z}$. Thus not bijective.

(ii) Injective, since $f_2(r) = f_2(s)$ yields $2 \times r = 2 \times s$ so $r = s$ Surjective since $f_2(2^{-1} \times r) = r$. Thus bijective.

(iii) Surjective, since $f_3(2r) = r$ for every $r \in \mathbb{Z}$. Not injective since $f_3(0) = f_3(1) = 0$. Thus not bijective.

(iv) Not injective, since $f_4(1) = f_4(-1)$. Not surjective, since $f_4(r) \geq 0$ for all $r \in \mathbb{Z}$, but $0 > -1$, so $f_4(r) \neq -1$ for all $r \in \mathbb{Z}$. So not bijective.

Exercise 3.4.11

(i) If $y \in Y$, then, setting $x = g(y)$, we have $f(x) = y$. Thus f is surjective.

If $g(u) = g(v)$, then $u = f(g(u)) = f(g(v)) = v$. Thus g is injective.

(ii) By (i), f and g are bijective. Theorem 3.4.10 and the definition that follows it tell us that $g = f^{-1}$.

(iii) and (iv) Let $X = \{0, 1\}$, $Y = \{0\}$, $f(0) = f(1) = 0$, $g(0) = 0$.

Exercise 3.4.15

(ii) Define the identity function $\iota : A \to A$ by $\iota(a) = a$ for all $a \in A$. Then ι is bijective and $\iota(a) + \iota(b) = a + b = \iota(a + b)$ for all $a, b \in A$.

It follows that ι is an isomorphism and $(A, +) \sim (A, +)$.

(iii) We know that there exist bijections $f : A \to B$ and $g : B \to C$ such that $f(a + a') = f(a) \oplus f(a')$ for all $a, a' \in A$ and $g(b \oplus b') = g(b) \boxplus g(b')$ for all $b, b' \in A$.

We define $h : A \to C$ by $h(a) = g(f(a))$ for $a \in A$.

If $h(a) = h(a')$, then $g(f(a)) = g(f(a')$, so, since g is injective, $f(a) = f(a')$ so, since f is injective, $a = a'$. Thus h is injective.

If $c \in C$ then, since g is surjective, we can find $b \in B$ such that $g(b) = c$ and, since f is surjective we can find $a \in A$ such that $f(a) = b$ and so $h(a) = c$. Thus h is surjective.

Finally

$$h(a+a') = g(f(a+a')) = g(f(a)\oplus f(a')) = g(f(a))\boxplus g(f(a')) = h(a)\boxplus h(a').$$

It follows that h is an isomorphism and $(A, +) \sim (C, \boxplus)$.

Exercise 4.1.2

(i) If $m \in \mathbb{Z}$, then $m > m - 1$.

(If you want to make a meal of this, $m = (m - 1) + 1 > m - 1$.)

(ii) If $a \in E$, then $(a + 1)/2 \in E$, but $a > (a + 1)/2$.

Formally,

$$a = 2^{-1}a + 2^{-1}a > 2^{-1}a + 2^{-1} = 2^{-1}(a + 1) = (a + 1)/2$$

and

$$(a + 1)/2 = 2^{-1}(a + 1) = 2^{-1}a + 2^{-1} > 2^{-1} + 2^{-1} = 1.$$

Exercise 4.1.3

Since $r > n$ the subtraction principle tells us that there is a $u \in \mathbb{N}^+$ such that $r = n + u$. We then have $n + 1 \geq n + u$ so, by cancellation, $1 \geq u$. By the base number principle $u = 1$. Thus $r = n + 1$.

Exercise 4.1.9

(i) If u and v are greatest members, $u \geq v$ and $v \geq u$ so, by trichotomy, $u = v$.

(ii) $\mathbb{N}^+$ itself has no greatest member. (If $n \in \mathbb{N}^+$, then $n + 1 \in \mathbb{N}^+$ and $n + 1 > n$.)

Exercise 4.1.10

Let E be the set of r for which $Q(r)$ is false. If E is non-empty, then it has a least member e_0. By hypothesis, $Q(1)$ is true, so (since 1 is the least element of $\mathbb{N}^+$) we have $e_0 > 1$.

The subtraction rule tells us that, if $a > b$, then we can find a c such that $b + c = a$. Taking $a = e_0$, $b = 1$ we see that there there is a c such that $e_0 = 1 + c = c + 1$. Now e_0 is the least natural number e such that $P(e)$ is false, so $P(r)$ is true for all $r \leq c$ and, by hypothesis, $P(e_0) = P(c + 1)$ is true.

Since the assumption that E is non-empty leads to a contradiction, we must have E empty and we are done.

Exercise 4.1.11

If $m = 1$, there is nothing to prove. If $m > 1$, the subtraction rule tells us that there exists a c such that $m = c + 1$. Let $Q(r)$ be the statement that $P(c+r)$ is true. Then $Q(1)$ is true and $Q(u)$ implies $Q(u+1)$ so, by induction, $Q(u)$ is true for all $u \in \mathbb{N}^+$.

If $n \geq m$ then since $m > c$, we have $n > c$, so there exists a $u \in \mathbb{N}^+$ with $n = c + u$ so, since $Q(u)$ is true, $P(n)$ is true.

Exercise 4.1.13

(i) Suppose, if possible, that

$$n_1 > n_2 > n_3 > \dots.$$

Then, automatically,

$$n_1 \geq n_2 \geq n_3 \geq \dots$$

so, by Lemma 4.1.12, there exists an N such that $n_j = n_N$ for all $j \geq N$. In particular $n_N = n_{N+1}$, so $n_N \not> n_{N+1}$ contrary to our original assumption.

(ii) $-1 > -2 > -3 > \dots$

Exercise 4.2.2

Define $h : S_p \to X$ by $h(r) = f_n(r)$ for all $r \in S_p$. We have $h(1) = f_n(1) = x_1$ and

$$h(r + 1) = f_n(r + 1) = g_{r+1}(f_n(r)) = g_{r+1}(h(r))$$

for all $r \in S_p$ with $r + 1 \leq p$. Thus, by uniqueness $h(r) = f_p(r)$ for all $r \in S_p$. In particular

$$f_n(m) = h(m) = f_p(m).$$

Exercise 4.2.5

(i) Let $n \in \mathbb{N}^+$, $a \in \mathbb{Q}$, $a > 0$. Then $a^{n+0} = a^n = a^n \times 1 = a^n \times a^0$, By commutativity of addition and multiplication, $a^{0+n} = a^0 \times a^n$. Finally $a^{0+0} = a^0 = 1 = 1 \times 1 = a^0 \times a^0$.

(ii) If $a,\ b \in \mathbb{Q}$, then $a^0 \times b^0 = 1 \times 1 = 1 = (a \times b)^0$.

(iii) If n is an integer with $n \geq 0$ and $a \in \mathbb{Q}$, then

$$(a^0)^n = 1^n = 1 = a^0 = a^{0\times n}$$

and

$$(a^n)^0 = 1 = a^0 = a^{0\times n}.$$

Exercise 4.2.6

(i) Let $P(n)$ be the statement that $a^{-n} = (a^{-1})^n$. Since

$$(a^{-1})^1 = a^{-1},$$

it follows that $P(1)$ is true.

Now suppose that $P(n)$ is true for some $n \in \mathbb{N}^+$. Then

$$(a^{(n+1)})^{-1} = (a^n \times a)^{-1} = (a^n)^{-1} \times a^{-1} = (a^{-1})^n \times a^{-1} = (a^{-1})^{n+1}$$

so $P(n + 1)$ is true.

By induction, $P(n)$ is true for all $n \geq 1$, so $a^{-n} = (a^{-1})^n$ for all $n \geq 1$.

Certainly $a^{-0} = a^0 = 1 = (a^{-1})^0$.

If n is a negative integer, then, setting $m = -n$,

$$a^n = a^{-m} = (a^{-1})^m = (a^m)^{-1}$$

so

$$(a^n)^{-1} = ((a^m)^{-1})^{-1} = a^m = a^{-n}.$$

(i) We wish to show that $a^{n+m} = a^n a^m$. We know that the result is true for $n, m \geq 0$. Using the commutativity of addition and multiplication, we need only check the cases $n \geq 0 \geq m$ and $0 > n, m$.

If $0 > n, m$ then

$$a^{n+m} = (a^{-1})^{-(n+m)} = (a^{-1})^{-n}(a^{-1})^{-m} = a^n a^m.$$

.

If $n \geq 0 \geq m$, set $p = -m$. If $n \geq p$, then

$$a^p a^{n+m} = a^p a^{n-p} = a^n$$

so

$$a^{n+m} = (a^p)^{-1} a^n = a^{-p} a^n = a^m a^n = a^n a^m.$$

If $p > n$ then, using the result just obtained,

$$(a^{n+m})^{-1} = a^{(-n)+(-m)} = a^{-n} a^{-m} = (a^n)^{-1}(a^m)^{-1} = (a^n a^m)^{-1}$$

so $a^{n+m} = a^n a^m$ again.

(ii) We wish to check that, if $a, b > 0$, then $(ab)^n = a^n b^n$ for all integers n. We know this true for $n \geq 0$, so we need only check it for $n < 0$.

In this case,

$$(ab)^n = ((ab)^{-1})^{-n} = (a^{-1}b^{-1})^{-n} = (a^{-1})^{-n}(b^{-1})^{-n} = ((a^{-1})^{-1})^n((b^{-1})^{-1})^n = a^n b^n,$$

so we are done.

(iii) We wish to show that $(a^n)^m = a^{nm}$ for all integers n and m.

We first prove it in the case that $m \geq 0$. If $n \geq 0$, we know the result is true. If $n < 0$, then

$$(a^n)^m = \big((a^{-1})^{-n}\big)^m = (a^{-1})^{(-n)\times m} = a^{-((-n)\times m)} = a^{nm},$$

and we are done.

We now prove the result for general m. If $m \geq 0$ we know the result to be true. If $m < 0$ then

$$(a^n)^m = \big((a^n)^{-1}\big)^{-m} = \big((a^{-1})^n\big)^{-m} = (a^{-1})^{n\times(-m)} = a^{-(n\times(-m))} = a^{nm},$$

and we are done.

Exercise 4.2.7

(i) Suppose $b > a$. Let $P(n)$ be the statement that $b^n > a^n$. Since $b^1 = b > a = a^1$, $P(1)$ is true.

If $P(n)$ is true,

$$a^{n+1} = a \times a^n < a \times b^n < b \times b^n = b^{n+1}$$

so $P(n+1)$ is true.

The required result follows by induction

(ii) We set $1! = 1$, $(n+1)! = (n+1) \times n!$

Let $P(n)$ be the statement that $2^{n-1} \leq n! \leq n^n$. Since

$$2^{1-1} = 2^0 = 1 = 1! = 1 = 1^1$$

$P(1)$ is true.

If $P(n)$ is true

$$2^{n+1} = 2 \times 2^n \leq 2 \times n! = (1+1) \times n! \leq (n+1) \times n! = (n+1)!.$$

and

$$(n+1)! = (n+1) \times n! \leq (n+1) \times n^n \leq (n+1) \times (n+1)^n = (n+1)^{n+1}.$$

The required result follows by induction

Exercise 4.3.2

Suppose that E is a non-empty subset of the integers bounded above by M. Then the set F of elements $-n$ with $n \in E$ is a non-empty subset of the integers bounded below by $-M$. Thus F has a least element f. We have $e = -f \in E$ and $-e \leq -g$ for all $g \in E$, so $e \geq g$ for all $g \in E$ and e is the greatest member of E.

Exercise 4.3.3

Let $Q(n) = P(n - m + 1)$. Then $Q(n)$ implies $Q(n+1)$ for all $n \geq 1$ and that $Q(1)$ is true. By induction $Q(n)$ is true for all $n \geq 1$ and so $P(n)$ is true for all $n \geq m$.

Exercise 4.3.6

Without loss of generality, we may suppose $r \geq r'$. Thus $m > r - r' \geq 0$. Since $m(k - k') = r - r'$ this gives us

$$m > m(k - k') \geq 0$$

so, by cancellation, $1 > k - k' \geq 0$, so, since no strictly positive integer is less than 1, we have $k - k' = 0$ so $k = k'$ and $r = r'$.

Exercise 4.3.9

(i) 6. (Note that, so far as this book is concerned, justification will come later.)

(ii) See Exercise 4.3.10.

Exercise 4.3.10

(i) We have

$$\begin{aligned} 156 &= 3 \times 42 + 30 \\ 42 &= 1 \times 30 + 12 \\ 30 &= 2 \times 12 + 6 \\ 12 &= 2 \times 6 \end{aligned}$$

Euclid delivers 6.

(ii) We have

$$\begin{aligned} 107748 &= 1 \times 69126 + 38622 \\ 69126 &= 1 \times 38622 + 30504 \\ 38622 &= 1 \times 30504 + 8118 \\ 30504 &= 3 \times 8118 + 6150 \\ 8118 &= 1 \times 6150 + 1968 \\ 6150 &= 3 \times 1968 + 246 \\ 1968 &= 8 \times 246 \end{aligned}$$

Euclid delivers 246.

Note $107748 = 438 \times 246$, $69126 = 281 \times 246$.

(iii) You are on your own.

Exercise 4.3.13

Suppose that we apply one step of Euclid's algorithm to a pair (u, v) with $u \geq v \geq 1$. If v divides u, then v is, indeed, the highest common factor of u and v, so the algorithm has delivered the right answer. Since e divides v, e divides $d = v$.

If not, then the algorithm delivers a new pair (u', v') with $u' = v$ and

$$u = kv + v'$$

We know that then $u = ae$, $v = be$ for some natural numbers a and b, so $u' = be$,

$$v' = u - kv = ae - kbd = (a - kb)e$$

and e divides u' and v'.

Thus e divides each of the entries in the ordered pairs produced by Euclid's algorithm. Since the final pair has d as second entry, e divides d.

EXERCISE 4.3.14

(i) Observe that, if $r \geq k+1$, then

$$\frac{p}{q} > \frac{1}{r}.$$

thus there must be a least natural number k' such that

$$\frac{p}{q} \geq \frac{1}{k'}.$$

We have

$$\frac{1}{k'-1} > \frac{p}{q} \geq \frac{1}{k'} \qquad \bigstar$$

as required.

If $p/q = 1/k'$, there is nothing to do. Otherwise,

$$\frac{p}{q} = \frac{1}{k'} + \frac{p'}{q'}$$

with

$$p' = k'p - q,\ q' = qk'.$$

Using $\bigstar$, we have

$$q > p(k'-1)$$

so $p - p' = q - p(k'-1)k'p - q > q - q = 0$ and $p > p'$. Observe that if q/p is an integer u, then $k' = u$ and, if p/q is not, then k' is the smallest integer greater than q'/p'.

Applying the Egyptian algorithm r times gives

$$x = \frac{1}{k_1} + \frac{1}{k_2} + \ldots + \frac{1}{k_r} + \frac{p_r}{q_r}$$

where the p_r form a strictly decreasing sequence and the k_j form a strictly increasing sequence. Since a strictly decreasing sequence of positive integers must terminate the algorithm halts and it will halt at an Egyptian fraction expansion.

(ii) Observe that

$$\frac{17}{4} = 4 + \frac{1}{4}$$
$$\frac{4}{17} = \frac{1}{5} + \frac{3}{85}$$
$$\frac{85}{3} = 28 + \frac{1}{3}$$
$$\frac{3}{85} = \frac{1}{29} + \frac{2}{2465}$$
$$\frac{2465}{2} = 1232 + \frac{1}{2}$$
$$\frac{2}{2465} = \frac{1}{1233} + \frac{1}{3039345},$$

so

$$\frac{4}{17} = \frac{1}{5} + \frac{1}{29} + \frac{1}{1233} + \frac{1}{3039345}.$$

Direct calculation (once we are told what to look for) gives

$$\frac{4}{17} = \frac{1}{5} + \frac{1}{30} + \frac{1}{510}.$$

Exercise 4.3.15

(i) In both cases m even and m odd, we have $m > m'$. We have $n' = 2n > n \geq m > m' \geq 2/2 = 1$. Further

$$n'm' + a' = \begin{cases} 2n \times (m/2) + a = nm + a & \text{if } m \text{ is even} \\ 2n(m-1)/2 + (a+n) = nm + a & \text{if } m \text{ is odd} \end{cases}$$

so $n'm' + a' = nm + a$.

Let $(n_1, m_1, a_1) = (N, M, 0)$ We get a sequence of triples (n_j, m_j, a_j) with $m_j > m_{j+1}$, so since a strictly decreasing sequence of natural numbers must halt, the system must halt at $j = k$, say, with $m_k = 1$ (since otherwise we could continue). Since $n_{j+1}m_{j+1} + a_{j+1} = n_jm_j + a_j$, we have $n_jm_j + a_j = n_1m_1 + a_1 = NM$ for each j. Thus writing $(u, 1, w) = (n_k, m_k, a_k)$ we have $MN = u + w$.

Note that n_j, m_j are the first two numbers in the jth row for Egyptian multiplication and a_j is the result of adding the numbers in the third column for the first j rows. Thus Egyptian multiplication works as promised.

(ii) Suppose $n = 2^{s-1}\epsilon_s + 2^{s-2}\epsilon_{s-1} + \ldots + 2^0\epsilon_1$ (with ϵ_j taking the value 0 or 1) and $m = 2^{r-1}\eta_r + 2^{r-2}\eta_{r-1} + \ldots + 2^0\eta_1$ (with η_t taking the value 0 or 1). Then long multiplication instructs us to add those numbers

$$2^t(2^{s-1}\epsilon_s + 2^{s-2}\epsilon_{s-1} + \ldots + 2^0\epsilon_1)$$

for which $\eta_t = 1$ and this is the Egyptian method.

Thus computers, which work in binary, are in some sense, using the Egyptian algorithm.

Exercise 4.3.17

(i) We have $u = rd$, $v = sd$ for some integers r and s, so, if $n = au + bv$, we have $n = ard + bsd = (ar + bs)d$ so d divides n.

By Bézout's identity
$$d = k|u| + l|v|$$
for some integers k and l, so
$$d = Ku + Lv$$
for some integers K and L. If d divides n, $n = Rd$ for some integer R so $n = au + bv$ with $a = RK$, $b = RL$ integers.

(ii) If $u, v > 1$ (so, for example, if $u = 2$, $v = 3$) any non-zero score exceeds 1, so 1 is not a possible score.

By Bézout's identity we can find integers a and b so that
$$1 = au + bv.$$
Let $N = u \times (u|a| + v|b|)$. If $r \geq N$, then
$$r = N + uk + s$$
with $k \geq 0$, $u > s \geq 0$. Thus
$$r = u \times (u|a| + v|b|) + uk + s(au + bv) = (u|a| + sa)u + (u|b| + sb)v$$
and $u|a| + sa \geq (u - s)|a| > 0$, $u|b| + sb \geq (u - s)|b| > 0$.

Exercise 4.3.18

We have $u = \epsilon|u|$, $v = \delta|v|$ with $\epsilon = \pm 1$, and $\delta = \pm 1$. We can find A, B such that $A|u| + B|v| = d$, so, setting $r = \epsilon A$ and $s = \delta B$, we have $ru + sv = d$.

EXERCISE 4.3.19

(i) We have $au + bv = 1$ for some integers a and b so

$$k = (au + bv)k = a(ku) + (bk)v = a(lv) + (bk)v = (al + bk)v$$

and v divides k.

(ii) Suppose that $ru + sv = 1$ and $r'u + s'v = 1$. Then

$$0 = 1 - 1 = (ru + sv) - (r'u + s'v) = (r - r')u + (s - s')v$$

and

$$(r - r')u = (s' - s)v.$$

By part (i), $s - s$ divides u, so there exists an integer k such that $s' - s = ku$. We now have $r - r' = kv$.

(iii) We may write $u = Ud$, $v = Vd$. Bézout's identity $au + bv = d$ gives $aU + bV = 1$, so U and V coprime.

If r, s are integers with

$$ru + sv = d$$

(that is to say $rU + sV = 1$) then integers r' and s' also satisfy

$$r'u + s'v = d$$

(that is to say $r'U + s'V = 1$) if and only if there exists an integer k such that $r - r' = kv$ and $s' - s = ku$.

(iv) If u and v have highest common factor d then Bézout's theorem give $au + bv = d$ for some a and b. If e divides u and v, then $u = EU$, $v = eV$ for some U and V, so

$$d = a(eU) + b(eV) = e(aU + bV)$$

and e divides d.

EXERCISE 4.3.20

Our initial calculations repeat Exercise 4.3.10.

(i) We have

$$\begin{aligned}156 &= 3 \times 42 + 30\\ 42 &= 1 \times 30 + 12\\ 30 &= 2 \times 12 + 6\\ 12 &= 2 \times 6\end{aligned}$$

Euclid delivers 6.

Reversing we get

$$\begin{aligned}6 &= 30 - (2 \times 12)\\ &= (42 - 12) - (2 \times 12) = 42 - (3 \times 12)\\ &= 42 - (3 \times (42 - 30)) = (-2 \times 42) + (3 \times 30)\\ &= (-2 \times 42) + (3 \times (156 - (3 \times 42)) = 3 \times 156 + (-11 \times 42)\end{aligned}$$

so $6 = 3 \times 156 + (-11) \times 42$.

(ii) We have

$$\begin{aligned}107748 &= 1 \times 69126 + 38622\\ 69126 &= 1 \times 38622 + 30504\\ 38622 &= 1 \times 30504 + 8118\\ 30504 &= 3 \times 8118 + 6150\\ 8118 &= 1 \times 6150 + 1968\\ 6150 &= 3 \times 1968 + 246\\ 1968 &= 8 \times 246\end{aligned}$$

Euclid delivers 246.

Reversing we get

$$\begin{aligned}246 &= 6150 - (3 \times 1968)\\ &= 6150 - (3 \times (8118 - 6150)) = (-3 \times 8118) + (4 \times 6150)\\ &= (-3 \times 8118) + (4 \times (30504 - (3 \times 8118))) = -(15 \times 8118) + (4 \times 30504)\\ &= (4 \times 30504) - (15 \times (38622 - 30504) = -(15 \times 38622) + (19 \times 30504)\\ &= -(15 \times 38622) + (19 \times (69126 - 38622)) = (19 \times 69126) - (34 \times 38622)\\ &= (19 \times 69126) - (34 \times (107748 - 69126)) = ((-34) \times 107748) \times (53 \times 69126)\end{aligned}$$

so $246 = (-34) \times 107748 + 53 \times 69126$.

EXERCISE 4.3.21★

Exercise 4.4.4

If $a, b \in S$, then $a = 10n + 1$, $b = 10m + 1$ for some integers $n, m \geq 0$. We have

$$ab = (10n+1)(10m+1) = 10^2nm+10m+10n+1 = (10nm+n+m)\times 10+1 \in S.$$

Let E be the collection of elements in S which are not the product of irreducibles. If E is non-empty, E has a least member e. Automatically, e is not itself irreducible. Thus $e = uv$ with $u, v \in S$ and $u \neq 1$, $v \neq 1$. Thus u, $v < e$, so u and v are the product of irreducibles, so e is, in fact, the product of irreducibles. This contradiction shows that E is empty and every element S can be written as the product of irreducibles.

$3 \times 7 = 21$ which is irreducible (since only factors 3 and 7)
$13 \times 17 = 221$ which is irreducible (since only factors 13 and 17)
$3 \times 7 \times 13 \times 17 = (3 \times 7) \times (13 \times 17)$
$3 \times 17 = 51$ which is irreducible (since only factors 3 and 17)
$7 \times 13 = 101$ which is irreducible (since only factors 7 and 13)
$21 \times 221 = (3 \times 7) \times (13 \times 17) = (3 \times 17) \times (7 \times 13) = 51 \times 101$.

Exercise 4.4.6

If u and v are natural numbers and p is a prime which divides ab, then $ab = kp$ for some k. If p does not divide a, then, since p is a prime, p and a are coprime and, by Exercise 4.3.19 (i), p divides b.

Exercise 4.4.7

Let p be a prime and $P(n)$ be the statement that, if $u_1, u_2, \dots u_n$ are natural numbers and p divides $u_1u_2 \dots u_n$, then p must divide at least one of the u_j.

$P(1)$ is trivially true. Suppose $P(n)$ is true. Then, if $u_1, u_2, \dots u_{n+1}$ are natural numbers and p divides $u_1u_2 \dots u_{n+1}$, we have, writing $u = u_1u_2 \dots u_n$, $v = u_{n+1}$, and applying Theorem 4.4.5, that either p divides u_{n+1} or p divides $u_1u_2 \dots u_n$ in which case, since $P(n)$ is true, p must divide at least one of the u_j with $1 \leq j \leq n$. Thus p must divide at least one of the u_j with $1 \leq j \leq n + 1$.

Since we have shown that $P(n)$ implies $P(n + 1)$, the result follows by induction.

Exercise 4.4.8

(i) Just another way of stating the uniqueness of factorisation.

(ii) If r_j and s_j are simultaneously non-zero, then p_j is a common factor. Thus a necessary condition for coprimality is that r_j and s_j are never both non-zero $[1 \leq j \leq n]$.

Conversely, if r_j and s_j are never both non-zero, k is a common factor of $p_1^{r_1}p^{r_2}\dots p_n^{r_n}$ and $p_1^{s_1}p^{s_2}\dots p_n^{s_n}$, then k cannot have p_j as a factor for any j and cannot be divisible by any prime not of the form p_j. Thus $k = 1$ and the two numbers are coprime.

Exercise 4.4.10

$$(2 \times 3 \times 5 \times 7 \times 11 \times 13) + 1 = 30031 = 509 \times 59.$$

Thus it may not be true that, if $p_1, p_2, \dots p_n$ are all primes less than or equal to p_n

$$N = p_1 p_2 \dots p_n + 1.$$

is itself a prime.

Exercise 4.4.13

Suppose that x is a rational number with $x^2 = a/b$. We may suppose $x > 0$ and so we can write $x = u/v$ with u and v coprime positive integers. Since n, u and v are strictly positive integers, we can find distinct primes p_1, $p_2, \dots p_n$ and integers $h_j,\ k_j,\ s_j,\ t_j \geq 0$ $[1 \leq j \leq n]$ such that

$a = p_1^{h_1}p_2^{h_2}\dots p_n^{h_n}$, $b = p_1^{k_1}p_2^{k_2}\dots p_n^{k_n}$, $u = p_1^{s_1}p_2^{s_2}\dots p_n^{s_n}$, and $v = p_1^{t_1}p_2^{t_2}\dots p_n^{t_n}$

where h_j and k_j are never simultaneously non-zero.

Since $a/b = x^2 = u^2/v^2$, we have $au^2 = bv^2$, so

$$p_1^{h_1+2t_1}p_2^{h_2+2t_2}\dots p_n^{h_n+2t_n} = p_1^{k_1+2s_1}p_2^{k_2+2s_2}\dots p_n^{k_n+2s_n}$$

and, by the uniqueness of factorisation,

$$h_j + 2t_j = k_j + 2s_j.$$

Since h_j and k_j are never simultaneously non-zero, they must both be even, so a and b are squares of integers.

Exercise 4.4.14★

Exercise 5.1.2★

Exercise 5.1.3★

Exercise 5.1.4

As in Exercise 3.2.14 (ii), we have $a \times 0 = 0$ so

$$a = a \times 1 = a \times 0 = 0$$

for all $a \in \mathbb{F}$.

Exercise 5.1.6

$$f(0) = f(0+0) = f(0) \oplus f(0)$$

so

$$\begin{aligned} 0 &= f(0) \oplus (-f(0)) = (f(0) \oplus f(0)) \oplus (-f(0)) \\ &= f(0) \oplus (f(0) \oplus (-f(0))) = f(0) \oplus 0 = f(0). \end{aligned}$$

Again

$$f(1) = f(1 \times 1) = f(1) \otimes f(1)$$

so, either $f(1) = 0$, or multiplying both sides by $f(1)^{-1}$, we have $f(1) = 1$. But f is injective, so $f(1) \neq f(0)$ and $f(1) = 1$.

Exercise 5.1.8

Typical checks.

(i) If $a, b \in \mathbb{G}$, then $a, b \in \mathbb{F}$ so $a + b = b + a$.

(iv) If $a \in \mathbb{G}$, then $-a \in \mathbb{G}$ and $a + (-a) = 0$.

Exercise 5.1.9

Everything goes through word for word.

Exercise 5.1.10

Reflexive $r - r = 0 = 0 \times n$ so $r \sim_n r$.
Symmetric If $r \sim_n s$, then $r - s = kn$ and $s - r = (-k)n$ for some k, so $s \sim_n r$.
Transitive If $r \sim_n s$ and $s \sim_n t$, then $r - s = kn$, $s - t = ln$ and $r - t = (r - s) + (s - t) = (k + l)n$ for some integers k and l so $r \sim_n t$.

If $n = 1$, then $r - s = (r - s) \times 1$, so $r \sim_1 s$ for all r and s. There is a single equivalence class $\mathbb{Z}$.

If $n = 0$, then $r \sim_0 s$ if and only if $r = s$. The equivalence classes are the one point sets $\{r\}$.

If $|n| > |m| > 0$, then $m \nsim_n n$ so the equivalence classes for $\sim_n$ and $\sim_m$ are different. If $|n| > 0 = m$ then $n \nsim_m m$ but $n \sim_m n$ so the equivalence classes are distinct. Thus the equivalence classes are the same for $\sim_n$ and $\sim_m$ only if $m = n$ or $m = -n$.

If $a \sim_m b$, then $a - b = km$ and $b - a = -km$ so $a \sim_{-m} b$. Thus the equivalence classes are the same for $\sim_n$ and $\sim_m$ if $m = n$ or $m = -n$.

Exercise 5.1.12

Since $u - u' = kn$ and $v - v' = ln$ for some integers l and k we have

$$u' + v' = (u - kn) + (v - ln) = u + v + (-k - l)n,$$

so $u + v \sim_n u' + v'$.

Exercise 5.1.14

(ii) We have $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a + b] + [c] = ([a] + [b]) + [c]$.

(v) We have $[a] \times [b] = [a \times b] = [b \times a] = [b] \times [a]$

(vi) We have $[a]\times([b]\times[c]) = [a]\times[b\times c] = [a\times(b\times c)] = [(a\times b)\times c] = [a \times b] \times [c] = ([a] \times [b]) \times [c]$.

(vii) We have $[1] \times [a] = [1 \times a] = [a]$.

Since $n \geq 2$, $1 \nsim_n 0$, so $[0] \neq [1]$.

Exercise 5.1.15

$2^3 \sim 8 \sim 2 \nsim 1 \sim 2^0$.

Exercise 5.1.16

Since $a = a^1$, we have $[a^1] = [a]$. Further $[a^{n+1}] = [a^n \times a] = [a^n] \times [a]$.

Exercise 5.1.17

(i) If $u \neq 0$, and $uv = 0$, then

$$0 = u^{-1} \times 0 = u^{-1} \times (uv) = (u^{-1}u)v = 1 \times v = v.$$

(ii) Since $1 \leq u, v < n$, we have $u \not\equiv 0 \mod n$ and $v \not\equiv 0 \mod n$, but

$$uv \equiv n \equiv 0 \mod n.$$

By part (i), $(\mathbb{Z}_n, +, \times)$ is not a field.

Exercise 5.1.19

Since n and a are coprime, Euclid's algorithm followed by Bézout's method gives us b and c such that $ac + bn = 1$ and so $ac \equiv 1 \mod n$.

Exercise 5.2.2

If $r \not\equiv 0$, then, by Fermat's little theorem (Theorem 5.2.1), $r^{p-1} \equiv 1 \mod p$ so $r^p \equiv r \times r^{p-1} \equiv r \mod p$. If $r \equiv 0$, then $r^p \equiv 0^p \equiv 0 \equiv r \mod p$.

Exercise 5.2.3

$(p-1)^p \equiv p - 1 \not\equiv 1 \equiv (p-1)^0$, although $p \equiv 0 \mod p$.

If $p = 2$, $r^k \equiv r \mod 2$ for all $k,\ r \geq 1$.

Exercise 5.2.4

Since $\mathbb{F}$ is a field (and, in particular, condition (viii) of Definition 5.1.1 holds) we know that if $a \neq 0$ then $a \times r = a \times s$ implies $r = s$. Thus, as x ranges over the $n-1$ non-zero elements of $\mathbb{F}$, $a \times x$ ranges over $n-1$ distinct non-zero elements of $\mathbb{F}$, so over the $n-1$ non-zero elements of $\mathbb{F}$.

We thus have, using the commutative and associative laws of multiplication together with the product notation, (see Appendix A, if necessary)

$$\prod_{x \in \mathbb{F}, x \neq 0} ax = \prod_{x \in \mathbb{F}, x \neq 0} x,$$

so

$$a^{n-1} \prod_{x \in \mathbb{F}, x \neq 0} x = \prod_{x \in \mathbb{F}, x \neq 0} x$$

and, since $\prod_{x \in \mathbb{F}, x \neq 0} x$ is the product of non-zero elements, $\prod_{x \in \mathbb{F}, x \neq 0} x \neq 0$ (proof by induction). Thus $a^{n-1} = 1$.

Exercise 5.2.5

(i) If $1 \leq s \leq p-1$, then p and s are coprime. Thus, if $1 \leq r \leq p-1$, it follows that $r!$ and $(p-r)!$ are coprime to p. Thus

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}$$

is divisible by p and

$$\binom{p}{r} \equiv 0 \mod p.$$

(ii) By the binomial theorem,

$$\begin{aligned}(k+1)^p &\equiv \binom{p}{0} + \binom{p}{1}k + \binom{p}{2}k^2 + \ldots + \binom{p}{p-1}k^{p-1} + \binom{p}{p}k^p \\ &\equiv 1 + 0 + 0 + \ldots + 0 + k^p \equiv 1 + k^p \mod p.\end{aligned}$$

(iii) $1^p \equiv 1$ and, if $k^p \equiv k$, then $(k+1)^p \equiv k^p + 1 \equiv k+1 \mod p$. Thus, by induction, $k^p \equiv k \mod p$ for all $k \in \mathbb{N}^+$ and so $k^p \equiv k \mod p$ for all k.

Exercise 5.2.7

If $x^2 \equiv 0 \mod p$, then p divides x^2, so (since if p divides uv, then p divides u and or p divides v) p divides x and so $x \equiv 0 \mod p$. We observe that $0^2 \equiv 0$.

Exercise 5.2.8

Recall that $x^2 \equiv a$ has two distinct roots or none, unless $a \equiv 0$, in which case, there is one root. Now observe that

$$-r \not\equiv r,\ r^2 \equiv (-r)^2$$

for $1 \leq r \leq (p-1)/2$ and that $[0]$ together with the $[r]$ and $[-r]$ where $1 \leq r \leq (p-1)/2$ form the distinct elements of $\mathbb{Z}_p$. The squares in $\mathbb{Z}_p$ are thus precisely the distinct elements $[0], [1]^2, \ldots, [(p-1)/2]^2$ and there are $(p-1)/2 + 1 = (p+1)/2$ of them.

Exercise 5.2.9

By inspection, both elements $0 \equiv 0^2$ and $1 \equiv 1^2$ of $\mathbb{Z}_2$ are squares and $x^2 \equiv a \mod 2$ always has exactly one solution.

Exercise 5.2.11

We have $(2-1)! \equiv 1! \equiv 1 \equiv -1 \mod 2$.

Exercise 5.3.1

$- \bullet \bullet \star - - - \star \star - - \star - - - \star \bullet - \bullet \star \bullet \star \star$

Exercise 5.3.2

(ii) 0000101100011000000010111001010110001100000000000

(iii) WELL$\star$DONE$\star\star$

Exercise 5.3.3

(i) We have

$$\zeta_8 \equiv -\zeta_8 \equiv 0 - \zeta_8 \equiv (\zeta_1 + \zeta_2 + \ldots + \zeta_8) - \zeta_8 \equiv \zeta_1 + \zeta_2 + \ldots + \zeta_7 \mod 2$$

Completely symmetric over the ζ_j, so any one particular ζ_j may be considered a check digit.

(ii) Dull answer, no. If the jth person takes n_j lumps and all the n_j are odd, then

$$n_1 + n_2 + \ldots + n_7 \equiv 1 + 1 + \ldots + 1 \equiv 1 \not\equiv 0 \equiv 20 \mod 2.$$

Joke answer, yes. Let each of the first 6 take one lump. The final participant must take 14, which is very odd number of lumps to put in your tea.

Exercise 5.3.4

If $\zeta_j \neq \zeta_j'$ for r values of j,

$$\begin{aligned}
\zeta_1' + \zeta_2' + \ldots + \zeta_8' &\equiv (\zeta_1' + \zeta_2' + \ldots + \zeta_8') - 0 \\
&\equiv (\zeta_1' + \zeta_2' + \ldots + \zeta_8') - (\zeta_1 + \zeta_2 + \ldots + \zeta_8) \\
&\equiv (\zeta_1' - \zeta_1) + (\zeta_2' - \zeta_2) + \ldots + (\zeta_8' - \zeta_8) \\
&\equiv r \equiv 0 \mod 2
\end{aligned}$$

if and only if r is even.

EXERCISE 5.3.5

(i) A typical example is 0201541998 for which

$$10 \times 0 + 9 \times 2 + 8 \times 0 + 7 \times 1 + 6 \times 5 + 5 \times 4 + 4 \times 1 + 3 \times 9 + 2 \times 9 + 1 \times 8$$
$$\equiv 0 - 4 + 0 - 4 - 3 - 2 + 4 + 5 - 4 - 3 \equiv -11 \equiv 0 \quad \text{mod } 11.$$

(ii) If **a** and **b** are ISBNs and $a_i = b_i$ for $i \neq j$, then

$$\begin{aligned} 0 &\equiv 0 - 0 \\ &\equiv (10a_1 + 9a_2 + \ldots + 2a_9 + a_{10}) - (10b_1 + 9b_2 + \ldots + 2b_9 + b_{10}) \\ &\equiv j(a_j - b_j) \end{aligned}$$

so, since 11 is a prime and $1 \leq j \leq 10$ (so $j \not\equiv 0$), we have $a_j - b_j \equiv 0$ mod 11 and so $a_j - b_j = 0$, so $\mathbf{a} = \mathbf{b}$. Thus two ISBNs cannot differ in exactly one place.

(iii) Let $a_{10} = 1$, $a_1 = 1$, $b_{10} = 2$, $b_1 = 2$ and $a_j = b_j = 0$ otherwise. Then **a** and **b** are ISBNs differing in two places only.

(iv) and (v) [Treated together since the answer to (v) is yes] Suppose that $10 \geq j > k \geq 1$. If **a** and **b** are ISBNs, $a_i = b_i$ for $i \neq j, k$ and $a_j = b_k$, $a_k = b_j$ then

$$\begin{aligned} 0 &\equiv 0 - 0 \\ &\equiv (10a_1 + 9a_2 + \ldots + 2a_9 + a_{10}) - (10b_1 + 9b_2 + \ldots + 2b_9 + b_{10}) \\ &\equiv (j - k)(a_j - a_k) \end{aligned}$$

so, since 11 is a prime and $1 \leq j - k \leq 10$ (so $j - k \not\equiv 0$), we have $a_j - a_k \equiv 0$ mod 11 and so $a_j - a_k = 0$, $a_j = a_k = b_j = b_k$ and $\mathbf{a} = \mathbf{b}$.

(vi) If there is a single error taking $\mathbf{x}$ to $\mathbf{x}'$

$$x_1' + 3x_2' + x_3' + 3x_4' + \cdots + x_{11}' + 3x_{12}' + x_{13}'$$

is congruent to $3y$ or y with $1 \leq |y| \leq 9$ and so (since 3 is coprime to 10) is not congruent to 0. Thus single errors are detected.

However if $x_1 = x_2' = 0$, $x_2 = x_1' = 5$ and $x_j = x_j' = 0$ otherwise, $\mathbf{x}$ and $\mathbf{x}'$ satisfy the check-sum condition. Thus not all transpositions can be detected.

Exercise 5.3.6

$$c_1 \equiv c_3 + c_5 + c_7 \mod 2$$
$$c_2 \equiv c_3 + c_6 + c_7 \mod 2$$
$$c_4 \equiv c_5 + c_6 + c_7 \mod 2$$

Since each of c_3, c_5, c_6, c_7 can be chosen freely in 2 ways and the remaining c_j are fixed, it follows that there are exactly $2\times 2\times 2\times 2 = 2^4 = 16$ possible words.

Exercise 5.3.8

Observe that the correcting system sees eight possible outcomes. Each of these is produced by either no mistake (in which case, the correcting system makes no change) or one mistake (in which case, the correcting system makes one change correcting the one mistake). Thus whatever the system sees, it returns a code word and changes at most one entry.

Thus, if there are two (or more) mistakes, it will return a code word, but will have made at most one change, so it will not return the initial code word.

Exercise 5.3.9

Observe that the numbers chosen are the

$$u = c_1 + 2c_2 + 4c_3 + \ldots + 2^7 c_7$$

with the $(c_1, c_2, \ldots, c_7)$ Hamming code words. We place u in A_j if and only if $c_j = 1$. When you state whether or not u is in A_j, I take $c'_j = 1$ if you answer yes and $c'_j = 0$ if you answer no. The Hamming procedure reveals the j (if any) with $c'_j \neq c_j$, so I can find which j (if any) has $c_j \neq c'_j$ (that is to say, where you lied) and recover u.

EXERCISE 5.3.10

(i) The tape will be accepted if each line contains an even number of errors. Since the probability of errors is small (and the number of bits, that is to say, zeros and ones, on each line is small) the probability of one error is much greater than the probability of an odd number of errors greater than 1. Thus

$$\begin{aligned}\Pr(\text{odd number of errors in one line}) &\approx \Pr(\text{exactly one error in one line})\\ &= 8\times 10^{-4}\times(1-10^{-4})^7 \approx 8\times 10^{-4}.\end{aligned}$$

Since the the probability λ of an odd number of errors in one line is very small, but there are a large number N of lines, we may use the Poisson approximation to get

$$1-\Pr(\text{odd number of errors in some line}) \approx e^{-\lambda N} \approx e^{-8} \approx 0.00034$$

and conclude that the probability of acceptance is less than .04%.

If we use the Hamming scheme, then, instead of having 7 freely chosen bits (plus a check bit) on each line, we only have 4 freely chosen bits (plus three check bits plus an unused bit) per line so we need approximately

$$\frac{1}{4}\times 7\times 10^4 = 1.75\times 10^4$$

lines.

If a line contains at most one error, it will be correctly decoded. A line will fail to be correctly decoded if it contains two errors or more (see Exercise 5.3.8). Since the probability of errors is small (and the number of bits on each line is small), the probability of two errors is much greater than the probability of more than two. Thus

$$\begin{aligned}\Pr(\text{decoding failure for one line}) &\approx \Pr(\text{exactly two errors in one line})\\ &= \binom{7}{2}\times(10^{-4})^2\times(1-10^{-4})^5 \approx 21\times 10^{-8}.\end{aligned}$$

Since the the probability of a decoding error in one line is very small but there are a large number of lines, we may use the Poisson approximation (or just a calculator) to get

$$\begin{aligned}\Pr(\text{decoding error for some line}) &= 1-\Pr(\text{no decoding error in any line})\\ &\approx 1-e^{-21\times 10^{-8}\times 17500} \approx 1-e^{-.003675} \approx 1-.9963 \approx 0.0037\end{aligned}$$

and conclude that the probability of a correct decode is greater than 99.6%.

(ii) The probability of one error or less in one particular line is

$$(9/10)^7 + 7\times(1/10)\times(9/10)^6 < .86$$

so with high probability many lines will be wrongly corrected.

EXERCISE 5.3.11

We work in $\mathbb{Z}_2$ and use words of length 15 The words $c_1c_2c_3\dots c_{15}$ with $c_j \in \mathbb{Z}_2$ are chosen to satisfy four conditions obtained as follows.

Observe that (working in $\mathbb{Z}$) each integer r with $1 \le r \le 15$ can be written uniquely as

$$r = \epsilon_0(r) + \epsilon_1(r)2 + \epsilon_2(r)2^2 + \epsilon_3(r)2^3$$

with ϵ_j taking the values 0 or 1. Our four conditions are

$$(\text{The sum of those } c_r \text{ with } \epsilon_j(r) = 1) \equiv 0 \mod 2$$

or more briefly

$$\sum_{\epsilon_j(r)=1} c_r \equiv 0 \mod 2 \qquad \text{(j)}$$

for $0 \le j \le 3$.

If one mistake is made in the kth place and $\mathbf{c}'$ is received then $c'_j = c_j$ for $j \ne k$ and $c'_k \equiv c_k + 1 \mod 2$. Thus

$$\sum_{\epsilon_j(r)=1} c'_r \equiv 0 \mod 2$$

if $\epsilon_j(k) = 0$ and

$$\sum_{\epsilon_j(r)=1} c'_r \equiv 1 \mod 2$$

if $\epsilon_j(k) = 1$.

If the received word satisfies all the Hamming conditions then we take it to be the sent word. Otherwise we proceed as follows. If the received word satisfies the jth condition that is to say

$$\sum_{\epsilon_j(r)=1} c'_r \equiv 0 \mod 2 \qquad \text{(j)}$$

write $\eta_j = 0$. If the received word fails to satisfy the jth Hamming condition, that is to say,

$$\sum_{\epsilon_j(r)=1} c'_r \equiv 1 \mod 2 \qquad \text{(j)}$$

write $\eta_j = 1$. Then $k = \eta_0 + 2\eta_1 + 2^2\eta_2 + 2^3\eta_3$ and $c_j = c'_j$ for $j \ne k$, $c_k \equiv c'_k + 1 \mod 2$.

In constructing a code word, we can choose c_j freely for $j \ne 1, 2, 4, 8$, c_1, c_2, c_4 and c_8. are then fixed. The original Hamming code uses 3 out of 7 places for check digits, so 3/7 of the transmitted bits do not convey information. Thus the coded message costs 7/4 times as much to transmit as the uncoded message. The new scheme only uses 4 out of 15 places for check digits, so 4/15 of the transmitted bits do not convey information and the coded message only costs 15/11 times as much to transmit as the original message. However it will fail to correct if there are more than one error in a 15 bit word and the probability of this happening is not negligible unless the error rate is very low.

Exercise 5.4.1

We have found u_1 and u_2 such that

$$u_1 n_1 + u_2 n_2 = 1.$$

Thus, if we set $y_2 = u_1 n_1$,

$$\begin{aligned} y_2 &\equiv u_1 n_1 \equiv 1 - u_2 n_2 \equiv 1 \mod n_2 \\ y_2 &\equiv u_1 n_1 \equiv 0 \mod n_1. \end{aligned}$$

Exercise 5.4.4

We first solve

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \end{aligned}$$

Applying Euclid's algorithm to 3 and 5,

$$\begin{aligned} 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$

and now applying Bézout's method,

$$1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 1 \times 3) = -1 \times 5 + 2 \times 3.$$

Thus

$$\begin{aligned} -5 &\equiv 1 \mod 3 \\ -5 &\equiv 0 \mod 5 \end{aligned}$$

$$\begin{aligned} 6 &\equiv 0 \mod 3 \\ 6 &\equiv 1 \mod 5 \end{aligned}$$

Thus if we consider $2 \times (-5) + 3 \times 6 = 8$ we have

$$\begin{aligned} 8 &\equiv 2 \mod 3 \\ 8 &\equiv 3 \mod 5 \end{aligned}$$

We now solve

$$\begin{aligned} x &\equiv 8 \mod 15 \\ x &\equiv 2 \mod 7 \end{aligned}$$

Euclid's algorithm applied to 7 and 15 stops at once, giving

$$15 = 2 \times 7 + 1$$

and the Bézout equation

$$1 = 15 - 2 \times 7.$$

Thus

$$
\begin{aligned}
-14 &\equiv 1 \quad \text{mod } 15\\
-14 &\equiv 0 \quad \text{mod } 7
\end{aligned}
$$

$$
\begin{aligned}
15 &\equiv 0 \quad \text{mod } 15\\
15 &\equiv 1 \quad \text{mod } 7
\end{aligned}
$$

Thus if we consider $8 \times (-14) + 2 \times 15 = -82$ we have

$$
\begin{aligned}
-82 &\equiv 8 \quad \text{mod } 15\\
-82 &\equiv 2 \quad \text{mod } 7
\end{aligned}
$$

Thus

$$
\begin{aligned}
x &\equiv 2 \quad \text{mod } 3\\
x &\equiv 3 \quad \text{mod } 5\\
x &\equiv 2 \quad \text{mod } 7.
\end{aligned}
$$

if and only if $x = -82 + n \times (3 \times 5 \times 7) = -82 + n \times 105$ for some integer n, or, equivalently, if and only if $x = 23 + m \times 105$ for some integer m.

Of course we could have got here sooner by judicious guess work, but, if the numbers chosen are even a little bigger, judicious guess work is much harder.

Exercise 5.4.5

Consider the the system $\bigstar_m$

$$\begin{aligned} x &\equiv a_1 \quad \bmod n_1 \\ x &\equiv a_2 \quad \bmod n_2 \\ &\vdots \\ x &\equiv a_m \quad \bmod n_m \end{aligned}$$

where $n_1, n_2, \ldots n_m$ are positive integers with each pair n_i, n_j $[i \neq j]$ coprime.

$\bigstar_1$ is solved just by repeating the equation $x \equiv a_1 \bmod n_1$.

If the general solution of $\bigstar_{m-1}$ has been obtained as

$$x \equiv b_{m-1} \quad \bmod n_1 n_2 n_3 \ldots n_{m-1}$$

then, since $n_1 n_2 n_3 \ldots n_{m-1}$ and n_m are coprime, applying the method of this chapter gives the general solution

$$x \equiv b_m \quad \bmod n_1 n_2 n_3 \ldots n_m$$

to the system

$$\begin{aligned} x &\equiv b_{m-1} \quad \bmod n_1 n_2 \ldots n_{m-1} \\ x &\equiv a_m \quad \bmod n_m \end{aligned}$$

and so to $\bigstar_m$.

Exercise 5.4.6

We have
$$n = p_1^{r(1)} \times p_2^{r(2)} \times \dots p_k^{r(k)}$$
with the p_j distinct primes and $r(j) \geq 1$. There are two cases.

If $k = 1$ then, since n is not a prime, $r(1) \geq 2$ and, since $n \geq 5$,
$$p_1, 2p_1, 3p_1, \dots, r(1)p_1 \leq n - 1,$$
so
$$r(1)!n = r(1)!p_1^{r(1)} = p_1 \times (2p_1) \times (3p_1) \times \dots (r(1)p_1)$$
divides $(n-1)!$ and so $(n-1)! \equiv 0 \mod n$.

If $k \geq 2$, then $p_j, 2p_j, 3p_j, \dots, r(j)p_j \leq n - 1$ so
$$r(j)!n = r(j)!p_j^{r(j)} = p_j \times (2p_j) \times (3p_j) \times \dots (r(j)p_j)$$
divides $p_j^{r(j)}$ and so $(n-1)! \equiv 0 \mod p_j^{n(j)}$ for each j. The Chinese remainder theorem tells us that $(n-1)! \equiv 0 \mod n$.

$$\begin{aligned}
(2-1)! &\equiv 1! \equiv 1 \not\equiv 0 \mod 2\\
(3-1)! &\equiv 2! \equiv 2 \not\equiv 0 \mod 3\\
(4-1)! &\equiv 3! \equiv 6 \not\equiv 0 \mod 4
\end{aligned}$$

EXERCISE 5.4.7

(i) If

$$y \equiv a_1 \mod n_1$$
$$y \equiv a_2 \mod n_2$$

then, since d divides n_1 and n_2,

$$y \equiv a_1 \mod d$$
$$y \equiv a_2 \mod d$$

so $a_1 - a_2 \equiv (a_1 - y) - (a_2 - y) \equiv 0 - 0 = 0 \mod d$

(ii) By Bézout's theorem we can find integers u_1 and u_2 with

$$u_1 n_1 + u_2 n_2 = d$$

If $z = u_1 n_1$, then

$$z \equiv 0 \mod n_1$$
$$z \equiv d \mod n_2$$

(iii) If $a_1 - a_2 \equiv 0 \mod d$, then $a_2 = a_1 + kd$ for some k and the system

$$x \equiv a_1 \mod n_1$$
$$x \equiv a_2 \mod n_2$$

is solved by $x = a_1 + kz$ with z as in (ii).

Exercise 5.5.2

(i) The equation

$$x^2 \equiv 1 \mod p$$

has exactly two solutions 1 and -1. The equation

$$x^2 \equiv 0 \mod q$$

has one root 0.

The Chinese remainder theorem tells us that the equation $x^2 \equiv 1 \mod pq$ has two distinct roots given by the two different sets of modular equations

$$\begin{cases} x \equiv 1 \mod p \\ x \equiv 0 \mod q \end{cases} \quad \begin{cases} x \equiv -1 \mod p \\ x \equiv 0 \mod q \end{cases}$$

If we denote the solution of the first set by η, then the the solution of the second set is $-\eta$.

Thus $x^2 \equiv a^2 \mod pq$ has 2 distinct roots ηa and $-\eta a$, so we are done.

(ii) If $a \equiv 0 \mod p$ and $a \equiv 0 \mod q$ then $a \equiv 0 \mod pq$. The equation

$$x^2 \equiv 0 \mod p$$

has one root 0 and the equation

$$x^2 \equiv 0 \mod q$$

has one root 0. The Chinese remainder theorem tells us that the equation $x^2 \equiv 0 \mod pq$ has one root, 0.

(iii) Consider the integers $0 \leq r \leq pq - 1$. Exactly one of them is 0. Exactly $(p-1)$ are divisible by p but not q and of these $(p-1)/2$ are squares (since each square of this form has two roots of the same type). Exactly $(q-1)$ are divisible by q but not p and of these $(q-1)/2$ are squares. Exactly $pq-(p-1)-(q-1)-1$ are not divisible by p or q so $(pq-p-q+1)/4$ of these are squares (since each square of this form has four roots of the same type). Thus

$$\begin{aligned} 1 + \frac{p-1}{2} + \frac{q-1}{2} + \frac{pq-(p-1)-(q-1)-1}{4} & \\ = \frac{4+2(p-1)+2(q-1)+pq-(p-1)-(q-1)-1}{4} & \\ = \frac{1+p+q+pq}{4} = \frac{(p+1)(q+1)}{4} & \end{aligned}$$

elements of $\mathbb{Z}_{pq}$ are squares.

Exercise 5.5.3

We seek the solution of

$$x \equiv 1 \mod 7$$
$$x \equiv -1 \mod 13$$

Euclid's algorithm gives

$$13 = 7 + 6$$
$$7 = 6 + 1$$

so using Bézout's method

$$1 = 7 - 6 = 7 - (13 - 7) = (2 \times 7) - 13$$

so

$$-13 \equiv 1 \mod 7$$
$$-13 \equiv 0 \mod 13$$

$$14 \equiv 0 \mod 7$$
$$14 \equiv 1 \mod 13$$

Thus $x = -13 - 14 = -27$ is a solution. The two required roots are -27 and 27 (as may be checked by direct calculation).

EXERCISE 5.5.6

We apply Euclid's algorithm to 437 and 112.

$$\begin{aligned}437 &= (3\times 112) + 101\\ 112 &= 101 + 11\\ 101 &= (9\times 11) + 2\\ 11 &= (5\times 2) + 1\end{aligned}$$

so, using Bézout's method,

$$\begin{aligned}1 &= 11 - (5\times 2) = 11 - (5\times(101 - (9\times 11))) = (46\times 11) - (5\times 101)\\ &= (46\times(112 - 101)) - (5\times 101) = (46\times 112) - (51\times 101)\\ &= (46\times 112) - (51\times(437 - (3\times 112)))\\ &= ((-51)\times 437) + (199\times 112).\end{aligned}$$

Thus, if we take $c \equiv 199 \mod 437$, we have $c \times 112 \equiv 1 \mod 437$.

Now consider $\eta \equiv c \times 302 \equiv 229$. We know that η is a square root of 1 modulo 437.

Applying Euclid's algorithm to 437 and $229 + 1 = 230$ we get

$$\begin{aligned}437 &= 230 + 207\\ 230 &= 207 + 23\\ 207 &= 9\times 23\end{aligned}$$

so 23 is one prime factor of 437 and, by division, the other is 19

EXERCISE 5.5.7

$$2^{10} = 1024 > 10^3$$

so $2^{-10} < 10^{-3}$ (and $2^{10} \approx 10^{-3}$).

The probability of failure in 400 attempts is

$$2^{-400} = (2^{-10})^{40} \le (10^{-3})^{40} = 10^{-120}$$

Exercise 5.5.8

$$u = ku' + v' \geq u' + v' > v' + v' = 2v' = 2u''$$

Thus the first entry in (u, v) at least halves every two steps. Thus in $2r$ steps the first entry decreases by a factor of at least 2^{-r}. In $20m$ steps the first entry deceases by a factor of at least 2^{10m} so if $U \leq 10^{3m}$ the process terminates in less than $20m$ steps.

Exercise 5.5.9

(i) We require $m-1$ squarings (so multiplications) to obtain $a^2, a^4, \dots, a^{2^m}$ and we then need to multiply at most $m+1$ numbers together which requires at most m multiplications. We require at most $2m - 1$ multiplications.

(ii) We have (working modulo 23)

$$\begin{aligned} 7^2 &\equiv 3 \\ 7^4 &\equiv 9 \\ 7^8 &\equiv -11 \\ 7^{16} &\equiv 6 \\ 7^{32} &\equiv -10 \\ 7^{64} &\equiv 8 \end{aligned}$$

so

$$7^{100} \equiv 7^{64} \times 7^{32} \times 7^4 \equiv 8 \times (-10) \times 9 \equiv (-11) \times 9 \equiv -7 \equiv 16.$$

Exercise 5.5.10

(i) Observe that, if $q_j \equiv 1 \mod 4$, then
$$q_1 q_2 \dots q_r \equiv 1^r \equiv 1 \mod 4.$$
Thus, if N has the prime factorisation
$$N = q_1 q_2 \dots q_r,$$
we have $N = 4n + 1$ for some n.

It follows that $N = 4M + 3$ (note N is odd, so 2 is not a factor) must have a prime factor p with $p \equiv 3 \mod 4$.

(ii) Suppose, if possible, that there are only finitely many primes $p_0 = 3$, $p_1, p_2, \dots, p_k$ of the form $4n + 3$. Then
$$N = 4(p_1 p_2 \dots p_k) + 3$$
is not divisible by any of $p_1, p_2, \dots, p_k$, but is divisible by some prime of the form $4n + 3$. Thus our initial assumption is false and the required result is true.

Exercise 5.5.11

If $4M^2 + 1$ is divisible by a prime p then
$$(2M)^2 \equiv -1 \mod p$$
so, by lemma 5.2.12 (i), p must have the form $4n + 1$.

Suppose, if possible, that there are only finitely many primes $p_1, p_2, \dots, p_k$ of the form $4n + 1$. Then
$$N = 4(p_1 p_2 \dots p_k)^2 + 1$$
is not divisible by any of $p_0, p_1, p_2, \dots, p_k$, but is divisible by some prime which, by the previous paragraph, must have the form $4n + 1$. Thus our initial assumption is false and the required result is true.

Exercise 5.5.12

Write u and v for the first and second encoded message. Observe that N and N' are coprime. (If not, I really have been stupid, since Euclid's algorithm will now give SNDO the common factor.) SNDO can use the known N and N' together with the Chinese remainder theorem to compute w with $w \equiv m^2 \pmod{NN'}$ and $0 \le w \le NN' - 1$. But $0 \le m^2 \le NN' - 1$, so $w = m^2$ and m is the positive square root of w.

[SNDO uses Euclid's algorithm to find a, b with $aN + bN' = 1$. If $w \equiv bN'u + aNv \pmod{NN'}$, then $w \equiv u \pmod{N}$ and $w \equiv v \pmod{N'}$.]

SNDO is no further forward in reading other messages. Effectively SNDO knows m and m^2 (modulo N) in one case and nothing else (since N' and m^2 (modulo N') are irrelevant).

Exercise 6.1.1

(i) (P1) False, since $1 = S_1(1)$.
(P2) True. If $x, y \in \mathbb{N}_1^+$, then $y = x$.
(P3) True. If $1 \in E$, then $E = \{1\} = \mathbb{N}_1^+$.

(ii) (P1) True, since $1 \neq S(1), S(2)$.
(P2) False. $1 \neq 2$ and $S_2(1) = S_2(2)$.
(P3) True. Suppose $1 \in E$ and whenever $x \in E$, we have $S(x) \in E$, Then $2 = S_2(1) \in E$, so $E = \mathbb{N}_2^+$.

(iii) (P1) True. If x is a positive integer then $S(x) = x + 1 > 1$. If $x = n + 1/2$ with n an integer then $S(x) = (n + 1) + 1/2$ is not an integer. In either case $Sx \neq 1$.
(P2) True. If $x, y \in \mathbb{N}_3^+$ and $Sx = Sy$, then $x + 1 = y + 1$, so $x = y$.
(P3) False. Let E be the set of all strictly positive integers. Then $1 \in E$ and $x \in E$ implies $Sx = x + 1 \in E$, but $1/2 \notin E$.

Exercise 6.3.2

Uniqueness We first prove that there is at most one function with the desired properties. Suppose that μ_x and ϕ_x have the properties stated so that

(a) $\phi_x(1) = x$

(b) $\phi_x(y') = \phi_x(y) + y$ for all natural numbers y.

Let E be the set of natural numbers y such that $\phi_x(y) = \mu_x(y)$. Condition (a) tells us that
$$\mu_x(1) = x = \phi_x(1),$$
so $1 \in E$. On the other hand, if $y \in E$, condition (b) tells us that
$$\phi_x(y') = \phi_x(y) + y = \mu_x(y) + y = \mu_x(y'),$$
so $y' \in E$. The axiom of induction (P3) now tells us that $E = \mathbb{N}^+$ which is what we wished to prove.

Existence Let E be the collection of natural numbers x such that we can define μ_x with properties (a) and (b). Observe that, if we set $\tilde{\mu}_1(y) = y$, then

(a) $\tilde{\mu}_1(1) = 1$, and

(b) $\tilde{\mu}_1(y') = y' = (\mu_1(y))'$ for all natural numbers y.

Thus $1 \in E$

We now suppose $y \in E$ and so there exists μ_x with properties (a) and (b). Observe that, if we set $\tilde{\mu}_{x'}(y) = \mu_x(y) + x$, then

(a') $\tilde{\mu}_{x'}(1) = \mu_x(1) + 1 = x + 1 = x'$ and

(b') $\tilde{\mu}_{x'}(y') = \mu_x(y') + x = (\mu_x(y) + x) + x = \tilde{\mu}_{x'}(y) + x$ for all natural numbers y.

Thus $x' \in E$. The axiom of induction (P3) now tells us that $E = \mathbb{N}^+$, which is what we wished to prove.

Exercise 6.3.3

Let E be the collection of natural numbers y such that $\mu_1(y) = y$. We have $\mu_1(1) = 1$, so $1 \in E$. If $y \in E$, then, by the definition of μ_1,

$$\mu_1(y') = \mu_1(y) + 1 = y'$$

so $y' \in E$. The axiom of induction (P3) now tells us that $E = \mathbb{N}^+$ and so $\mu_1(y) = y$ for all y.

Let x be a natural number and let E_x be the collection of natural numbers y such that

$$\mu_{x'}(y) = \mu_x(y').$$

We know that

$$\mu_{x'}(1) = x' = \mu_x(1)' = \mu_x(1) + 1 = \mu_x(1')$$

so $1 \in E_x$. Further, if $y \in E_x$, then

$$\mu_{x'}(y') = \mu_{x'}(y) + x = \mu_x(y') + x = \mu_x(y'')$$

so $y' \in E_x$. Thus, by the axiom of induction (P3), $E_x = \mathbb{N}^+$ and this is equivalent to the statement we were asked to prove.

Exercise 6.3.6★

Exercise 6.3.9

Observe that A corresponds to $\mathbb{N}^+$, α to 1, a to n and $S(a)$ to $n+1$.

Exercise 6.3.10

Observe that, if we write $\alpha_{[x]}([y])) = [x] + [y]$, then

(a) $\alpha_{[x]}([1]) = [x] + [1] = [x+1] = S([x])$

(b) $\alpha_{[x]}(S([y])) = [x] + ([y] + [1]) = ([x] + [y]) + [1] = S(\mu_{[x]}([y]))$ for all $[y] \in \mathbb{Z}_q$.

By uniqueness, $\alpha_{[x]} = \phi_{[x]}$ so $\phi_{[x]}([y]) = [x] + [y]$.

Similarly, if we consider multiplication, we can use (Q3) to obtain the following analogue of Theorem 6.3.1 (i). Let $[x] \in \mathbb{Z}_q$. There is a unique function $\psi_{[x]} : \mathbb{Z}_q \to \mathbb{Z}_q$ satisfying the following conditions.

(a) $\psi_{[x]}([1]) = [x]$

(b) $\psi_{[x]}(S([y])) = \psi_{[x]}([y]) + [y]$ for all $[y] \in \mathbb{Z}_q$.

We claim that $\psi_{[x]}([y]) = [x] \times [y]$.

Observe that, if we write $\beta_{[x]}([y])) = [x] \times [y]$, then

(a) $\beta_{[x]}([1]) = [x]$

(b) $\beta_{[x]}(S([y])) = \beta_{[x]}([y]) + [y]$ for all $[y] \in \mathbb{Z}_q$.

By uniqueness, $\beta_{[x]} = \psi_{[x]}$ so $\psi_{[x]}([y]) = [x] \times [y]$.

Exercise 6.4.2

We prove the following results.

(i) If there exist natural numbers m and n with $n > m$ and a surjective function $f : F_m \to F_n$, then there exists a surjective function $g : F_{n-1} \to F_n$.

(ii) If there exists a natural number n and an surjective function $f : F_{n+1} \to F_{n+2}$, then there exists an surjective function $g : F_n \to F_{n+1}$.

(iii) If n and m are natural numbers with $n > m$, then there does not exist an surjective function $f : F_m \to F_n$.

(iv) If m and n are natural numbers, then there exists a bijective function $f : F_m \to F_n$ if and only if $m = n$.

Proof. (i) Define $g : F_{n-1} \to F_n$ by $g(r) = f(r)$ for $1 \leq r \leq m$, $g(r) = 1$ otherwise.

(ii) There are two possibilities. Either $f(n+1) = n+2$ or not. If $f(n+1) = n + 2$, we set $g(r) = f(r)$ for $1 \leq r \leq n$.

If $f(n + 1) \neq n + 2$, then $f(n + 1) = u$ for some u with $1 \leq u \leq n$ and $f(v) = n + 2$ for some v with $1 \leq v \leq n$. Set $g(r) = f(r)$, if $1 \leq r \leq n$ and $r \neq v$, and set $g(v) = u$.

(iii) By part (i), it is sufficient to prove the result for $n = m + 1$. To this end, let E be the collection of natural numbers such that there does not exist an surjective function $f : F_m \to F_{m+1}$. We observe that if f is a function from F_1 to F_2, then

$$f(1) = 1, \text{or } f(1) = 2,$$

so f is not surjective. Thus $1 \in E$.

On the other hand, part (ii) tells us that if $m \in E$, then $m + 1 \in E$. The axiom of induction (P3) now tells us that $E = \mathbb{N}^+$, which is what we wished to prove.

(iv) If $m \neq n$, then either $n > m$ or $m > n$. If $m > n$, we know that there is no surjective and so no bijective function $f : E_n \to E_m$. If $n > m$, then the same argument shows us that there is no bijective function $g : E_m \to E_n$ and so no bijective function $f : E_n \to E_m$.

If $n = m$, the identity map $f(r) = r$ gives a bijection between E_n and itself. ∎

EXERCISE 6.4.5

(i) There is a bijection $f : S_n \to A$ and a bijection $g : A \to B$. The map $h : S_n \to B$ given by $h(r) = g(f(r))$ is a bijection, so B is finite and $|A| = |B|$.

(ii) If $|A| = n$ there is a bijection $f : S_n \to A$ and a bijection $h : S_n \to B$. The map $g = hf^{-1}$ given by $g(a) = h(f^{-1}(a))$ is a bijection $g : A \to B$.

EXERCISE 6.4.7

Theorem *The set P of primes is infinite.*
Proof If P is finite then there is a bijection $f : F_n \to P$ for some natural number n. Consider

$$N = (f(1)f(2)\dots f(n)) + 1.$$

We observe that if $1 \leq j \leq n$, then $f(j)$ does not divide N since it leaves remainder 1 when divided into N. However, we know that N factorises into primes, so we have a contradiction.

EXERCISE 6.4.10

Suppose $|A| \geq |B|$. We have $A \cap (B \setminus A) = \emptyset$ so

$$|A \cup B| = |A \cup (B \setminus A)| = |A| + |B \setminus A| \geq |A|.$$

The case $A \supseteq B$ (for example, $A = F_n$, $B = F_m$ with $n \geq m$) shows this is best possible.

Also $B \supseteq B \setminus A$ so

$$|A \cup B| = |A| + |B \setminus A| \leq |A| + |B|.$$

The case $A \cap B = \emptyset$ (for example,$A = F_n$, $B = F_{n+m} \setminus F_n$) shows this is best possible.

In general, $|A| + |B| \geq |A \cup B| \geq \max\{|A|, |B|\}$.

Exercise 6.4.11

Let $P(m)$ be the statement that there is a bijective function from F_{n^m} to the collection $\mathcal{F}_n(m)$ of functions $f : F_m \to F_n$.

Observe that the map $\theta_1 : F_{n^1} \to \mathcal{F}_n(1)$ given by $(\theta_1(r))(1) = r$ is a bijection, so $P(1)$ is true.

Now suppose that $P(m)$ is true. Then there is a bijection $\theta_m : F_{n^m} \to \mathcal{F}_n(m)$. If we now define $\theta_{m+1} : F_{n^{m+1}} \to \mathcal{F}_n(m+1)$ by

$$(\theta_{m+1}((k-1)n^m + r))(u) = \begin{cases} (\theta_m(r))(u) & \text{if } 1 \le u \le m \\ k & \text{if } u = m+1 \end{cases}$$

for $1 \le r \le n^m$, $1 \le k \le n$, then $\theta_{m+1} : F_{n^{m+1}} \to \mathcal{F}_n(m+1)$ is a bijection so $P(m+1)$ is true.

Thus, by induction, $P(m)$ is true for all m and there is a bijective function from F_{n^m} to the collection $\mathcal{F}_n(m)$ of functions $f : F_m \to F_n$.

Now we can find n and m and bijections $f : F_n \to A$, $g : F_m \to B$ and $\theta : F_{n^m} \to F_n(m)$. The map $\phi : \mathcal{F}_n(m) \to A^B$ given by

$$\phi(h)(a) = g\big(\theta(f^{-1}(a))\big)$$

is a bijection, so $|A^B| = |\mathcal{F}_n(m)| = |F_{n^m}| = n^m = |A|^{|B|}$.

Exercise 6.4.12

(i) Let $P(n)$ be the statement that, if $|A| = |B| = n$ and $f : A \to B$ is injective, then f is bijective.

P(1) is true because then $A = \{a\}$ and $B = \{b\}$ and the only $f : A \to B$ is given by $f(a) = b$ and is bijective.

Suppose $P(n)$ is true and A has $n + 1$ elements. Choose $a \in A$ and take $b = f(a)$. Take $A' = A \setminus \{a\}$ and $B' = B \setminus \{b\}$. Then (since f is injective) the map $h : A' \to B'$ given by $h(x) = f(x)$ for $x \in A'$ is well defined and A' and B' have n elements. Since f is injective, h is injective so, by the inductive hypothesis, bijective. It follows that f is bijective. Thus $P(n+1)$ is true and the induction is complete.

(ii) Let $P(n)$ be the statement that if $|A| = |B| = n$ and $g : A \to B$ is surjective, then g is bijective.

P(1) is true because then $A = \{a\}$ and $B = \{b\}$ and the only $g : A \to B$ is given by $g(a) = b$ which is bijective.

Suppose $P(n)$ is true and A has $n + 1$ elements. Choose distinct b, $c \in B$ and using the fact that g is surjective take some $a \in A$ with $g(a) = b$. Take $A' = A \setminus \{a\}$ and $B' = B \setminus \{b\}$. Consider the map the map $k : A' \to B'$ given by $k(x) = g(x)$ if $g(x) \neq b$ and $k(x) = c$ if $g(x) = b$. Since g is surjective, k is surjective so, by the inductive hypothesis, bijective. We write u for the unique element of A' with $k(u) = c$ and observe that we must have $f(u) = c$. Thus there is no $x \in A'$ with $f(x) = b$. We now claim that f is injective so bijective.

We prove this by cases. If $f(x) = f(y)$ and $f(x) \neq b, c$, then $k(x) = k(y)$, so $x = y$. If $f(x) = f(y) = c$, then $k(x) = k(y) = c$, so $x = y = u$. If $f(x) = f(y) = b$, then $x = y = a$.

It follows that f is bijective. Thus $P(n + 1)$ is true and the induction is complete.

If $A = B = \mathbb{N}^+$ and we define $f, g : \mathbb{N}^+ \to \mathbb{N}^+$ by $f(n) = 2n$ and $g(2n) = n$, $g(2n - 1) = 1$ for all n, then f is injective, but not surjective and g is surjective, but not injective.

Exercise 6.4.13

It suffices to prove that, if $\succ$ is an order on F_n, then F_n has a least element for that order. Let $P(n)$ be the statement just made.

$P(1)$ is true, since F_1 has only one element. Suppose that $P(n)$ is true. If $\succ$ is an order on F_{n+1}, then it remains an order when restricted to F_n so, by the inductive hypothesis, F_n has a least element u say. If $n + 1 \succ u$, then u is a least element of F_{n+1}. If not, $u \succ n + 1$ and, by transitivity, $r \succ n + 1$ for all $n \geq r \geq 1$, so $n + 1$ is a least element of F_{n+1} under the given order. Thus $P(n + 1)$ is true.

The required result follows by induction.

Exercise 6.4.15

(i) (Reflexivity) Since the identity map is bijective, $A \sim A$.
(Symmetry) If $A \sim B$, there is a bijective function $f : A \to B$. The inverse function $f^{-1} : B \to A$ is defined and bijective, so $B \sim A$.
(Transitivity) If $A \sim B$ and $B \sim C$, then there are bijective functions $f : A \to B$, $g : B \to C$. If we set $h(a) = g(f(a))$, we obtain a bijective function $h : A \to C$. Thus $A \sim C$.

(ii) Let $n = |A|$, $m = |B|$. By definition $A \sim F_n$, $B \sim F_m$ The rules given in (i), show that if $A \sim B$ then $F_n \sim F_m$ so, by Lemma 6.4.1 (iv), $n = m$. On the other hand if $n = m$, then $F_n \sim F_m$ so, by the rules given in (i), $A \sim B$.

(iii) The function $f : A \times B \to B \times A$ given by $f((a, b)) = (b, a)$ is a bijection.

(iv) The function : $\mathbb{N} \to A$ given by $f(n) = n^2$ is a bijection.

Exercise 6.5.2

(i) If d is the highest common factor of a and b, then d always divides $an + b$ so, if d is not prime, $an + d$ is never prime and, if d is prime, $an + b$ is prime if and only if $an + b = d$.

(ii) The only arithmetic progressions to be considered are $4n+1$ and $4n+3$ and these have been shown to obey the conclusion of Dirichlet's theorem in Exercises 5.5.10 and 5.5.11.

Exercise 6.5.3

We seek an upper bound, not a best upper bound. Because of the population explosion, ten times the present population of the globe certainly exceeds the number of people who have lived since the invention of writing. Today (2017) the population of the globe is less than 10×10^9 so we have an upper bound of $10 \times 10^{10} = 10^{11}$ on the number of people since the invention of writing. A lifetime (measured in seconds) may be bounded by

$$120 \times 366 \times 24 \times 60 \times 60 \leq 4 \times 10^9 < 10^{10}.$$

So we have at most 10^{21} seconds of writing time available. It takes at least $1/10$th of a second to write down a number Thus at most 10^{22} numbers of size between 10^{79} and $10^{80} - 1$ have been written down and, if we choose a number with 80 digits at random, the chance of it having been written down before is negligible. My choice is

$$65\,263\,415\,628\,715\,381\,283\,876\,699\,979\,568\,924\,424$$
$$784\,517\,504\,945\,692\,273\,771\,682\,964\,294\,422\,844\,790\,817.$$

Exercise 6.5.4★

Exercise 7.2.2

Suppose that (x)′ and (xiii)′ hold.

(x) If $a > b$, then, by (xii), $a + (-b) > b + (-b) = 0$. Thus if $a > b$, $b > c$, then

$$\begin{aligned} a + (-c) &= (a + 0) + (-c) = \big(a + (b + (-b))\big) + (-c) \\ &= \big(a + ((-b) + b)\big) + (-c) = \big((a + (-b)) + b\big) + (-c) \\ &= (a + (-b)) + (b + (-c)) > 0 + (b + (-c)) = b + (-c) > 0. \end{aligned}$$

Thus

$$a = a+0 = a+\big(c+(-c)\big) = a+\big((-c)+c\big) = \big(a+(-c)\big)+c = c+\big(a+(-c)\big) > c.$$

(xiii) If $a > b$ and $c > 0$ then, as before, $a + (-b) > 0$, so

$$(a \times c) + ((-b) \times c) = (a + (-b)) \times c > 0.$$

But $(-b) \times c = -(b \times c)$ (see Exercise 3.2.14 (iii)) so $(a \times c) - (b \times c) > 0$ and

$$a \times c = ((a \times c) - (b \times c)) + (b \times c) > (b \times c).$$

Conversely, suppose that (x) and (xiii) hold. Then (x)′ and (xiii)′ follow on setting $b = 0$.

Exercise 7.2.3

We know, from Exercise 5.1.8, that $(\mathbb{G}, +, \times)$ is a field. The remaining conditions are checked in much the same way. For example:-

(x) If $a, b, c \in \mathbb{G}$, and $a > b$ and $b > c$, then $a, b, c \in \mathbb{F}$, $a > b$ and $b > c$ so $a > c$.

Exercise 7.2.4

We just do this case by case.

(i) If $a > 0$, then $|a| = a > 0$. If $0 > a$, then $|a| = -a > 0$. By trichotomy, it follows that if $|a| = 0$, then $a = 0$.

If $a = 0$, then $a \geq 0$, so $|a| = 0$.

(ii) If $a \geq 0$, then $0 = a - a \geq -a$, so $|-a| = -(-a) = a = |a|$.
If $0 > a$, then $-a > a + (-a) = 0$, so $|-a| = -a = |a|$.

(iii) If $a,\ b \geq 0$, then $ab \geq 0$, so $|ab| = ab = |a||b|$.
If $a \geq 0 > b$ then $-b > 0$ so $|ab| = |-(ab)| = |a(-b)| = |a||-b| = |a|b|$.
The case $b \geq 0 > a$ is similar.
If $0 > a, b$ then $|ab| = |(-a)(-b)| = |-a||-b| = |a||b|$.

(iv) If $a, b \geq 0$, then $a + b \geq a \geq 0$ so $|a| + |b| = a + b = |a + b|$.
If $0 > a, b$, then $-a, -b > 0$ so $|a| + |b| = -a - b = -(a + b) = |a + b|$.
If $a \geq 0 \geq b$ and $a > -b$, then $|a| + |b| = a - b \geq a + b = |a + b|$.
If $a \geq 0 \geq b$ and $-b \geq a$, then $|a| + |b| = b - a \geq a + b = |a + b|$.
The remaining cases are similar.

(v) If $a \geq b$, then $(a + b) + |a - b| = (a + b) + (a - b) = 2a = 2\max\{a, b\}$.
If $b \geq a$, then $(a + b) + |a - b| = (a + b) + (b - a) = 2b = 2\max\{a, b\}$.
Thus $(a + b) + |a - b| = 2\max\{a, b\}$.

If $a \geq b$, then $\max\{a, b\} + \min\{a, b\} = a + b$. If $b > a$, then

$$\max\{a, b\} + \min\{a, b\} = b + a = a + b$$

Thus $\max\{a, b\} + \min\{a, b\} = a + b$ for all a and b and so

$$2\min\{a, b\} = 2(a + b) - 2\max\{a, b\} = (a + b) - |a - b|.$$

Exercise 7.2.5

(i) Observe that $\mathbf{1} = \mathbf{1}^2 \geq \mathbf{0}$. Since $\mathbf{1} \neq \mathbf{0}$ we have $\mathbf{1} > \mathbf{0}$.

(ii) If $m > n$, we know that $m = n + r$ for some $r \in \mathbb{N}^+$. Thus it is sufficient to show that, if m is fixed, the statement $P(r)$ which claims that $f(m + r) > f(m)$ is true for all $r \in \mathbb{N}^+$.

Now $f(m + 1) = f(m) + \mathbf{1} > f(m) + \mathbf{0} = f(m)$, so $P(1)$ is true.

Suppose $P(r)$ is true. Then

$$f(m+(r+1)) = (f(m+r)+1) = f(m+r)+\mathbf{1} > f(m)+\mathbf{1} > f(m)+\mathbf{0} = f(m),$$

so $P(r + 1)$ is true. The required result follows.

If $m \neq n$ either $n > m$ or $m > n$. Without loss of generality suppose $m > n$. Then $f(m) > f(n)$ so $f(m) \neq f(n)$. Thus f is injective.

(iii) (a) Fix m. Let $P(n)$ be the statement that $f(m + n) = f(m) + f(n)$.

Since $f(m + 1) = f(m) + \mathbf{1} = f(m) + f(1)$, $P(1)$ is true.

Suppose that $P(n)$ is true. Then

$$\begin{aligned} f(m + (n + 1)) &= f((m + n) + 1) = f(m + n) + \mathbf{1} \\ &= (f(m) + f(n)) + \mathbf{1} = f(m) + (f(n) + \mathbf{1}) = f(m) + f(n + 1) \end{aligned}$$

and $P(n + 1)$ is true. Our required result follows by induction.

(b) Fix m. Let $Q(n)$ be the statement that $f(m \times n) = f(m) \times f(n)$.

Since $f(m \times 1) = f(m) = f(m) \times \mathbf{1} = f(m) \times f(1)$, $Q(1)$ is true.

Suppose that $Q(n)$ is true. Then, using (a),

$$\begin{aligned} f(m \times (n + 1)) &= f((m \times n) + (1 \times m)) = f((m \times n) + m) \\ &= (f(m \times n)) + f(m) = (f(m) \times f(n)) + (f(m) \times \mathbf{1}) \\ &= f(m) \times (f(n) + \mathbf{1}) = f(m) \times f(n + 1) \end{aligned}$$

and $Q(n + 1)$ is true. Our required result follows by induction.

(iv) $u(1) \times u(1) = u(1 \times 1) = u(1) = \mathbf{1} \times u(1)$ so, by cancellation, either $u(1) = \mathbf{0}$ or $u(1) = \mathbf{1}$. If $u(1) = \mathbf{0}$, then $u(2) = u(1 + 1) = u(1) + u(1) = u(1) + \mathbf{0} = u(1)$ and u is not injective. Thus $u(1) = \mathbf{1}$

Let $P(n)$ be the statement that $u(n) = f(n)$.

$P(1)$ is true, since we now know that $u(1) = \mathbf{1} = f(1)$.

If $P(n)$ is true, then

$$u(n + 1) = u(n) + u(1) = f(n) + f(1) = f(n + 1)$$

and $P(n + 1)$ is true. The desired result follows by induction.

Exercise 7.2.6

$\mathbb{Z}_2$ has two elements and $\mathbb{N}^+$ has infinitely many, so there cannot be an injective map $f : \mathbb{N}^+ \to \mathbb{Z}$.

Since $\mathbb{Z}_2$ is not an ordered field, the argument of the previous question does not apply.

EXERCISE 7.2.7

(i) Let $\mathbb{N}^+$ be the copy of the natural numbers in $\mathbb{Q}^+$. By Exercise 7.2.5, we can find $u : \mathbb{N}^+ \to \mathbb{F}$ which preserves $>$, $+$ and $\times$.

We observe that if $n,\ m,\ n'\ m' \in \mathbb{N}^+$ and $n/m = n'/m'$ in $\mathbb{Q}^+$, then $n \times m' = n' \times m$ so

$$u(n) \times u(m') = u(n \times m') = u(n' \times m) = u(n') \times u(m)$$

so $u(n) \times u(m)^{-1} = u(n') \times u(m')^{-1}$. Thus

$$g(n/m) = u(n) \times u(m)^{-1}$$

gives a well defined map $g : \mathbb{Q}^+ \to \mathbb{F}$. We observe that if $g(n/m) = g(n'/m')$, reversing the calculations above gives $n/m = n'/m'$, so g is injective.

$$\begin{aligned} g(n/m) + g(a/b) &= (g(n) \times g(m)^{-1}) + (g(a) \times g(b)^{-1}) \\ &= ((g(n) \times g(b)) + (g(m) \times g(a))) \times (g(m)^{-1} \times g(b)^{-1}) \\ &= ((u(n) \times u(b)) + (u(m) \times u(a))) \times (u(m)^{-1} \times u(b)^{-1}) \\ &= (u((n \times b) + (m \times a)) \times (u(m \times b))^{-1} \\ &= g\big(((n \times b) + (m \times a))/(m \times b)\big) = g(n/m + a/b), \end{aligned}$$

so g preserves addition.

$$\begin{aligned} g(n/m) \times g(a/b) &= (g(n) \times g(m)^{-1}) \times (g(a) \times g(b)^{-1}) \\ &= (g(n) \times g(a)) \times (g(m) \times g(b))^{-1} \\ &= (u(n) \times u(a)) \times (u(m) \times u(b))^{-1} \\ &= u(n \times a) \times (u(m \times b))^{-1} \\ &= g\big((n \times b)/(m \times b)\big) = g(n/m \times a/b), \end{aligned}$$

so g preserves multiplication.

If $n/m > a/b$, then $n \times b > m \times a$, so

$$g(n) \times g(b) = u(n) \times u(b) = u(n \times b) > u(m \times a) = g(m) \times g(a)$$

so since $g(m),\ g(b) > g(0) = 0$ whence $g(m)^{-1}, g(b)^{-1} > 0$ so $g(m)^{-1}g(b)^{-1} > 0$, we have

$$g(n/m) = g(n) \times g(m)^{-1} > g(a) \times g(b)^{-1} = g(a/b).$$

(ii) Suppose $g,\ G : \mathbb{Q}^+ \to \mathbb{F}$ preserves $=$, $\times$ and $>$. If we restrict g and h to $\mathbb{N}^+$ we know, by Exercise 7.2.5, that $g(n) = G(n)$ for all $n \in \mathbb{N}^+$. Since g preserves $\times$

$$g(n) \times g(n)^{-1} = g(n \times n^{-1}) = g(1) = 1$$

so $g(n)^{-1} = g(n^{-1})$ and similarly $G(n)^{-1} = G(n^{-1})$. Thus

$$g(n/m) = g(n) \times g(m^{-1}) = g(n) \times g(m)^{-1} = G(n) \times G(m)^{-1} = G(n/m).$$

The mapping g is unique.

(iii) Observe that if $x, x', y, y' \in \mathbb{Q}$ and $x - x' = y - y'$, then $x + y' = x' + y$ so $g(x) + g(y') = g(x') + g(y)$ and $g(x) - g(x') = g(y) - g(y')$. Since any element of $a \in \mathbb{Q}$ can be written as $a = x - x'$ with $x,\ x' \in \mathbb{Q}^+$ (if $a \geq 0$ take $x = a + 1$, $x' = 1$, if $a < 0$, take $x = 1$, $x' = 1 - a$), we have well defined map $h : \mathbb{Q} \to \mathbb{F}$ given by $h(x - x') = g(x) - g(x')$ for $x,\ x' \in \mathbb{Q}^+$.

If $h(x - x') = h(y - y')$ for $x,\ x',\ y,\ y' \in \mathbb{Q}^+$ then

$$g(x) - g(x') = h(x - x') = h(y - y') = g(y) - g(y')$$

so

$$g(x + y') = g(x) + g(y') = g(x') + g(y) = g(x' + y)$$

and, since g is injective, $x+y' = x'+y$ and $x-x' = y-y'$. Thus h is injective.

Since

$$\begin{aligned} h((x - x') + (y - y')) &= h((x + y) - (x' + y')) = g((x + y) - (x' + y')) \\ &= (g(x) + g(y)) - (g(x') + g(y')) \\ &= (g(x) - g(x')) + (g(y) - g(y')) \\ &= h(x - x') + h(y - y') \end{aligned}$$

for $x,\ x',\ y,\ y' \in \mathbb{Q}^+$, it follows that h preserves $+$.

Since

$$\begin{aligned} &h((x - x') \times (y - y')) = h(((x \times y) + (x' \times y')) - ((x' \times y) + (x \times y'))) \\ &\quad = g((x \times y) + (x' \times y')) - g((x' \times y) + (x \times y')) \\ &\quad = ((g(x) \times g(y)) + (g(x') \times g(y')) - (g(x') \times g(y)) + (g(x) \times g(y')) \\ &\quad = (g(x) - g(x')) \times (g(y) - g(y')) = h(x - x') \times h(y - y') \end{aligned}$$

for $x,\ x',\ y,\ y' \in \mathbb{Q}^+$, it follows that h preserves $\times$.

Suppose that $x - x' > y - y'$, Then

$$x + y' = (x - x') + (x' + y') > (y - y') + (x' + y') = x' + y$$

so

$$h(x) + h(y') = h(x + y') = g(x + y') > g(x' + y) = h(x' + y) = h(x') + h(y)$$

and

$$\begin{aligned} h(x - x') &= h(x) - h(x') = (h(x) + h(y')) + ((-h(x')) + (-h(y'))) \\ &> (h(x') + h(y)) + (-h(x') - h(y')) = h(y) - h(y') = h(y - y') \end{aligned}$$

for $x,\ x',\ y,\ y' \in \mathbb{Q}^+$. It follows that h preserves $>$.

(iv) Suppose $h,\ H : \mathbb{Q} \to \mathbb{F}$ preserve $+$, $\times$ and $>$. If we restrict h and H to $\mathbb{Q}^+$, we know, by (ii), that $h(x) = H(x)$ for all $x \in \mathbb{Q}^+$. Since h preserves $+$,

$$h(x) + h(-x) = h(x + (-x)) = h(0) = 0,$$

so $-h(x) = h(-x)$ and similarly $-H(x) = H(-x)$. Thus

$$h(x-x') = h(x+(-x')) = h(x)+h(-x') = h(x)-h(x') = H(x)-H(x') = H(x-x')$$

for $x,\ x' \in \mathbb{Q}^+$. Since every $y \in \mathbb{Q}$ can be written $y = x - x'$ with $x,\ x' \in \mathbb{Q}^+$, the mapping h is unique.

Exercise 7.2.8

We know that every ordered field contains a subfield isomorphic to the rationals. Thus an ordered field with no strictly smaller subfield must be isomorphic to the rationals.

Conversely, suppose $\mathbb{G}$ is a subfield of $\mathbb{Q}$. We know that $\mathbb{G}$ contains a multiplicative unit u and and a zero v. Now $u^2 = u$, $v^2 = v$, so $u = 1$ or $u = 0$, $v = 1$ or $v = 0$. Since $u \neq v$ and $uv = v$ we have $u = 1$ and $v = 0$. Thus, if $a \in \mathbb{G}$, we have $a + 1 \in \mathbb{G}$. By induction, $\mathbb{G}$ contains $\mathbb{N}^+$, so $\mathbb{G}$ contains n/m for all $n, m \in \mathbb{N}^+$, so $\mathbb{G}$ contains $-n/m$ for all $n, m \in \mathbb{N}^+$ so $\mathbb{G}$ is $\mathbb{Q}$ itself.

Exercise 7.2.9

Just follow Exercise 2.3.7. $u(1) \times u(1) = u(1 \times 1) = u(1) = \mathbf{1} \times u(1)$ so, by cancellation, $u(1) = \mathbf{1}$.

Let $P(n)$ be the statement that $u(n) = f(n)$.

$P(1)$ is true, since we now know that $u(1) = \mathbf{1} = f(1)$.

If $P(n)$ is true, then

$$u(n + 1) = u(n) + u(1) = f(n) + f(1) = f(n + 1)$$

and $P(n + 1)$ is true. The desired result follows by induction.

We did not have induction when we first looked at Exercise 2.3.7.

Lemma 3.2.18 can extended by adding: If F and G are injective functions $F,\ G : \mathbb{N}^+ \to \mathbb{Q}$ such that

$F(n+m) = F(n)+F(m),\ F(n\times m) = F(n)\times F(m)$ and $n > m$ implies $F(n) > F(m)$

and

$G(n+m) = G(n)+G(m),\ G(n\times m) = G(n)\times G(m)$ and $n > m$ implies $G(n) > G(m)$,

then $F = G$.

Exercise 7.2.10

Part (i) We have

$$\begin{aligned}
(a_1, a_2) \otimes &\left(\frac{a_1}{a_1^2 - 2a_2^2}, \frac{a_2}{a_1^2 - 2a_2^2}\right) \\
&= \Bigg(a_1 \times \frac{a_1}{a_1^2 - 2a_2^2} + (-2 \times a_2) \times \frac{a_2}{a_1^2 - 2a_2^2}, \\
&\qquad \frac{a_1}{a_1^2 - 2a_2^2} \times a_2 + a_1 \times \frac{(-a_2)}{a_1^2 - 2a_2^2}\Bigg) \\
&= \left(\frac{a_1^2 - 2a_2^2}{a_1^2 - 2a_2^2}, \frac{(a_1 \times a_2) - (a_1 \times a_2)}{a_1^2 - 2a_2^2}\right) = (1, 0)
\end{aligned}$$

Part (ii)

(i) Using the commutative law of addition for $\mathbb{R}$,

$$\mathbf{a} \oplus \mathbf{b} = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + a_2) = \mathbf{b} \oplus \mathbf{a}.$$

(ii) Using the associative law of addition for $\mathbb{R}$,

$$\begin{aligned}
\mathbf{a} \oplus (\mathbf{b} \oplus \mathbf{c}) &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) = (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) \\
&= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (a_1 + b_1, a_2 + b_2) + (c_1, c_2) \\
&= (\mathbf{a} \oplus \mathbf{b}) \oplus \mathbf{c}.
\end{aligned}$$

(iii) $\mathbf{0} \oplus \mathbf{a} = (0, 0) \oplus (a_1, a_2) = (0 + a_1, 0 + a_2) = (a_1, a_2) = \mathbf{a}$.

(iv) If we write $-\mathbf{a} = (-a_1, -a_2)$, then

$$\mathbf{a} \oplus (-\mathbf{a}) = (a_1 - a_1, a_2 - a_2) = (0, 0) = \mathbf{0}.$$

(v) Using the commutative laws of multiplication and addition for $\mathbb{R}$

$$\begin{aligned}
\mathbf{a} \otimes \mathbf{b} &= ((a_1 \times b_1) + (2 \times (a_2 \times b_2)), (a_1 \times b_2) + (a_2 \times b_1)) \\
&= ((b_1 \times a_1) + (2 \times (b_2 \times a_2)), (b_2 \times a_1) + (b_1 \times a_2)) \\
&= ((b_1 \times a_1) + (2 \times (b_2 \times a_2)), (b_1 \times a_2) + (b_2 \times a_1)) = \mathbf{b} \otimes \mathbf{a}.
\end{aligned}$$

(vi) Making free use of the laws governing $\mathbb{Q}$, we have

$$
\begin{aligned}
\mathbf{a}\otimes(\mathbf{b}\otimes\mathbf{c}) &= (a_1,a_2)\times\big((b_1\times c_1)+((2\times b_2)\times c_2),(b_1\times c_2)+(b_2\times c_1)\big)\\
&= \Big(a_1\times((b_1\times c_1)+((2\times b_2)\times c_2)+(2\times a_2)\times((b_1\times c_2)+(b_2\times c_1)),\\
&\qquad a_1\times((b_1\times c_2)+(b_2\times c_1))+a_2\times((b_1\times c_1)-(b_2\times c_2))\Big)\\
&= \Big(((a_1\times b_1)+((2\times(a_2\times b_2)))\times c_1((a_2\times b_1)+((2\times a_1)\times b_2))\times c_2),\\
&\qquad ((a_1\times b_1)+((2\times a_2)\times b_2))\times c_2+((a_1\times b_2)+(a_2\times b_1))\times c_1\Big)\\
&= (\mathbf{a}\otimes\mathbf{b})\otimes\mathbf{c}.
\end{aligned}
$$

(vii) We have

$$
\begin{aligned}
\mathbf{1}\otimes\mathbf{a} &= (1,0)\times(a_1,a_2) = ((1\times a_1)+(2\times(0\times a_2)),(1\times a_2)+(0\times a_1))\\
&= (a_1-0,a_2+0) = (a_1,a_2) = \mathbf{a}.
\end{aligned}
$$

(Multiplicative unit.)

(viii) Done in part (i).

(ix) Using the distributive law for $\mathbb{Q}$ and making free use of the associative and commutative laws of addition.

$$
\begin{aligned}
\mathbf{a}\otimes(\mathbf{b}\oplus\mathbf{c}) &= (a_1,a_2)\times(b_1+c_1,b_2+c_2)\\
&= (a_1\times(b_1+c_1)+(2\times a_2)\times(b_2+c_2),a_1\times(b_2+c_2)+a_2\times(b_1+c_2))\\
&= (((a_1\times b_1)+(a_1\times c_1))+((-a_2)\times b_2)+((2\times a_2)\times c_2),\\
&\qquad ((a_1\times b_2)+(a_1\times c_2))+((a_2\times b_1)+(a_2\times c_1)))\\
&= (((a_1\times b_1)+((2\times a_2)\times b_2))+((a_1\times c_1)+((2\times a_2)\times c_2)),\\
&\qquad ((a_1\times b_2)+(a_2\times b_1))+((a_1\times c_1)+(a_2\times c_1)))\\
&= ((a_1\times b_1)+((2a_2)\times b_2),(a_1\times b_2)+(a_2\times b_1)\\
&\qquad +((a_1\times c_1)+((2\times a_2)\times c_2)),+((a_1\times c_1)+(a_2\times c_1)))\\
&= (\mathbf{a}\otimes\mathbf{b})\oplus(\mathbf{a}\otimes\mathbf{c})
\end{aligned}
$$

We note that $\mathbf{1}=(1,0)\neq(0,0)=\mathbf{0}$.

Part (iii) Immediate. For example

$$f(a\times b)=(a\times b,0)=(a,0)\otimes(b,0)=f(a)\otimes f(b).$$

Part (iv) Observe that $(0,1)\otimes(0,1)=(1,0)=f(2)$.

Part (v) Suppose that $(a,b)\otimes(a,b)=f(3)$. Then $(a^2+2b^2,2ab)=(3,0)$ so $ab=0$ and either $a=0$ and $2b^2=3$ or $b=0$ and $a^2=3$. Theorem 4.4.12 tells us that neither condition can be satisfied.

Part (vi) ★ (The only direct proof I can think of involves pages of case by case arguments.)

Exercise 7.2.11

(i) 12 miles, 4 furlongs, 9 chains, 5 yards, 1 foot and 10 inches.

(ii) 12797.199 metres.

Exercise 7.2.12

(i) We have

$$\frac{3}{19} - \frac{4}{23} = \frac{3 \times 23 - 4 \times 19}{19 \times 23} = \frac{69 - 76}{19 \times 23} < 0$$

so $3/19 < 4/23$.

(ii) $0.361 > 0.353$.

(iii) The average is

$$\frac{1}{3}\left(\frac{3}{19} + \frac{4}{23} + \frac{4}{21}\right) = \frac{1}{3} \times \frac{4793}{9177} = \frac{4793}{27531}.$$

(iv) The average is

$$\frac{1}{3} \times (0.353 + 0.361 + 0.362) = \frac{1}{3} \times 1.076 = 0.359$$

to 3 places of decimals.

Exercise 7.2.13

(i) 56 pounds and 12 shillings is $56 \times 20 + 12 = 1132$ shillings
1132 shillings and 5 pence is $1132 \times 12 + 5 = 13589$ pence
13589 pence and 2 farthings is $13589 \times 4 + 2 = 54358$ farthings
After a year we have $1.03 \times 54358 = 55988.74$ farthings
Rounding up we have 55989 farthings
that is to say 13997 pence and 1 farthing
13997 pence is 1166 shillings and 5 pence
1166 shillings is 58 pounds and 6 shillings
so the debt is now 58 pounds, 6 shillings, 5 pence and 1 farthing (correct to the nearest farthing).

(ii) The debt is $1.03 \times 56.53 = 58.2259$, that is to say 58 dollars and 23 cents correct to the closest cent.

Exercise 7.2.15

Observe that $\log_{10} a \div b = \log_{10} a - \log_{10} b$.

Take $a = 8.626$, $b = 3.679$. To the appropriate accuracy $\log_{10} 8.626 = 0.9358$, $\log_{10} 3.679 = 0.5657$ so
$$\log(a \div b) = \log_{10} a - \log_{10} b = 0.3701 = \log_{10} 2.345$$
and $8.626 \div 3.679 = 2.345$.

If we consider $2.345 \div 3.679$
$$\begin{aligned}\log_{10} 2.345 \div 3.679 &= \log_{10} 2.345 - \log_{10} 3.679 = 0.3701 - 0.5657\\ &= -0.1956 = 0.8044 - \log_{10} 10 = \log_{10} 6.374 - \log_{10} 10 = \log_{10} .6374\end{aligned}$$
so $2.345 \div 3.679 = 0.6374$.

Exercise 7.2.16

(i) We first prove the result for $n \geq 0$. Let $P(n)$ be the statement that $n \log_{10} x = \log_{10} x^n$. Since
$$\log_{10} 1 = \log_{10} 1 \times 1 = \log_{10} 1 + \log_{10} 1$$
we have $\log 1 = 0$, so $P(0)$ is true.

If $P(n)$ is true then
$$(n+1)\log_{10} x = n \log_{10} x + \log_{10} x = \log_{10} x^n + \log_{10} x = \log_{10}(x^n \times x) = \log_{10} x^{n+1}$$
so $P(n + 1)$ is true. The required result follows by induction.

If $n < 0$, then using the result just proved,
$$n \log_{10} x = -|n| \log_{10} x = -\log_{10} x^{|n|} = \log_{10}(1/x^{|n|}) = \log x^n.$$

(ii) We have
$$\log_{10} 10^a = a \log_{10} 10 = a = b \log_{10} u/v = \log_{10}(u/v)^b$$
so $10^a = (u/v)^b$ and $10^a v^b = u^b$. By the uniqueness of factorisation, any prime factor of v must be a prime factor of u^b and so of u. Since u and v are coprime $v = 1$. Thus $10^a = u^b$. By the uniqueness of factorisation, any prime factor of u must be a prime factor of 10^a, so must be 2 or 5. If $u = 2^r 5^s$ we have
$$2^a 5^a = 2^{br} 5^{bs}$$
so $br = bs = a$, whence $r = s = k$ for some strictly positive integer k. We now have $u = 10^k$. The converse is immediate.

(iii) If $x > 1$ this is the result of (ii). If $x = 1$ then $x = 10^0$. If $1 > x > 0$, then, since $\log_{10}(1/x) = -\log_{10} x$, part (ii) shows that $1/x$ is rational and so x is rational.

Exercise 7.2.17★

Exercise 7.3.4

(i) Observe that, if $\epsilon > 0$, then

$$|a_n - a| = 0 < \epsilon$$

for all $n \geq 1$.

(ii) If $\epsilon > 0$, then, by definition, we can find a N such that $|a - a_n| < \epsilon$ for $n \geq N$. Thus

$$|(-a) - (-a_n)| = |a - a_n| \leq \epsilon$$

for $n \geq N$.

(iii) Suppose, if possible, that $a \not\geq b$. Then $b > a$. Set $\epsilon = (b - a)/4$. Since $\epsilon > 0$, there exists an N_1, N_2 such that $|a_n - a| < \epsilon$ for $n \geq N_1$ and $|b_n - b| < \epsilon$ for $n \geq N_2$. Taking $q = \max\{M, N_1, N_2\}$ we have

$$b-a \leq (b-a)-(a_q-b_q) = (b-b_q)-(a-a_q) \leq |b-b_q|+|a-a_q| < 2\epsilon \leq (b-a)/2$$

which is impossible. Thus $a \geq b$. The same argument gives $b \geq a$, so, by trichotomy, $a = b$.

(iv) Just use (i) and (iii).

Exercise 7.3.6

The limit of the sum is the sum of the limits, so, if $t_n \to t$,

$$h(t_n) = f(t_n) + g(t_n) \to f(t) + g(t) = h(t)$$

as $n \to \infty$. Thus h is continuous.

The limit of the product is the product of the limits, so, if $t_n \to t$,

$$k(t_n) = f(t_n) \times g(t_n) \to f(t) \times g(t)$$

as $n \to \infty$. Thus k is continuous.

Exercise 7.4.5

If $b \leq 0$ just take $n = 1$. From now on we suppose $b > 0$.

Suppose $\mathbb{F}$ satisfies the axiom of Archimedes and $a,\ b > 0$. Since $a/b > 0$ we can find an integer $n \geq 1$ such that $a/b > 1/n$ and so $na > b$.

Conversely, suppose that, given $a,\ b \in \mathbb{F}$ with $a > 0$. We can then find an $n \in \mathbb{N}^+$ such that $na > b$. If $\epsilon > 0$ then, taking $a = \epsilon$ and $b = 1$, we can find an $n \in \mathbb{N}^+$ such that $n\epsilon > 1$ and so $\epsilon > 1/n$.

Exercise 7.4.6

If $c = 0$ take $n = m = 0$. If $c > 0$ take $m = 0$ and apply Exercise 7.4.5 with $c = b$, $a = 1$. If $c < 0$ consider $-c$.

Exercise 7.4.7

Suppose that every increasing sequence bounded above tends to a limit.

If a_n is a decreasing sequence bounded below by A, then $-a_n$ is an increasing sequence bounded above by $-A$. Thus $-a_n \to b$ as $n \to \infty$ for some b. It follows that $a_n \to -b$ and so a_n tends to a limit.

Suppose that every decreasing sequence bounded below tends to a limit.

If a_n is an increasing sequence bounded above by A, then $-a_n$ is an decreasing sequence bounded below by $-A$. Thus $-a_n \to b$ as $n \to \infty$ for some b. It follows that $a_n \to -b$ and so a_n tends to a limit.

Exercise 7.4.9

Suppose that $1 > x \geq 0$. A simple induction shows that that $x^{n+1} \geq x^n \geq 0$ for all integers $n \geq 1$. Thus the x^n form a decreasing sequence bounded below by 0 and so must tend to a limit α. Thus, given any $\epsilon > 0$, we can find an N such that $|\alpha - x^N| < \epsilon$ and so, automatically, $|\alpha - x^{2n}| < \epsilon$ for all $n \geq N$. Thus $x^{2n} \to \alpha$.

However, taking $a_n = b_n = x^n$ in Lemma 7.3.3 (iii), we see that

$$x^{2n} = x^n \times x^n \to \alpha \times \alpha = \alpha^2,$$

so the uniqueness of limits (Lemma 7.3.3 (i)) tells us that

$$\alpha^2 = \alpha.$$

Thus $\alpha = 0$ or $\alpha = 1$. Since $1 > x \geq x^n$ for all $n \geq 1$, Exercise 7.3.4 tells us that $1 > x \geq \alpha$ and so $\alpha = 0$.

A simple induction gives $|x|^n = |x^n|$ so, if $|x| < 1$, we have $|x^n| = |x|^n \to 0$.

Exercise 7.4.13

Suppose $a, b > 0$.

We have $\sqrt{a}, \sqrt{b} > 0$. If $\sqrt{b} \geq \sqrt{a}$, then

$$b = \sqrt{b} \times \sqrt{b} \geq \sqrt{a} \times \sqrt{b} \geq \sqrt{a} \times \sqrt{a} = a.$$

Thus, if $a > b > 0$, we must have $\sqrt{a} > \sqrt{b}$.

Exercise 7.4.14

(i) Since $x_n \to x$ certainly implies $x_n \to x$, we have f_1 continuous. If f_n is continuous, it follows that f_{n+1} is a product of f_n and f_1, and f_{n+1} is continuous. By induction, f_n is continuous.

Automatically, $f_1(y) > f_1(x) > 0$ for $y > x > 0$. If $y > x > 0$ and $f_n(y) > f_n(x) > 0$, then

$$f_{n+1}(y) = y \times f_n(y) > x \times f_n(y) > x \times f_n(x) = f_{n+1}(x)$$

and similarly $f_{n+1}(x) = x \times f_n(x) > 0$. By induction $f_n(y) > f_n(x) > 0$ whenever $y > x > 0$.

(ii) Since $a + 1 > 1$, a simple induction shows that $(a + 1)^n \geq a + 1$ for $n \geq 1$. Since f_n is continuous and $f_n(a + 1) > a > f_n(0)$, the intermediate value theorem tells us that $f_n(x) = a$ has a solution.

(iii) We have $x^2 = (-x)^2$ so, by a simple induction, $x^{2n} = (-x)^{2n}$, for all $n \geq 1$. Thus, if m is even, $x^m \geq 0$ for all x and $x^m = -a$ has no solution.

Again, $(-x)^{2n+1} = (-x)\times(-x)^{2n} = -x^{2n+1}$ for $n \geq 1$. Thus, if $m \geq 1$ and m is odd, then, if $y^m = a$, we have $(-y)^m = -a$. Thus $x^m = -a$ has a solution.

Since $f_n(t) > f_n(s)$ for $t > s > 0$ $f_n(x) = a$ has exactly one root y with $y > 0$. Hence $x^n = a$ has a unique solution if and only if n is odd.

Exercise 7.6.5

(i) No supremum. If $b \in \mathbb{F}$, then $|b| + 1 \in A$ and $|b| + 1 > b$.

(ii) Supremum 1, since $1 \in A$ (so $b \geq a$ for all $a \in A$ yields $b \geq 1$) and $1 \geq a$ for all $a \in A$. We have observed that $a \in A$.

(iii) Supremum 1, since $1 \geq a$ for all $a \in A$, and if $b < 1$ then $(b+1)/2 \in A$ and $b < (b+1)/2$. We have $1 \notin A$.

Exercise 7.6.7

Suppose $\mathbb{F}$ is an ordered field with the supremum property and E is a non-empty subset bounded below, by b say. Then if A consists of the points $-e$ with $e \in E$, A is non-empty bounded below by $-b$. Thus A has a supremum a_0 say. We have

(i) $a_0 \geq a$ for all $a \in A$.

(ii) If $d \geq a$ for all $a \in A$ then $d \geq a_0$.

Set $e_0 = -a_0$,

(1) $-e_0 = a_0 \geq -e$ for all $e \in E$, so $e_0 \leq e$ for all $e \in E$.

(2) If $c \leq e$ for all $e \in E$, then $-c \geq a$ for all $a \in A$, so $-c \geq a_0 = -e_0$ and $e_0 \geq c$.

Exercise 7.6.10

Suppose $a_n \to a$. If $\epsilon > 0$, then $\epsilon/2 > 0$ so we can find an N with $|a_n - a| < \epsilon/2$ for all $n \geq N$. Now

$$|a_n - a_m| = |(a_n - a) + (a - a_n)| \leq |a_n - a| + |a_n - a| < \epsilon/2 + \epsilon/2 = \epsilon$$

for all $n \geq N$. The sequence is Cauchy.

Exercise 7.6.13

By definition, there exists an N such that $|a_n - a_m| \leq 1$ for all n, $m \geq N$. Thus

$$|a_m| \leq |a_m - a_N| + |a_N| \leq |a_N| + 1$$

for all $m \geq N$. If we set

$$A = \max_{1 \leq n \leq N} |a_n| + 1,$$

we then have $|a_m| \leq A$ for all $m \geq 1$.

Exercise 7.6.15

(i) We work in $\mathbb{Q}$. If $\epsilon > 0$, then $\epsilon = u/v$ with u, v strictly positive integers. Thus $\epsilon \geq 1/v$. We have shown that $1/n \to 0$ as $n \to \infty$.

(ii) The set E of strictly positive integers r with $r^2 \leq 2^{2n+1}$ is non-empty since $1 \in E$ and bounded above by 2^{2n+1}. Thus E has a greatest member r_n and, by definition,

$$r_n^2 \leq 2^{2n+1} < (r_n + 1)^2.$$

(iii) We have

$$\begin{aligned} a_n^2 &= r_n^2 2^{-2n} \leq 2 < 2^{-2n}(r_n + 1)^2 \\ &= r_n^2 2^{-2n} + 2r_n 2^{-2n} + 2^{-2n} = a_n^2 + 2r_n 2^{-2n} + 2^{-2n} \\ &\leq a_n^2 + 2^{2-n} + 2^{-2n}. \end{aligned}$$

Thus $|a_n^2 - 2| \leq 2^{2-n} + 2^{-2n} \to 0$ as $n \to \infty$, so $a_n^2 \to 2$. By the product rule for limits, it follows that, if $a_n \to a$ as $n \to \infty$, then $a^2 = 2$. Since this is impossible, the sequence a_n has no limit.

(iv) Note that $(2r_n)^2 \leq 2^{2(n+1)+1}$ so $r_{n+1} \geq 2r_n$ and $a_n \leq a_{n+1}$. Since $r_n^2 \leq 2^{2n+1} < 2^{2n+2}$, $r_n < 2^{n+1}$ and $a_n < 2$. (Or we could have used the fact that $a_n^2 < 2$.) Thus we have an increasing sequence a_n bounded above which does not converge. Thus $\mathbb{Q}$ does not satisfy the fundamental axiom of analysis.

(v) If $b \geq a_n$ for all n then $b > 0$ and $b^2 \geq a_n^2$. Since $a_n^2 \to 2$, we must have $b^2 \geq 2$. Since the equation $x^2 = 2$ has no solution, we must have $b^2 > 2$. If

$$c = \frac{1}{2}\left(b + \frac{2}{b}\right)$$

we have $c > 0$ and

$$b - c = \frac{b}{2} - \frac{1}{b} = \frac{b^2 - 2}{b} > 0$$

so $b > c$. However

$$\begin{aligned} c^2 &= \frac{1}{4}\left(b^2 + 4 + \frac{4}{b^2}\right) = 2 + \frac{1}{4}\left(b^2 - 4 + \frac{4}{b^2}\right) \\ &= 2 + \frac{1}{4}\left(b - \frac{2}{b}\right)^2 \geq 2 \end{aligned}$$

so $c \in A$. Thus A has no supremum.

(vi) Note that $(2r_n+2)^2 = 2^2(r_n+1)^2 > 2^{2n+2}$ so $2r_n+2 \geq r_{n+1}$ and $a_n+2^{-n} \geq a_{n+1}$. Since we showed earlier that $a_{n+1} \geq a_n$, we have $|a_n - a_{n+1}| \leq 2^{-n}$. By induction or summing a geometrical progression,

$$|a_n - a_m| \leq 2^{-n+1}(1 - 2^{-(m-n)})$$

so

$$|a_n - a_m| \leq 2^{-n+2}(1 - 2^{-(m-n)})$$

for $m \geq n+1$. Thus (using the Archimedian property) the a_n form a Cauchy sequence which we have already shown has no limit.

Exercise 8.1.1

(i) Observe that $a_n - a_n = 0 \to 0$. Thus $\mathbf{a} \sim \mathbf{a}$. (Reflexivity.)

(ii) If $\mathbf{a} \sim \mathbf{b}$, then

$$b_n - a_n = -(a_n - b_n) = (-1) \times (a_n - b_n) \to (-1) \times 0 = 0$$

as $n \to \infty$, so $\mathbf{b} \sim \mathbf{a}$. (Symmetry.)

(iii) If $\mathbf{a} \sim \mathbf{b}$ and $\mathbf{b} \sim \mathbf{c}$, then

$$a_n - c_n = (a_n - b_n) + (b_n - c_n) \to 0 + 0 = 0$$

so $\mathbf{a} \sim \mathbf{c}$. (Transitivity)

Exercise 8.1.3

(i) Let $\epsilon > 0$. Since $\mathbf{a}, \mathbf{b} \in \mathcal{S}$, we can find N_1 and N_2 such that $|a_n - a_m| < \epsilon/2$ for $n, m \geq N_1$ and $|b_n - b_m| < \epsilon/2$ for $n, m \geq N_2$.

Taking $N = \max\{N_1, N_2\}$, we have

$$|(a_n+b_n)-(a_m+b_m)| = |(a_n-a_m)+(b_n-b_m)| \leq |a_n-a_m|+|b_n-b_m| < \epsilon/2+\epsilon/2 = \epsilon$$

for all $n \geq N$. Thus $\mathbf{a} + \mathbf{b} \in \mathcal{S}$.

(ii) Suppose $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}' \in \mathcal{S}$ and $\mathbf{a} \sim \mathbf{a}'$, $\mathbf{b} \sim \mathbf{b}'$. If $\epsilon > 0$, we can find N_1 and N_2 such that $|a_n - a_n'| < \epsilon/2$ for $n \geq N_1$ and $|b_n - b_n'| < \epsilon/2$ for $n \geq N_2$.

Taking $N = \max\{N_1, N_2\}$, we have

$$|(a_n+b_n)-(a_n'+b_n')| = |(a_n-a_n')+(b_n-b_n')| \leq |a_n-a_n'|+|b_n-b_n'| < \epsilon/2+\epsilon/2 = \epsilon$$

for all $n \geq N$. Thus $\mathbf{a} + \mathbf{b} \sim \mathbf{a}' + \mathbf{b}'$.

EXERCISE 8.1.6

(i) $a_n + b_n = b_n + a_n$, so $\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}$ and

$$[\mathbf{a}] + [\mathbf{b}] = [\mathbf{b}] + [\mathbf{a}].$$

(Commutative law of addition.)

(ii) $a_n + (b_n + c_n) = a_n + (b_n + c_n)$, so $\mathbf{a} + (\mathbf{b} + \mathbf{c}) = (\mathbf{a} + \mathbf{b}) + \mathbf{c}$ and

$$[\mathbf{a}] + ([\mathbf{b}] + [\mathbf{c}]) = ([\mathbf{a}] + [\mathbf{b}]) + [\mathbf{c}].$$

(Associative law of addition.)

(iii) $0 + a_n = a_n$, so $\mathbf{0} + \mathbf{a} = \mathbf{a}$ and

$$[\mathbf{0}] + [\mathbf{a}] = [\mathbf{a}].$$

(Existence additive zero.)

(v) $a_n \times b_n = b_n \times a_n$, so $\mathbf{a} \times \mathbf{b} = \mathbf{b} \times \mathbf{a}$ and

$$[\mathbf{a}] \times [\mathbf{b}] = [\mathbf{b}] \times [\mathbf{a}]$$

(Commutative law of multiplication.)

(vi) $a_n \times (b_n \times c_n) = a_n \times (b_n \times c_n)$ so $\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{a} \times \mathbf{b}) \times \mathbf{c}$ and

$$[\mathbf{a}] \times ([\mathbf{b}] \times [\mathbf{c}]) = ([\mathbf{a}] \times [\mathbf{b}]) \times [\mathbf{c}].$$

(Associative law of multiplication.)

(vii) $1 \times a_n = a_n$, so $\mathbf{1} \times \mathbf{a} = \mathbf{a}$ and

$$[\mathbf{1}] \times [\mathbf{a}] = [\mathbf{a}].$$

(Multiplicative unit.)

(ix) $a_n \times (b_n + c_n) = (a_n \times b_n) + (a_n \times c_n)$, so $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = (\mathbf{a} \times \mathbf{b}) + (\mathbf{a} \times \mathbf{c})$ and

$$[\mathbf{a}] \times ([\mathbf{b}] + [\mathbf{c}]) = ([\mathbf{a}] \times [\mathbf{b}]) + ([\mathbf{a}] \times [\mathbf{c}])$$

(Distributive law.)

Since $1 \nrightarrow 0$, $[\mathbf{1}] \neq [\mathbf{0}]$.

EXERCISE 8.1.12

(x) (Transitivity of order,) If $[\mathbf{a}] > [\mathbf{b}]$ and $[\mathbf{b}] > [\mathbf{c}]$, then $\mathbf{a} \succ \mathbf{b}$ and $\mathbf{b} \succ \mathbf{c}$, that is to say, we can find strictly positive integers M_1 and N_1 such that

$$a_j \geq b_j + \frac{1}{M_1}$$

for $j \geq N_1$ and we can find strictly positive integers M_2 and N_2 such that

$$b_j \geq c_j + \frac{1}{M_2}$$

for $j \geq N_2$.

Taking $N = \max\{N_1, N_2\}$, we have

$$a_j \geq b_j + \frac{1}{M_1} \geq c_j + \frac{1}{M_1} + \frac{1}{M_2}$$

for $j \geq N$. Thus $\mathbf{a} \succ \mathbf{c}$ and $[\mathbf{a}] > [\mathbf{c}]$

(xii) (Order and addition.) If $[\mathbf{a}] > [\mathbf{b}]$, then $\mathbf{a} \succ \mathbf{b}$, that is to say, we can find strictly positive integers M and N such that

$$a_j \geq b_j + \frac{1}{M}$$

for $j \geq N$. It follows that

$$a_j + c_j \geq (b_j + c_j) + \frac{1}{M}$$

so $\mathbf{a} + \mathbf{c} \succ \mathbf{b} + \mathbf{c}$ and $[\mathbf{a}] + [\mathbf{c}] > [\mathbf{b}] + [\mathbf{c}]$.

(xiii) (Order and multiplication.) If $[\mathbf{a}] > [\mathbf{b}]$ and $[\mathbf{c}] > [\mathbf{0}]$, then $\mathbf{a} \succ \mathbf{b}$ and $\mathbf{a} \succ \mathbf{0}$. Thus we can find we can find strictly positive integers M_1 and N_1 such that

$$a_j \geq b_j + \frac{1}{M_1}$$

for $j \geq N_1$ and we can find strictly positive integers M_2 and N_2 such that

$$c_j \geq \frac{1}{M_2}$$

for $j \geq N_2$.

Taking $N = \max\{N_1, N_2\}$ we have

$$(a_j - b_j)c_j \geq \frac{1}{M_1} \times \frac{1}{M_2}$$

so

$$a_j c_j \geq b_j c_j + \frac{1}{M_1 M_2}$$

for $j \geq N$. Thus Thus $\mathbf{a} \times \mathbf{c} \succ \mathbf{b} \times \mathbf{c}$ and

$$[\mathbf{a}] \times [\mathbf{c}] > [\mathbf{b}] \times [\mathbf{c}].$$

Exercise 8.1.13

(i) If $q_n = q$, then $q_n \to q$ as $n \to \infty$, so the q_n form a Cauchy sequence and $\mathbf{u}(q) \in \mathcal{S}$.

(ii) If $f(q) = f(q')$, then $q - q' \to 0$ as $n \to \infty$, so $q - q' = 0$ and $q = q'$. Thus f is injective.

(iii) We have

$$f(q + q') = [\mathbf{u}(q + q')] = [\mathbf{u}(q) + \mathbf{u}(q')] = [\mathbf{u}(q)] + [\mathbf{u}(q')] = f(q) + f(q')$$

and

$$f(q \times q') = [\mathbf{u}(q \times q')] = [\mathbf{u}(q) \times \mathbf{u}(q')] = [\mathbf{u}(q)] \times [\mathbf{u}(q')] = f(q) \times f(q').$$

If $q > q'$, then $q - q' = u/v$ with u, v strictly positive integers, so $q > q' + 1/(2v)$ and so $\mathbf{u}(q) \succ \mathbf{u}(q')$ and $f(q) > f(q')$.

Exercise 8.1.18

(i) Let $x,\ y \in \mathbb{G}$ We have
$$h(h^{-1}(x+y)) = x+y = h(h^{-1}(x)) + h(h^{-1}(y)) = h(h^{-1}(x)+h^{-1}(y))$$
so, since h is injective,
$$h^{-1}(x+y) = h^{-1}(x)+h^{-1}(y).$$
Similarly,
$$h(h^{-1}(x\times y)) = x\times y = h(h^{-1}(x)) \times h(h^{-1}(y)) = h(h^{-1}(x)\times h^{-1}(y))$$
so, since h is injective,
$$h^{-1}(x\times y) = h^{-1}(x)\times h^{-1}(y).$$

Further, if $h^{-1}(x) > h^{-1}(y)$, then $x = h(h^{-1}(x)) > h(h^{-1}(y)) = y$, if $h^{-1}(y) > h^{-1}(x)$, then, as before, $y > x$ and, if $h^{-1}(x) = h^{-1}(y)$, then $x = y$. Thus, by trichotomy, $x > y$ implies $h^{-1}(x) > h^{-1}(y)$.

(ii) If $a \geq 0$, then $h(a) \geq 0$, so $a = |a|$ and $|h(a)| = h(a) = h(|a|)$.
If $a < 0$, then $h(a) < 0$ so $a = -|a|$ and $|h(a)| = -h(a) = h(-a) = h(|a|)$.

(iii) Suppose $\epsilon \in \mathbb{G}$ and $\epsilon > 0$. Then $h^{-1}(\epsilon) > 0$. Thus we can find an N such that
$$|a_n - a| < h^{-1}(\epsilon)$$
for all $n \geq N$. Using part (ii), we obtain
$$|h(a_n) - h(a)| = |h(a_n - a)| = h(|a_n - a|) < h(h^{-1}(\epsilon)) = \epsilon$$
for all $n \geq N$. Thus $h(a_n) \to h(a)$ as $n \to \infty$.

(iv) Suppose $\epsilon \in \mathbb{G}$ and $\epsilon > 0$. Then $h^{-1}(\epsilon) > 0$. Thus we can find an N such that
$$|x_n - x_m| < h^{-1}(\epsilon)$$
for all $n,\ m \geq N$. Using part (ii), we obtain
$$|h(x_n) - h(x_m)| = |h(x_n - x_m)| = h(|x_n - x_m|) < h(h^{-1}(\epsilon)) = \epsilon$$
for all $n,\ m \geq N$. Thus the $h(x_n)$ form a Cauchy sequence.

Exercise 8.1.20

We must check that g is an injection.

Suppose that $g(\mathbf{a}) = g(\mathbf{b})$ so that
$$a_1 + a_2\sqrt{2} = b_1 + b_2\sqrt{2}.$$
If $a_2 \neq b_2$ we have
$$\sqrt{2} = \frac{a_1 - b_1}{b_2 - b_1} \in \mathbb{Q}$$
which is impossible. Thus $a_2 = b_2$, so $a_1 = b_1$ and $\mathbf{a} = \mathbf{b}$. Thus g is injective.

The rest of the proof is immediate. For example,
$$\begin{aligned} g(\mathbf{a} \otimes \mathbf{b}) &= g((a_1b_1 + 2a_2b_2, a_1b_2 + a_2b_1) \\ &= (a_1b_1 + 2a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{2} = g(\mathbf{a}) \times g(\mathbf{b}) \end{aligned}$$
and similar but simpler remark covers addition.

The conditions defining $\circledgt$ are precisely those which give $\mathbf{a} \circledgt \mathbf{b}$ if and only if $g(\mathbf{a}) > g(\mathbf{b})$.

Since a subfield of an ordered field is an ordered field, $\mathbb{G}$ is ordered by $>$ and so $\mathbb{Q}[\sqrt{2}]$ is an ordered field.

Exercise 8.2.2

(i) Let $P(n)$ be the statement that
$$S_n(x) = \frac{1 - x^{n+1}}{1 - x}.$$
Since
$$S_0(x) = 1 = \frac{1 - x}{1 - x},$$
$P(0)$ is true.

If $P(n)$ is true,
$$\begin{aligned} S_{n+1}(x) = S_n(x) + x^{n+1} &= \frac{1 - x^{n+1}}{1 - x} + x^{n+1} \\ &= \frac{(1 - x^{n+1}) + x^{n+1}(1 - x)}{1 - x} = \frac{(1 - x^{n+1}) + (x^{n+1} - x^{n+2})}{1 - x} \\ &= \frac{1 - x^{n+2}}{1 - x} \end{aligned}$$
so $P(n + 1)$ is true.

The required result follows by induction with base case 0.

(ii) Now, if $1 > x \geq 0$, then $x^n \to 0$ (see Exercise 7.4.9) and
$$S_n(x) = \frac{1 - x^{n+1}}{1 - x} \to \frac{1}{1 - x}.$$
Setting $x = 1/2$, we get
$$S_n(1/2) \to 2$$
and, setting $x = 1/10$, we get
$$9S_n(1/10) \to 1$$
as $n \to \infty$.

Exercise 8.2.3

Set
$$b_n = \frac{a_1}{10} + \frac{a_2}{10^2} + \dots \frac{a_n}{10^n}.$$
A simple induction shows that
$$b_n \leq \frac{9}{10} + \frac{9}{10^2} + \dots \frac{9}{10^n},$$
so, by summing a geometric series, we see that $b_n \leq 1$. Since the b_j form an increasing sequence, the fundamental axiom of analysis tells us that $b_j \to x$ for some $x \in \mathbb{R}$. Since $0 \leq b_j \leq 1$, we have $0 \leq x \leq 1$.

Exercise 8.2.4

(i) Let $P(n)$ be the statement that $1 > b_n \geq 0$ and $9 \geq a_n \geq 0$. If $P(n)$ is true, then $10 > 10b_n \geq 0$, so $9 \geq a_{n+1} \geq 0$ and $1 > b_{n+1} \geq 0$ by definition. Thus $P(n)$ implies $P(n+1)$. Essentially the same argument shows that $P(1)$ is true, so, by induction, $1 > b_n \geq 0$ and $9 \geq a_n \geq 0$ for all $n \geq 1$.

(ii) Let $Q(n)$ be the statement that $10^n a = 10^n a_n + b_n$. The definition of a_1 and b_1 tells us that $Q(1)$ is true. If $Q(n)$ is true, then
$$\begin{aligned} 10^{n+1}a &= 10 \times (10^n a) = 10 \times (10^n x_n + b_n) \\ &= 10^{n+1}x_n + 10b_n = 10^{n+1}x_n + 10a_{n+1} + b_{n+1} \quad = 10^{n+1}x_{n+1} + b_{n+1}. \end{aligned}$$
Thus, by induction, $Q(n)$ is true for all n.

Since $0 \leq b_n < 1$, we have
$$x_n \leq a < x_n + 10^{-n}.$$
Thus $|x_n - a| < 10^{-n} \to 0$ as $n \to \infty$. and so $x_n \to a$ as $n \to \infty$.

(iii) x_n is the nth place entry in a decimal expansion of x.

Exercise 8.2.5

(i) Let $P(n)$ be the statement that $b_n = u_n/v$, where u_n is a positive integer with $v > u_n \geq 0$. If $P(n)$ is true, then, since Ta_n is an integer,

$$b_{n+1} = 10b_n - Ta_n = 10\frac{u_n}{v} - Ta_n$$

Since Ta_n is an integer, it follows that $b_{n+1} = u_{n+1}/v$ where u_{n+1} is an integer. Since $1 > b_{n+1} \geq 0$, we have $v > u_{n+1} \geq 0$. Thus $P(n)$ implies $P(n+1)$. A similar argument shows that $P(1)$ is true so, by induction, $b_n = u_n/v$, where u_n is an integer with $v > u_n \geq 0$.

Since there are only v possible values of u_n, there exist integers p and q with $v + 1 \geq p > q \geq 1$ such that $u_p = u_q$. Let $Q(m)$ be the statement that $u_{p+m} = u_{q+m}$. Certainly $Q(0)$ is true and, if $Q(m)$ is true,

$$\frac{u_{p+m+1}}{v} = b_{p+m+1} = Sa_{p+m+1} = 10b_{p+m} - Tb_{p+m} = 10b_{q+m} - Tb_{q+m} = \frac{u_{q+m}}{v}.$$

By induction, $u_{p+m} = u_{q+m}$ for all $m \geq 0$, so $a_{m+(p-q)} = a_m$ for all $m \geq q+1$.

(ii) If $\alpha = 10^q a - n$ (where n is the integer part of $10^q a$) is rational, so is α. Thus there is no loss in generality in taking $q = 0$. If we take $A = a_1 + 10^{-1}a_2 + \ldots + 10^{-q}a_q$, then (summing a geometric series and using the axiom of Archimedes)

$$\begin{aligned} a_1 + 10^{-1}a_2 + \ldots + 10^{-q}a_q + \ldots + 10^{-rq}a_{rq} &= A(1 + 10^{-q} + \ldots + 10^{-q(r-1)}) \\ &= A\frac{1 - 10^{-qr}}{1 - 10^{-q}} \to \frac{A}{1 - 10^{-q}} \in \mathbb{Q}, \end{aligned}$$

so $\alpha \in \mathbb{Q}$ and we are done.

Exercise 8.2.6

(i) No. Set

$$c_1 = 1,\ c_2 = c_3 = \ldots = c_N = 6,\ c_{N+1} = 9,\ c_r = 0 \text{ for } r \geq N+2,$$
$$c'_1 = 1,\ c'_2 = c'_3 = \ldots = c'_N = 6,\ c'_{N+1} = 0,\ c_r = 0 \text{ for } r \geq N+2,$$
$$d_1 = 1,\ d_2 = d_3 = \ldots = d_N = 3,\ d_{N+1} = 9,\ d_r = 0 \text{ for } r \geq N+2,$$
$$d'_1 = 1,\ d'_2 = d'_3 = \ldots = d'_N = 3,\ d'_{N+1} = 0,\ d_r = 0 \text{ for } r \geq N+2$$

and define a'_j in the appropriate manner.

Then $a_1 = 2$, $a'_1 = 1$.

(ii) No. Set

$$c_1 = c_2 = c_3 = \ldots = c_M = 3,\ c_{M+1} = 9,\ c_r = 0 \text{ for } r \geq M+2,$$
$$c'_1 = c'_2 = c'_3 = \ldots = c'_M = 3,\ c'_{M+1} = 0,\ c_r = 0 \text{ for } r \geq M+2,$$
$$d_1 = 3,\ d_2 = d_3 = \ldots = d_M = 0,\ d_{M+1} = 9,\ d_r = 0 \text{ for } r \geq M+2$$
$$d'_1 = 3,\ d'_2 = d'_3 = \ldots = d'_M = 0,\ d'_{M+1} = 0,\ d_r = 0 \text{ for } r \geq M+2$$

and define b'_j in the appropriate manner.

Then $b_1 = 1$, $b'_1 = 0$.

Exercise 8.2.9

Set $f(1) = x_1$. Once $f(r)$ has been defined for $1 \leq r \leq m$, let $f(m+1) = x_k$ where k is the least integer with the property that $x_k \neq f(r)$ for $1 \leq r \leq m$.

EXERCISE 9.1.4

(i) Using the commutative law of addition for $\mathbb{R}$,

$$\mathbf{a} + \mathbf{b} = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + a_2) = \mathbf{b} + \mathbf{a}.$$

(ii) Using the associative law of addition for $\mathbb{R}$,

$$\begin{aligned}\mathbf{a} + (\mathbf{b} + \mathbf{c}) &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) = (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2))\\ &= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (a_1 + b_1, a_2 + b_2) + (c_1, c_2)\\ &= (\mathbf{a} + \mathbf{b}) + \mathbf{c}\end{aligned}$$

(iii) $\mathbf{0} + \mathbf{a} = (0, 0) + (a_1, a_2) = (0 + a_1, 0 + a_2) = (a_1, a_2) = \mathbf{a}$.

(iv) If we write $-\mathbf{a} = (-a_1, -a_2)$, then

$$\mathbf{a} + (-\mathbf{a}) = (a_1 - a_1, a_2 - a_2) = (0, 0) = \mathbf{0}.$$

(v) Using the commutative laws of multiplication and addition for $\mathbb{R}$,

$$\begin{aligned}\mathbf{a} \times \mathbf{b} &= ((a_1 \times b_1) - (a_2 \times b_2), (a_1 \times b_2) + (a_2 \times b_1))\\ &= ((b_1 \times a_1) - (b_2 \times a_2), (b_2 \times a_1) + (b_1 \times a_2))\\ &= ((b_1 \times a_1) - (b_2 \times a_2), (b_1 \times a_2) + (b_2 \times a_1)) = \mathbf{b} \times \mathbf{a}.\end{aligned}$$

(vii) We have

$$\begin{aligned}\mathbf{1} \times \mathbf{a} &= (1, 0) \times (a_1, a_2) = ((1 \times a_1) - (0 \times a_2), (1 \times a_2) + (0 \times a_1))\\ &= (a_1 - 0, a_2 + 0) = (a_1, a_2) = \mathbf{a}.\end{aligned}$$

(Multiplicative unit.)

(ix) Using the distributive law for $\mathbb{R}$ and making free use of the associative and commutative laws of addition,

$$\begin{aligned}\mathbf{a} \times (\mathbf{b} + \mathbf{c}) &= (a_1, a_2) \times (b_1 + c_1, b_2 + c_2)\\ &= ((a_1 \times (b_1 + c_1)) + ((-a_2 \times (b_2 + c_2)), (a_1 \times (b_2 + c_2)) + (a_2 \times (b_1 + c_2)))\\ &= (((a_1 \times b_1) + (a_1 \times c_1)) + ((-a_2) \times b_2) + ((-a_2) \times c_2)),\\ &\qquad ((a_1 \times b_2) + (a_1 \times c_2)) + ((a_2 \times b_1) + (a_2 \times c_1)))\\ &= (((a_1 \times b_1) + ((-a_2) \times b_2)) + ((a_1 \times c_1) + ((-a_2) \times c_2)),\\ &\qquad ((a_1 \times b_2) + (a_2 \times b_1)) + ((a_1 \times c_1) + (a_2 \times c_1)))\\ &= ((a_1 \times b_1) + ((-a_2) \times b_2), (a_1 \times b_2) + (a_2 \times b_1))\\ &\qquad + ((a_1 \times c_1) + ((-a_2) \times c_2), (a_1 \times c_1) + (a_2 \times c_1))\\ &= (\mathbf{a} \times \mathbf{b}) + (\mathbf{a} \times \mathbf{c})\end{aligned}$$

We note that $\mathbf{1} = (1, 0) \neq (0, 0) = \mathbf{0}$.

Our rules give

$$(0, 1) \times (0, 1) = ((0 \times 0) - (1 \times 1), (0 \times 1) + (1 \times 0)) = (-1, 0) = -\mathbf{1}.$$

Exercise 9.1.5

We observe that $f(x) = f(y)$ implies $(x, 0) = (y, 0)$ which, in turn, implies $x = y$. Thus f is injective.

We have $f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$ and

$$\begin{aligned} f(x) \times f(y) &= (x, 0) \times (y, 0) = ((x \times y) - (0 \times 0), (x \times 0) + (0 \times y)) \\ &= ((x \times y) - 0, 0 + 0) = (x \times y, 0) = f(x) \times f(y). \end{aligned}$$

Exercise 9.1.6

Observe that the conditions and so the arguments of Exercise 3.2.16 hold.

Exercise 9.2.4

Throughout we take $z = x + iy$, $w = u + iv$ with x, y, u, v real.

(i) $(z^*)^* = (x - iy)^* = x + iy = z$.
$|z^*| = |x + i(-y)| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$.
$(z+w)^* = ((x+u)+(y+v)i)^* = ((x+u)-(y+v)i) = (x-iy)+(u-iv) = z^*+w^*$.
Also

$$\begin{aligned}(zw)^* &= \big((xu - yv) + (xv + yu)i\big)^* = (xu - yv) - (xv - yu)i\\ &= (x - iy)(u - iv) = z^*w^*.\end{aligned}$$

(ii) $zz^* = (x + iy)(x - iy) = x^2 - (iy)^2 = x^2 + y^2 = |z|^2$.

(iii) $|zw|^2 = (zw)(zw)^* = (zw)(z^*w^*) = (zz^*)(ww^*) = |z|^2|w|^2 = (|z||w|)^2$, so, taking positive square roots, $|zw| = |z||w|$.

(iv) $z + z^* = (x + iy) + (x + iy)^* = (x + iy) + (x - iy) = 2x$ is real.
Further $z + z^* = 2x \leq 2|x| \leq 2\sqrt{x^2 + y^2} = 2|z|$.

(v) We have

$$\begin{aligned}|z + w|^2 &= (z + w)(z + w)^* = (z + w)(z^* + w^*)\\ &= zz^* + zw^* + z^*w + ww^* = |z|^2 + ((zw^*) + (zw^*)^*) + |w|^2\\ &\leq |z|^2 + 2|zw^*| + |w|^2 = |z|^2 + 2|z||w^*| + |w|^2\\ &= |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2,\end{aligned}$$

so, taking positive square roots, $|z + w| \leq |z| + |w|$.

(vi) If $|z| = 0$ then $\sqrt{x^2 + y^2} = 0$, so $x^2 + y^2 = 0$, so $x^2 = y^2 = 0$, $x = y = 0$ and $z = 0$. Automatically, $|0| = 0$.

(a) $d(z, w) = |z - w| \geq 0$.

(b) If $d(z, w) = 0$, then $|z - w| = 0$ so $z - w = 0$ and $z = w$. $d(z, z) = 0$ automatically.

(c) We have $|-z| = |-x - iy| = \sqrt{(-x)^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|$. Thus $d(z, w) = d(w, z)$.

(d) $d(z, w)+d(w, a) = |z-w|+|w-a| \geq |(z-w)+(w-a)| = |z-a| = d(z, a)$.

Exercise 9.2.5

(i) $|x|_{\mathbb{C}} = |x + i0|_{\mathbb{C}} = \sqrt{x^2} = |x|_{\mathbb{R}}$.

(ii) $|x| = \sqrt{x^2} \leq \sqrt{x^2 + y^2} = |z|$ and $|y| = \sqrt{y^2} \leq \sqrt{x^2 + y^2} = |z|$.

Also

$$|x + iy| \leq |x| + |iy| = |x| + |y|.$$

Exercise 9.2.7

All much the same as in the real case.

(i) If $z_n \to z$, $z_n \to w$ and $z \neq w$, then $|z-w| > 0$. Setting $\epsilon = |z-w|/3$, we can find N_1 and N_2 such that $|z_n - z| < \epsilon$ for $n \geq N_1$ and $|z_n - w| < \epsilon$ for $n \geq N_2$. If $N = \max\{N_1, N_2\}$ then

$$|z-w| \leq |z_n - w| + |z_n - z| \leq \frac{2}{3}|z-w|$$

which is impossible.

(ii) Let $\epsilon > 0$. We can find N_1 and N_2 such that $|z_n - z| < \epsilon/2$ for $n \geq N_1$ and $|w_n - w| < \epsilon/2$ for $n \geq N_2$. Taking $N = \max\{N_1, N_2\}$, we have

$$|(z_n + w_n) - (z+w)| = |(z_n - z) + (w_n - w)| \leq |z_n - z| + |w_n - w| < \epsilon/2 + \epsilon/2 = \epsilon$$

for $n \geq N$. Thus $z_n + w_n \to z + w$ as $n \to \infty$.

(iii) Let $\epsilon > 0$. We can find N_1, N_2 and N_3 such that

$$\begin{aligned}|z_n - z| &\leq 1 \text{ for } n \geq N_1,\\ |z_n - z| &\leq \frac{\epsilon}{2|w|+2} \text{ for } n \geq N_2,\\ |w_n - w| &\leq \frac{\epsilon}{2|z|+2} \text{ for } n \geq N_3.\end{aligned}$$

Taking $N = \max\{N_1, N_2, N_3\}$, we have

$$\begin{aligned}|z_n w_n - zw| &= |z_n(w - w_n) + w(z - z_n)| \leq |z_n(w - w_n)| + |w(z - z_n)|\\ &= |z_n||w - w_n| + |w||z - z_n| \leq (|z| + |z - z_n|)|w - w_n| + |w||z - z_n|\\ &\leq (|z|+1)\frac{\epsilon}{2|z|+2} + |w|\frac{\epsilon}{2|w|+2} < \epsilon\end{aligned}$$

for $n \geq N$. Thus $z_n w_n \to zw$ as $n \to \infty$.

(iv) If $\epsilon > 0$, then $|z_n - z| = 0 < \epsilon$ for $n \geq 1$.

Exercise 9.2.8

(i) If $|a| \geq |b|$, then $|a-b| + |b| \geq |a|$, so $|a-b| \geq |b| - |a| = \big||b| - |a|\big|$. Since $|a-b| = |b-a|$, we have $|a-b| \geq \big||b| - |a|\big|$ for $|b| \geq |a|$.

(ii) Let $\epsilon > 0$. We can find N such that $|z_n - z| < \epsilon$ for $n \geq N$. Automatically

$$\big||z_n| - |z|\big| \leq |z_n - z| < \epsilon.$$

for $n \geq N$.

(iii) Use (i) and Exercise 7.3.4 (iii).

Exercise 9.2.9

If $x_n \to x$ and $y_n \to y$, then, given $\epsilon > 0$, we can find N_1 and N_2 such that $|x_n - x| < \epsilon/2$ for $n \geq N_1$ and $|y_n - y| < \epsilon/2$ for $n \geq N_2$. If $N = \max\{N_1, N_2\}$ then

$$|z_n - z| = |(x_n - x) + i(y_n - y)| \leq |x_n - x| + |y_n - y| < \epsilon$$

for all $n \geq N$. Thus $z_n \to z$ as $n \to \infty$.

If $z_n \to z$, then, given $\epsilon > 0$, we can find N such that $|z_n - z| < \epsilon$ for $n \geq N$ and so

$$|x_n - x|,\ |y_n - y| \leq |z_n - z| < \epsilon$$

for all $n \geq N$. Thus $x_n \to x$ and $y_n \to y$ as $n \to \infty$.

We now use the results just proved. If $z_n \to z$, then $x_n \to x$ and $y_n \to y$, so $x_n \to x$ and $-y_n \to -y$, whence $z_n^* \to z^*$ as $n \to \infty$.

Exercise 9.2.12

Exactly as in Exercise 7.6.10.

Suppose $a_n \to a$. If $\epsilon > 0$, then $\epsilon/2 > 0$, so we can find an N with $|a_n - a| < \epsilon/2$ for all $n \geq N$. Now

$$|a_n - a_m| = |(a_n - a) + (a - a_n)| \leq |a_n - a| + |a_n - a| < \epsilon/2 + \epsilon/2 = \epsilon$$

for all $n \geq N$. The sequence is Cauchy.

Exercise 9.2.14

(i) Given $\epsilon > 0$, we can find an N such that $|z_n - z_m| < \epsilon$ for $n, m \geq N$. Thus
$$|x_n - x_m|, |y_n - y_m| \leq |z_n - z_m| < \epsilon$$
for $n, m \geq N$. The x_n, y_n form Cauchy sequences.

(ii) Since $\mathbb{R}$ is complete, we can find $x, y \in \mathbb{R}$ such that $x_n \to x$ and $y_n \to y$ as $n \to \infty$.

(iii) Setting $z = x + iy$, we have
$$|z_n - z| \leq |x_n - x| + |y_n - y| \to 0$$
as $n \to \infty$.

Exercise 9.2.15

(ii) We can find an N such that $|z_n - z_m| < 1$ for all $n, m \geq N$. In particular, setting
$$R = 1 + \max_{1 \leq j \leq N} |z_j|,$$
we have $|z_n| \leq R$ for all n.

(iii) By Theorem 9.2.10 (Bolzano–Weierstrass for $\mathbb{C}$), we can find $z \in \mathbb{C}$ and $n(j) \to \infty$ such that $z_{n(j)} \to z$ as $j \to \infty$.

(iv) Given $\epsilon > 0$, we can find an N such that $|z_n - z_m| < \epsilon/2$ for all $n, m \geq N$. We can now find a J such that $n(J) \geq N$ and $|z_{n(J)} - z| < \epsilon/2$. Thus, if $m \geq N$,
$$|z - z_m| \leq |z - z_{n(J)}| + |z_{n(J)} - z_m| < \epsilon/2 + \epsilon/2 = \epsilon.$$
Thus $z_m \to z$ as $m \to \infty$.

Exercise 9.3.2

Exactly as in Exercise 7.3.6.

The limit of the sum is the sum of the limits, so, if $z_n \to z$,

$$h(z_n) = f(z_n) + g(z_n) \to f(z) + g(z) = h(z)$$

as $n \to \infty$. Thus h is continuous.

The limit of the product is the product of the limits so if $z_n \to z$,

$$k(z_n) = f(z_n) \times g(z_n) \to f(z) \times g(z) = k(z)$$

as $n \to \infty$. Thus k is continuous.

Exercise 9.3.3

Observe that

$$|g(z_n) - g(z)| = \big||f(z_n)| - |f(z)|\big| \leq |f(z_n) - f(z)| \to 0$$

as $n \to \infty$.

Exercise 9.3.4

We say that $h : \mathbb{R} \to \mathbb{C}$ is *continuous at* $x \in \mathbb{R}$ if, whenever $x_n \to x$, we have $h(x_n) \to f(x)$. We say that h is *continuous* if it is continuous at every point x of $\mathbb{R}$.

The algebraic part of the first paragraph was done in Exercise 9.1.5. Continuity follows from the fact that $|x-x'| = |(x,0)-(x',0)|$, so $(x_n, 0) \to (x, 0)$ whenever $x_n \to x$ as $n \to \infty$.

We now look at the second paragraph. Our initial argument follows a standard pattern. If $g(1) = 0$ then $g(t) = g(t \times 1) = g(t) \times 0 = 0$ for all t. Thus $g(1) \neq 0$. Since $g(1) \times g(1) = g(1 \times 1) = g(1)$ cancellation now gives $g(1) = 1$. Simple induction using the observation that $g(n+1) = g(n) + g(1)$ now gives $g(n) = (n, 0)$ for all strictly positive integers n. The relation $g(n - m) = g(n) - g(m)$ gives $g(n) = n$ for all integers n. We now use the relation $g(p/q)g(q) = g(p)$ to give $g(p/q) = p/q$ for all integers p and q with $q \neq 0$. Thus $g(x) = f(x)$ whenever x is rational.

We now use the continuity of g. By Theorem 7.4.11, every element of $\mathbb{R}$ is the limit of a sequence in $\mathbb{Q}$. If $x \in \mathbb{R}$, choose $x_n \in \mathbb{Q}$ with $x_n \to x$. We have $g(x_n) \to g(x)$ and $g(x_n) = (x_n, 0) \to (x, 0)$ so, by the uniqueness of limits, $g(x) = (x, 0) = f(x)$ as required.

Exercise 9.3.8

We follow the proof of Theorem 9.3.6 word for word d replacing $|z| \leq R$ by $|z| = R$. We prove the existence of w. (The proof of the existence of w' follows by a similar argument or considering $-g$.)

By Theorem 9.3.7, the set E of $g(z)$ with $|z| = R$ forms a non-empty subset of $\mathbb{R}$ which is bounded above. By the supremum property of $\mathbb{R}$, it follows that E has a supremum, that is to say, there exists an $a \in \mathbb{R}$ with the following properties.

(1) $a \geq g(z)$ for all z with $|z| = R$.

(2) If $b \geq g(z)$ for all z with $|z| = R$, then $b \geq a$.

By condition (2), there exist z_n with $|z_n| = R$ such that $g(z_n) \geq a - 1/n$. Using (1), we see that $a - 1/n = g(z_n) = a$ and so, by the axiom of Archimedes $g(z_n) \to a$. By the Bolzano–Weierstrass theorem for $\mathbb{C}$, we can find a $w \in \mathbb{C}$ and a sequence $n(1) < n(2) < \dots$ such that $z_{n(j)} \to w$ as $j \to \infty$. By the continuity of g, we have $g(z_{n(j)}) \to g(w)$. By the uniqueness of limits $g(w) = a$ By (1), $g(a) \geq g(z)$ for all z with $|z| = R$.

Finally we note that $|z_{n(j)}| = R$ and $|z_{n(j)}| \to a$ so $|a| = R$ and we are done.

Exercise 9.3.9

(i) Let $z_k = a_k + ib_k$ with $a_k,\ b_k \in \mathbb{Q}$. We have

$$\begin{aligned} z_1 + z_2 &= (a_1 + a_2) + i(b_1 + b_2) \in \mathbb{A}, \\ z_1 \times z_2 &= (a_1 a_1 - b_1 b_2) + i(a_1 b_2 + a_2 b_1) \in \mathbb{A}, \\ -z_1 &= (-a_1) + i(-b_1) \in \mathbb{A} \end{aligned}$$

and, if $z_1 \neq 0$,

$$z_1^{-1} = \frac{a_1}{a_1^2 + b_1^2} + i\frac{(-b_1)}{a_1^2 + b_1^2} \in \mathbb{A}.$$

The field axioms are automatically satisfied. (Note $0,\ 1 \in \mathbb{A}$.)

(ii) (Lots of ways of doing this.) Suppose $z^2 = 2$ and $z \in \mathbb{A}$. Automatically $z \in \mathbb{C}$ so (working in $\mathbb{C}$) $(z - \sqrt{2})(z + \sqrt{2}) = 0$ so, since $\mathbb{C}$ is a field, $z - \sqrt{2} = 0$ or $z + \sqrt{2} = 0$. Thus $z = \sqrt{2}$ or $z = -\sqrt{2}$ and $z \notin \mathbb{A}$. The result now follows by reductio ad absurdum.

(iii) If $\epsilon > 0$ then, by Theorem 7.4.11, we can find $a \in \mathbb{Q}$ such that

$$|a - \sqrt{2}| < \min\{1/2, \epsilon/5\}.$$

Thus, since $1 < \sqrt{2} < 2$, we have $1/2 < a < 3$, and $a + \sqrt{2} \leq 5$, whence

$$|a^2 - 2| = |a - \sqrt{2}| \times |a + \sqrt{2}| \leq 5|a - \sqrt{2}| < \epsilon,$$

it follows that $\inf_{z \in A} |z^2 - 2| = 0$. Thus $2 \in \mathbb{A}$, but there is no $w \in \mathbb{A}$ with $|w^2 - 2| \leq |z^2 - 2|$ for all $z \in \mathbb{A}$.

Exercise 10.1.2

We have $P(0) = 0^2 + 0 = 0 + 0 = 0$, $P(1) = 1^2 + 1 = 1 + 1 = 0$ and $Q(0) = 0 = R(0)$, $Q(1) = 1 = R(1)$.

Exercise 10.1.3

(i) Let $\alpha(n)$, be the statement that a polynomial of degree at most n is either the zero polynomial or a polynomial of degree r for some r with $0 \leq r \leq n$.

$\alpha(0)$ is automatically true. Suppose that $\alpha(n)$ is true. If P is a polynomial of degree at most $n+1$, then, by definition, either P is of degree $n+1$, or $P = Q$ where Q is a polynomial of degree of degree at most n and so, by our inductive hypothesis, P is either the zero polynomial or P has degree r with $n \geq r \geq 0$. Thus $\alpha(n+1)$ is true.

The required result follows by induction.

(ii) Suppose that P is a polynomial of degree n with leading coefficient a and R is a polynomial of degree m with leading coefficient b. If $n > m \geq 0$, then $P(t) = at^n + Q(t)$ with Q a polynomial of degree at most $n-1$. Since R is a polynomial of degree at most $n-1$, $U = Q+R$ is a polynomial of degree at most $n-1$ and, since $P(t) = at^n + U(t)$, P is a polynomial of degree n.

If $n = m \geq 1$ then $P(t) = at^n + Q(t)$, $R(t) = bt^n + S(t)$ with R and S polynomials of degree at most $n-1$. It follows that $U = Q + S$ is a polynomial of degree at most $n-1$. We have $P(t) + Q(t) = (a+b)t^n + U(t)$ so, if $a + b \neq 0$, then $P + R$ is a polynomial of degree n with leading coefficient $a+b$ and, if $a+b = 0$, then $P+R$ is a polynomial of degree at most $n-1$. If $n = m = 0$, then, if $a+b \neq 0$, $P+Q = a+b$ is polynomial of degree 0 and, if $a+b = 0$, $P+Q = 0$.

(iii) The case when P is the zero polynomial is trivial. Suppose $c \in \mathbb{F}$, $c \neq 0$. Let $\alpha(n)$ be the statement that, if $n \geq r \geq 0$ and P is a polynomial of degree r with leading coefficient a, then the function $R = cP$ (defined by $R(u) = cP(u)$) is a polynomial of degree r with leading coefficient ca.

$\alpha(0)$ is automatically true. Suppose that $\alpha(n)$ is true. If P is a polynomial of degree r with $n+1 \geq r \geq 0$ and leading coefficient a, then $P(t) = at^r + Q(t)$ with Q a polynomial of degree at most $r-1$ (so at most n). If Q is not the zero polynomial, then, by the inductive hypothesis, cQ is a polynomial of degree at most $r-1$ (so at most n). If $Q = 0$, then $cQ = 0$. In either case,

$$cP(t) = cat^{n+1} + cQ(t)$$

defines a polynomial of degree $n+1$ with leading coefficient ca. Thus $\alpha(n+1)$ is true.

The required result follows by induction.

(iv) Let $\alpha(n)$ be the statement that, if $n \geq r \geq 0$ and P is a polynomial of degree r with leading coefficient a, then the function R defined by $R(u) = uP(u)$ is a polynomial of degree $r+1$ with leading coefficient a.

If $P(u) = a$ then $uP(u) = au$ so $P(0)$ is true. Suppose $\alpha(n)$ is true and P is a polynomial of degree $n + 1$ with leading coefficient a. Then $P(u) = au^{n+1} + Q(u)$ where Q is a polynomial of degree at most n. We have $uP(u) = au^{n+2} + uQ(u)$ and, by the inductive hypothesis, we know that the polynomial S given by $S(u) = uQ(u)$ has degree at most $n + 1$. Thus the function R defined by $R(u) = uP(u)$ is a polynomial of degree $n + 2$ with leading coefficient a.

The required result follows by induction.

(v) Suppose $b \in \mathbb{F}$. Let $\alpha(n)$ be the statement that the formula $P_n(u) = (u - b)^n$ defines a polynomial of degree n.

$\alpha(1)$ is true by inspection. Suppose that $\alpha(n)$ is true. Since

$$P_{n+1}(u) = uP_n(u) + (-b)P_n(u),$$

earlier parts of the lemma tell us that $\alpha(n + 1)$ is true.

The required result follows by induction.

(vi) Let $\alpha(n)$ be the statement that, if $n \geq r \geq 0$ and P is a polynomial of degree r, then the function R defined by $R(u) = P(u - b)$ is a polynomial of degree r.

$\alpha(0)$ is true by inspection. Suppose $\alpha(n)$ is true. If P is a polynomial of degree $n + 1$, we have $P(u) = au^{n+1} + Q(u)$ where Q is a polynomial of degree at most n. It follows that

$$P(u - b) = a(u - b)^{n+1} + Q(u - b)$$

so, using the inductive hypothesis and earlier parts of the lemma, the function R defined by $R(u) = P(u - b)$ is a polynomial of degree $n + 1$.

(vii) If P is a polynomial of degree n with leading coefficient a and Q is a polynomial of degree m with leading coefficient b, then

$$P(u) = au^n + R(u), \; Q(u) = bu^m + S(u)$$

with R of degrees at most $n - 1$ and U of degree at most $m - 1$. We have

$$P(u)Q(u) = abu^{n+m} + T(u)$$

where $T(u) = au^nS(u) + bu^mR(u) + R(u)S(u)$. By earlier parts $au^nS(u)$ corresponds to a polynomial of degree at most $n + m - 1$, $bu^mR(u)$ corresponds to a polynomial of degree at most $n+m-1$, and $R(u)S(u)$ to a polynomial of degree at most $n+m-2$. Thus T is a polynomial of degree at most $n+m-1$ and $P \times Q$ is a polynomial of degree $n + m$ with leading coefficient ab.

Exercise 10.1.6

(i) By Theorem 10.1.5, we can find a polynomial Q of degree $n-1$ such that

$$P(u) = (u-a)Q(u) + P(a) = (u-a)Q(u).$$

(ii) Let $R(u) = P(u) - P(a)$. Then R is a polynomial of degree n with $R(a) = 0$. By part (i), we can find a polynomial Q of degree $n-1$ such that

$$P(u) - P(a) = R(u) = (u-a)Q(u).$$

Exercise 10.1.8

Consider R given by $R(u) = P(u) - Q(u)$. We know that R is a polynomial of degree at most n. Since R vanishes at the $n+1$ points a_j, Theorem 10.1.7 tells us that $R = 0$ and this is the stated result.

Exercise 10.1.9

We use induction.

The result is immediate if $n = 1$. Suppose that it is true for $n = N$ and P is a polynomial of degree at most $N+1$. Since $P(a) = 0$, we know (for example, by Exercise 10.1.6) that $P(u) = (u-a)R(u)$, where R is a polynomial of degree at most N. Either $R(a) \neq 0$, and we are done, or $R(a) = 0$, so, by the inductive hypothesis,

$$R(u) = (u-a)^m Q(u)$$

and

$$P(u) = (u-a)^{m+1} Q(u)$$

where $N \geq m \geq 1$ and Q is a polynomial of degree at most $n-m$ such that $Q(a) \neq 0$. We have proved the result for $n = N+1$.

The full result follows by induction.

Exercise 10.1.10

Theorem 10.1.7 tells us that if P is a polynomial of degree at most n and we can find distinct $a_1, a_2, \ldots, a_{n+1} \in \mathbb{F}$ such that $P(a_j) = 0$ for $1 \leq j \leq n+1$, then $P = 0$. Thus, if P has degree $n \geq 0$, $P(u) \neq 0$ for some $u \in \mathbb{F}$.

Exercise 10.1.11

(i) Since $z_n \to z$ certainly implies $z_n \to z$, we have f_1 continuous. Since the product of continuous functions is continuous and $f_{n+1}(z) = f_1(z) \times f_n(z)$, it follows that, if f_n is continuous, so is f_{n+1}. Thus, by induction, f_n is continuous for all $n \geq 1$.

(ii) The constant polynomials are automatically continuous. If all polynomials of degree n or less are continuous, then, since any polynomial P of degree $n+1$ or less can be written as

$$P(z) = af_{n+1}(z) + Q(z)$$

where $a \in \mathbb{F}$ and Q is a polynomial of degree n or less and since sums and products of continuous functions are continuous, it follows that all polynomials of degree $n+1$ or less are continuous. The required result follows by induction.

Exercise 10.1.13

Let n be a positive odd integer. We know that $P(u) = Bu^n + Q(u)$ with $B \neq 0$ and Q a polynomial of degree at most $n-1$. By considering $B^{-1}P$, we may suppose that $B = 1$. By Lemma 10.1.12, we can find an $A > 0$ and $R \geq 1$ such that $|Q(u)| \leq A|u|^{m-1} \leq Au^{n-1}$. Taking $b = \max\{R, 2A\}$ and $a = -b$, we have

$$P(b) \geq b^n - Ab^{n-1} = b^{n-1}(b - A) > 0$$

and, similarly, $P(a) \leq -b^n + Ab^{n-1} = b^{n-1}(A - b) < 0$.

Since P is continuous, the intermediate value theorem tells us that there exists a c with $a < c < b$ such that $P(c) = 0$.

Exercise 10.1.14

Let $P(n)$ be the statement that we can find an $A_n > 0$ such that

$$|(1+u)^n - 1 - nu| \leq A_n|u|^2$$

for all $u \in \mathbb{F}$ with $|u| \leq 1/2$.

If we take $A_1 = 1$, we obtain, trivially,

$$|(1+u)^1 - 1 - (1 \times u)| = 0 \leq A_1|u|^2$$

for $|u| \leq 1/2$. Thus $P(1)$ is true.

Now suppose that $P(n)$ is true. If $|u| \leq 1/2$, we then have

$$\begin{aligned}
|(1+u)^{n+1} - 1 - (n+1)u| &= |(1+u)((1+u)^n - 1 - nu) + nu^2| \\
&\leq |(1+u)((1+u)^n - 1 - nu)| + n|u|^2 \\
&= |1+u||(1+u)^n - 1 - nu| + n|u|^2 \\
&\leq 2|(1+u)^n - 1 - nu| + nu^2 \\
&\leq 2A_n|u|^2 + n|u|^2 = A_{n+1}|u|^2
\end{aligned}$$

where $A_{n+1} = 2A_n + n$.

(Of course, there are better ways to approach this result.)

Exercise 10.2.6

If $A \neq 0$, then $Az + B = A(z - B/A)$, so $\mathcal{P}_1$ is the collection of all polynomials of degree 1.

Suppose $\mathcal{P}_n$ is the collection of all polynomials of degree n. If Q is a polynomial of degree $n+1$, then, by the fundamental theorem of algebra, Q has a root a and, by the remainder theorem for polynomials, $Q(z) = (z-a)R(z)$ with R a polynomial of degree n, and so $Q \in \mathcal{P}_{n+1}$.

The required result follows by induction.

Exercise 10.2.7

(i) $(z-\alpha)(z-\alpha^*) = z^2+(\alpha+\alpha^*)z+\alpha\alpha^* = z^2+(2\Re\alpha)z+|\alpha|^2 = z^2+az+b$ with $a = 2\Re\alpha$ and $b = |\alpha|^2$ real.

(ii) If $P(z) = a$ with a real, we say that P is a polynomial with real coefficients Inductively, we say that, if $P(z) = az^{n+1} + Q(z)$ with a real and non-zero and Q is a polynomial of degree at most n with real coefficients, then P is a polynomial of degree $n+1$ with real coefficients,

(iii) Since $a = \Re a + i\Im a$, any polynomial of degree at most 0 can be written as $P(z) = P_1(z) + iP_2(z)$ where P_1 and P_2 are polynomials of degree at most 0 with real coefficients.

Suppose that any polynomial P of degree at most n can be written as $P(z) = P_1(z)+iP_2(z)$ where P_1 and P_2 are polynomials with real coefficients of degree at most n. If P has degree $n+1$ then

$$P(z) = az^{n+1} + Q(z)$$

where $a \neq 0$ and Q is a polynomial of degree at most n. By hypothesis $Q(z) = Q_1(z) + iQ_2(z)$ where Q_1 and Q_2 are polynomials with real coefficients of degree at most n. Setting

$$P_1(z) = (\Re a)z^{n+1} + Q_1(z),\ P_2(z) = (\Im a)z^{n+1} + Q_2(z),$$

we see that $P(z) = P_1(z)+iP_2(z)$ where P_1 and P_2 are polynomials with real coefficients of degree at most $n+1$.

By induction, any polynomial P can be written as $P(z) = P_1(z) + iP_2(z)$ where P_1 and P_2 are polynomials with real coefficients.

If P is a polynomial of degree at most zero with real coefficients, then $P(z)$ is real for all z and so, in particular, for z real. If every polynomial Q of degree at most n with real coefficients has the property that $Q(x)$ is real when x is real, then, if

$$P(z) = az^{n+1} + Q(z)$$

with a real and Q of degree at most n with real coefficients, we have $P(x) = ax^{n+1}+Q(x)$ real. Thus, by induction, if a polynomial P has real coefficients then $P(x)$ is real for all x real.

Now suppose P any polynomial. We can write $P(z) = P_1(z) + iP_2(z)$ where P_1 and P_2 are polynomials with real coefficients. Since $P_1(x)$ and $P_2(x)$ are real

$$0 = \Im P(x) = \Im P_1(x) + \Re P_2(x) = P_2(x)$$

for all $x \in \mathbb{R}$ and, since a non-zero polynomial only has finitely many zeros, P_2 is the zero polynomial and $P = P_1$ has real coefficients.

(iv) A simple induction shows that $(az^n)^* = a^*(z^*)^n$ so, if $P(z) = az^{n+1} + Q(z)$ with a real and $Q(z)^* = Q(z^*)$, we have $P(z)^* = P(z^*)$. By induction on degree, any polynomial P with real coefficients satisfies $P(z)^* = P(z^*)$. In particular, if $P(\alpha) = 0$, then $P(\alpha^*) = 0$.

(v) By the fundamental theorem of algebra, P has a root α. If α is real, the remainder theorem gives us $P(z) = (z - \alpha)Q(z)$ with Q of degree $n - 1$. If x is real and $x \neq \alpha$ then $Q(x)$ must be real, so by continuity, $Q(x)$, is real for all real x. Thus Q is a polynomial of degree $n - 1$ with real coefficients.

If α is not real, then $\alpha \neq \alpha^*$. The remainder theorem gives us $P(z) = (z - \alpha)Q(z)$ with Q of degree $n - 1$. Part (iv) now tells us that

$$0 = 0^* = P(\alpha)^* = P(\alpha^*) = (\alpha^* - \alpha)Q(\alpha^*).$$

Since $\alpha^* - \alpha \neq 0$, we have $Q(\alpha^*) = 0$, so $n \geq 2$ and $Q(z) = (z - \alpha^*)R(z)$ with R of degree $n - 2$. Now

$$P(z) = (z - \alpha)(z - \alpha^*)R(z)$$

so since $(x - \alpha) \times (x - \alpha^*)$ is real and non-zero for all real x, $R(x)$ is real whenever x is real and so R is a polynomial of degree $n - 2$ with real coefficients.

(vi) Induction on degree now shows that any polynomial of degree $n \geq 1$ with real coefficients can be written as the product of linear and quadratic polynomials with real coefficients.

Exercise 10.3.3

(i) Let $\alpha(n)$ be the statement that, if P is a polynomial of degree n with rational coefficients, we can find an integer $N \geq 1$ such that $U(x) = NP(x)$ defines a polynomial with integer coefficients.

If P has degree at most 0, we have $P(x) = a$ with $a = u/N$, u an integer and N a strictly positive integer. If $U = NP$ then U has integer coefficients.

Suppose $\alpha(r)$ is true for $r \leq n$. If P is a polynomial of degree $n+1$ with rational coefficients, we can find a polynomial Q with rational coefficients of degree at most n and a $a \in \mathbb{Q}$ such that $P(z) = ax^{n+1} + Q(x)$. Thus we can find N_1, N_2 strictly positive integers such that $N_1 Q$ is a polynomial with integer coefficients and $N_2 a \in \mathbb{Z}$. Simple induction shows that sums of polynomials with integer coefficients and integer multiples of such polynomials are themselves polynomials with integer coefficients, so $(N_1 N_2)P$ is a polynomial with integer coefficients.

The required result follows by induction.

(ii) If α is the root of a polynomial P with rational coefficients, then we can choose N so that $U = NP$ has integer coefficients so α is the root of of a polynomial U with integer coefficients.

Thus we may replace the words ‘integer coefficients’ by ‘rational coefficients’ in Liouville’s theorem.

Exercise 10.3.5

(i) The result is trivially true for polynomials with integer coefficients of degree at most 0.

Suppose it is true for polynomials with integer coefficients of degree N or less. If P is a polynomial with integer coefficients of degree $N+1$ then

$$P(t) = at^{N+1} + Q(t),$$

where a is an integer and Q is a polynomial with integer coefficients of degree N or less. Thus

$$q^{N+1}P(p/q) = ap^{N+1} + q \times (q^N Q(p/q)) \in \mathbb{Z}.$$

The required result now follows by induction.

(ii) The result is trivially true for polynomials of degree at most 0.

Suppose it is true for polynomials of degree N or less. If P is a polynomial of degree $N+1$ then

$$P(t) = at^{N+1} + Q(t),$$

where $a \in \mathbb{R}$ and Q coefficients of degree N or less. By hypothesis, we can find a $K_1 > 0$ such that $|Q(x)| \leq K_1$ whenever $|x| \leq R$. Setting $K = K_1 + |a|R^{n+1}$ we have

$$|P(t)| = |a||t|^{n+1} + |Q(t)| \leq K$$

for all $|t| \leq R$.

The required result now follows by induction.

Alternatively (But using more advanced ideas.) We have shown earlier that polynomials are continuous and that continuous functions are bounded on sets of points t with $|t| \leq R$.

Exercise 10.3.7

We have

$$10^{-1} + 10^{-2} + 10^{-6} + 10^{-24} \leq x \leq 10^{-1} + 10^{-2} + 10^{-6} + 10^{-24} + 2 \times 10^{-120}$$

so

$$\alpha = .110\,001\,000\,000\,000\,000\,000\,001\,000\,000\ldots$$

correct to 30 places of decimals.

Exercise 10.3.8

Observe that, if $k > n$, then $10^{-k!} \leq 10^{-(n+1)!} \times 10^{-k+1}$ and so (by induction or summing a geometric series)

$$a_n \leq a_m \leq a_n + 2\frac{10}{9}(1 - 10^{n-m})10^{-(n+1)!} \leq a_n + 4 \times 10^{-(n+1)!}$$

for all $m \geq n$. Thus the a_n form an increasing sequence bounded above and so $a_n \to \alpha$ for some $\alpha \in \mathbb{R}$. Further we have

$$a_n \leq \alpha \leq 4 \times 10^{-(n+1)!}.$$

A simple induction shows that $10^{n!}a_n$ is an integer. Thus, if we write $q_n = 10^{n!}$ and $p_n = 10^{n!}a_n$, we have p_n and q_n integers with $q_n \geq 1$ and

$$\left|\alpha - \frac{p_n}{q_n}\right| = |\alpha - a_n| \leq \frac{4}{10^{(n+1)!}} = \frac{4}{q_n^{n+1}}.$$

Thus, if m is a fixed integer with $m \geq 1$ and A is a fixed real number with $A > 0$, we have

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{A}{q_n^m}$$

for n sufficiently large. By Theorem 10.3.4, it follows that α cannot be the root of a polynomial with integral coefficients.

Exercise 10.4.2

Suppose $0 + P = P$ and $\tilde{0} + P = P$ for all P. Then, using the commutative law of addition,

$$\tilde{0} = 0 + \tilde{0} = \tilde{0} + 0 = 0.$$

Suppose $1 \times P = P$ and $\tilde{1} \times P = P$ for all P. Then, using the commutative law of multiplication,

$$\tilde{1} = 1 \times \tilde{1} = \tilde{1} \times 1 = 1.$$

If $P + Q = 0$ and $P + R = 0$ then, using the commutative and associative laws of addition freely,

$$Q = 0 + Q = (P + R) + Q = (R + P) + Q = R + (P + Q) = R + 0 = R.$$

Exercise 10.4.3

(i) We use the commutative associative and distributive laws freely. Since

$$(0 \times R) + (0 \times R) = (0 + 0) \times R = 0 \times R$$

we have

$$\begin{aligned} 0 &= (0 \times R) + (-(0 \times R)) = ((0 \times R) + (0 \times R)) + (-(0 \times R)) \\ &= (0 \times R) + (0 \times R + (-(0 \times R))) = (0 \times R) + 0 = 0 \times R \end{aligned}$$

(ii) If $P \times Q = P \times R$ then, since

$$(P \times R) + (P \times (-R)) = P \times (R + (-R)) = P \times 0 = 0 \times P = 0,$$

it follows that

$$(Q+(-R))\times P = P\times(Q+(-R)) = (P\times Q)+(P\times(-R)) = (P\times R)+(P\times(-R)) = 0$$

Since $P \neq 0$ we have $Q + (-R) = 0$, so

$$Q = 0+Q = (R+(-R))+Q = R+((-R)+Q) = R+(Q+(-R)) = R+0 = 0+R = R.$$

Exercise 10.4.4

Observe that $(P \times Q)(0) = P(0) \times Q(0) = P(0) \times 0 = 0 \neq 1$.

Exercise 10.4.6

(ii) By the associative law of addition for fields, $P(u) + (Q(u) + R(u)) = (P(u) + Q(u)) + R(u)$ for all u so $P + (Q + R) = (P + Q) + R$.

(iii) Let R_0 be the zero polynomial. We have $R_0(u) + P(u) = 0 + P(u) = P(u)$ for all u so $R_0 + P = P$ for all P.

(iv) We know from Exercise 10.1.3 that $P = (-1) \times P$ is a polynomial. Since $P(u) + (-P(u)) = 0 = R_0(u)$, we have $P + (-P) = R_0$.

(v) By the commutative law of multiplication for fields, $P(u) \times Q(u) = Q(u) \times P(u)$ for all u so $P \times Q = Q \times P$.

(vi) By the associative law of multiplication for fields. $P(u) \times (Q(u) \times R(u)) = (P(u) \times Q(u)) \times R(u)$ for all u so $P \times (Q \times R) = (P \times Q) \times R$.

(vii) Let R_1 be the polynomial given by $R_1(u) = 1$. We have $R_1(u)\times P(u) = 1 \times P(u) = P(u)$ for all u, so $R_1 \times P = P$ for all P.

(ix) By the distributive law for fields $P(u) \times (Q(u) + R(u)) = (P(u) \times Q(u)) + (P(u) \times R(u))$ for all u so so $P \times (Q + R) = (P \times Q) + (P \times R)$.

Since $R_0(0) = 0 \neq 1 = R_1(0)$, we have $R_0 \neq R_1$.

Exercise 10.4.9

If $P(x) = x - 1$, then $P \succ 0$, but $P(0) = -1 < 0$.

Exercise 10.4.11

(i) $P \times Q = P \times Q$, so $(P, Q) \sim (P, Q)$. (Reflexive)

(ii) If $(P, Q) \sim (R, S)$, then $P \times S = R \times Q$, so $R \times Q = P \times S$ and $(R, S) \sim (P, Q)$ (Symmetric)

(iii) If $(P, Q) \sim (R, S)$ and $(R, S) \sim (U, V)$, then $P \times S = R \times Q$, $R \times V = U \times S$. Using the associative and commutative laws,

$$\begin{aligned}(P \times V) \times R &= P \times (V \times R) = P \times (R \times V)\\ &= P \times (U \times S) = P \times (S \times U)\\ &= (P \times S) \times U = (R \times Q) \times U\\ &= R \times (Q \times U) = R \times (U \times Q)\\ &= (U \times Q) \times R.\end{aligned}$$

Since $R \neq 0$, the cancellation law for multiplication yields $P \times V = U \times Q$ so $(P, Q) \sim (U, V)$.

Exercise 10.4.12

$2 \times 3 \equiv 0 \equiv 2 \times 3 \mod 6$, $3 \times 4 \equiv 0 \equiv 3 \times 2 \mod 6$ so

$$([2], [2]) \sim ([3], [3]), \; ([3], [3]) \sim ([4], [2]).$$

However, $2 \times 2 \equiv 4 \not\equiv 2 \equiv 2 \times 4 \mod 6$, so

$$([2], [2]) \nsim ([4], [2]).$$

The proof of transitivity in Exercise 10.4.11 made use of the cancellation law for multiplication which fails for $(\mathbb{Z}_6, +, \times)$.

Exercise 10.4.13

Throughout we make free use of the associative and commutative laws.
(i) We know that $P_1 \times Q_2 = P_2 \times Q_1$, so

$$(P_1 \times R_1) \times (Q_2 \times U_1) = (P_1 \times Q_2) \times (R_1 \times U_1) = (P_2 \times Q_1) \times (R_1 \times U_1)$$
$$= (P_2 \times U_1) \times (Q_1 \times R_1)$$

Thus $(P_1 \times U_1, Q_1 \times R_1) \sim (P_2 \times U_1, Q_2 \times R_1)$.

(ii) Similarly, $(P_2 \times U_1, Q_2 \times R_1) \sim (P_2 \times U_2, Q_2 \times R_2)$, so, by transitivity,

$$(P_1 \times U_1, Q_1 \times R_1) \sim (P_2 \times U_2, Q_2 \times R_2).$$

We have shown that if $[P_1] = [P_2]$, $[Q_1] = [Q_2]$, $[R_1] = [R_2]$ and $[U_1] = [U_2]$, then

$$[(P_1 \times R_1, Q_1 \times U_1)] = [(P_2 \times R_2, Q_2 \times U_2)].$$

Thus we can define multiplication on $\mathcal{B}/\sim$ by

$$[(P, Q)] \times [(R, U)] = [(P \times R, Q \times U)].$$

(iii) We use the distributive law at the beginning and and end of the calculation.

$$\begin{aligned}
&\big((P_1 \times R_1) + (Q_1 \times U_1)\big) \times (Q_2 \times R_2)\\
&\qquad = ((P_1 \times R_1) \times (Q_2 \times R_2)) + ((Q_1 \times U_1) \times (Q_2 \times R_2))\\
&\qquad = ((P_1 \times Q_2) \times (R_1 \times R_2)) + ((U_1 \times R_2) \times (Q_1 \times Q_2))\\
&\qquad = ((P_2 \times Q_1) \times (R_1 \times R_2)) + ((U_2 \times R_1) \times (Q_1 \times Q_2)\\
&\qquad = ((P_2 \times R_2) \times (Q_1 \times R_1)) + ((Q_2 \times U_2) \times (Q_1 \times R_1))\\
&\qquad = \big((P_2 \times R_2) + (Q_2 \times U_2)\big) \times (Q_1 \times R_1)
\end{aligned}$$

We have shown that if $[P_1] = [P_2]$, $[Q_1] = [Q_2]$, $[R_1] = [R_2]$ and $[U_1] = [U_2]$, then

$$[(P_1 \times R_1) + (Q_1 \times U_1), Q_1 \times R_1)] = [(P_2 \times R_2) + (Q_2 \times U_2), Q_2 \times R_2)]$$

Thus we can define addition on $\mathcal{B}/\sim$ by

$$[(P, Q)] + [(U, R)] = [((P \times R) + (Q \times U), Q \times R].$$

EXERCISE 10.4.15

We write $[P,Q] = [(P,Q)]$.

(i) We have

$$\begin{aligned}[P,Q]+[U,R] &= [(P\times R)+(Q\times U), Q\times R]\\ &= [(R\times P)+(U\times Q), R\times Q]\\ &= [(U\times Q)+(R\times P), R\times Q] = [U,R]+[P,Q]\end{aligned}$$

(Commutative law of addition.)

(ii) We have

$$\begin{aligned}((U\times Q)\times R))+((V\times P)\times R) &= (R\times(U\times Q))+(R\times(V\times P))\\ &= R\times((U\times Q)+(V\times P))\\ &= ((U\times Q)+(V\times P))\times R\end{aligned}$$

so

$$\begin{aligned}&[U,V]+([P,Q]+[U,R]) = [U,V]+[(P\times R)+(Q\times U), Q\times R]\\ &= [(U\times(Q\times R))+(V\times((P\times R)+(Q\times U)\times R), V\times(Q\times R)]\\ &= [(U\times(Q\times R))+((V\times(P\times R))+(Q\times(U\times R))), V\times(Q\times R)]\\ &= [(U\times(Q\times R))+(V\times(P\times R))+(Q\times(U\times R)), (V\times Q)\times R)]\\ &= [((U\times Q)+(V\times P))\times R))+(Q\times U)\times R)), (V\times Q)\times R)]\\ &= ([U,V]+[P,Q])+[U,R]\end{aligned}$$

(Associative law of addition.)

(iii) $[0,1]+[P,Q] = [(0\times Q)+(1\times P), 1\times Q] = [0+P,Q] = [P,Q]$
(Additive zero.)

(iv) We have

$$\begin{aligned}[P,Q]+[-P,Q] &= [(P\times Q)+(-P\times Q), Q\times Q]\\ &= [(P+(-P))\times Q, Q\times Q] = [0\times Q, Q\times Q]\\ &= [0, Q\times Q] = [0,1]\end{aligned}$$

(Additive inverse.)

(v) $[P,Q]\times[U,R] = [P\times U, Q\times R] = [U\times P, R\times Q] = [U,R]\times[P,Q]$
(Commutative law of multiplication.)

(vi) We have

$$\begin{aligned}[P,Q]\times([U,R]\times[S,T]) &= [P,Q]\times[U\times S, R\times T]\\ &= [P\times(U\times S), Q\times(R\times T)]\\ &= [(P\times U)\times S, (Q\times R)\times T]\\ &= [P\times U, Q\times R]\times[S,T]\\ &= ([P,Q]\times[U,R])\times[S,T]\end{aligned}$$

(Associative law of multiplication.)

(vii) $[1, 1] \times [P, Q] = [1 \times P, 1 \times Q] = [P, Q]$
(Multiplicative unit.)

(viii) If $[P, Q] \neq [0, 1]$, then $P \times 1 \neq Q \times 0$ so $P \neq 0$. We have $[P, Q] \times [Q, P] = [QP, QP] = [1, 1]$. (Multiplicative inverse.)

(ix) We have

$$\begin{aligned}
[P, Q] \times ([U, R] + [S, T]) &= [P, Q] \times [(U \times T) + (R \times S), R \times T] \\
&= [P \times ((U \times T) + (R \times S)), Q \times (R \times T)] \\
&= [(P \times (U \times T)) + (P \times (R \times S)), Q \times (R \times T)] \\
&= [P \times (U \times T), Q \times (R \times T)] + [P \times (R \times S), Q \times (R \times T)] \\
&= [(P \times U) \times T, (Q \times R) \times T] + [(P \times S) \times R)), (Q \times T) \times R] \\
&= (P \times U, Q \times R] + [P \times S, Q \times T] \\
&= ([P, Q] \times [U, R]) + ([P, Q] \times [S, T])
\end{aligned}$$

(Distributive law.)

We note that $[1, 1] \neq [0, 1]$.

EXERCISE 10.4.16

(i) If $P > 0$, then $0 = P + (-P) > 0 + (-P) = -P$. If $0 > P$, then $-P = -P + 0 > -P + P = P + (-P) = 0$.

(ii) We know that $-P = (-1) \times P$ since

$$0 = 0 \times P = (1 + (-1)) \times P = (1 \times P) + ((-1) \times P) = P + ((-1) \times P).$$

If $P, Q > 0$, then, from the rules for an ordered integral domain, $P \times Q > 0$. If $0 > P, Q$ then $(-P), (-Q) > 0$ so, since $(-1)^2 = -(-1) = 1$,

$$P \times Q = (-1)^2 \times (P \times Q) = ((-1) \times P)((-1) \times Q) > 0.$$

If $P > 0 > Q$, then $-Q > 0$, so

$$-(P \times Q) = (-1) \times (P \times Q) = P \times ((-1) \times Q) = P \times (-Q) > 0,$$

and thus $0 > P \times Q$.

(iii) If $(P, Q) \sim (0, 1)$, then

$$P = (1 \times P) = (0 \times Q) = 0.$$

Conversely, if $P = 0$, then $P \times 1 = 0 = 0 \times Q$, so $(P, Q) \sim (0, 1)$.

(iv) If $P \times Q > 0$, then either $P > 0$ or $0 > P$. Since $(-P, -Q) \sim (P, Q)$, we may suppose $P > 0$ so, by (ii), $Q > 0$. Similarly, we may suppose $U > 0$. Since $P \times U = Q \times R$ it follows that $Q \times R = P \times U > 0$ and so $R > 0$ whence $R \times U > 0$.

(v) Follows at once.

Exercise 10.4.18

We write $\mathbf{P} = [P_1, P_2] = [(P_1, P_2)]$ and so on.

(x) If $\mathbf{P} > \mathbf{Q}$ and $\mathbf{Q} > \mathbf{R}$, then writing $\mathbf{U} = \mathbf{P} - \mathbf{Q}$, $\mathbf{V} = \mathbf{Q} - \mathbf{R}$, we have $\mathbf{U}$, $\mathbf{V} > [0, 1]$, so $U_1 \times U_2 > 0$, $V_1 \times V_2 > 0$. As noted in the previous question we may take $U_1,\ V_1 > 0$ and so $U_2,\ V_2 > 0$. Thus $(U_1 \times V_2) + (U_1 \times V_2) > 0$ and $U_2 \times V_2 > 0$ so

$$(U_1 \times V_2) + (U_1 \times V_2)) \times (U_2 \times V_2) > 0$$

Thus $\mathbf{P} - \mathbf{R} = \mathbf{U} + \mathbf{V} > [0, 1]$ and $\mathbf{P} > \mathbf{R}$.
(Transitivity of order.)

(xi) Consider $\mathbf{U} = [U_1, U_2]$. Observe that exactly one of the statements $U_1 \times U_2 > 0$, $U_1 \times U_2 = 0$, or $U_1 \times U_2 < 0$ holds. In the first case $\mathbf{U} > 0$, in the second $\mathbf{U} = [0, 1]$, in the third $\mathbf{U} > 0$. Setting $\mathbf{U} = \mathbf{P} - \mathbf{Q}$, we see that exactly one of the conditions holds: $\mathbf{P} > \mathbf{Q}$, $\mathbf{P} = \mathbf{Q}$ or $\mathbf{Q} > \mathbf{P}$.
(Trichotomy.)

(xii) If $\mathbf{P} > \mathbf{Q}$ then

$$(\mathbf{P} + \mathbf{R}) - (\mathbf{Q} + \mathbf{R}) = \mathbf{P} - \mathbf{Q} > [0, 1]$$

so $\mathbf{P} + \mathbf{R} > \mathbf{Q} + \mathbf{R}$.
(Order and addition.)

(xiii) If $\mathbf{P} > \mathbf{Q}$ and $\mathbf{R} > [0, 1]$, then, writing $\mathbf{U} = \mathbf{P} - \mathbf{Q}$, we have $\mathbf{U} > [0, 1]$. As earlier, we may suppose $R_1,\ U_1 > 0$ and so $R_2,\ U_2 > 0$. Thus

$$(R_1 \times U_1) \times (R_2 \times U_2) > 0$$

and we have shown $\mathbf{R} \times \mathbf{U} > [0, 1]$.

It follows that

$$\begin{aligned}(\mathbf{R} \times \mathbf{P}) - (\mathbf{R} \times \mathbf{Q}) &= (\mathbf{R} \times \mathbf{P}) + (\mathbf{R} \times (-\mathbf{Q}))\\ &= \mathbf{R} \times (\mathbf{P} + (-\mathbf{Q}))\\ &= \mathbf{R} \times \mathbf{U} > [0, 1]\end{aligned}$$

and $\mathbf{P} \times \mathbf{R} > \mathbf{Q} \times \mathbf{R}$.
(Order and multiplication.)

Exercise 10.4.20

(i) Let $\alpha(n)$ be the statement that, if P has degree at most n, then P can be written as
$$P(t) = Q(t) \times (t^2 - v) + (at + b)$$
where $a, b \in \mathbb{F}$.

Observe that $\alpha(1)$ is automatically true. Suppose $\alpha(n)$ is true for some $n \geq 1$. If P is a polynomial of degree $n+1$ then
$$P(t) = At^{n+1} + U(t)$$
where U is a polynomial of degree at most n and so $V(t) = U(t) + (A \times v)t^{n-1}$ is a polynomial of degree at most n. By our inductive hypothesis
$$V(t) = R(t) \times (t^2 - v) + (at + b)$$
where $a, b \in \mathbb{F}$. We now have
$$\begin{aligned} P(t) &= At^{n-1}(t^2 - v) + V(t) = At^{n-1}(t^2 - v) + (R(t) \times (t^2 - v) + (at + b)) \\ &= (At^{n-1} + R(t)) \times (t^2 - v) + (at + b) = Q(t) \times (t^2 - v) + (at + b) \end{aligned}$$
where $Q(t) = At^{n-1} + R(t)$. Thus $\alpha(n+1)$ is true.

The required result follows by induction.

(ii) Suppose that
$$Q_1(t) \times (t^2 - v) + (a_1 t + b_1) = Q_2(t) \times (t^2 - v) + (a_2 t + b_2).$$
Setting $Q(t) = Q_2(t) - Q_1(t)$, $a = a_2 - a_1$, $b = b_2 - b_1$, we have
$$Q(t) \times (t^2 - v) + (at + b) = 0.$$
If Q is not the zero polynomial, then the polynomial R given by $R(t) = Q(t) \times (t^2 - v)$ has degree at least 2, so the polynomial U given by $U(t) = Q(t) \times (t^2 - v) + (at + b)$ has degree at least 2 and so (by Exercise 10.1.10) cannot be the zero polynomial. Thus $Q = 0$ and
$$at + b = 0,$$
whence, by Exercise 10.1.10 or a direct argument, $a = b = 0$. Thus $a_1 = a_2$ and $b_1 = b_2$.

(iii) $P(t) - P(t) = 0 \times (t^2 - v)$ so $P \sim_v P$.
If $P_1 \sim_v P_2$, then $P_1(t) - P_2(t) = Q(t) \times (t^2 - v)$ for some $Q \in \mathcal{P}$, so $P_2(t) - P_1(t) = (-Q(t)) \times (t^2 - v)$ and $P_2 \sim_v P_1$
If $P_1 \sim_v P_2$ and $P_2 \sim_v P_3$ then
$$P_1(t) - P_2(t) = Q_1(t) \times (t^2 - v), \ P_2(t) - P_3(t) = Q_2(t) \times (t^2 - v)$$
and, writing $Q(t) = Q_1(t) + Q_2(t)$, we have
$$P_1(t) - P_3(t) = (P_1(t) - P_2(t)) + (P_2(t) - P_3(t)) = Q(t) \times (t^2 - v)$$
so $P_1 \sim_v P_3$.

(iv) If $P_1 \sim_v P_2$, $R_1 \sim_v R_2$, then

$$P_1(t) - P_2(t) = Q_1(t) \times (t^2 - v),\ R_1(t) - R_2(t) = Q_2(t) \times (t^2 - v)$$

for some polynomials $Q_1,\ Q_2$ so

$$(P_1(t) + R_1(t)) - (P_2(t) + R_2(t)) = Q(t) \times (t^2 - v),$$

with $Q(t) = Q_1(t) + Q_2(t)$, and

$$\begin{aligned}
(P_1(t) &\times R_1(t)) - (P_2(t) \times R_2(t)) \\
&= (P_1(t) \times (R_1(t) - R_2(t))) + ((P_1(t) - P_2(t))R_2(t)) \\
&= (P_1(t) \times (Q_2(t) \times (t^{2)} - v))) + ((Q_1(t) \times (t^2 - v)) \times R_2(t)) \\
&= U(t) \times (t^2 - v)
\end{aligned}$$

where $U(t) = \big(P_1(t) \times Q_2(t)\big) + \big(Q_1(t) \times R_2(t)\big)$.

Thus $P_1 + R_1 \sim_v P_2 + R_2$ and $P_1 \times R_1 \sim_v P_2 \times R_2$, so we may make the unambiguous definitions

$$[P] + [R] = [P + R] \text{ and } [P] \times [Q] = [P \times Q].$$

(v) All the verifications follow the pattern:- Since $\mathbb{F}$ is a field we have

$$(P + Q)(u) = P(u) + Q(u) = Q(u) + P(u) = (P + Q)(u)$$

for all $u \in \mathbb{R}$ and so $P + Q = Q + P$ for all polynomials. Thus

$$[P] + [Q] = [P + Q] = [Q + P] = [Q] + [P].$$

(vi) If $\mathbb{F} = \mathbb{R}$ and $v = 1$, $P(u) = u - 1$, $Q(u) = u + 1$ then $P(u) \times Q(u) = u^2 - 1$. Now $P,\ Q \nsim_v 0$ (using (ii)), but $P \times Q \sim_v 0$ so $[P],\ [Q] \neq [0]$, but $[P] \times [Q] = [0]$ and $\mathcal{P}/{\sim_v}$ is not an integral domain.

If $\mathbb{F} = \mathbb{R}$ and $v \geq 0$, we observe that if $P(u) = u - \sqrt{v}$, $Q(u) = u + \sqrt{v}$ then $P(u) \times Q(u) = u^2 - v$. Now $P,\ Q \nsim_v 0$ (using (ii)) but $P \times Q \sim_v 0$ so $[P],\ [Q] \neq [0]$, but $[P] \times [Q] = [0]$ and $\mathcal{P}/{\sim_v}$ is not an integral domain.

If $\mathbb{F} = \mathbb{C}$ and $v = -1$, we observe that if $P(u) = u - i$, $Q(u) = u + i$ then $P(u) \times Q(u) = u^2 + 1 = u^2 - v$. Now $P,\ Q \nsim_v 0$ (using (ii)) but $P \times Q \sim_v 0$ so $[P],\ [Q] \neq [0]$, but $[P] \times [Q] = [0]$ and $\mathcal{P}/{\sim_v}$ is not an integral domain.

(vii) We work over $\mathbb{R}$ with $v = -1$. Suppose R is a polynomial. Then, by (i), $R \sim U$ where $U(t) = at + b$. If $[R] \neq [0]$, then a and b can not both be zero. Setting

$$Q(t) = \frac{-a}{a^2 + b^2}t + \frac{b}{a^2 + b^2},$$

we have

$$[P] \times [Q] = [U] \times [Q] = [U \times Q]$$

Now

$$U(t) \times Q(t) = \frac{b^2 - a^2t^2}{b^2 + a^2} = 1 - \frac{a^2}{a^2 + b^2}(t^2 + 1)$$

so $U \times Q \sim_v 1$ and $[P] \times [Q] = [1]$. Thus every non-zero element has a multiplicative inverse and, by (v), $\mathcal{P}/\sim_v$ is a field.

We work over $\mathbb{Q}$ with $v = 2$. Suppose R is a polynomial. Then, by (i), $R \sim U$ where $U(t) = at + b$. If $[R] \neq [0]$, then a and b can not both be zero. Setting

$$Q(u) = \frac{-a}{-2a^2 + b^2}u + \frac{b}{-2a^2 + b^2},$$

we have

$$[P] \times [Q] = [U] \times [Q] = [U \times Q]$$

Now

$$U(t) \times Q(t) = \frac{b^2 - a^2t^2}{b^2 - 2a^2} = 1 - \frac{a^2}{2a^2 - b^2}(t^2 - 2)$$

so $U \times Q \sim_v 1$ and $[P] \times [Q] = [1]$. Thus every non-zero element has a multiplicative inverse and, by (v), $\mathcal{P}/\sim_v$ is a field.

(viii) Observe that, if $f(b + ai) = f(c + di)$ (with $a,\ b,\ c,\ d \in \mathbb{R}$), then

$$(b - c) + (a - d)u = (b + au) - (c + du) = Q(u)(u^2 - 1)$$

for some polynomial Q so, by (ii), $b - c = a - d = 0$ and $ai + b = ci + d$. Thus f is injective. Part (i) shows that f is surjective.

Write $z_j = ia_j + b_j$, $P_j(t) = a_ju + b_j$. Since

$$P_1(u) + P_2(u) = (a_1 + a_2)u + (b_1 + b_2),$$

we have

$$f(z_1 + z_2) = [P_1 + P_2] = [P_1] + [P_2] = f(z_1) + f(z_2).$$

Since

$$P_1(u) \times P_2(u) = a_1a_2u^2 + (a_1b_2 + a_2b_1)u + b_1b_2 = S(u) \times (u^2 + 1) + R(u)$$

with $S(u) = a_1a_2$, $R(u) = (a_1b_2 + a_2b_1)u + (b_1b_2 - a_1a_2)$ we have

$$f(z_1 \times z_2) = [R] = [P_1 \times P_2] = [P_1] \times [P_2] = f(z_1) \times f(z_2).$$

Thus $f : \mathbb{C} \to \mathbb{R}/\sim_1$ is a field isomorphism.

Exercise 11.1.1

(i) *Informally* (since we have not really specified the rules we are using),

$$
\begin{aligned}
\mathbf{x} \otimes \mathbf{y} &= (x_0 + x_1 i + x_2 j + x_3 k) \times (y_0 + y_1 i + y_2 j + y_3 k)\\
&= (x_0 y_0 + x_1 y_1 i^2 + x_2 y_2 j^2 + x_3 y_3 k^2) + (x_0 y_1 i + x_1 y_0 i + x_2 y_3 jk + x_3 y_2 kj)\\
&\qquad + (x_0 y_2 j + x_2 y_0 j + x_3 y_1 ki + x_1 y_3 ik) + (x_0 y_3 k + x_3 y_0 k + x_1 y_2 ij + x_2 y_1 ji)\\
&= (x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3) + (x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2) i\\
&\qquad + (x_0 y_2 + x_2 y_0 + x_3 y_1 - x_1 y_3) j + (x_0 y_3 + x_3 y_0 + x_1 y_2 - x_2 y_1) k.
\end{aligned}
$$

(ii) Again *informally*. Suppose that

$$i^2 = j^2 = k^2 = ijk = -1.$$

We observe that

$$1 = -i^2 = i(-1)i = i(ijk)i = i^2(jki) = -jki$$

so $jki = -1$ and similarly $kij = -1$.

Now $ij = -ij(k^2) = -(ijk)k = k$ and similarly, using the results of the first paragraph, $jk = i$ and $ki = j$.

We now observe that $ji = (ki)i = ki^2 = -k$ and similarly $kj = -i$, $ik = -j$.

Conversely if

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j,$$

then $ijk = (ij)k = k^2 = -1$.

Exercise 11.1.2

We write $\mathbf{x} = (x_0, x_1, x_2, x_3)$ and so on. Let $g : \mathbb{H}_2 \to \mathbb{H}_1$ be defined by

$$g(x_0 + ix_1, x_2 + ix_3) = (x_0, x_1, x_2, x_3)$$

We have $g(f(z_1, z_2)) = (z_1, z_2)$ and $f(g(\mathbf{x})) = \mathbf{x}$ so f and g are inverses and f is bijective

We check that

$$\begin{aligned}
f(\mathbf{x} + \mathbf{y}) &= f(x_0 + y_0, x_1 + y_1, x_2 + y_2, x_3 + y_3) \\
&= \big((x_0 + y_0) + i(x_1 + y_1), (x_2 + y_2) + i(x_3 + y_3)\big) \\
&= \big((x_0 + ix_1) + (y_0 + iy_1), (x_2 + ix_3) + (y_2 + iy_3)\big) \\
&= (x_0 + ix_1, x_2 + ix_3) + (y_0 + iy_1, y_2 + iy_3) \\
&= f(\mathbf{x}) + f(\mathbf{y})
\end{aligned}$$

whilst

$$\begin{aligned}
f(\mathbf{x}) \otimes f(\mathbf{y}) &= (x_0 + ix_1, x_2 + ix_3) \otimes (y_0 + iy_1, y_2 + iy_3) \\
&= \big((x_0 + ix_1) \times (y_0 + iy_1) - (x_2 + ix_3) \times (y_2 - iy_3), \\
&\qquad (x_0 + ix_1) \times (y_2 + iy_3) + (x_2 + ix_3) \times (y_0 - iy_1)\big) \\
&= \big((x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3) + i(x_1y_0 + x_0y_1 + x_2y_3 - x_3y_2), \\
&\qquad (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3) + i(x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)\big) \\
&= f(\mathbf{x} \otimes \mathbf{y})
\end{aligned}$$

and

$$\begin{aligned}
f(\mathbf{x}^*) &= f(x_0, -x_1, -x_2, -x_3) = (x_0 - x_1 i, -x_2 - x_3 i) \\
&= ((x_0 + ix_1)^*, -(x_2 + ix_3)) = f(\mathbf{x})^*
\end{aligned}$$

Exercise 11.1.4

Let $(\mathbb{A}, +, \times)$ be a skew field with additive zero 0, additive inverse of a given by $-a$, multiplicative unit 1 and multiplicative inverse of a (with $a \neq 0$) given by a^{-1}.

(i) If $\tilde{0} + a = a$ for all $a \in \mathbb{A}$, then $\tilde{0} = 0$.

Proof $\tilde{0} = 0 + \tilde{0} = \tilde{0} + 0 = 0$.

(ii) If $a + a^\bullet = 0$, then $a^\bullet = -a$.

Proof We have

$$\begin{aligned} -a &= -a + 0 = -a + (a + a^\bullet) = (-a + a) + a^\bullet \\ &= (a + (-a)) + a^\bullet = 0 + a^\bullet = a^\bullet. \end{aligned}$$

(iii) If $\tilde{1} \times a = a$ for all $a \in \mathbb{A}$, then $\tilde{1} = 1$.

Proof $\tilde{1} = \tilde{1} \times 1 = 1$.

(iii)′ If $a \times \tilde{1} = a$ for all $a \in \mathbb{A}$, then $\tilde{1} = 1$.

Proof $\tilde{1} = 1 \times \tilde{1} = 1$.

(iv) If $a \neq 0$ and $a \times a^\blacktriangle = 1$, then $a^\blacktriangle = a^{-1}$.

Proof $a^{-1} = a^{-1} \times 1 = a^{-1} \times (a \times a^\blacktriangle) = (a^{-1} \times a) \times a^\blacktriangle = 1 \times a^\blacktriangle = a^\blacktriangle$.

(iv)′ If $a \neq 0$ and $a^\blacktriangle \times a = 1$, then $a^\blacktriangle = a^{-1}$.

Proof $a^{-1} = 1 \times a^{-1} = (a^\blacktriangle \times a) \times a^{-1} = a^\blacktriangle \times (a \times a^{-1}) = a^\blacktriangle \times 1 = a^\blacktriangle$.

Exercise 11.1.6

We consider the quaternions in the form $\mathbb{H}_2$ of Exercise 11.1.2 We write $\mathbf{a} = (a_1, a_2)$ with $a_j \in \mathbb{C}$ and so on.

(i) (Commutative law of addition.) We have

$$\begin{aligned} \mathbf{a} + \mathbf{b} &= (a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \\ &= (b_1 + a_1, b_2 + a_2) = (b_1, b_2) + (a_1, a_2) = \mathbf{a} + \mathbf{b}. \end{aligned}$$

(ii) (Associative law of addition.) We have

$$\begin{aligned} \mathbf{a} + (\mathbf{b} + \mathbf{c}) &= (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) \\ &= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (\mathbf{a} + \mathbf{b}) + \mathbf{c}. \end{aligned}$$

(iii) (Additive zero.) Set $\mathbf{0} = (0, 0)$. Then

$$\mathbf{0} + \mathbf{a} = (0 + a_1, 0 + a_2) = (a_1, a_2) = \mathbf{a}.$$

(iv) (Additive inverse.) If we set $-\mathbf{a} = (-a, -a)$, then

$$\mathbf{a} + (-\mathbf{a}) = (a, a) + (-a, -a) = (a - a, a - a) = (0, 0) = \mathbf{0}.$$

(v) (Associative law of multiplication.) We have

$$\begin{aligned}
\mathbf{a} \otimes (\mathbf{b} \otimes \mathbf{c}) &= \mathbf{a} \otimes (b_1c_1 - b_2c_2^*, b_1c_2 + b_2c_1^*) \\
&= \big(a_1(b_1c_1 - b_2c_2^*) - a_2(b_1c_2 + b_2c_1^*)^*, a_1(b_1c_2 + b_2c_1^*) + a_2(b_1c_1 - b_2c_2^*)^*\big) \\
&= \big(a_1(b_1c_1 - b_2c_2^*) - a_2(b_1^*c_2^* + b_2^*c_1), a_1(b_1c_2 + b_2c_1^*) + a_2(b_1^*c_1^* - b_2^*c_2)\big) \\
&= \big(a_1b_1c_1 - a_1b_2c_2^* - a_2b_1^*c_2^* - a_2b_2^*c_1, a_1b_1c_2 + a_1b_2c_1^* + a_2b_1^*c_1^* - a_2b_2^*c_2\big) \\
&= \big((a_1b_1 - a_2b_2^*)c_1 - (a_1b_2 - a_2b_1^*)c_2^*, (a_1b_1 - a_2b_2^*)c_2 + (a_1b_2 - a_2b_1^*)c_1^*\big) \\
&= (\mathbf{a} \otimes \mathbf{b}) \otimes \mathbf{c}
\end{aligned}$$

(vi) (Multiplicative unit) Set $\mathbf{1} = (1, 0)$. Then

$$\mathbf{1} \otimes \mathbf{a} = ((1 \times a_1) - (0 \times a_2^*), (1 \times a_2) + (0 \times a_1^*)) = (a_1, a_2) = \mathbf{a}$$

and (since $\mathbf{0}^* = \mathbf{0}$ and $\mathbf{1}^* = \mathbf{1}$)

$$\mathbf{a} \otimes \mathbf{1} = (a_1 \times 1 - a_2 \times 0, a_1 \times 0 + a_2 \times 1^*) = (a_1, a_2 \times 1) = \mathbf{a}.$$

so that $1 \otimes \mathbf{a} = \mathbf{a} \otimes 1 = \mathbf{a}$. (Multiplicative unit.)

(viii) (Distributive law.) We have

$$\begin{aligned}
\mathbf{a} \otimes (\mathbf{b} + \mathbf{c}) &= (a_1, a_2) \otimes (b_1 + c_1, b_2 + c_2) \\
&= (a_1(b_1 + c_1) - a_2(b_2 + c_2)^*, a_1(b_2 + c_2) + a_2(b_1 + c_1)^*) \\
&= (a_1b_1 + a_1c_1 - a_2b_2^* - a_2c_2^*, a_1b_2 + a_1c_2 + a_2b_1^* + a_2c_1^*) \\
&= (a_1b_1 - a_2b_2^*, a_1b_2 + a_2b_1^*) + (a_1c_1 - a_2c_2^*, a_1c_2 + a_2c_1^*) \\
&= (\mathbf{a} \otimes \mathbf{b}) + (\mathbf{a} \otimes \mathbf{c})
\end{aligned}$$

whilst

$$\begin{aligned}
(\mathbf{b} + \mathbf{c}) \otimes \mathbf{a} &= (b_1 + c_1, b_2 + c_2) \times (a_1, a_2) \\
&= ((b_1 + c_1)a_1 - (b_2 + c_2)a_2^*, (b_1 + c_1)a_2 + (b_2 + c_2)a_1^*) \\
&= ((b_1a_1 + c_1a_1 - b_2a_2^* - c_2a_2^*, b_1a_2 + c_1a_2 + b_2a_1^* + c_2a_1^*) \\
&= (b_1a_1 - b_2a_2^*, b_1a_2 + b_2a_1^*) + (c_1a_1 - c_2a_2^*, c_1a_2 + c_2a_1^*) \\
&= (\mathbf{b} \otimes \mathbf{a}) + (\mathbf{c} \otimes \mathbf{a}).
\end{aligned}$$

We also have $\mathbf{1} = (1, 0) \neq (0, 0) = \mathbf{0}$.

Exercise 11.1.8

The proofs (apart from the commutative law of multiplication) are exactly as for the quaternions suppressing the * wherever it appears. The commutative law of multiplication is immediate from the commutative laws of multiplication and addition for $\mathbb{C}$.

$$\begin{aligned}\mathbf{z} \boxtimes \mathbf{w} &= (z_1 w_1 - z_2 w_2, z_1 w_2 + z_2 w_1) = (w_1 z_1 - w_2 z_2, w_2 z_1 + w_1 z_2)\\ &= (w_1 z_1 - w_2 z_2, w_1 z_2 + w_2 z_1) = \mathbf{w} \boxtimes \mathbf{z}.\end{aligned}$$

However
$$(1, i) \boxtimes (i, 1) = (i - i, i - i) = (0, 0).$$
We now say that 'we have zero multipliers' or give the associated argument as follows:–

The associative law of multiplication shows that, if $(i, 1)\boxtimes\mathbf{a} = (1, 0)$, then
$$(0, 0) = (0, 0)\boxtimes\mathbf{a} = ((1, i)\boxtimes(i, 1))\boxtimes\mathbf{a} = (1, i)\boxtimes((i, 1)\boxtimes\mathbf{a}) = (1, i)\boxtimes(1, 0) = (1, i)$$
which is false. Thus (vii) fails.

EXERCISE 11.1.7

All these calculations can be done in many different ways, some faster than the ones given here.

(i) We have

$$(\mathbf{i} \otimes \mathbf{j})^\star = (0, 0, 0, 1)^\star = (0, 0, 0, -1)$$

and

$$\mathbf{i}^\star \otimes \mathbf{j}^\star = (0, -1, 0, 0) \otimes (0, 0, -1, 0) = (0, 0, 0, 1)$$

so

$$(\mathbf{i} \otimes \mathbf{j})^\star \neq \mathbf{i}^\star \otimes \mathbf{j}^\star.$$

(ii) We have

$$\begin{aligned}
(\mathbf{x} \otimes \mathbf{y})^\star &= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3, x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2,\\
&\qquad x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3, x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)^*\\
&= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3, -x_0y_1 - x_1y_0 - x_2y_3 + x_3y_2,\\
&\qquad - x_0y_2 - x_2y_0 - x_3y_1 + x_1y_3, -x_0y_3 - x_3y_0 - x_1y_2 + x_2y_1)\\
&= (y_0, -y_1, -y_2, -y_3) \otimes (x_0, -x_1, -x_2, -x_3)\\
&= \mathbf{y}^\star \otimes \mathbf{x}^\star.
\end{aligned}$$

(iii) We have

$$\begin{aligned}
\mathbf{y} \otimes \mathbf{y}^* &= (y_0, y_1, y_2, y_3) \otimes (y_0, -y_1, -y_2, -y_3)\\
&= (y_0y_0 + y_1y_1 + y_2y_2 + y_3y_3, -y_0y_1 + y_1y_0 - y_2y_3 + y_3y_2,\\
&\qquad - y_0y_2 + y_2y_0 - y_3y_1 + y_1y_3, -y_0y_3 + y_3y_0 - y_1y_2 + y_2y_1)\\
&= (||\mathbf{y}||^2, 0, 0, 0).
\end{aligned}$$

Similarly

$$\mathbf{y}^\star \otimes \mathbf{y} = (y_0, -y_1, -y_2, -y_3) \otimes (y_0, y_1, y_2, y_3) = (||\mathbf{y}||^2, 0, 0, 0).$$

(iv) If

$$\mathbf{y} = \left(\frac{x_0}{||\mathbf{x}||}, \frac{x_1}{||\mathbf{x}||}, \frac{x_2}{||\mathbf{x}||}, \frac{x_3}{||\mathbf{x}||}\right),$$

then, from (iii), $\mathbf{y} \otimes \mathbf{y}^* = \mathbf{y}^* \otimes \mathbf{y} = (1, 0, 0, 0)$.

(v) Direct calculation or use the uniqueness of inverses and the standard observation that

$$\begin{aligned}
(\mathbf{x} \otimes \mathbf{y}) \otimes (\mathbf{y}^{-1} \otimes \mathbf{x}^{-1}) = \mathbf{x} \otimes (\mathbf{y} \otimes \mathbf{y}^{-1}) \otimes \mathbf{x}^{-1} &= \mathbf{x} \otimes (1, 0, 0, 0) \otimes \mathbf{x}^{-1}\\
&= \mathbf{x} \otimes \mathbf{x}^{-1} = (1, 0, 0, 0).
\end{aligned}$$

(vi) We have

$$
\begin{aligned}
(\mathbf{i} \otimes \mathbf{j})^{-1} &= (0, 0, 0, -1) \neq (0, 0, 0, 1) \\
&= (0, -1, 0, 0) \times (0, 0, -1, 0) = \mathbf{i}^{-1} \otimes \mathbf{j}^{-1}
\end{aligned}
$$

(vii) We have

$$
\begin{aligned}
(\mathbf{x} + \mathbf{y})^{\star} &= (x_0 + y_0, x_1 + y_1, x_2 + y_2, x_3 + y_3)^{\star} \\
&= (x_0 + y_0, -(x_1 + y_1), -(x_2 + y_2), -(x_3 + y_3)) \\
&= (x_0, -x_1, -x_2, -x_3) + (y_0, -y_1, -y_2, -y_3) = \mathbf{x}^{\star} + \mathbf{y}^{\star}
\end{aligned}
$$

and

$$
(\mathbf{x}^{\star})^{\star} = (x_0, -x_1, -x_2, -x_3)^{\star} = (x_0, x_1, x_2, x_3) = \mathbf{x}.
$$

Exercise 11.1.9

(i) We have

$$\begin{aligned}(||\mathbf{x}\otimes\mathbf{y}||^2,0,0,0) &= (||\mathbf{x}\otimes\mathbf{y}||,0,0,0)\otimes(||\mathbf{x}\otimes\mathbf{y}||,0,0,0)^\star\\ &= (\mathbf{x}\otimes\mathbf{y})\otimes(\mathbf{x}\otimes\mathbf{y})^\star\\ &= (\mathbf{x}\otimes\mathbf{y})\otimes(\mathbf{y}^\star\otimes\mathbf{x}^\star)\\ &= \mathbf{x}\otimes(\mathbf{y}\otimes\mathbf{y}^\star)\otimes\mathbf{x}^\star\\ &= \mathbf{x}\otimes(||\mathbf{y}||^2,0,0,0)\otimes\mathbf{x}^\star\\ &= (\mathbf{x}\otimes\mathbf{x}^\star)\otimes(||\mathbf{y}||^2,0,0,0)\\ &= (||\mathbf{x}||^2,0,0,0)\otimes(||\mathbf{y}||^2,0,0,0) = (||\mathbf{x}||^2||\mathbf{y}||^2,0,0,0)\end{aligned}$$

so $||\mathbf{x}\otimes\mathbf{y}||^2 = ||\mathbf{x}||^2||\mathbf{y}||^2$ and $||\mathbf{x}\otimes\mathbf{y}|| = ||\mathbf{x}||||\mathbf{y}||$.

(ii) Consider the quaternions

$$\mathbf{m} = (m_0, m_1, m_2, m_3),\ \ \mathbf{n} = (n_0, n_1, n_2, n_3).$$

The rules for quaternionic multiplication show that $\mathbf{q} = \mathbf{n}\otimes\mathbf{m}$ has integer entries $\mathbf{q} = (q_0, q_1, q_2, q_3)$. Applying part (i) with $\mathbf{x} = \mathbf{n}$ and $\mathbf{m} = \mathbf{y}$ gives the result.

Exercise 11.1.10

(i) We have

$$\begin{aligned}\mathbf{x}^2 &= (x_0, x_1, x_2, x_3) \otimes (x_0, x_1, x_2, x_3)\\ &= (x_0^2 - x_1^2 - x_2^2 - x_3^2, 2x_0x_1, 2x_0x_2, 2x_0x_3).\end{aligned}$$

(ii) Thus $\mathbf{x}^2 = (1, 0, 0, 0)$ yields the 4 equations

$$\begin{aligned}x_0^2 - x_1^2 - x_2^2 - x_3^2 &= 1,\\ 2x_0x_1 &= 0,\\ 2x_0x_2 &= 0,\\ 2x_0x_3 &= 0.\end{aligned}$$

Since $-x_1^2 - x_2^2 - x_3^2 \leq 0$, we must have $x_0 \neq 0$, so $x_1 = x_2 = x_3 = 0$ and $x_0^2 = 1$, whence $x_0 = \pm 1$. Thus $(1, 0, 0, 0)$ and $(-1, 0, 0, 0)$ are the only possible solutions. We check that these are solutions.

(iii) $\mathbf{x}^2 = (-1, 0, 0, 0)$ yields the 4 equations

$$\begin{aligned}x_0^2 - x_1^2 - x_2^2 - x_3^2 &= -1,\\ 2x_0x_1 &= 0,\\ 2x_0x_2 &= 0,\\ 2x_0x_3 &= 0.\end{aligned}$$

Since $x_0^2 \geq 0$, at least one of x_1, x_2, x_3 must be non-zero, so $x_0 = 0$. We see that

$$\mathbf{x}^2 = (-1, 0, 0, 0)$$

if and only if $\mathbf{x} = (0, x_1, x_2, x_3)$ with $x_1^2 + x_2^2 + x_3^2 = 1$. This gives an infinity of solutions.

Exercise 11.1.11

Thus if a, b, c, d are real,

$$\begin{aligned}f((a + ib) + (c + id)) = f((a + c) + (b + d)i) &= (a + c) + (b + d)\mathbf{u}\\ &= (a + b\mathbf{u}) + (c + d\mathbf{u}) = f(a + ib) + f(c + id))\end{aligned}$$

and

$$\begin{aligned}f((a + ib) \times (c + id)) = f((ab - cd) + (bc + ad)i) &= (ab - cd) + (bc + ad)\mathbf{u}\\ &= ab + (bc + ad)\mathbf{u} + ac\mathbf{u}^2\\ &= (a + b\mathbf{u}) \otimes (c + d\mathbf{u}) = f(a + ib) \otimes f(c + id))\end{aligned}$$

Now recall from the previous question that (using the representation of $\mathbb{H}$ as ordered quadruples) $\mathbf{u} = (0, u_1, u_2, u_3)$ with $u_1^2 + u_2^2 + u_3^2 = 1$, so, in particular, $\mathbf{u}^* = -\mathbf{u}$.

Thus, if a, b are real,

$$f((a + bi)^*) = f(a - bi) = a - b\mathbf{u} = f^(a + bi)^*.$$

Finally, using the results we have proved earlier in the question, if z, $w \in \mathbb{C}$

$$\begin{aligned} f(z) = f(w) &\Rightarrow f(z - w) = 0 \\ &\Rightarrow f(|z - w|^2) = f((z - w)(z - w)^*) = f(z - w) \otimes f((z - w)^*)) = 0 \\ &\Rightarrow |z - w|^2 = f(|z - w|^2) = 0 \Rightarrow z = w. \end{aligned}$$

(But, of course, just easy to prove directly,)

Exercise 11.2.1

Lots of ways of setting this out. (But all trivial verifications.)

$$
\begin{aligned}
(x_0, \underline{x}) \otimes (y_0, \underline{y}) &= (x_0, x_1, x_2, x_3) \otimes (y_0, y_1, y_2, y_3) \\
&= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3, x_0y_1 + x_3y_0 + x_2y_3 - x_3y_2, \\
&\qquad x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3, x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1) \\
&= (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3, 0) + (0, x_2y_3 - x_3y_2, x_3y_1 - x_1y_3) \\
&\qquad + (0, x_0y_1, x_0y_2, x_0y_3) + (0, x_3y_0, x_2y_0, x_3y_0) \\
&= (x_0y_0 - \underline{x} \cdot \underline{y}, 0, 0, 0) + (0, \underline{x} \wedge \underline{y}) + (0, x_0\underline{y}) + (0, y_0\underline{x}) \\
&= (x_0y_0 - \underline{x} \cdot \underline{y}, x_0\underline{y} + y_0\underline{x} + \underline{x} \wedge \underline{y}).
\end{aligned}
$$

Exercise A.3

Take $n = 4$, $x_1 = y_4 = a$, $x_2 = y_3 = b$, $x_3 = y_2 = c$, $x_4 = y_1 = d$.

Exercise A.5

Definition If we have a sequence $x_j \in \mathbb{F}$, then we define $\sum_{j=1}^{n} x_j$ inductively by the rule $\sum_{j=1}^{1} x_j = x_1$ and

$$\sum_{j=1}^{n+1} x_j = \left(\sum_{j=1}^{n} x_j\right) + x_{n+1}.$$

Theorem If $y_1, y_2, \dots y_n$ form a rearrangement of $x_1, x_2, \dots x_n$, then

$$\sum_{j=1}^{n} x_j = \sum_{j=1}^{n} y_j.$$

Lemma If $a_j \in \mathbb{F}$, we have

$$\left(\sum_{j=1}^{m} a_j\right) + \left(\sum_{k=1}^{n} a_{m+k}\right) = \sum_{j=1}^{m+n} a_j.$$

Exercise A.6

(i) Let $\alpha(n)$ be the statement that, if $\zeta_j \in \{0,1\}$, then

$$\sum_{j=0}^{n} \zeta_j 2^j \leq 2^{n+1} - 1.$$

$\alpha(0)$ is the statement that if $\zeta_0 \in \{0,1\}$, then $\zeta_0 \leq 1 = 2 - 1$ which is certainly true.

If $\alpha(n)$ is true and $\zeta_j \in \{0,1\}$, then

$$\begin{aligned}\sum_{j=0}^{n+1} \zeta_j 2^j &= \zeta_{n+1} 2^{n+1} + \left(\sum_{j=0}^{n} \zeta_j 2^j\right)\\ &\leq \zeta_{n+1} 2^{n+1} + (2^{n+1} - 1) = (2^{n+1} - 1) + \zeta_{n+1} 2^{n+1}\\ &\leq (2^{n+1} - 1) + 2^{n+1} = (2^{n+1} + 2^{n+1}) - 1 = 2^{n+2} - 1.\end{aligned}$$

Thus $\alpha(n+1)$ is true.

The required result follows by induction.

(ii) If $n > m \geq 0$, $\zeta_j \in \{0,1\}$ for $0 \leq j \leq n$, $\eta_k \in \{0,1\}$ for $0 \leq k \leq m$, $\zeta_n = 1$, we have

$$\begin{aligned}\sum_{j=0}^{n} \zeta_j 2^j &= 2^n + \left(\sum_{j=0}^{n-1} \zeta_j 2^j\right)\\ &\geq 2^n > 2^{m+1} - 1 \geq \sum_{k=0}^{m} \eta_k 2^k\end{aligned}$$

Similarly, if $m = n$ but $\eta_n = 0$,

$$\sum_{j=0}^{n} \zeta_j 2^j \geq 2^n > 2^n - 1 \geq \sum_{k=0}^{m} \eta_k 2^k$$

Thus, by trichotomy, the conditions $\zeta_n = 1$ and

$$\sum_{j=0}^{n} \zeta_j 2^j = \sum_{k=0}^{m} \eta_k 2^k$$

imply $m = n$ and $\eta_n = 1$.

(iii) Let $\alpha(n)$ be the statement that, if $\zeta_j,\ \eta_j \in \{0,1\}$ for $0 \leq j \leq n$, and

$$\sum_{j=0}^{n} \zeta_j 2^j = \sum_{j=0}^{n} \eta_j 2^j,$$

then $\zeta_j = \eta_j$ for $0 \leq j \leq n$.

$\alpha(0)$ is immediate. Suppose $\alpha(n)$ is true. If $\zeta_j,\ \eta_j \in \{0,1\}$ for $0 \le j \le n$, and

$$\sum_{j=0}^{n+1} \zeta_j 2^j = \sum_{j=0}^{n+1} \eta_j 2^j,$$

then part (iii) tells us that $\zeta_{n+1} = \eta_{n+1}$. It follows that

$$\left(\sum_{j=0}^{n} \zeta_j 2^j\right) + \eta_{n+1}2^{n+1} = \sum_{j=0}^{n+1} \zeta_j 2^j = \sum_{j=0}^{n+1} \eta_j 2^j = \left(\sum_{j=0}^{n} \eta_j 2^j\right) + \eta_{n+1}2^{n+1}$$

and so, by additive cancellation,

$$\sum_{j=0}^{n} \zeta_j 2^j = \sum_{j=0}^{n} \eta_j 2^j.$$

The inductive hypothesis now tells us that $\zeta_j = \eta_j$ for $0 \le j \le n$, so, using our previous result $\zeta_j = \eta_j$ for $0 \le j \le n+1$. We have shown that $\alpha(n+1)$ is true.

The required result follows by induction.

(iv) Let $\alpha(n)$ be the statement that if $n \ge m \ge 0$ and $2^{m+1} - 1 \ge r \ge 2^m$, then we can find $\zeta_j \in \{0,1\}$ with $\zeta_m = 1$ such that

$$r = \sum_{j=0}^{m} \zeta_j 2^j.$$

Since $1 = 1 \times 2^0$, $\alpha(0)$ is true. Suppose α_n is true and $2^{n+2} - 1 \ge r \ge 2^{n+1}$. Then we set $\zeta_{n+1} = 1$ and consider $s = r - 2^n$. If $s = 0$, we set $\zeta_j = 0$ for $n \ge j \ge 0$ and observe that $r = \sum_{j=0}^{n+1} \zeta_j 2^k$. If $s > 0$, we can find an m with $n \ge m \ge 0$ such that $2^{m+1} - 1 \ge r \ge 2^m$ and so we can find $\zeta_j \in \{0,1\}$ with $\zeta_m = 1$ $[0 \le j \le m]$ such that

$$s = \sum_{j=0}^{m} \zeta_j 2^j.$$

If $n > m$, we set $\zeta_j = 0$ for $n \ge j > m$. Once again

$$r = \sum_{j=0}^{n+1} \zeta_j 2^k$$

We have shown that $\alpha(n+1)$ is true.

The required result follows by induction.

(v) Every integer $r \ge 1$ satisfies $2^{n+1} \ge r > 2^n$ for some n and so satisfies an equation of the form

$$r = \sum_{j=0}^{n} \zeta_j 2^k$$

with $\zeta_j \in \{0, 1\}$ for $0 \leq j \leq n-1$ and $\zeta_n = 1$. Part (iii) tells us that the representation is unique.

(vi) Let $\alpha(n)$ be the statement that if a is a strictly positive integer and

$$r = \sum_{j=0}^{n} \zeta_j 2^k$$

with $\zeta_j \in \{0, 1\}$ for $0 \leq j \leq n$, then

$$a^r = \prod_{\zeta_j = 1} a^{2^j}.$$

$\alpha(0)$ is true by inspection. Suppose $\alpha(n)$ is true and

$$r = \sum_{j=0}^{n+1} \zeta_j 2^j.$$

Then

$$\begin{aligned}
a^r &= a^{\sum_{j=0}^{n+1} \zeta_j 2^j} = a^{\left(\sum_{j=0}^{n} \zeta_j 2^j\right) + \zeta_{n+1} 2^{n+1}} \\
&= a^{\left(\sum_{j=0}^{n} \zeta_j 2^j\right)} \times a^{\zeta_{n+1} 2^{n+1}} = \left(\prod_{\zeta_j = 1,\, j \leq n} a^{2^j} \right) \times a^{\zeta_{n+1} 2^{n+1}} \\
&= \prod_{\zeta_j = 1} a^{2^j}.
\end{aligned}$$

Thus $\alpha(n + 1)$ is true.

The required result follows by induction.

Exercise B.3

Suppose that $y < 0$. Observing that all the terms in the final inequality are real, we now have

$$g(z_\eta) \geq g(w) - my\eta - 2|a|C\eta^2.$$

Choosing $\eta > 0$ with $\eta > (2|a|C)/(my)$ gives $g(z_\eta) > g(w)$ contrary to our definition of w.

Exercise C.2

Choose coordinate axes so that $\underline{q} = (1, 0, 0)$, $\underline{n} = (0, 1, 0)$.

(i) We have

$$\underline{q} \cdot \underline{q} = 1^2 + 0^2 + 0^2 = 1,$$
$$\underline{q} \wedge \underline{n} = (0, 0, 1) = -(0, 0, -1) = -\underline{n} \wedge \underline{q},$$
$$\underline{q} \wedge \underline{q} = (0 \times 0 - 0 \times 0, 0 \times 1 - 0 \times 0, 0 \times 0 - 1 \times 0) = (0, 0, 0) = \underline{0}.$$

(ii) $\underline{q} \wedge \underline{n} = (0, 0, 1)$, so $\underline{q}$, $\underline{n}$ and $\underline{q} \wedge \underline{n}$ are mutually orthogonal.

For example

$$(\underline{q} \wedge \underline{n}) \cdot \underline{q} = (0, 0, 1) \cdot (1, 0, 0) = 0 \times 1 + 0 \times 0 + 1 \times 0 = 0.$$

(iii) We have

$$(\underline{q} \wedge \underline{n}) \wedge \underline{q} = (0, 0, 1) \wedge (1, 0, 0) = (0, 1, 0) = \underline{n}.$$

(iv) Set $\alpha = \beta = \theta/2$ in the formulae

$$\sin(\alpha + \beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha,$$
$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta.$$

Exercise C.3

We write

$$\mathbf{p} = (p_0, \underline{p}) = (p_0, p_1, p_2, p_3).$$

Let $||\mathbf{p}||$ be the quaternion norm of $\mathbf{p}$, that is to say,

$$||\mathbf{p}|| = \sqrt{p_0^2 + p_1^2 + p_2^2 + p_3^2}.$$

If we write $\mathbf{q} = ||\mathbf{p}||^{-1}\mathbf{p}$, then $\mathbf{q}$ is a unit quaternion, $\mathbf{p} = ||\mathbf{p}||\mathbf{q}$ and $\mathbf{p}^{-1} = ||\mathbf{p}||^{-1}\mathbf{q}^{-1}$. Thus

$$\begin{aligned} \mathbf{p} \otimes (0, \underline{x}) \otimes \mathbf{p}^{-1} &= (||\mathbf{p}||\mathbf{q}) \otimes (0, \underline{x}) \otimes (||\mathbf{p}||^{-1}\mathbf{q}^{-1}) \\ &= \mathbf{q} \otimes (0, \underline{x}) \otimes \mathbf{q}^{-1} \end{aligned}$$

By Theorem C.1, we have a rotation about $\underline{p}$ through θ, where

$$\cos\theta/2 = p_0/||\mathbf{p}||,\ 0 \le \theta \le 2\pi.$$

Exercise C.4

Write

$$\mathbf{q}_j \otimes (0, \underline{x}) \otimes \mathbf{q}_j^{-1} = (0, R_j(\underline{x})).$$

Then

$$\begin{aligned} (\mathbf{q}_2 \otimes \mathbf{q}_1) \otimes (0, \underline{x}) \otimes (\mathbf{q}_2 \otimes \mathbf{q}_1)^{-1} &= (\mathbf{q}_2 \otimes \mathbf{q}_1) \otimes (0, \underline{x}) \otimes (\mathbf{q}_1^{-1} \otimes \mathbf{q}_2^{-1}) \\ &= \mathbf{q}_2 \otimes (\mathbf{q}_1 \otimes (0, \underline{x} \otimes \mathbf{q}_1^{-1})) \otimes \mathbf{q}_2^{-1}) \\ &= \mathbf{q}_2 \otimes (0, R_1(\underline{x})) \otimes \mathbf{q}_2^{-1} \\ &= (0, R_2(R_1(\underline{x}))). \end{aligned}$$

Thus $\mathbf{q}_2 \otimes \mathbf{q}_1$ corresponds to the rotation R_1 followed by the rotation R_2.

Exercise C.5

(i) If A and B are 3×3 matrices and we obtain their product C from the expressions
$$c_{ij} = (a_{i1} \times b_{1j}) + (a_{i2} \times b_{2j}) + (a_{i3} \times b_{3j}),$$
then each entry c_{ij} requires 3 multiplications and 2 additions. There are $9 = 3 \times 3$ entries, so we need $27 = 3 \times 9$ multiplications and $18 = 2 \times 9$ additions.

If we do the quaternion multiplication $\mathbf{r} = \mathbf{p} \times \mathbf{q}$ then $\mathbf{r}$ has 4 entries each of which requires 4 multiplications and 3 additions so 16 multiplications and 12 additions in all.

(ii) The author does not know how 'renormalisation' is carried out in practice for matrices, but one could use Gramm-Schmidt on the columns.

Exercise C.6

Observe that if we write

$$f_{\mathbf{p}}(\mathbf{u}) = \mathbf{p} \otimes \mathbf{u} \otimes \mathbf{p}^{-1}$$

then

$$f_{\mathbf{p}^{-1}}(f_{\mathbf{p}}(\mathbf{u})) = \mathbf{u} = f_{\mathbf{p}}(f_{\mathbf{p}^{-1}}(\mathbf{u}))$$

so $f_{\mathbf{p}} : \mathbb{H} \to \mathbb{H}$ is bijective with inverse $f_{\mathbf{p}}^{-1} = f_{\mathbf{p}^{-1}}$.

From now on we keep $\mathbf{p}$ fixed and write $f = f_{\mathbf{p}}$. We have

$$\begin{aligned} f(\mathbf{u}) + f(\mathbf{v}) &= \mathbf{p} \otimes \mathbf{u} \otimes \mathbf{p}^{-1} + \mathbf{p} \otimes \mathbf{v} \otimes \mathbf{p}^{-1} \\ &= \mathbf{p} \otimes (\mathbf{u} \otimes \mathbf{p}^{-1} + \mathbf{v} \otimes \mathbf{p}^{-1}) \\ &= \mathbf{p} \otimes (\mathbf{u} + \mathbf{v}) \otimes \mathbf{p}^{-1} = f(\mathbf{u} + \mathbf{v}) \end{aligned}$$

and

$$\begin{aligned} f(\mathbf{u}) \otimes f(\mathbf{v}) &= (\mathbf{p} \otimes \mathbf{u} \otimes \mathbf{p}^{-1}) \otimes (\mathbf{p} \otimes \mathbf{v} \otimes \mathbf{p}^{-1}) \\ &= (\mathbf{p} \otimes \mathbf{u}) \otimes (\mathbf{p}^{-1} \otimes \mathbf{p}) \otimes (\mathbf{v} \otimes \mathbf{p}^{-1}) \\ &= (\mathbf{p} \otimes \mathbf{u}) \otimes (\mathbf{v} \otimes \mathbf{p}^{-1}) \\ &= \mathbf{p} \otimes (\mathbf{u} \otimes \mathbf{v}) \otimes \mathbf{p}^{-1} = f(\mathbf{u} \otimes \mathbf{v}). \end{aligned}$$

Thus f is a skew-field isomorphism.

Since $\mathbf{p}^{-1} = \mathbf{p}^*||\mathbf{p}||^{-2}$, we have

$$(\mathbf{p}^{-1})^* = \mathbf{p}||\mathbf{p}||^{-2}.$$

Thus

$$\begin{aligned} f(\mathbf{u})^* &= (\mathbf{p} \otimes \mathbf{u} \otimes \mathbf{p}^{-1})^* \\ &= (\mathbf{p}^{-1})^* \otimes \mathbf{u}^* \otimes \mathbf{p}^* \\ &= ||\mathbf{p}||^{-2}(\mathbf{p} \otimes \mathbf{u}^*) \otimes \mathbf{p}^* \\ &= (\mathbf{p} \otimes \mathbf{u}^*) \otimes \mathbf{p}^{-1} = f(\mathbf{u}^*). \end{aligned}$$

Finally, $\hat{\imath}^2 = f(i)^2 = f(i^2) = f(-1) = -1$ and, similarly, $\hat{\jmath}^2 = \hat{k}^2 = -1$ whilst

$$\hat{\imath} \otimes \hat{\jmath} \otimes \hat{k} = f(i) \otimes f(j) \otimes f(k) = f(ijk) = f(-1) = -1.$$

Exercise D.3

$$g(((x+iy)+(a+bi)) = g((x+a)+(y+b)i) = (x+a)\underset{\sim}{e} + (y+b)\underset{\sim}{i}$$
$$= (x\underset{\sim}{e} + y\underset{\sim}{i}) + (a\underset{\sim}{e} + b\underset{\sim}{i}) = g(x+iy) + g(a+bi)$$

and

$$g(((x+iy)\times(a+bi)) = g((xa-yb)+(xb+ya)i) = (xa-yb)\underset{\sim}{e} + (xb+ya)\underset{\sim}{i}$$
$$= (x\underset{\sim}{e} + y\underset{\sim}{i}) \otimes (a\underset{\sim}{e} + b\underset{\sim}{i}) = g(x+iy) \otimes g(a+bi)$$

for $a,\ b,\ x,\ y \in \mathbb{R}$.

Exercise D.5

Using the associative rule of multiplication, we have

$$(\lambda\underset{\sim}{v}) \otimes \underset{\sim}{w} = \big((\lambda\underset{\sim}{e}) \otimes \underset{\sim}{v}\big) \otimes \underset{\sim}{w} = (\lambda\underset{\sim}{e}) \otimes (\underset{\sim}{v} \otimes \underset{\sim}{w}) = \lambda(\underset{\sim}{v} \otimes \underset{\sim}{w}).$$

Using the associative law of multiplication again,

$$\underset{\sim}{v} \otimes (\lambda\underset{\sim}{w}) = \underset{\sim}{v} \otimes \big((\lambda\underset{\sim}{e}) \otimes \underset{\sim}{w}\big) = \big(\underset{\sim}{v} \otimes (\lambda\underset{\sim}{e})\big) \otimes \underset{\sim}{w} = (\lambda\underset{\sim}{v}) \otimes \underset{\sim}{w}$$

so, using the first and second result,

$$\underset{\sim}{v} \otimes (\lambda\underset{\sim}{w}) = \lambda(\underset{\sim}{v} \otimes \underset{\sim}{w}).$$

Exercise D.7

(i) Suppose $\underset{\sim}{f},\ \underset{\sim}{f}' \in F$ and $y,\ y' \in \mathbb{R}$. Setting $\underset{\sim}{z} = \underset{\sim}{f} + y\underset{\sim}{v}$ and $\underset{\sim}{z}' = \underset{\sim}{f}' + y'\underset{\sim}{v}$ we have

$$\begin{aligned}\underset{\sim}{z} \otimes \underset{\sim}{z}' &= \underset{\sim}{f} \otimes \underset{\sim}{f}' + y\underset{\sim}{v} \otimes \underset{\sim}{f}' + y'\underset{\sim}{f} \otimes \underset{\sim}{v} + yy'\underset{\sim}{v} \otimes \underset{\sim}{v}\\ &= \underset{\sim}{f}' \otimes \underset{\sim}{f} + y\underset{\sim}{f}' \otimes \underset{\sim}{v} + y'\underset{\sim}{v} \otimes \underset{\sim}{f} + y'y\underset{\sim}{v} \otimes \underset{\sim}{v}\\ &= \underset{\sim}{z}' \otimes \underset{\sim}{z}.\end{aligned}$$

(ii) If $\underset{\sim}{x},\ \underset{\sim}{y} \in F$, then

$$\begin{aligned}(\underset{\sim}{x} \otimes \underset{\sim}{y}) \otimes \underset{\sim}{f} &= \underset{\sim}{x} \otimes (\underset{\sim}{y} \otimes \underset{\sim}{f}) = \underset{\sim}{x} \otimes (\underset{\sim}{f} \otimes \underset{\sim}{y})\\ &= (\underset{\sim}{x} \otimes \underset{\sim}{f}) \otimes \underset{\sim}{y} = (\underset{\sim}{f} \otimes \underset{\sim}{x}) \otimes \underset{\sim}{y}\\ &= \underset{\sim}{f} \otimes (\underset{\sim}{x} \otimes \underset{\sim}{y})\end{aligned}$$

so $\underset{\sim}{x} \otimes \underset{\sim}{y} \in F$.

Exercise D.8

(i) $(x + y\mathbf{i}) \otimes \mathbf{j} = x\mathbf{j} + y\mathbf{i} \otimes \mathbf{j} = x\mathbf{j} + y\mathbf{k}$ so E consists of the quaternions $\lambda\mathbf{j} + \mu\mathbf{k}$ with $\lambda, \mu \in \mathbb{R}$. E^+ is a vector space with basis 1 and $\mathbf{i}$, E^- is a vector space with basis $\mathbf{j}$ and $\mathbf{k}$.-

(ii) Write $\mathbf{a} = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$. Then

$$\mathbf{a} \otimes \mathbf{i} = a_0\mathbf{i} - a_1 - a_2\mathbf{k} + a_3\mathbf{j}$$
$$\mathbf{i} \otimes \mathbf{a} = a_0\mathbf{i} - a_1 + a_2\mathbf{k} - a_3\mathbf{j}$$

Thus $\mathbf{a} \otimes \mathbf{i} = \mathbf{i} \otimes \mathbf{a}$ if and only if $a_2 = a_3 = 0$, that is to say if and only if $\mathbf{a} \in E^+$. On the other hand, $\mathbf{a} \otimes \mathbf{i} = -\mathbf{i} \otimes \mathbf{a}$ if and only if $a_0 = a_1 = 0$, that is to say, if and only if $\mathbf{a} \in E^-$.

(iii) If $\mathbf{a} \in E^+$, $\mathbf{b} \in E^-$, then $\mathbf{a} = a_0 + a_1\mathbf{i}$ and $\mathbf{b} = b_2\mathbf{j} + b_3\mathbf{k}$. If $\mathbf{a} = \mathbf{b}$, then

$$a_0 + a_1\mathbf{i} - b_2\mathbf{j} - b_3\mathbf{k} = 0,$$

so $a_0 = a_1 = b_2 = b_3 = 0$ and $\mathbf{a} = 0$. Thus $E^+ \cap E^- = \{0\}$.

Since

$$x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} = (x_0 + x_1\mathbf{i}) + (x_2\mathbf{j} + x_3\mathbf{k}),$$

and $x_0 + x_1\mathbf{i} \in E^+$, $x_2\mathbf{j} + x_3\mathbf{k} \in E^-$, $\mathbb{H}$ is the direct sum of E^+ and E^-.

(iv) Direct calculation.

$$(x_2\mathbf{j} + x_3\mathbf{k})^2 = -x_2^2 - x_3^2$$

is real and strictly negative if $x_2\mathbf{j} + x_3\mathbf{k}$ is non-zero.

Exercise D.9

(i) We have

$$\underset{\sim}{u} \otimes \underset{\sim}{a} = -c\underset{\sim}{e} + d\underset{\sim}{u} \otimes \underset{\sim}{a}$$

$$\underset{\sim}{a} \otimes \underset{\sim}{u} = -c\underset{\sim}{e} - d\underset{\sim}{u} \otimes \underset{\sim}{a}$$

so, adding,

$$c\underset{\sim}{e} = -\frac{1}{2}(\underset{\sim}{a} \otimes \underset{\sim}{u} + \underset{\sim}{u} \otimes \underset{\sim}{a}).$$

Thus

$$c\underset{\sim}{u} = c\underset{\sim}{e} \otimes \underset{\sim}{u} = \frac{1}{2}(\underset{\sim}{a} - \underset{\sim}{u} \otimes \underset{\sim}{a} \otimes \underset{\sim}{u}).$$

It follows that

$$d\underset{\sim}{v} = \underset{\sim}{a} - c\underset{\sim}{u} = \frac{1}{2}(\underset{\sim}{a} + \underset{\sim}{u} \otimes \underset{\sim}{a} \otimes \underset{\sim}{u}).$$

(ii) Take $\underset{\sim}{a} = \underset{\sim}{0}$ in (i). Or prove directly.

Exercise D.10

(i) $0 \in D^+$. If $\underset{\sim}{a}, \underset{\sim}{b} \in D^+$, λ, $\mu \in \mathbb{R}$, then

$$(\lambda\underset{\sim}{a} + \mu\underset{\sim}{b}) \otimes \underset{\sim}{i} = \lambda\underset{\sim}{a} \otimes \underset{\sim}{i} + \mu\underset{\sim}{b} \otimes \underset{\sim}{i} = \lambda\underset{\sim}{i} \otimes \underset{\sim}{a} + \mu\underset{\sim}{i} \otimes \underset{\sim}{b} = \underset{\sim}{i} \otimes (\lambda\underset{\sim}{a} + \mu\underset{\sim}{b})$$

so $\lambda\underset{\sim}{a} + \mu\underset{\sim}{b} \in D^+$ and D^+ is a subspace.

$0 \in D^-$. If $\underset{\sim}{a}, \underset{\sim}{b} \in D^-$, λ, $\mu \in \mathbb{R}$, then

$$(\lambda\underset{\sim}{a} + \mu\underset{\sim}{b}) \otimes \underset{\sim}{i} = \lambda\underset{\sim}{a} \otimes \underset{\sim}{i} + \mu\underset{\sim}{b} \otimes \underset{\sim}{i} = -\lambda\underset{\sim}{i} \otimes \underset{\sim}{a} - \mu\underset{\sim}{i} \otimes \underset{\sim}{b} = -\underset{\sim}{i} \otimes (\lambda\underset{\sim}{a} + \mu\underset{\sim}{b})$$

so $\lambda\underset{\sim}{a} + \mu\underset{\sim}{b} \in D^-$ and D^- is a subspace.

(ii) The right distributive law gives

$$T(\underset{\sim}{a} + \underset{\sim}{b}) = (\underset{\sim}{a} + \underset{\sim}{b}) \otimes \underset{\sim}{p} = (\underset{\sim}{a} \otimes \underset{\sim}{p}) + (\underset{\sim}{b} \otimes \underset{\sim}{p}) = T(\underset{\sim}{a}) + T(\underset{\sim}{b})$$

and the associative law of multiplication gives

$$T(\lambda\underset{\sim}{a}) = T(\lambda\underset{\sim}{e} \otimes \underset{\sim}{a}) = ((\lambda\underset{\sim}{e}) \otimes \underset{\sim}{a}) \otimes \underset{\sim}{p} = (\lambda\underset{\sim}{e}) \otimes (\underset{\sim}{a} \otimes \underset{\sim}{p}) = (\lambda\underset{\sim}{e}) \otimes T(\underset{\sim}{a}) = \lambda T\underset{\sim}{a}$$

for all $\lambda \in \mathbb{C}$.

(iii) If $\underset{\sim}{p} \in D^-$, then

$$\begin{aligned} \underset{\sim}{p}^{-1} \otimes \underset{\sim}{i} &= (\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}) \otimes \underset{\sim}{e} = (\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}) \otimes (\underset{\sim}{p} \otimes \underset{\sim}{p}^{-1}) \\ &= (\underset{\sim}{p}^{-1} \otimes (\underset{\sim}{i} \otimes \underset{\sim}{p})) \otimes \underset{\sim}{p}^{-1} = -(\underset{\sim}{p}^{-1} \otimes (\underset{\sim}{p} \otimes \underset{\sim}{i})) \otimes \underset{\sim}{p}^{-1} \\ &= -((\underset{\sim}{p}^{-1} \otimes \underset{\sim}{p}) \otimes \underset{\sim}{i})) \otimes \underset{\sim}{p}^{-1} = -(\underset{\sim}{e} \otimes \underset{\sim}{i}) \otimes \underset{\sim}{p}^{-1} = -\underset{\sim}{i} \otimes \underset{\sim}{p}^{-1}, \end{aligned}$$

so $\underset{\sim}{p}^{-1} \in D^-$.

Or (slightly shorter but not really different)

$$\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i} = -(\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}^{-1}) = -(\underset{\sim}{i} \otimes \underset{\sim}{p}))^{-1} = (\underset{\sim}{p} \otimes \underset{\sim}{i})^{-1} = \underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}^{-1} = -(\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}).$$

(iv) If $\underset{\sim}{b} \in D^-$, then

$$\begin{aligned} S(\underset{\sim}{b}) \otimes \underset{\sim}{i} &= (\underset{\sim}{b} \otimes \underset{\sim}{p}^{-1}) \otimes \underset{\sim}{i} = \underset{\sim}{b} \otimes (\underset{\sim}{p}^{-1} \otimes \underset{\sim}{i}) \\ &= -\underset{\sim}{b} \otimes (\underset{\sim}{i} \otimes \underset{\sim}{p}^{-1}) = -(\underset{\sim}{b} \otimes \underset{\sim}{i}) \otimes \underset{\sim}{p}^{-1} \\ &= (\underset{\sim}{i} \otimes \underset{\sim}{b}) \otimes \underset{\sim}{p}^{-1} = \underset{\sim}{i} \otimes (\underset{\sim}{b} \otimes \underset{\sim}{p}^{-1}) \\ &= \underset{\sim}{i} \otimes S(\underset{\sim}{b}), \end{aligned}$$

so $S(\underset{\sim}{b}) \in D^+$.

(v) We have

$$\underset{\sim}{k}\otimes\underset{\sim}{j}=(\underset{\sim}{i}\otimes\underset{\sim}{j})\otimes\underset{\sim}{j}=\underset{\sim}{i}\otimes\underset{\sim}{j}^2=-\underset{\sim}{i}$$

$$\underset{\sim}{k}\otimes\underset{\sim}{i}=(\underset{\sim}{i}\otimes\underset{\sim}{j})\otimes\underset{\sim}{i}=(-(\underset{\sim}{j}\otimes\underset{\sim}{i}))\otimes\underset{\sim}{i}=-\underset{\sim}{j}\otimes\underset{\sim}{i}^2=\underset{\sim}{j}$$

$$\underset{\sim}{i}\otimes\underset{\sim}{k}=\underset{\sim}{i}\otimes(\underset{\sim}{i}\otimes\underset{\sim}{j})=\underset{\sim}{i}^2\otimes\underset{\sim}{j}=-\underset{\sim}{j}.$$

(vi) (I not think this much detail is necessary.) Since U has basis $\underset{\sim}{e}$, $\underset{\sim}{j}$ when considered as a vector space over $\mathbb{C}$, any $\underset{\sim}{u}\in U$ can be written uniquely as

$$\underset{\sim}{u}=(a+b\underset{\sim}{i})\otimes\underset{\sim}{e}+(u+v\underset{\sim}{i})\otimes\underset{\sim}{j}=a\underset{\sim}{e}+b\underset{\sim}{i}+u\underset{\sim}{j}+v\underset{\sim}{k}$$

with $a, b, u, v\in\mathbb{R}$,

Thus any $\underset{\sim}{x}\in U$ can be written uniquely as

$$\underset{\sim}{x}=x_0+x_1\underset{\sim}{i}+x_2\underset{\sim}{j}+x_3\underset{\sim}{k}$$

with $x_r\in\mathbb{R}$ and the map $f:\mathbb{H}\to U$ given by

$$f(x_0+x_1i+x_2j+x_3k)=x_0\underset{\sim}{e}+x_1\underset{\sim}{i}+x_2\underset{\sim}{j}+x_3\underset{\sim}{k}$$

for $x_r\in\mathbb{R}$ is a bijection.

Automatically (and evidently)

$$\begin{aligned}
&f((x_0+x_1i+x_2j+x_3k)+(y_0+y_1i+y_2j+y_3k))\\
&\quad=f((x_0+y_0)+(x_1+y_1)i+(x_2+y_2)j+(x_3+y_3)k)\\
&\quad=(x_0+y_0)\underset{\sim}{e}+(x_1+y_1)\underset{\sim}{i}+(x_2+y_2)\underset{\sim}{j}+(x_3+y_3)\underset{\sim}{k}\\
&\quad=(x_0\underset{\sim}{e}+x_1\underset{\sim}{i}+x_2\underset{\sim}{j}+x_3\underset{\sim}{k})+(y_0\underset{\sim}{e}+y_1\underset{\sim}{i}+y_2\underset{\sim}{j}+y_3\underset{\sim}{k}))\\
&\quad=f(x_0+x_1i+x_2j+x_3k)+f(y_0+y_1i+y_2j+y_3k)
\end{aligned}$$

$$\begin{aligned}
&f((x_0+x_1i+x_2j+x_3k)\otimes(y_0+y_1i+y_2j+y_3k))\\
&\quad=f((x_0y_0-x_1y_1-x_2y_2-x_3y_3)+(x_0y_1+x_1y_0+x_2y_3-x_3y_2)iy\\
&\qquad\quad+(x_0y_2+x_2y_0+x_3y_1-x_1y_3)j+(x_0y_3+x_3y_0+x_1y_2-x_2y_1)k)\\
&\quad=(x_0y_0-x_1y_1-x_2y_2-x_3y_3)\underset{\sim}{e}+(x_0y_1+x_1y_0+x_2y_3-x_3y_2)\underset{\sim}{i}\\
&\qquad\quad+(x_0y_2+x_2y_0+x_3y_1-x_1y_3)\underset{\sim}{j}+(x_0y_3+x_3y_0+x_1y_2-x_2y_1)\underset{\sim}{k})\\
&\quad=(x_0\underset{\sim}{e}+x_1\underset{\sim}{i}+x_2\underset{\sim}{j}+x_3\underset{\sim}{k})\otimes(y_0\underset{\sim}{e}+y_1\underset{\sim}{i}+y_2\underset{\sim}{j}+y_3\underset{\sim}{k})\\
&\quad=f(x_0+x_1i+x_2j+x_3k)\otimes f(y_0+y_1i+y_2j+y_3k).
\end{aligned}$$

Thus f preserves the operations $+$ and $\otimes$ and must be a skew-field isomorphism.

Le hareng saur
Charles Cros

Il était un grand mur blanc – nu, nu, nu,
Contre le mur une échelle – haute, haute, haute,
Et, par terre, un hareng saur – sec, sec, sec.

Il vient, tenant dans ses mains – sales, sales, sales,
Un marteau lourd, un grand clou – pointu, pointu, pointu,
Un peloton de ficelle – gros, gros, gros.

Alors il monte l'échelle – haute, haute, haute,
Et plante le clou pointu – toc, toc, toc,
Tout en haut du grand mur blanc – nu, nu, nu.

Il laisse aller le marteau – qui tombe, qui tombe, qui tombe,
Attache au clou la ficelle – longue, longue, longue,
Et, au bout, le hareng saur – sec, sec, sec.

Il redescend de l'échelle – haute, haute, haute,
L'emporte avec le marteau – lourd, lourd, lourd,
Et puis, il s'en va ailleurs – loin, loin, loin.

Et, depuis, le hareng saur – sec, sec, sec,
Au bout de cette ficelle – longue, longue, longue,
Très lentement se balance – toujours, toujours, toujours.

J'ai composé cette histoire – simple, simple, simple,
Pour mettre en fureur les gens – graves, graves, graves,
Et amuser les enfants - petits, petits, petits.

The Smoked Herring

Translated by Kenneth Rexroth

Once upon a time there was a big white wall – bare, bare, bare,
Against the wall there stood a ladder – high, high, high,
And on the ground a smoked herring – dry, dry, dry,

He comes, holding in his hands – dirty, dirty, dirty,
A heavy hammer and a big nail – sharp, sharp, sharp,
A ball of string – big, big, big,

Then he climbs the ladder – high, high, high,
And drives the sharp nail – tock, tock, tock,
Way up on the big white wall – bare, bare, bare,

He drops the hammer – down, down, down,
To the nail he fastens a string – long, long, long,
And, at the end, the smoked herring – dry, dry, dry,

He comes down the ladder – high, high, high,
He picks up the hammer – heavy, heavy, heavy,
And goes off somewhere – far, far, far,

And ever afterwards the smoked herring – dry, dry, dry,
At the end of that string – long, long, long,
Very slowly sways – forever and ever and ever.

I made up this story – silly, silly, silly,
To infuriate the squares – solemn, solemn, solemn,
And to amuse the children – little, little, little.