Chapter 2

Fields

2.1 Binary Operations

2.1 Definition (Binary operation.) Let A be a set. A *binary operation* on A is a function $\circ\colon A \times A \to A$. Binary operations are usually denoted by special symbols such as

$$+, -, \cdot, /, \times, \circ, \wedge, \vee, \cup, \cap$$

rather than by letters. If $\circ\colon A \times A \to A$ is a binary operation, we write $a \circ b$ instead of $\circ(a, b)$. By the definition of function (1.57), a binary operation is a triple $(A \times A, A, \circ)$, but as is usual for functions, we refer to "the binary operation $\circ$" instead of "the binary operation $(A \times A, A, \circ)$".

2.2 Examples. The usual operations of addition $(+)$, subtraction $(-)$ and multiplication $(\cdot)$ are binary operations on $\mathbf{Z}$ and on $\mathbf{Q}$. Subtraction is not a binary operation on $\mathbf{N}$, because $3 - 5$ is not in $\mathbf{N}$. Division is not a binary operation on $\mathbf{Q}$, because division by 0 is not defined. However, division is a binary operation on $\mathbf{Q} \setminus \{0\}$.

Let $\mathcal{S}$ be the set of all sets.[1] Then union $(\cup)$ and intersection $(\cap)$ and set difference $(\setminus)$ are binary operations on $\mathcal{S}$.

[1] Some mathematicians cringe at the mention of the set of all sets, because it occurs in Russell's paradox, and in some other set-theoretic paradoxes. Any cringers can modify this example and the next one however they please.

Let $\mathcal{P}$ be the set of all propositions. Then *and* and *or* are binary operations on $\mathcal{P}$. In mathematical logic, *and* is usually represented by $\wedge$ or &, and *or* is represented by $\vee$ or $\bigvee$.

2.3 Definition (Identity element.) Let $\circ$ be a binary operation on a set A. An element $e \in A$ is an *identity element for* $\circ$ (or just an *identity for* $\circ$) if

$$\text{for all } a \in A, \quad e \circ a = a = a \circ e.$$

2.4 Examples. 0 is an identity for addition on $\mathbf{Z}$, and 1 is an identity for multiplication on $\mathbf{Z}$. There is no identity for subtraction on $\mathbf{Z}$, since for all $e \in \mathbf{Z}$ we have

$$\begin{aligned} e \text{ is an identity for } - \quad &\Longrightarrow \quad e - 1 = 1 \text{ and } 1 = 1 - e, \\ &\Longrightarrow \quad e = 2 \text{ and } e = 0, \\ &\Longrightarrow \quad 0 = 2. \end{aligned} \tag{2.5}$$

Since (2.5) is false, the first statement is also false; i.e., for all $e \in \mathbf{Z}$, e is not an identity for $-$. |||

2.6 Exercise. Let $\mathcal{S}(\mathbf{Z})$ denote the set of all subsets of $\mathbf{Z}$. Then union $\cup$ and intersection $\cap$ are binary operations on $\mathcal{S}(\mathbf{Z})$. Is there an identity element for $\cup$? If so, what is it? Is there an identity element for $\cap$? If so, what is it?

2.7 Theorem (Uniqueness of identities.) *Let $\circ$ be a binary operation on a set A. Suppose that e, f are both identity elements for $\circ$. Then $e = f$. (Hence we usually talk about* the *identity for $\circ$, rather than* an *identity for $\circ$.)*

Proof: Let e, f be identity elements for $\circ$. Then

$$e = e \circ f \qquad \text{(since } f \text{ is an identity for } \circ\text{)}$$

and

$$e \circ f = f \qquad \text{(since } e \text{ is an identity for } \circ\text{).}$$

It follows that $e = f$. |||

2.8 Remark. The conclusion of the previous proof used transitivity of equality (Cf page 12). I usually use the properties of equality without explicitly mentioning them.

2.9 Definition (Inverse.) Let $\circ$ be a binary operation on a set A, and suppose that there is an identity element e for $\circ$. (We know that this identity is unique.) Let x be an element of A. We say that an element y of A *is an inverse for x under* $\circ$ if

$$x \circ y = e = y \circ x.$$

We say that x is *invertible under* $\circ$ if x has an inverse under $\circ$.

2.10 Examples. For the operation $+$ on $\mathbf{Z}$, every element x has an inverse, namely $-x$.

For the operation $+$ on $\mathbf{N}$, the only element that has an inverse is 0; 0 is its own inverse.

For the operation $\cdot$ on $\mathbf{Z}$, the only invertible elements are 1 and -1. Both of these elements are equal to their own inverses.

If $\circ$ is any binary operation with identity e, then $e \circ e = e$, so e is always invertible, and e is equal to its own inverse.

2.11 Exercise. Let $\mathcal{S}(\mathbf{Z})$ be the set of all subsets of $\mathbf{Z}$. In exercise 2.6 you should have shown that both of the operations $\cup$ and $\cap$ on $\mathcal{S}(\mathbf{Z})$ have identity elements.

a Which subsets A of $\mathbf{Z}$ have inverses for $\cup$? What are these inverses?

b Which subsets A of $\mathbf{Z}$ have inverses for $\cap$? What are these inverses?

2.12 Entertainment. Let S be a set, and let $\mathcal{S}(S)$ be the set of all subsets of S. Define a binary operation Δ on $\mathcal{S}(S)$ by

$$A \Delta B = (A \setminus B) \cup (B \setminus A) \text{ for all } A, B \in \mathcal{S}(S).$$

Thus $A\Delta B$ consists of all points that are in exactly one of the sets A, B. We call $A\Delta B$ the *symmetric difference* of A and B. Show that there is an identity element for Δ, and that every element of $\mathcal{S}(S)$ is invertible for Δ.

2.13 Definition (Associative operation.) Let $\circ$ be a binary operation on a set A. We say that $\circ$ is *associative* if

$$\text{for all } a, b, c \in A, \quad a \circ (b \circ c) = (a \circ b) \circ c.$$

2.14 Examples. Both $+$ and $\cdot$ are associative operations on $\mathbf{Q}$. Subtraction $(-)$ is not an associative operation on $\mathbf{Z}$, since

$$(1-1)-1 \neq 1-(1-1).$$

Observe that to show that a binary operation $\circ$ on a set A is not associative, it is sufficient to find one point (a,b,c) in A^3 such that $a \circ (b \circ c) \neq (a \circ b) \circ c$.

You should convince yourself that both $\cap$ and $\cup$ are associative operations on the set $\mathcal{S}$ of all sets. If A, B, C are sets, then

$$\begin{aligned} A \cap (B \cap C) = (A \cap B) \cap C &= \text{set of points in all three of } A, B, C \\ A \cup (B \cup C) = (A \cup B) \cup C &= \text{set of points in at least one of } A, B, C. \end{aligned}$$

2.15 Theorem (Uniqueness of inverses.) *Let $\circ$ be an associative operation on a set A, and suppose that there is an identity e for $\circ$. Let $x, y, z \in A$. If y and z are inverses for x, then $y = z$.*

Proof: Since y and z are inverses for x, we have

$$y \circ x = e = x \circ y$$

and

$$z \circ x = e = x \circ z.$$

Hence,

$$y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z. \ \|\!|$$

2.16 Definition (Invertible element.) Let $\circ$ be a binary operation on a set A, having an identity element e. I will say that an element $x \in A$ is *invertible* for $\circ$, if x has an inverse. If $\circ$ is associative, then every invertible element for $\circ$ has a unique inverse, which I call *the inverse for x under* $\circ$.

2.17 Theorem (Double inverse theorem.) *Let $\circ$ be an associative binary operation on a set A, with identity e, and let $x \in A$. If x is invertible for $\circ$, let x^{-1} denote the (unique) inverse for x. Then x^{-1} is invertible and $(x^{-1})^{-1} = x$.*

Proof: If y is the inverse for x, then

$$y \circ x = e = x \circ y.$$

But this is exactly the condition for x to be the inverse for y. $\|\!|$

2.18 Examples. As special cases of the double inverse theorem, we have

$$-(-x) = x \qquad \text{for all } x \in \mathbf{Q}$$

and

$$(x^{-1})^{-1} = x \qquad \text{for all } x \in \mathbf{Q} \setminus \{0\}.$$

Here, as usual, x^{-1} denotes the multiplicative inverse for x.

2.19 Theorem (Cancellation law.) *Let $\circ$ be an associative binary operation on a set A, having identity e, and let $v \in A$ be an invertible element for $\circ$. Then*

$$\textit{for all } x, y \in A \;\; (x \circ v = y \circ v) \implies (x = y), \tag{2.20}$$

and

$$\textit{for all } x, y \in A \;\; (v \circ x = v \circ y) \implies (x = y). \tag{2.21}$$

Proof: Let v be invertible, and let w be the inverse for v. Then for all $x, y \in A$,

$$\begin{aligned} x \circ v = y \circ v &\implies (x \circ v) \circ w = (y \circ v) \circ w \\ &\implies x \circ (v \circ w) = y \circ (v \circ w) \\ &\implies x \circ e = y \circ e \\ &\implies x = y. \end{aligned}$$

This proves (2.20). The proof of (2.21) is left to you.

2.22 Exercise. Prove the second half of the cancellation theorem.

2.23 Warning. If $\circ$ is a binary operation on a set A, then an expression such as

$$a \circ b \circ c \circ d$$

is ambiguous, and should not be written without including a way of resolving the ambiguity. For example in $\mathbf{Z}$, $a - b - c - d$ could be interpreted as any of

$$(a - (b - c)) - d, \tag{2.24}$$
$$((a - b) - c) - d, \tag{2.25}$$
$$(a - b) - (c - d), \tag{2.26}$$
$$a - (b - (c - d)), \tag{2.27}$$
$$a - ((b - c) - d). \tag{2.28}$$

2.29 Entertainment. Is it possible to find integers a, b, c, d such that the five numbers (2.24)-(2.28) are all different? If so, find four such integers

2.30 Exercise. Let $\circ$ be an associative binary operation on a set A, and let a, b, c, d be elements of A.

a) Show that there are five different ways to sensibly put parentheses in the expression

$$a \circ b \circ c \circ d,$$

and that all five ways produce the same result. (Each way will use two sets of parentheses, e.g. $(a \circ (b \circ c)) \circ d$ is one way. If you arrange things correctly, you will just need to apply the associative law four times.)

b) Show that if a, b, c, d, e are elements of A, then there are 14 ways to put parentheses in

$$a \circ b \circ c \circ d \circ e,$$

and that all 14 ways lead to the same result. Here each sensible way of inserting parentheses will involve three pairs.

2.31 Entertainment. Show that there are 42 ways to put parentheses in

$$a_1 \circ a_2 \circ a_3 \circ a_4 \circ a_5 \circ a_6.$$

This can be done without actually writing down all the ways (and there isn't much point in writing down all the ways, because no one would read it if you did). If you did part b. of the previous exercise in such a way that really showed that there are just 14 ways, you should be able to do this, and then to calculate the number of ways to parenthesize products with seven factors. There is a simple (but hard to guess) formula for the number of ways to put parentheses in products with n factors. You can find the formula, along with a derivation, in [44].

2.32 Definition (Commutative operation.) Let $\circ$ be a binary operation on a set A. We say that $\circ$ is *commutative* if

$$\text{for all } a, b \in A \quad a \circ b = b \circ a.$$

2.33 Examples. Both + and · are commutative operations on $\mathbf{Q}$. However − is not a commutative operation on $\mathbf{Q}$, because $3-2 \neq 2-3$.

The operations ∪ and ∩ are both commutative operations on the set $\mathcal{S}$ of all sets, and *and* and *or* are commutative operations on the set $\mathcal{P}$ of all propositions. The set difference operation (\) is not commutative on $\mathcal{S}$, since

$$\{1,2\} \setminus \{2,3\} \neq \{2,3\} \setminus \{1,2\}.$$

2.2 Some Examples

2.34 Example (non-commutative *and*.) Many computer languages support an *and* operation that is not commutative. Here is a script of a Maple session. My statements are shown in `typewriter font`. Maple's responses are shown in *italics*.

```
> P := (x = 1/y);
```

$$P := x = \frac{1}{y}$$

```
> Q := (x*y=1);
```

$$Q := x\,y = 1$$

```
> y:= 0;
```

$$y := 0$$

```
> x := 1;
```

$$x := 1$$

```
> Q and P;
```

false

```
> P and Q;
```

Error, division by zero

When evaluating Q *and* P, Maple first found that Q is false, and then, without looking at P, concluded that Q *and* P must be false. When evaluating P *and* Q, Maple first tried to evaluate P, and in the process discovered that P is not a proposition. Mathematically, both Q *and* P and P *and* Q are errors when $y = 0$ and $x = 1$. Many programmers consider the non-commutativity of *and* to be a *feature* (i.e. good), rather than a *bug* (i.e. bad).

2.35 Example (Calculator operations.) Let $\widetilde{C}$ denote the set of all numbers that can be entered into your calculator. The exact composition of $\widetilde{C}$ depends on the model of your calculator. Let $C = \widetilde{C} \cup \{E\}$ where E is some object not in $\widetilde{C}$. I will call E *the error*. I think of E as the result produced when you enter $1/0$. Define four binary operations $\oplus, \ominus, \odot$, and $\oslash$ on C by

$$\begin{aligned} a \oplus b &= \text{result produced when you calculate } a + b. \\ a \ominus b &= \text{result produced when you calculate } a - b. \\ a \odot b &= \text{result produced when you calculate } a \cdot b. \\ a \oslash b &= \text{result produced when you calculate } a/b. \end{aligned}$$

On my calculator

$$\begin{aligned} &2 \oplus 2 = 4. \\ &10^{50} \odot 10^{50} = E. \\ &1111111111 \odot 1111111111 = 1.2345679 \times 10^{18}. \end{aligned}$$

If $\circ$ denotes any of $\oplus, \ominus, \odot, \oslash$, I define

$$E \circ x = E = x \circ E \text{ for all } x \in C.$$

On all calculators with which I am familiar, $\oplus$ and $\odot$ are commutative operations, 0 is an identity for $\oplus$, 1 is an identity for $\odot$, and every element of C except for E is invertible for $\oplus$. On my calculator

$$1 \oslash 3 = 0.333333333 \tag{2.36}$$

$$0.333333333 \odot 3 = 0.999999999 \tag{2.37}$$

$$0.333333333 \odot 3.000000003 = 1 \tag{2.38}$$

$$0.333333333 \odot 3.000000004 = 1. \tag{2.39}$$

Thus 0.333333333 has two different inverses! It follows from theorem 2.15 that $\odot$ is not associative. Your calculator may give different results for the calculations (2.38) and (2.39) but none of the calculator operations are associative.

2.40 Exercise. Verify that calculator addition ($\oplus$) and calculator multiplication ($\odot$) are not associative, by finding calculator numbers a, b, c, x, y, and z such that $a \oplus (b \oplus c) \neq (a \oplus b) \oplus c$, and $x \odot (y \odot z) \neq (x \odot y) \odot z$.

2.41 Notation. If $n \in \mathbf{N}$, let

$$\mathbf{Z}_n = \{x \in \mathbf{N} \colon x < n\}.$$

Hence, for example

$$\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}.$$

2.42 Definition ($\oplus_n, \odot_n$.) Let $n \in \mathbf{N}$, with $n \geq 2$. We define two binary operations $\oplus_n$ and $\odot_n$ on $\mathbf{Z}_n$ by:

for all $a, b \in \mathbf{Z}_n$,

$$a \oplus_n b = \text{ remainder when } a + b \text{ is divided by } n$$

and for all $a, b \in \mathbf{Z}_n$,

$$a \odot_n b = \text{ remainder when } a \cdot b \text{ is divided by } n.$$

Thus,

$$\begin{aligned} 4 \oplus_5 4 &= 3 \quad \text{since } 4 + 4 = 1 \cdot 5 + 3, \\ 1 \odot_5 4 &= 4 \quad \text{since } 1 \cdot 4 = 0 \cdot 5 + 4, \end{aligned}$$

and

$$4 \odot_5 4 = 1 \quad \text{since } 4 \cdot 4 = 3 \cdot 5 + 1.$$

The operations $\oplus_n$ and $\odot_n$ are both commutative (since $+$ and $\cdot$ are commutative on $\mathbf{Z}$). Clearly 0 is an identity for $\oplus_n$, and 1 is an identity for $\odot_n$. Every element of $\mathbf{Z}_n$ is invertible for $\oplus_n$ and

$$\text{inverse for } k \text{ under } \oplus_n = \begin{cases} n - k & \text{if } k \neq 0 \\ 0 & \text{if } k = 0. \end{cases}$$

2.43 Definition (Multiplication table.) Let $\circ$ be a binary operation on a finite set $A = \{a_1, a_2, \cdots, a_n\}$ having n elements. We construct a *multiplication table* for $\circ$ as follows: We write down a table with n rows and n columns. Along the top of the table we list the elements of A as labels for the columns. Along the left side of the table we list the elements of A (in the same order) as labels for the rows. (See the figure to see what is meant by this.) If $(x, y) \in A^2$, we write the product $x \circ y$ in the box of our table whose row label is x and whose column label is y.

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

Multiplication table for $\circ$

2.44 Examples. Below are the multiplication tables for $\oplus_5$ and $\odot_5$:

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

By looking at the multiplication table for $\odot_5$ we see that

$$\begin{array}{ll} 1 \odot_5 1 = 1 & 2 \odot_5 3 = 1 \\ 4 \odot_5 4 = 1 & 3 \odot_5 2 = 1. \end{array}$$

Hence all the non-zero elements of $\mathbf{Z}_5$ have inverses under $\odot_5$.

Both of the operations $\oplus_n$ and $\odot_n$ are associative. This follows from the fact that $+$ and $\cdot$ are associative operations on $\mathbf{Z}$, by a straightforward but lengthy argument. The details are given in appendix A.

2.45 Exercise. Write down the multiplication table for $\odot_6$ on $\mathbf{Z}_6$. Determine which elements of $\mathbf{Z}_6$ are invertible for $\odot_6$, and find the inverse for each invertible element.

2.46 Exercise. Let $\{x, y, z\}$ be a set containing three distinct elements. ($x \neq y$, $y \neq z$, $z \neq x$). Let $\circ$ be the binary operation on $\{x, y, z\}$ determined by the multiplication table:

	x	y	z
x	x	y	z
y	y	x	x
z	z	x	x

a) Show that there is an identity element for $\circ$. (Which of x, y, z is the identity?)

b) Show that y has two different inverses for $\circ$.

c) Explain why the result of part b does not contradict the theorem on uniqueness of inverses.

2.47 Note. An early example of a binary operation that was not an obvious generalization of one of the operations $+, -, \cdot, /$ on numbers was the use of union and intersection as binary operations on the set of all sets by George Boole[11]. In *Laws of Thought* (1854), Boole introduces the operation $+$ (for union) and $\times$ (for intersection) on "classes" (although he usually writes xy instead of $x \times y$). He explicitly states

$$\begin{aligned} x+y &= y+x \\ xy &= yx \\ x(y+z) &= xy+xz \end{aligned}$$

which he calls commutative and distributive laws. He does not mention associativity, and writes xyz without parentheses. He denotes "Nothing" by 0 and "the Universe" by 1, and notes that 0 and 1 have the usual properties. As an example of the distributive law, Boole gives

European men and women = European men and European women.

Boole's $+$ is not really a binary operation since he only defines $x+y$ when x and y have no elements in common.

The word *associative*, in its mathematical sense, was introduced by William Hamilton[24, p114] in 1843 in a paper on quaternions. According to [14, p284], the words *commutative* and *distributive* were introduced by François -Joseph Servois in 1813.

2.3 The Field Axioms

2.48 Definition (Field.) A *field* is a triple $(F, +, \cdot)$ where F is a set, and $+$ and $\cdot$ are binary operations on F (called *addition* and *multiplication* respectively) satisfying the following nine conditions. (These conditions are called the *field axioms.*)

1. **(Associativity of addition.)** *Addition* $(+)$ *is an associative operation on* F.

2. **(Existence of additive identity.)** *There is an identity element for addition.*

   We know that this identity is unique, and we will denote it by 0.

3. **(Existence of additive inverses.)** *Every element* x *of* F *is invertible for* $+$.

   We know that the additive inverse for x is unique, and we will denote it by $-x$.

4. **(Commutativity of multiplication.)** *Multiplication* $(\cdot)$ *is a commutative operation on* F.

5. **(Associativity of multiplication.)** *Multiplication is an associative operation on* F.

6. **(Existence of multiplicative identity.)** *There is an identity element for multiplication.*

   We know that this identity is unique, and we will denote it by 1.

7. **(Existence of multiplicative inverses.)** *Every element* x *of* F except possibly for 0 *is invertible for* $\cdot$.

   We know that the multiplicative inverse for x is unique, and we will denote it by x^{-1}. We do not assume 0 is not invertible. We just do not assume that it is.

8. **(Distributive law.)** *For all* x, y, z *in* F, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

9. **(Zero-one law.)** *The additive identity and multiplicative identity are distinct; i.e.,* $0 \neq 1$.

We often speak of "the field F" instead of "the field $(F, +, \cdot)$".

2.49 Remark. Most calculus books that begin with the axioms for a field (e.g., [47, p5], [1, p18], [13, p5], [12, p554]) add an additional axiom.

10. **(Commutativity of addition.)** *Addition is a commutative operation on* F.

I have omitted this because, as Leonard Dickson pointed out in 1905[18, p202], it can be proved from the other axioms (see theorem 2.72 for a proof). I agree with Aristotle that

> It is manifest that it is far better to make the principles finite in number. Nay, they should be the fewest possible provided they enable all the same results to be proved. This is what mathematicians insist upon; for they take as principles things finite either in kind or in number[26, p178].

2.50 Remark (Parentheses.) The distributive law is usually written as

$$x \cdot (y + z) = x \cdot y + x \cdot z \tag{2.51}$$

The right side of (2.51) is ambiguous. There are five sensible ways to interpret it:

$$\begin{aligned}&x \cdot ((y + x) \cdot z)\,,\\&x \cdot (y + (x \cdot z))\,,\\&(x \cdot y) + (x \cdot z),\\&((x \cdot y) + x) \cdot z\\&(x \cdot (y + x)) \cdot z.\end{aligned}$$

The conventions presently used for interpreting ambiguous statements such as $x \cdot y + x \cdot z$ and involving operations $+, -, \cdot, /$ are:

1. Multiplication and division have equal precedence.
2. Addition and subtraction have equal precedence.
3. Multiplication has higher precedence than addition.

This means that to interpret

$$1 \cdot 2/3 + 4 \cdot 5 \cdot 6 - 7 \cdot 8 + 9, \tag{2.52}$$

you first read (2.52) from left to right and perform all the multipliations and divisions as you come to them, getting

$$((1 \cdot 2)/3) + ((4 \cdot 5) \cdot 6) - (7 \cdot 8) + 9. \tag{2.53}$$

Then read (2.53) from left to right performing all additions and subtractions as you come to them, getting

$$((((1 \cdot 2)/3) + ((4 \cdot 5) \cdot 6)) - (7 \cdot 8)) + 9.$$

When I was in high school, multiplication had higher precedence than division, so

$$a \cdot b/c \cdot d/e \cdot f$$

meant

$$((a \cdot b)/(c \cdot d))\,/(e \cdot f),$$

whereas today it means

$$((((a \cdot b)/c) \cdot d)\,/e) \cdot f.$$

In 1713, addition often had higher precedence than multiplication. Jacob Bernoulli [8, p180] wrote expressions like

$$n \cdot n + 1 \cdot n + 2 \cdot n + 3 \cdot n + 4$$

to mean

$$n \cdot (n+1) \cdot (n+2) \cdot (n+3) \cdot (n+4).$$

2.54 Examples. $\mathbf{Q}$ with the usual operations of addition and multiplication is a field.

$(\mathbf{Z}_5, \oplus_5, \odot_5)$ is a field. (See definition 2.42 for the definitions.) We showed in section 2.2 that $(\mathbf{Z}_5, \oplus_5, \odot_5)$ satisfies all the field axioms except possibly the distributive law. In appendix A, it is shown that the distributive property holds for $(\mathbf{Z}_n, \oplus_n, \odot_n)$ for all $n \in \mathbf{N}$, $n \geq 2$. (The proof assumes that the distributive law holds in $\mathbf{Z}$.)

For a general $n \in \mathbf{N}$, $n \geq 2$, the only field axiom that can possibly fail to hold in $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is the existence of multiplicative inverses, so to determine whether $\mathbf{Z}_n$ is a field, it is just necessary to determine whether every non-zero element in $\mathbf{Z}_n$ is invertible for $\odot_n$.

2.55 Exercise. In each of the examples below, determine which field axioms are valid and which are not. Which examples are fields? In each case that an axiom fails to hold, give an example to show why it fails to hold.

a) $(\mathbf{Z}, +, \cdot)$ where $+$ and $\cdot$ are usual addition and multiplication.

b) $(G, +, \cdot)$ where $G = \mathbf{Q}^+ \cup \{0\}$ is the set of non-negative rational numbers, and $+$ and $\cdot$ are the usual addition and multiplication.

c) $(H, +, \cdot)$ where $H = \{x\}$ is a set with just one element and both $+$ and $\cdot$ are the only binary operation on H; i.e.,

$$x + x = x, \qquad x \cdot x = x.$$

d) $(\mathbf{Q}, \oplus, \odot)$ where both $\oplus$ and $\odot$ are the usual operation of addition on $\mathbf{Q}$, e.g., $3 \oplus 4 = 7$ and $3 \odot 4 = 7$.

2.56 Exercise. Determine for which values of $n = 2, 3, 4, 5, 6$, $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. (You already know that $n = 5$ produces a field.)

2.57 Notation (The field $\mathbf{Z}_n$.) Let $n \in \mathbf{N}$, $n \geq 2$ be a number such that $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. Then "the field $\mathbf{Z}_n$" means the field $(\mathbf{Z}_n, \oplus_n, \odot_n)$. I will often denote the operations in $\mathbf{Z}_n$ by $+$ and $\cdot$ instead of $\oplus_n$ and $\odot_n$.

2.58 Entertainment. Determine for which values of n in $\{7, 8, 9, 10, 11\}$ the system $(\mathbf{Z}_n, \oplus_n, \odot_n)$ is a field. If you do this you will probably conjecture the exact (fairly simple) condition on n that makes the system into a field.

2.4 Some Consequences of the Field Axioms.

2.59 Theorem (Cancellation laws.) *Let $(F, +, \cdot)$ be a field, let x, y, z be elements in F, and let $v \in F \backslash \{0\}$. Then*

$$x + z = y + z \implies x = y. \tag{2.60}$$

$$z + x = z + y \implies x = y. \tag{2.61}$$

$$x \cdot v = y \cdot v \implies x = y. \tag{2.62}$$

$$v \cdot x = v \cdot y \implies x = y. \tag{2.63}$$

(2.60) and (2.61) are called cancellation laws for addition*, and (2.62) and (2.63) are called* cancellation laws for multiplication.

Proof: All of these results are special cases of the cancellation law for an associative operation (theorem 2.19). |||

2.64 Theorem. *In any field* $(F,+,\cdot)$

$$-0=0 \textit{ and } 1^{-1}=1.$$

Proof: These are special cases of the remark made earlier that an identity element is always invertible, and is its own inverse. |||

2.65 Theorem (Double inverse theorem.) *In any field* $(F,+,\cdot)$,

$$\begin{array}{rl} \textit{for all } x\in F & \qquad -(-x)=x, \\ \textit{for all } x\in F\backslash\{0\} & \qquad (x^{-1})^{-1}=x. \end{array}$$

Proof: These are special cases of theorem 2.17. |||

I will now start the practice of calling a field F. If I say "let F be a field" I assume that the operations are denoted by $+$ and $\cdot$.

2.66 Theorem. *Let F be a field. Then*

$$\textit{for all } a\in F, \quad a\cdot 0=0.$$

Proof: We know that $0=0+0$, and hence

$$a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0.$$

Also, $a\cdot 0+0=a\cdot 0$, so

$$a\cdot 0+0=a\cdot 0+a\cdot 0.$$

By the cancellation law for addition, $0=a\cdot 0$. |||

2.67 Corollary. *Let F be a field. Then for all $a\in F$, $0\cdot a=0$.*

2.68 Theorem. *Let F be a field. Then for all x,y in F*

$$\big(x\cdot y=0\big) \implies \big(x=0 \textit{ or } y=0\big). \tag{2.69}$$

Proof:

Case 1: Suppose $x=0$. Then (2.69) is true because every statement implies a true statement.

Case 2: Suppose $x \neq 0$. By theorem 2.66, $x \cdot 0 = 0$, so

$$x \cdot y = 0 \implies x \cdot y = x \cdot 0.$$

Since $x \neq 0$, we can use the cancellation law for multiplication to get

$$\Big(x \cdot y = x \cdot 0\Big) \implies \Big(y = 0\Big) \implies \Big(x = 0 \text{ or } y = 0\Big),$$

and hence

$$\Big(x \cdot y = 0\Big) \implies \Big(x = 0 \text{ or } y = 0\Big).$$

Thus (2.69) holds in all cases. |||

2.70 Remark. We can combine theorem 2.66, corollary 2.67 and theorem 2.68 into the statement: In any field F,

$$\text{for all } x, y \in F \qquad x \cdot y = 0 \iff (x = 0 \text{ or } y = 0).$$

2.71 Exercise. Let F be a field. Prove that 0 has no multiplicative inverse in F.

2.72 Theorem (Commutativity of addition.) *Let F be any field. Then $+$ is a commutative operation on F.*

Proof: Let x, y be elements in F. Then since multiplication is commutative, we have

$$(1 + x) \cdot (1 + y) = (1 + y) \cdot (1 + x).$$

By the distributive law,

$$((1 + x) \cdot 1) + ((1 + x) \cdot y) = ((1 + y) \cdot 1) + ((1 + y) \cdot x)\,.$$

Since 1 is the multiplicative identity,

$$(1 + x) + ((1 + x) \cdot y) = (1 + y) + ((1 + y) \cdot x)\,,$$

and hence

$$1 + (x + ((1 + x) \cdot y)) = 1 + (y + ((1 + y) \cdot x)).$$

By the cancellation law for addition

$$x + ((1 + x) \cdot y) = y + ((1 + y) \cdot x)\,.$$

By commutativity of multiplication and the distributive law,

$$x + (y \cdot (1 + x)) = y + (x \cdot (1 + y))$$

and

$$x + ((y \cdot 1) + (y \cdot x)) = y + ((x \cdot 1) + (x \cdot y)) .$$

Since 1 is the multiplicative identity and addition is associative

$$x + (y + (y \cdot x)) = y + (x + (x \cdot y))$$

and hence

$$(x + y) + (y \cdot x) = (y + x) + (x \cdot y).$$

Since multiplication is commutative

$$(x + y) + (x \cdot y) = (y + x) + (x \cdot y)$$

and by the cancellation law for addition,

$$x + y = y + x.$$

Hence, + is commutative. |||

2.73 Remark. Let F be a field, and let $x, y \in F$. Then

$$\text{To prove } x = -y, \text{ it is sufficient to prove } x + y = 0. \tag{2.74}$$

$$\text{To prove } x = y^{-1}, \text{ it is sufficient to prove } x \cdot y = 1. \tag{2.75}$$

Proof:

$$\begin{aligned} x + y = 0 &\implies ((x + y = 0) \text{ and } (y + x = 0)) \\ &\implies y = -x \text{ and } x = -y. \\ x \cdot y = 1 &\implies ((x \cdot y = 1) \text{ and } (y \cdot x = 1)) \\ &\implies x = y^{-1} \text{ and } y = x^{-1}. \ ||| \end{aligned}$$

2.76 Theorem. *Let F be a field. Then*

$$\textit{for all } x, y \in F, \qquad x \cdot (-y) = -(x \cdot y).$$

Proof: Let $x, y \in F$. By (2.74) it is sufficient to prove

$$x \cdot (-y) + x \cdot y = 0.$$

Well,

$$\begin{aligned} x \cdot (-y) + x \cdot y &= x \cdot ((-y) + y) \\ &= x \cdot 0 \\ &= 0. \ \| \end{aligned}$$

2.77 Exercise. Let F be a field, and let $a, b \in F$. Prove that

a) $(-a) \cdot b = -(a \cdot b)$.

b) $a \cdot (-1) = -a$.

c) $(-a) \cdot (-b) = a \cdot b$.

2.78 Exercise. Let F be a field and let b, d be non-zero elements in F. Prove that

$$b^{-1} \cdot d^{-1} = (b \cdot d)^{-1}.$$

2.79 Definition (Digits.) Let F be a field. We define

$$\begin{array}{ll} 2 = 1 + 1, & 6 = 5 + 1, \\ 3 = 2 + 1, & 7 = 6 + 1, \\ 4 = 3 + 1, & 8 = 7 + 1, \\ 5 = 4 + 1, & 9 = 8 + 1, \\ & t = 9 + 1. \end{array}$$

I'll call the set

$$\mathbf{D}_F = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

the set of *digits in* F. If a, b, c are digits, I define

$$ab = t \cdot a + b, \tag{2.80}$$

and

$$abc = t \cdot (ab) + c. \tag{2.81}$$

Here ab should not be confused with $a \cdot b$.

2.82 Example.

$$\begin{aligned} 10 &= t\cdot 1+0=t. \\ 100 &= t\cdot 10+0=t\cdot 10=10\cdot 10. \\ 37 &= t\cdot 3+7=10\cdot 3+7. \end{aligned}$$

In general, if $x \in F$, I define

$$x^2 = x\cdot x.$$

Then for all digits a, b, c

$$\begin{aligned} abc &= t\cdot(ab)+c=t\cdot(t\cdot a+b)+c=(t\cdot(t\cdot a)+t\cdot b)+c \\ &= ((t\cdot t)\cdot a+t\cdot b)+c \\ &= t^2\cdot a+t\cdot b+c=10^2\cdot a+10\cdot b+c, \end{aligned}$$

so, for example

$$375 = 10^2\cdot 3+10\cdot 7+5.$$

2.83 Remark. The set $\mathbf{D}_F$ of digits in F may contain fewer than ten elements. For example, in $(\mathbf{Z}_5, \oplus_5, \odot_5)$,

$$\begin{aligned} 2 &= 1\oplus_5 1=2. \\ 3 &= 2\oplus_5 1=3. \\ 4 &= 3\oplus_5 1=4. \\ 5 &= 4\oplus_5 1=0. \end{aligned}$$

and you can see that $\mathbf{D}_{\mathbf{Z}_5} = \{0, 1, 2, 3, 4\}$.

2.84 Theorem. *In any field F, $2+2=4$ and $2\cdot 2=4$.*

Proof:

$$\begin{aligned} 2+2 &= 2+(1+1) && \text{(by definition of 2)} \\ &= (2+1)+1 && \text{(by associativity of +)} \\ &= 3+1 && \text{(by definition of 3)} \\ &= 4 && \text{(by definition of 4).} \end{aligned}$$

Also,

$$2\cdot 2=2\cdot(1+1)=2\cdot 1+2\cdot 1=2+2=4. \; \|$$

2.85 Exercise. Prove that in any field F, $3+3=6$ and $3\cdot 2=6$.

2.86 Exercise. Prove that in any field F, $9+8=17$.

2.87 Remark. After doing the previous two exercises, you should believe that the multiplication and addition tables that you learned in elementary school are all theorems that hold in any field, and you should feel free to use them in any field.

2.88 Exercise. Let F be a field and let $x \in F$. Prove that

$$x+x=2\cdot x.$$

2.5 Subtraction and Division

2.89 Definition (Subtraction.) In any field F, we define a binary operation $-$ (called subtraction) by

$$\text{for all } x,y \in F \qquad x-y=x+(-y).$$

Unfortunately we are now using the same symbol $-$ for two different things, a binary operation on F, and a symbol denoting additive inverses.

2.90 Exercise (Distributive laws.) Let F be a field, and let $a,b,c \in F$. Prove that

a) $a\cdot(b-c)=(a\cdot b)-(a\cdot c)$.

b) $-(a-b)=b-a$.

2.91 Definition (Division.) Let F be a field. If $a \in F$ and $b \in F\backslash\{0\}$ we define

$$a/b=a\cdot b^{-1}.$$

We also write $\dfrac{a}{b}$ for a/b. If a,b are both in $F\backslash\{0\}$, then $a\cdot b^{-1} \in F\backslash\{0\}$ so $/$ defines a binary operation on $F\backslash\{0\}$. Also, if $b \neq 0$, then $\dfrac{1}{b}=1/b=1\cdot b^{-1}=b^{-1}$.

2.92 Example. In the field $(\mathbf{Z}_5, \oplus_5, \odot_5)$, $3^{-1} = 2$ and $4^{-1} = 4$. Hence

$$\frac{1}{3} = 2 \text{ and } \frac{2}{3} = 2 \cdot 2 = 4.$$

Thus,

$$\frac{1}{3} + \frac{2}{3} = 2 + 4 = 1.$$

2.93 Exercise. Let F be a field, and let a, b, c, d be elements of F with $b \neq 0$ and $d \neq 0$. Prove all of the following propositions. In doing any part of this problem, you may assume that all of the earlier parts have been proved.

a) $\dfrac{a \cdot d}{b \cdot d} = \dfrac{a}{b}$.

b) $\dfrac{d \cdot a}{d \cdot b} = \dfrac{a}{b}$.

c) $-\left(\dfrac{a}{b}\right) = \dfrac{-a}{b}$.

d) $\dfrac{a}{b} + \dfrac{c}{b} = \dfrac{a+c}{b}$.

e) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a \cdot d + b \cdot c}{b \cdot d}$.

f) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{a \cdot d - b \cdot c}{b \cdot d}$.

g) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$.

h) $\left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$.

I will now start the practice of using steps in proofs that involve multiple uses of the associative and commutative laws. For example, I'll write statements such as

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

with no explanation, because I believe that you recognize that it is correct, and that you can prove it. I'll also write ab for $a \cdot b$ when I believe that no confusion will result, and I'll use distributive laws like

$$(x+y) \cdot z = x \cdot z + y \cdot z$$

and

$$(x-y) \cdot z = x \cdot z - y \cdot z$$

even though we haven't proved them. I will write

$$(a+b)(c+d) = (a+b)c + (a+b)d = ac + bc + ad + bd$$

and assume that you know (because of our conventions about omitting parentheses; cf. Remark 2.50) that the right side of this means

$$(((a \cdot c) + (b \cdot c)) + (a \cdot d)) + (b \cdot d)$$

and you also know (by exercise 2.30) that the parentheses can be rearranged in other sensible orders without changing the value of the expression.

2.94 Exercise. Let F be a field. Show that for all a, b, x in F

a) $(a+b)^2 = a^2 + 2ab + b^2$.

b) $(a-b)^2 = a^2 - 2ab + b^2$.

c) $(a-b) \cdot (a+b) = (a^2 - b^2)$.

d) $(x-a)(x-b) = x^2 - (a+b)x + a \cdot b$.

e) $(2a+b)^2 = 4a^2 + 4ab + b^2$.

2.95 Theorem. *Let F be a field. Then for all $x, y \in F$,*

$$(x^2 = y^2) \iff (x = y \text{ or } x = -y).$$

Proof:

$$\begin{aligned} x^2 = y^2 &\iff x^2 - y^2 = 0 \\ &\iff (x-y)(x+y) = 0 \\ &\iff (x-y=0) \text{ or } (x+y=0) \\ &\iff x = y \text{ or } x = -y. \ \| \end{aligned}$$

2.96 Theorem (Quadratic formula.) *Let F be a field such that $2 \neq 0$ in F. Let $A \in F\backslash\{0\}$, and let B, C be elements of F. Then the equation*

$$Ax^2 + Bx + C = 0 \tag{2.97}$$

has a solution x in F if and only if $B^2 - 4AC$ is a square in F (i.e., if and only if there is some element $y \in F$ such that $y^2 = B^2 - 4AC$). If y is any element of F satisfying

$$y^2 = B^2 - 4AC,$$

then the complete set of solutions of (2.97) is

$$\left\{\frac{-B+y}{2A}, \frac{-B-y}{2A}\right\}.$$

(This corresponds to the familiar quadratic formula

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.)$$

Proof: The proof uses the algebraic identity

$$(px+q)^2 = p^2x^2 + 2pqx + q^2 \text{ for all } p, q, x \in F.$$

Since $A \neq 0$ and $2 \neq 0$, we have $2^2A \neq 0$ and hence

$$\begin{aligned} Ax^2 + Bx + C = 0 &\iff 2^2A(Ax^2 + Bx + C) = 0 \\ &\iff (2A)^2x^2 + 2 \cdot (2A)Bx = -4AC \\ &\iff (2A)^2x^2 + 2 \cdot (2A)Bx + B^2 = B^2 - 4AC \\ &\iff (2Ax + B)^2 = B^2 - 4AC. \end{aligned}$$

Hence if $B^2 - 4AC$ is not a square, then (2.97) has no solutions. If $B^2 - 4AC = y^2$ for some $y \in F$, then

$$\begin{aligned} Ax^2 + Bx + C = 0 &\iff (2Ax + B)^2 = y^2 \\ &\iff 2Ax + B = y \text{ or } 2Ax + B = -y \\ &\iff x = \frac{-B+y}{2A} \text{ or } x = \frac{-y-B}{2A}. \ \| \end{aligned}$$

2.98 Entertainment. $\mathbf{Z}_7$ is a field. (You can take my word for it or check it for yourself.) Find all solutions to the quadratic equations below in $\mathbf{Z}_7$.

a) $x^2 - x + 2 = 0$.

b) $3x^2 + 5x + 2 = 0$.

c) $2x^2 + x + 5 = 0$.

2.99 Note. The definition of field that we use is roughly equivalent to the definition given by H. Weber in 1893 [48, p526]. Weber does not give the zero-one axiom but he remarks that 0 is different from 1 except in the uninteresting case where the field has only one element. He includes commutativity of addition as an axiom, and he also appears to take $a(-b) = -(ab)$ as an axiom. Individual fields, both finite fields and subfields of the real and complex numbers, had been studied before Weber's paper, but Weber's definition provided an abstraction that included both finite and infinite fields.

There are many other choices we could have made for the field axioms. In [29], Edward Huntington gives eight different sets of axioms that are equivalent to ours. (Two sets of propositions $\mathcal{A}, \mathcal{B}$ are equivalent if every statement in $\mathcal{A}$ can be proved using statements in $\mathcal{B}$, and every statement in $\mathcal{B}$ can be proved from statements in $\mathcal{A}$.)

2.6 Ordered Fields

2.100 Definition (Ordered field axioms.) An *ordered field* is a pair $(F, F^+) = ((F, +, \cdot), F^+)$ where F is a field, and F^+ is a subset of F satisfying the conditions

1. For all $a, b \in F^+$, $\quad a + b \in F^+$.

2. For all $a, b \in F^+$, $\quad a \cdot b \in F^+$.

3. (Trichotomy) For all $a \in F$, exactly one of the statements

$$a \in F^+, \quad -a \in F^+, \quad a = 0$$

is true. The set F^+ is called the set of *positive elements* of F. A field F is *orderable* if it has a subset F^+ such that 1), 2) and 3) are satisfied.

2.101 Example. The rational numbers $(\mathbf{Q}, \mathbf{Q}^+)$ form an ordered field, where $\mathbf{Q}^+$ denotes the familiar set of positive rationals.

2.102 Notation (F^-.) Let (F, F^+) be an ordered field. We let

$$F^- = \{x \in F\colon -x \in F^+\}.$$

We call F^- the set of *negative* elements in F. Thus

$$x \in F^- \iff -x \in F^+,$$

and

$$-x \in F^- \iff -(-x) \in F^+ \iff x \in F^+.$$

We can restate the Trichotomy axiom as: For all $x \in F$, exactly one of the statements

$$x \in F^+, \qquad x = 0, \qquad x \in F^-$$

is true.

2.103 Theorem. *Let (F, F^+) be an ordered field. Then for all $x \in F\backslash\{0\}$, $x^2 \in F^+$.*

Proof: Since $x \neq 0$, we know $x \in F^+$ or $x \in F^-$. Now

$$x \in F^+ \implies x \cdot x \in F^+ \implies x^2 \in F^+,$$

and

$$x \in F^- \implies (-x)(-x) \in F^+ \implies x^2 \in F^+. \parallel$$

2.104 Corollary. *In any ordered field, $1 \in F^+$.*

2.105 Example. The field $\mathbf{Z}_5$ is not orderable.
First Proof: If there were a subset $\mathbf{Z}_5^+$ of $\mathbf{Z}_5$ such that $(\mathbf{Z}_5, \mathbf{Z}_5^+)$ were an ordered field, we would have $4 = 2^2 \in \mathbf{Z}_5^+$. But in $\mathbf{Z}_5$, $4 = -1$ so $-1 \in \mathbf{Z}_5^+$ and $1 \in \mathbf{Z}_5^+$, which contradicts trichotomy. $\parallel$
Second Proof: If $(\mathbf{Z}_5, \mathbf{Z}_5^+)$ were an ordered field, we would have $1 \in \mathbf{Z}_5^+$, so $1+1 = 2 \in \mathbf{Z}_5^+$, so $1+2 = 3 \in \mathbf{Z}_5^+$, so $3+1 = 4 \in \mathbf{Z}_5^+$ so $4+1 = 0 \in \mathbf{Z}_5^+$. This contradicts trichotomy. $\parallel$

2.106 Remark. The method used in the second proof above shows that none of the fields $\mathbf{Z}_n$ are orderable.

2.107 Definition $(<, \leq, >, \geq)$ Let (F, F^+) be an ordered field, and let $a, b \in F$. We define

$$\begin{aligned} a < b &\iff b - a \in F^+. \\ a \leq b &\iff a < b \text{ or } a = b. \\ a > b &\iff a - b \in F^+. \\ a \geq b &\iff a > b \text{ or } a = b. \end{aligned}$$

2.108 Remark. In any ordered field (F, F^+):

$$\begin{aligned} 0 < b &\iff b \in F^+. \\ b < 0 &\iff 0 - b \in F^+ \iff b \in F^-. \end{aligned}$$

2.109 Exercise. Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that exactly one of the statements

$$b < a, \qquad b = a, \qquad b > a$$

is true.

2.110 Theorem (Transitivity of $<$.) *Let (F, F^+) be an ordered field. Then for all $a, b, c \in F$,*

$$((a < b) \text{ and } (b < c)) \implies (a < c).$$

Proof: For all $a, b, c \in F$ we have

$$\begin{aligned} (a < b) \text{ and } (b < c) &\iff b - a \in F^+ \text{ and } c - b \in F^+ \\ &\implies (c - b) + (b - a) \in F^+ \\ &\implies c - a \in F^+ \\ &\implies a < c. \ \| \end{aligned}$$

2.111 Exercise (Addition of inequalities.) Let (F, F^+) be an ordered field, and let $a, b, c, d \in F$. Show that

$$((a < b) \text{ and } (c < d)) \implies (a + c) < (b + d)$$

and

$$a < b \iff a + c < b + c$$

2.112 Exercise. Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that

$$a < b \iff -b < -a.$$

2.113 Notation. Let (F, F^+) be an ordered field, and let $a, b, c, d \in F$. We use notation like

$$a \leq b < c = d \tag{2.114}$$

to mean $(a \leq b)$ and $(b < c)$ and $(c = d)$, and similarly we write

$$a > b = c \geq d \tag{2.115}$$

to mean $a > b$ and $b = c$ and $c \geq d$. By transitivity of $=$ and of $<$, you can conclude $a < c$ from (2.114), and you can conclude $b \geq d$ and $a > c$ from (2.115). A chain of inequalities involving both $<$ and $>$ shows bad style, so you should not write

$$a < b \geq c.$$

2.116 Exercise (Laws of signs.) Let (F, F^+) be an ordered field, and let $a, b \in F$. Show that

1. $(a \in F^+ \text{ and } b \in F^-) \implies ab \in F^-$
2. $(a \in F^- \text{ and } b \in F^+) \implies ab \in F^-$
3. $(a \in F^- \text{ and } b \in F^-) \implies ab \in F^+$

These laws together with the axiom

$$a \in F^+ \text{ and } b \in F^+ \implies ab \in F^+$$

are called the *laws of signs.*

2.117 Notation. Let F be an ordered field, and let a, b be non-zero elements of F. We say a and b *have the same sign* if either (a, b are both in F^+) or (a, b are both in F^-). Otherwise we say *a and b have opposite signs.*

2.118 Corollary (of the law of signs.) *Let (F, F^+) be an ordered field and let $a, b \in F \backslash \{0\}$. Then*

$$a \cdot b \in F^+ \iff a \text{ and } b \text{ have the same sign },$$
$$a \cdot b \in F^- \iff a \text{ and } b \text{ have opposite signs.}$$

2.119 Notation. I will now start to use the convention that "let F be an ordered field" means "let (F, F^+) be an ordered field"; i.e., the set of positive elements of F is assumed to be called F^+.

2.120 Exercise. Let F be an ordered field and let $a, b, c \in F$. Prove that

$$\begin{aligned} ((a < b) \text{ and } (c < 0)) &\implies ac > bc. \\ ((a < b) \text{ and } (c = 0)) &\implies ac = bc = 0. \\ ((a < b)) \text{ and } (c > 0)) &\implies ac < bc. \end{aligned}$$

2.121 Theorem (Multiplication of inequalities.) *Let F be an ordered field and let a, b, c, d be elements of F. Then*

$$((0 < a < b) \textit{ and } (0 < c < d)) \implies 0 < ac < bd.$$

Proof: By the previous exercise we have

$$\begin{aligned} (0 < a < b) \text{ and } (0 < c < d) &\implies ((ca < da) \text{ and } (ad < bd)) \\ &\implies ((ac < ad) \text{ and } (ad < bd)). \end{aligned}$$

Hence, by transitivity of $<$,

$$(0 < a < b) \text{ and } (0 < c < d) \implies ac < bd. \parallel$$

2.122 Exercise. Let F be an ordered field, and let $a \in F\backslash\{0\}$. Show that a and a^{-1} have the same sign.

2.123 Exercise. Let F be an ordered field, and let $a, b \in F\backslash\{0\}$. Under what conditions (if any) can you say that

$$a < b \implies b^{-1} < a^{-1}?$$

Under what conditions (if any) can you say that

$$a < b \implies a^{-1} < b^{-1}?$$

2.124 Definition (Square root.) Let F be a field, and let $x \in F$. A square root for x is any element y of F such that $y^2 = x$.

2.125 Examples. In $\mathbf{Z}_5$, the square roots of -1 are 2 and 3.

In an ordered field F, no element in F^- has a square root.

In $\mathbf{Q}$, there is no square root of 2. (See theorem 3.45 for a proof.)

2.126 Theorem. *Let F be an ordered field and let $x \in F^+$. If x has a square root, then it has exactly two square roots, one in F^+ and one in F^-, so if x has a square root, it has a unique positive square root.*

Proof: Suppose x has a square root y. Then $y \neq 0$, since $x \in F^+$. If z is any square root of x, then $z^2 = x = y^2$, so, as we saw in theorem 2.95, $z = y$ or $z = -y$. By trichotomy, one of $y, -y$ is in F^+, and the other is in F^-. |||

2.127 Theorem. *Let F be an ordered field and let x, y be elements of F with $x \geq 0$ and $y \geq 0$. Then*

$$x < y \iff x^2 < y^2. \tag{2.128}$$

Proof: Let x, y be elements of $F^+ \cup \{0\}$. Then $x + y > 0$, unless $x = y = 0$, so $x^2 < y^2 \implies x + y > 0$. Hence

$$\begin{aligned} x^2 < y^2 &\iff y^2 - x^2 > 0 \\ &\iff (y-x)(y+x) > 0 \\ &\iff y - x \text{ and } y + x \text{ have the same sign.} \\ &\iff y - x > 0 \\ &\iff x < y. \ ||| \end{aligned}$$

2.129 Remark. The implication (2.128) is also true when $<$ is replaced by $\leq$ in both positions. I'll leave this to you to check.

2.7 Absolute Value

2.130 Definition (Absolute value.) Let F be an ordered field, and let $x \in F$. Then we define

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

2.131 Remark. It follows immediately from the definition that

1. $|x| \geq 0$ for all $x \in F$.
2. $|x| > 0$ for all $x \in F\backslash\{0\}$.
3. $(|x| = 0) \iff (x = 0)$.

2.132 Theorem. *Let F be an ordered field. Then for all $x \in F$,*

$$-|x| \leq x \leq |x|. \tag{2.133}$$

Proof: If $x = 0$ then (2.133) becomes $-0 \leq 0 \leq 0$, which is true. If $x > 0$ then $-|x| < 0 < x = |x|$. If $x < 0$ then $-|x| = -(-x) = x < 0 \leq |x|$. Hence (2.133) holds in all cases. $\|$

2.134 Exercise. Let F be an ordered field. Prove that $|x| = |-x|$ for all $x \in F$ and $|x|^2 = x^2$ for all $x \in F$.

2.135 Exercise (Product formula for absolute value.) Prove that for all $x, y \in F$,

$$|xy| = |x||y|.$$

2.136 Theorem. *Let F be an ordered field, let $x \in F$, and let $p \in F$ with $p \geq 0$. Then*

$$(|x| \leq p) \iff (-p \leq x \leq p) \tag{2.137}$$

and

$$(|x| > p) \iff ((x < -p) \text{ or } (x > p)). \tag{2.138}$$

Proof: We first show that

$$(|x| \leq p) \implies (-p \leq x \leq p). \tag{2.139}$$

Case 1. If $x > 0$, then

$$|x| \leq p \implies x \leq p \implies -p \leq 0 \leq x \leq p.$$

Case 2. If $x < 0$, then

$$|x| \leq p \implies -x \leq p \implies -p \leq x < 0 \leq p.$$

Case 3. If $x = 0$, then $-p \leq x \leq p$ is true, so (2.139) is true. Hence (2.139) is valid in all cases.

Next we show that

$$(-p \leq x \leq p) \implies (|x| \leq p). \tag{2.140}$$

Case 1. If $x > 0$, then

$$-p \leq x \leq p \implies x \leq p \implies |x| \leq p.$$

Case 2. If $x < 0$, then

$$-p \leq x \leq p \implies -p \leq x \implies -x \leq p \implies |x| \leq p.$$

Case 3. If $x = 0$ then $x \leq p$ is true, so (2.140) is true. Hence (2.140) is true in all cases.

We have proved (2.137).

Since $P \Longleftrightarrow Q$ is true if and only if $((\text{ not } P) \Longleftrightarrow (\text{ not } Q))$ is true,

$$\text{not } (|x| \leq p) \quad \Longleftrightarrow \quad \text{not } ((-p \leq x) \text{ and } (x \leq p))\,;$$

i.e.,

$$\begin{aligned} |x| > p \quad &\Longleftrightarrow \quad (\text{ not } (-p \leq x)) \text{ or } (\text{ not } (x \leq p)) \\ &\Longleftrightarrow \quad -p > x \text{ or } x > p, \\ &\Longleftrightarrow \quad x < -p \text{ or } x > p. \end{aligned}$$

This is 2.138. ‖

2.141 Remark. I leave it to you to check that (2.137) holds when $\leq$ is replaced by $<$, and (2.138) holds when $>$ and $<$ are replaced by $\geq$ and $\leq$, respectively.

2.142 Theorem (Triangle inequality.) *Let F be an ordered field. Then*

$$\textit{for all } x, y \in F, \qquad |x + y| \leq |x| + |y|. \tag{2.143}$$

Proof: The obvious way to prove this is by cases. But there are many cases to consider, e.g. ($x < 0$ and $y > 0$ and $x + y < 0$). I will use an ingenious trick to avoid the cases. For all $x, y \in F$, we have

$$-|x| \leq x \leq |x|,$$

and

$$-|y| \leq y \leq |y|.$$

By adding the inequalities, we get

$$-(|x| + |y|) \leq x + y \leq (|x| + |y|).$$

By theorem 2.136 it follows that $|x + y| \leq |x| + |y|$. ‖

2.144 Exercise. Let F be an ordered field. For each statement below, either prove the statement, or explain why it is not true.

a) for all $x, y \in F$, $|x - y| \leq |x| + |y|$.

b) for all $x, y \in F$, $|x - y| \leq |x| - |y|$.

2.145 Exercise (Quotient formula for absolute value.) Let F be an ordered field. Let $a, b \in F$ with $a \neq 0$. Show that

a) $\left|\frac{1}{a}\right| = \frac{1}{|a|}$,

b) $\left|\frac{b}{a}\right| = \frac{|b|}{|a|}$.

2.146 Definition (Distance.) Let F be an ordered field, and let $a, b \in F$. We define the *distance from a to b* to be $|b - a|$.

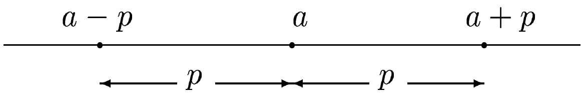
2.147 Remark. If F is the ordered field of real or rational numbers, $|b - a|$ represents the familiar notion of distance between the points a, b on the real line (or the rational line).

2.148 Exercise. Let F be an ordered field. Let $x, a, p \in F$ with $p \geq 0$. Show that

$$(|x - a| \leq p) \iff (a - p \leq x \leq a + p). \tag{2.149}$$

HINT: Use theorem 2.136. Do not reprove theorem 2.136.

2.150 Remark. We can state the result of exercise 2.148 as follows. Let $a \in F$, and let $p \in F^+$. Then the set of points whose distance from x is smaller than p, is the set of points between $a - p$ and $a + p$.



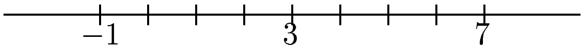
2.151 Definition (Intervals and endpoints.) Let F be an ordered field. Let $a, b \in F$ with $a \le b$. Then we define

$$\begin{array}{rcl}
(a,b) &=& \{x \in F : a < x < b\} \\
(a,b] &=& \{x \in F : a < x \le b\} \\
[a,b) &=& \{x \in F : a \le x < b\} \\
[a,b] &=& \{x \in F : a \le x \le b\} \\
(-\infty,a] &=& \{x \in F : x \le a\} \\
(-\infty,a) &=& \{x \in F : x < a\} \\
(a,\infty) &=& \{x \in F : x > a\} \\
[a,\infty) &=& \{x \in F : x \ge a\} \\
(-\infty,\infty) &=& F.
\end{array}$$

A set that is equal to a set of any of these nine types is called an *interval.* Note that $[a,a) = (a,a] = (a,a) = \emptyset$ and $[a,a] = \{a\}$, so the empty set is an interval and so is a set containing just one point. Sets of the first four types have *endpoints* a and b, except that (a,a) has no endpoints. Sets of the second four types have just one endpoint, namely a. The interval $(-\infty,\infty)$ has no endpoints.

2.152 Examples. Let F be an ordered field. By exercise 2.148 the set of solutions to $|x-3| \le 4$ is

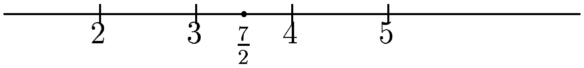
$$\{x \in F : 3-4 \le x \le 3+4\} = \{x \in F : -1 \le x \le 7\} = [-1,7].$$



I can read this result from the figure by counting 4 units to the left and right of 3. This method is just a way of remembering the result of theorem 2.148.

Now suppose I want to find the solutions in F to

$$|x-2| < |x-5| \tag{2.153}$$



Here, thinking of $|a-b|$ as the distance from a to b, I want to find all elements that are nearer to 2 than to 5. From the picture I expect the answer to be $(-\infty, \frac{7}{2})$. Although this picture method is totally unjustified by anything I've done, it is the method I would use to solve the inequality in practice. If I had to use results we've proved to solve (2.153), I'd say (since $|x-2| \geq 0$)

$$\begin{aligned}
|x-2| < |x-5| &\iff |x-2|^2 < |x-5|^2 \\
&\iff (x-2)^2 < (x-5)^2 \\
&\iff x^2 - 4x + 4 < x^2 - 10x + 25 \\
&\iff 6x < 21 \\
&\iff x < \frac{21}{6} = \frac{7}{2} \\
&\iff x \in (-\infty, \frac{7}{2})
\end{aligned}$$

which agrees with my answer by picture.

2.154 Exercise. Let F be an ordered field, let $x, a, p \in F$ with $p > 0$. Show that

$$|x-a| > p \iff x \in (-\infty, a-p) \cup (a+p, \infty).$$

Interpret the result geometrically on a number line.

2.155 Exercise. Let F be an ordered field. Express each of the following subsets of F as an interval, or a union of intervals. Sketch the sets on a number line.

a) $A = \{x \in F\colon |x-3| < 2\}$

b) $B = \{x \in F\colon |x+2| < 3\}$

c) $C = \{x \in F\colon |x-1| > 1\}$

d) $D = \{x \in F\colon |x+1| \geq 1\}$

2.156 Note. Girolamo Cardano (1501–1576), in an attempt to make sense of the square root of a negative number, proposed an alternate law of signs in which the product of two numbers is negative if at least one factor is negative. He concluded that "plus divided by plus gives plus", and "minus divided by plus gives minus", but "plus divided by minus gives nothing" (i.e. zero), since both of the assertions "plus divided by minus gives plus" and "plus divided by minus gives minus" are contradictory.[40, p 25]

I believe that our axioms for an ordered field are due to Artin and Schreier in 1926 [6, page 259].

Systems satisfying various combinations of algebraic and order axioms were considered by Huntington [28] in 1903.

The notation $|x|$ for absolute value was introduced by Weierstrass in 1841[15, vol.2, page 123]. It was first introduced for complex numbers rather than real numbers.