Chapter 3

Induction and Integers

3.1 Natural Numbers and Induction

3.1 Definition (Inductive set.) Let F be a field. A subset J of F is *inductive* if it satisfies the two conditions:

i) $0 \in J$.

ii) for all $x \in F$, $((x \in J) \implies (x+1) \in J)$.

3.2 Examples. $\mathbf{Z}, \mathbf{N}$ and $\mathbf{Q}$ are inductive sets in $\mathbf{Q}$. Every field is an inductive subset of itself.

If J is an inductive subset of F, then

$$\begin{array}{lll} 1 \in J & \text{since} & 0 \in J \text{ and } 1 = 0+1 \\ 2 \in J & \text{since} & 1 \in J \text{ and } 2 = 1+1 \\ 3 \in J & \text{since} & 2 \in J \text{ and } 3 = 2+1, \end{array}$$

etc. Hence every inductive set contains

$$\{0, 1, 2, 3, 4, 5, \cdots\}.$$

If J is an inductive subset of $\mathbf{Z}_5$, then

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

so the only inductive subset of $\mathbf{Z}_5$ is $\mathbf{Z}_5$ itself. The set

$$\left\{0, \frac{2}{2}, \frac{4}{2}, \frac{5}{2}, \frac{6}{2}, \frac{7}{2}, \frac{8}{2}, \cdots\right\}$$

is an inductive subset in $\mathbf{Q}$.

3.3 Exercise. Which of the following subsets of $\mathbf{Q}$ are inductive?

$$\begin{aligned} A &= \text{ The set of even numbers } = \{2n : n \in \mathbf{Z}\} \\ B &= \left\{n + \frac{1}{2} : n \in \mathbf{Z}\right\} \\ C &= \{x \in \mathbf{Z} : x \geq 3\} = \{3, 4, 5, \cdots\} \\ D &= \{x \in \mathbf{Z} : x \geq -3\} = \{-3, -2, -1, \cdots\} \end{aligned}$$

3.4 Exercise.

a) Find an inductive subset J of $\mathbf{Q}$, such that $J \neq \mathbf{Q}$ and $\frac{3}{4} \in J$.

b) Find an inductive subset K of $\mathbf{Q}$, such that $K \neq \mathbf{Z}$ and $\frac{3}{4} \notin K$.

3.5 Definition (Natural numbers in F.) Let F be a field, and let $n \in F$. Then n is a *natural number in F* if n is in every inductive subset of F. The set of all natural numbers in F will be denoted by $\mathbf{N}_F$.

3.6 Example. By the first example in 3.2, for every field F

$$0 \in \mathbf{N}_F, 1 \in \mathbf{N}_F, 2 \in \mathbf{N}_F, 3 \in \mathbf{N}_F, \cdots.$$

If $F = \mathbf{Z}_5$, $\mathbf{N}_F = \mathbf{Z}_5$.

3.7 Remark. By the definition of $\mathbf{N}_F$, $\mathbf{N}_F$ is a subset of every inductive subset of F, i.e.,

$$\text{If } n \in \mathbf{N}_F, \text{ and } J \text{ is inductive, then } n \in J.$$

3.8 Theorem. *Let F be a field. Then the set $\mathbf{N}_F$ of natural numbers in F is an inductive set.*

Proof: Since 0 is in every inductive set, $0 \in \mathbf{N}_F$. Let J be an inductive subset of F. Then for all $n \in F$,

$$\begin{aligned} n \in \mathbf{N}_F &\implies n \in J \text{ (by definition of } \mathbf{N}_F) \\ &\implies n + 1 \in J \text{ (since } J \text{ is inductive) .} \end{aligned}$$

Hence

$$\begin{aligned} n \in \mathbf{N}_F &\implies (n + 1 \in J \text{ for every inductive subset } J \text{ of } F) \\ &\implies n + 1 \in \mathbf{N}_F. \end{aligned}$$

Hence $\mathbf{N}_F$ is inductive. |||

3.9 Remark. We summarize the previous theorem and remark by saying "$\mathbf{N}_F$ is the smallest inductive subset of F." $\mathbf{N}_F$ is an inductive set, and it's a subset of every other inductive set. You should expect that

$$\mathbf{N_F} = \{0, 1, 2, 3, 4, \cdots\}$$

(whatever "$\cdots$" might mean).

3.10 Theorem (Induction theorem.) *Let F be a field, and let P be a proposition form on $\mathbf{N}_F$. Suppose that*

$$P(0) \textit{ is true .} \tag{3.11}$$

$$\textit{For all } n \in \mathbf{N}_F, (P(n) \implies P(n+1)) \textit{ is true .} \tag{3.12}$$

Then $P(n)$ is true for all $n \in \mathbf{N}_F$.

Proof: Let P be a proposition form on $\mathbf{N}_F$ satisfying (3.11) and (3.12). Let

$$T = \{n \in \mathbf{N}_F \colon P(n) \text{ is true }\}.$$

I want to show that T is inductive. Well, $0 \in T$, by (3.11). Let n be any element in F.

Case 1. $n \in T$:

$$\begin{aligned} n \in T &\implies P(n) \text{ is true} \\ &\implies P(n+1) \text{ is true (by 3.12)} \\ &\implies n+1 \in T. \end{aligned}$$

Case 2. $n \notin T$:

If $n \notin T$, then $n \in T$ is false, so $(n \in T \implies n+1 \in T)$ is true.

Thus for all $n \in F$,

$$n \in T \implies n+1 \in T.$$

This shows that T is inductive. Since every inductive set contains $\mathbf{N}_F$, $\mathbf{N}_F \subset T$; i.e., for all $n \in \mathbf{N}_F$, $P(n)$ is true. $\|$

3.13 Theorem. *Let F be a field, and let a, m be natural numbers in F. Then $a + m$ and $a \cdot m$ are in $\mathbf{N}_F$.*

Proof: Let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{“for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F)\text{” for all } n \in \mathbf{N}.$$

Then $P(0)$ says “for all $a \in \mathbf{N}_F(a+0 \in \mathbf{N}_F)$” which is true. For all $n \in \mathbf{N}_F$,

$$\begin{aligned} P(n) &\implies \text{for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F((a+n)+1 \in \mathbf{N}_F) \text{ (since } \mathbf{N}_F \text{ is inductive)} \\ &\implies \text{for all } a \in \mathbf{N}_F(a+(n+1) \in \mathbf{N}_F) \\ &\implies P(n+1). \end{aligned}$$

By the induction theorem, $P(n)$ is true for all $n \in \mathbf{N}_F$; i.e.,

$$\text{for all } n \in \mathbf{N}_F(\text{ for all } a \in \mathbf{N}_F(a+n \in \mathbf{N}_F)).$$

Now define a proposition form Q on $\mathbf{N}_F$ by

$$Q(n) = \text{“for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F)\text{” for all } n \in \mathbf{N}.$$

Then $Q(0)$ says “for all $a \in \mathbf{N}_F(a \cdot 0 \in \mathbf{N}_F)$” which is true. For all $n \in \mathbf{N}_F$,

$$\begin{aligned} Q(n) &\implies \text{for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F(a \cdot n + a \in \mathbf{N}_F) \text{ (a sum of things in } \mathbf{N}_F \text{ is in } \mathbf{N}_F) \\ &\implies \text{for all } a \in \mathbf{N}_F(a \cdot (n+1) \in \mathbf{N}_F) \\ &\implies Q(n+1). \end{aligned}$$

By the induction theorem, $Q(n)$ is true for all $n \in \mathbf{N}_F$; i.e.,

$$\text{for all } n \in \mathbf{N}_F(\text{for all } a \in \mathbf{N}_F(a \cdot n \in \mathbf{N}_F)). \ \|$$

3.14 Theorem. *Let F be an ordered field. Then for all $n \in \mathbf{N}_F$, we have*

$$n = 0 \text{ or } n \geq 1.$$

Proof: Define a proposition form P on $\mathbf{N}_F$ by

$$P(n) = \text{“}n = 0 \text{ or } n \geq 1\text{” for all } n \in \mathbf{N}_F.$$

Clearly $P(0)$ is true. let $n \in \mathbf{N}_F$. To show that $P(n) \implies P(n+1)$, I'll show that $n = 0 \implies P(n+1)$ and that $n \geq 1 \implies P(n+1)$. Well

$$n = 0 \implies n+1 = 1 \implies n+1 \geq 1 \implies P(n+1)$$

and

$$n \geq 1 \implies n+1 \geq 1+1 > 1 \implies n+1 \geq 1 \implies P(n+1).$$

Hence $P(n) \implies P(n+1)$, and by induction $P(n)$ is true for all $n \in \mathbf{N}_F$. $\|$

3.15 Corollary. *Let F be an ordered field. Then there is no element $x \in \mathbf{N}_F$ such that*

$$0 < x < 1.$$

3.16 Lemma. *Let F be an ordered field. Then*

$$\textit{for all } n \in \mathbf{N}_F, (n-1 \in \mathbf{N}_F \textit{ or } n = 0) \tag{3.17}$$

Proof: Define a proposition form P on $\mathbf{N}_F$ by

$$P(n) = \text{“}(n-1 \in \mathbf{N}_F) \text{ or } (n = 0)\text{” for all } n \in \mathbf{N}_F. \tag{3.18}$$

Then $P(0)$ is true. Let $n \in \mathbf{N}_F$. To show that $P(n) \implies P(n+1)$, I'll show that $(n-1 \in \mathbf{N}_F) \implies P(n+1)$ and that $(n = 0) \implies P(n+1)$. Well,

$$\big(n-1 \in \mathbf{N}_F\big) \implies \big((n-1)+1 \in \mathbf{N}_F\big) \implies \big((n+1)-1 \in \mathbf{N}_F\big) \implies P(n+1),$$

and

$$(n = 0) \implies \big((n+1) - 1 = 0\big) \implies \big((n+1) - 1 \in \mathbf{N}_F\big) \implies P(n+1).$$

Hence $P(n) \implies P(n+1)$, and by induction, $P(n)$ is true for all $n \in \mathbf{N}_F$. ‖

3.19 Theorem. *Let F be an ordered field and let $p, k \in \mathbf{N}_F$. Then*

$$p - k \in \mathbf{N}_F \textit{ or } p - k < 0.$$

Proof: For each $p \in \mathbf{N}_F$ define a proposition form P_p on $\mathbf{N}_F$ by

$$P_p(n) = \text{“}p - n \in \mathbf{N}_F \text{ or } p - n < 0\text{” for all } n \in \mathbf{N}_F.$$

I'll show that for each $p \in \mathbf{N}_F$, $P_p(n)$ is true for all $n \in \mathbf{N}_F$. Now $P_p(0)$ says “$p \in \mathbf{N}_F$ or $p < 0$” which is true, since $p \in \mathbf{N}_F$. Now let $n \in \mathbf{N}_F$. To show that $P_p(n) \implies P_p(n+1)$, I'll show that

$$p - n \in \mathbf{N}_F \implies P_p(n+1)$$

and that

$$p - n < 0 \implies P_p(n+1).$$

By the previous lemma

$$\begin{aligned} p-n\in \mathbf{N}_F &\implies (p-n)-1\in \mathbf{N}_F \text{ or } p-n=0\\ &\implies p-(n+1)\in \mathbf{N}_F \text{ or } p-(n+1)=-1\\ &\implies p-(n+1)\in \mathbf{N}_F \text{ or } p-(n+1)<0\\ &\implies P_p(n+1). \end{aligned}$$

Also

$$\begin{aligned} p-n<0 &\implies (p-n)-1<-1 \implies p-(n+1)<-1<0\\ &\implies p-(n+1)<0\\ &\implies P_p(n+1). \end{aligned}$$

This completes the proof that $P_p(n) \implies P_p(n+1)$, so by induction $P_p(n)$ is true for all $n\in\mathbf{N}_F$. |||

3.20 Corollary. Let F be an ordered field, and let $p,k\in\mathbf{N}_F$. If $p\geq k$, then $p-k\in\mathbf{N}_F$.

3.21 Theorem. *Let F be an ordered field and let $p\in\mathbf{N}_F$. Then there is no natural number k such that $p<k<p+1$. In other words,*

$$\textit{for all } k,p\in\mathbf{N}_F(k>p\implies k\geq p+1).$$

Proof: Suppose

$$p<k<p+1. \tag{3.22}$$

Then

$$0<k-p<1.$$

Since $k-p>0$, the previous theorem says $k-p\in\mathbf{N}_F$. This contradicts corollary 3.15, so (3.22) is false. |||

3.23 Theorem (Least Element Principle.) *Let F be an ordered field. Then every non-empty subset S of $\mathbf{N}_F$ contains a least element, i.e. if $S\neq\emptyset$, then there is some element $k\in S$ such that $k\leq n$ for all $n\in S$.*

Proof: I will show that if S is a subset of $\mathbf{N}_F$ having no least element, then $S=\emptyset$.

Let S be a subset of $\mathbf{N}_F$ having no least element. For each $n \in \mathbf{N}_F$ define a proposition $P(n)$ by

$$P(n) = \text{“For all } k \in S, (k > n)\text{”}.$$

Now $0 \notin S$, since if 0 were in S it would be a least element for S. Hence all elements in S are greater than 0, and $P(0)$ is true. Now let n be a generic element of $\mathbf{N}_F$. Then

$$\begin{aligned} P(n) &\implies \text{for all } k \in S, (k > n) \\ &\implies \text{for all } k \in S, (k \geq n+1) \\ &\implies \text{for all } k \in S, (k > n+1) \end{aligned}$$

since if $n+1$ were in S, it would be a least element for S. Thus

$$P(n) \implies P(n+1),$$

and by induction, $P(n)$ is true for all $n \in \mathbf{N}_F$. It follows that $S = \emptyset$, since if S contained an element n, then $P(n)$ would say that $n > n$. |||

3.24 Exercise. Let F be an ordered field. Show that there is a non-empty subset S of F^+ that has no smallest element, i.e. there is a set $S \subset F^+$ such that

$$\text{for every } a \in S \text{ there is some } b \in S \text{ with } b < a.$$

3.25 Example. Let F be an ordered field. Let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{“}n^2 > \frac{1}{2}(n^2+n).\text{”} \tag{3.26}$$

Then for all $n \in \mathbf{N}_F$

$$\begin{aligned} P(n) &\implies n^2 > \frac{1}{2}(n^2+n) \\ &\implies n^2 + (2n+1) > \frac{1}{2}(n^2+n) + (2n+1) \\ &\implies (n+1)^2 > \frac{1}{2}(n^2+n+4n+2) = \frac{1}{2}[(n^2+2n+1)+(n+1)+2n] \\ &\qquad = \frac{1}{2}[(n+1)^2+(n+1)] + n \geq \frac{1}{2}[(n+1)^2+(n+1)] \\ &\implies (n+1)^2 > \frac{1}{2}\left((n+1)^2+(n+1)\right) \\ &\implies P(n+1). \end{aligned}$$

Hence $P(n) \implies P(n+1)$ for all $n \in \mathbf{N}_F$. Now note:

$$\begin{aligned} &P(0) \text{ says } (0 > 0) \text{ so } P(0) \text{ is false!}\\ &P(1) \text{ says } (1 > 1) \text{ so } P(1) \text{ is false!}\\ &P(2) \text{ says } (4 > 3) \text{ so } P(2) \text{ is true.} \end{aligned}$$

Since $P(0)$ is false, I cannot apply the induction theorem. Notice that when I prove $P(n) \implies P(n+1)$ I do *not* assume that $P(n)$ is true. (Although I might as well, since I know $P(n) \implies P(n+1)$ is true if $P(n)$ is false.)

3.27 Theorem (Induction theorem generalization.) *Let F be an ordered field. Let $k \in \mathbf{N}_F$ and let P be a proposition form defined on $\{n \in \mathbf{N}_F : n \geq k\}$. Suppose*

$$P(k) \text{ is true.} \tag{3.28}$$

$$\text{For all } n \in \{n \in \mathbf{N}_F : n \geq k\} \qquad P(n) \implies P(n+1). \tag{3.29}$$

Then $P(n)$ is true for all $n \in \{n \in \mathbf{N}_F : n \geq k\}$.

Proof: Let Q be the proposition form on $\mathbf{N}_F$ defined by

$$Q(n) = P(n+k) \text{ for all } n \in \mathbf{N}_F$$

(observe that $n \in \mathbf{N}_F \implies n+k \in \{n \in \mathbf{N}_F : n \geq k\}$ so $Q(n)$ is defined). Then $Q(0) = P(k)$, so $Q(0)$ is true by (3.28). For all $n \in \mathbf{N}_F$,

$$\begin{aligned} Q(n) &\iff P(n+k) \implies P\left((n+k)+1\right)\\ &\iff P\left((n+1)+k\right) \iff Q(n+1) \end{aligned}$$

so

$$Q(n) \implies Q(n+1).$$

By the induction theorem, $Q(n)$ is true for all $n \in \mathbf{N}_F$; i.e., $P(n+k)$ is true for all $n \in \mathbf{N}_F$. To complete the proof, I need to show that

$$\{n+k : n \in \mathbf{N}_F\} = \{n \in \mathbf{N}_F : n \geq k\}.$$

It is clear that

$$\{n+k : n \in \mathbf{N}_F\} \subset \{n \in \mathbf{N}_F : n \geq k\}.$$

To show the opposite inclusion, observe that if $n \in \mathbf{N}_F$ and $n \geq k$, then $n = (n-k)+k$, and by theorem 3.19, $n - k \in \mathbf{N}_F$. ‖

3.30 Example. Let F be an ordered field, and let P be the proposition form on $\mathbf{N}_F$ defined by

$$P(n) = \text{“}n^2 > \frac{1}{2}(n^2 + n).\text{”}$$

In example 3.25, we showed that $P(n) \implies P(n+1)$ for all $n \in \mathbf{N}_F$ and that $P(2)$ is true. Hence, by our generalized induction theorem we can conclude that $P(n)$ is true for all $n \in \mathbf{N}_F$ with $n \geq 2$.

3.31 Exercise. Let F be a field and let $x \in \mathbf{N}_F$. We say x is *even* if $x = 2 \cdot y$ for some $y \in \mathbf{N}_F$, and we say x is *odd* if $x = 2 \cdot z + 1$ for some $z \in \mathbf{N}_F$.

a) What are the even numbers in $\mathbf{Z}_5$?

b) What are the odd numbers in $\mathbf{Z}_5$?

3.32 Exercise.

a) Let F be a field. Prove that every element in $\mathbf{N}_F$ is either even or odd. HINT: Let $P(n) =$ “n is even or n is odd”.

b) Let F be an ordered field. Prove that no element of $\mathbf{N}_F$ is both even and odd. Why doesn't this contradict the result of exercise 3.31?

3.33 Note. The question of whether to consider 0 to be a natural number is not settled. Some authors start the natural numbers at 0, other authors start them at 1. It is interesting to note that Aristotle did not consider 1 to be a number.

> ... for “one” signifies a measure of some plurality, and “a number” signifies a measured plurality or a plurality of measures. Therefore, it is also with good reason that unity is not a number; for neither is a measure measures, but a measure is a principle, and so is unity .... [5, page 237, N, 1, 1088a5]

Zero was first recognized to be a number around the ninth century. According to [31, page 185] Mahavira (ninth century) noted that any number multiplied by zero produces zero, and any number divided by zero remains unchanged! Bhaskara (1114–1185) said that a number divided by 0 is called an infinite quantity.

Although arguments that are essentially arguments by induction appear in Euclid, the first clear statement of the induction principle is usually credited to Blaise Pascal (1623-1662) who used induction to prove properties of Pascal's Triangle.[36, page 73]

I believe that the idea of defining the natural numbers to be things that are in every inductive set should be credited to Giuseppe Peano [37, page 94, Axiom 9]. In 1889, Peano gave a set of axioms for natural numbers $\mathbf{N}$ (starting with 1), one of which can be paraphrased as: If K is any set, such that $1 \in K$ and for all $x \in \mathbf{N}$, $(x \in K \implies x + 1 \in K)$, then $\mathbf{N} \subset K$.

3.2 Integers and Rationals.

3.34 Definition (Integers in F.) Let F be a field. We define an element z in F to be an *integer in F* if and only if z can be written as the difference of two natural numbers; i.e., if and only if

$$z = q - p \text{ for some } p, q \in \mathbf{N}_F.$$

We denote the set of integers in F by $\mathbf{Z}_F$.

3.35 Exercise. What are the integers in $\mathbf{Z}_5$?

3.36 Exercise. Let F be a field. Show that for all $x, y \in F$,

$$x \in \mathbf{Z}_F \text{ and } y \in \mathbf{Z}_F \implies x + y \in \mathbf{Z}_F$$

and that

$$x \in \mathbf{Z}_F \text{ and } y \in \mathbf{Z}_F \implies x \cdot y \in \mathbf{Z}_F.$$

Also show that $x \in \mathbf{Z}_F \implies -x \in \mathbf{Z}_F$.

3.37 Theorem. *Let F be an ordered field and let $-\mathbf{N}_F = \{-x : x \in \mathbf{N}_F\}$. Then*

$$\mathbf{Z}_F = \mathbf{N}_F \cup (-\mathbf{N}_F) \textit{ and } \mathbf{N}_F \cap (-\mathbf{N}_F) = \{0\}.$$

Proof:

$$n \in \mathbf{N}_F \implies n = n - 0 \in \mathbf{Z}_F$$

and

$$n \in -\mathbf{N}_F \implies -n \in \mathbf{N}_F \implies 0 - (-n) \in \mathbf{Z}_F \implies n \in \mathbf{Z}_F.$$

Hence, $\mathbf{N}_F \subset \mathbf{Z}_F$ and $-\mathbf{N}_F \subset \mathbf{Z}_F$, so

$$\mathbf{N}_F \cup (-\mathbf{N}_F) \subset \mathbf{Z}_F. \tag{3.38}$$

Now suppose $n \in \mathbf{Z}_F$. Then $n = p - q$ where $p, q \in \mathbf{N}_F$. If $p - q \geq 0$, then $p - q \in \mathbf{N}_F$. If $p - q \leq 0$, then $q - p \geq 0$, so $q - p \in \mathbf{N}_F$, so $-(p-q) \in \mathbf{N}_F$, so $-n \in \mathbf{N}_F$, so $n \in -\mathbf{N}_F$. Therefore, $n \in \mathbf{N}_F$ or $n \in -\mathbf{N}_F$; i.e., $n \in \mathbf{N}_F \cup -\mathbf{N}_F$, so

$$\mathbf{Z}_F \subset \mathbf{N}_F \cup (-\mathbf{N}_F).$$

This combined with (3.38) shows that $\mathbf{Z}_F = \mathbf{N}_F \cup (-\mathbf{N}_F)$. Since all elements of $\mathbf{N}_F$ are ≥ 0, and all elements of $-\mathbf{N}_F$ are ≤ 0, it follows that $\mathbf{N}_F \cap (-\mathbf{N}_F) \subset \{0\}$, and clearly $0 \in \mathbf{N}_F \cap -\mathbf{N}_F$, so $\mathbf{N}_F \cap (-\mathbf{N}_F) = \{0\}$. |||

3.39 Definition (Rational numbers in F.) Let F be a field. Let

$$\mathbf{Q}_F = \left\{ \frac{n}{m} : n, m \in \mathbf{Z}_F \text{ and } m \neq 0 \right\}.$$

The elements of $\mathbf{Q}_F$ will be called *rational numbers* in F. We note $0 = \dfrac{0}{1} \in \mathbf{Q}_F$ and $1 = \dfrac{1}{1} \in \mathbf{Q}_F$.

3.40 Theorem. *Let F be a field. Then the set $\mathbf{Q}_F$ of rational numbers in F form a field (with the operations of F).*

Proof: The various commutative, associative and distributive laws hold in $\mathbf{Q}_F$, because they hold in F, and we've noted that the additive and multiplicative identities of F are in $\mathbf{Q}_F$, and they act as identities in $\mathbf{Q}_F$ because they are identities in F. We note that $+$ and $\cdot$ define binary operations on $\mathbf{Q}_F$; i.e., the sum and product of elements in $\mathbf{Q}_F$ is in $\mathbf{Q}_F$. Let $a, b \in \mathbf{Q}_F$ write $a = \dfrac{p}{q}$, $b = \dfrac{r}{s}$ where $p, q, r, s \in \mathbf{Z}_F$ and $q \neq 0$, $s \neq 0$. Then

$$\begin{aligned} a + b &= \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \\ a \cdot b &= \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \end{aligned}$$

and $ps+qr, qs, pr$ are all in $\mathbf{Z}_F$ and $q\cdot s\neq 0$. Hence $a+b$ and $a\cdot b$ are in $\mathbf{Q}_F$. Also, $-a = -\left(\dfrac{p}{q}\right) = \dfrac{-p}{q}$ where $-p, q\in\mathbf{Z}_F$, so $-a\in\mathbf{Q}_F$ and

$$\begin{aligned} b\neq 0 \quad &\Longrightarrow \quad b=\frac{r}{s} \text{ where } r,s\neq 0 \quad r,s\in\mathbf{Z}_F \\ &\Longrightarrow \quad b^{-1}=\frac{s}{r} \\ &\Longrightarrow \quad b^{-1}\in\mathbf{Q}_F. \end{aligned}$$

Hence $\mathbf{Q}_F$ is a field. |||

3.41 Definition (Even and odd.) In exercise 3.31 we defined *even* and *odd* natural numbers. We now extend this definition to integers. Let F be a field and let $x\in\mathbf{Z}_F$. We say x is even if and only if $x=2y$ for some $y\in\mathbf{Z}_F$, and we say x is odd if and only if $x=2z+1$ for some $z\in\mathbf{Z}_F$.

3.42 Remark. In exercise 3.32 you showed that in an ordered field, every element of $\mathbf{N}_F$ is even or odd, and no element of $\mathbf{N}_F$ is both even and odd. Since $\mathbf{Z}_F=\mathbf{N}_F\cup -\mathbf{N}_F$, it follows fairly easily that if F is an ordered field, then every element of $\mathbf{Z}_F$ is even or odd, and no element of $\mathbf{Z}_F$ is both even and odd.

3.43 Exercise.

a) Let F be a field, and let $n\in\mathbf{Z}_F$. Show that

$$n \text{ is even} \implies n^2 \text{ is even,}$$

and

$$n \text{ is odd} \implies n^2 \text{ is odd.}$$

b) Let F be an ordered field and let $n\in\mathbf{Z}_F$. Show that

$$\begin{aligned} n^2 \text{ is even} &\implies n \text{ is even} \\ n^2 \text{ is odd} &\implies n \text{ is odd.} \end{aligned}$$

I want to show that in any ordered field F, 2 is not a square in $\mathbf{Q}_F$. To show this I will use the following lemma.

3.44 Lemma. *Let F be an ordered field. Then every element in $\mathbf{Q}_F$ can be written as $\dfrac{m}{n}$, where $m, n \in \mathbf{Z}_F$ and m, n are not both even.*

Proof: Let F be an ordered field, and let $r \in \mathbf{Q}_F$. Then $r = \dfrac{m}{n}$ where $m, n \in \mathbf{Z}_F$ and $n \neq 0$. Since $r = \dfrac{-m}{-n}$, we may assume without loss of generality that $n > 0$. Then $n \in \mathbf{N}_F$ so we can write any element of $\mathbf{Q}_F$ in the form $r = \dfrac{m}{n}$ where $m \in \mathbf{Z}_F$, $n \in \mathbf{N}_F$ and $n \geq 1$. Let

$$S = \left\{ q \in \mathbf{N}_F : \text{ for some } p \in \mathbf{Z}_F \left(r = \frac{p}{q} \right) \right\}.$$

Then $n \in S$, since $r = \frac{m}{n}$. By the least element principle, S has a least element k. We have

$$r = \frac{p}{k} \text{ for some } p \in \mathbf{Z}_F.$$

Then p and k are not both even, since if $p = 2P$ and $k = 2K$ where P and K are in $\mathbf{Z}_F$, then

$$r = \frac{p}{k} = \frac{2P}{2K} = \frac{P}{K},$$

and hence $K \in S$. But this is impossible because $K = \frac{1}{2}k < k$, i.e. K is less than the least element for S. ‖

3.45 Theorem. *Let F be an ordered field. Then 2 is not a square in $\mathbf{Q}_F$.*

Proof: Suppose there were an element $r \in \mathbf{Q}_F$ such that $r^2 = 2$. By our lemma, we can write $r = \dfrac{m}{n}$ where $m, n \in \mathbf{Z}_F$, m, n not both even. Now

$$\begin{aligned} r^2 = 2 \implies & \frac{m^2}{n^2} = 2 \\ \implies & m^2 = 2 \cdot n^2 \\ \implies & m \text{ is even (since } n^2 \in \mathbf{Z}_F). \end{aligned}$$

Now

$$m \text{ is even } \implies m = 2k \text{ for some } k \in \mathbf{Z}_F,$$

so

$$\begin{aligned} r^2 = 2 &\implies m^2 = 2\cdot n^2 \\ &\implies (2k)^2 = 2\cdot n^2 \\ &\implies 2^2k^2 = 2n^2 \\ &\implies 2k^2 = n^2 \\ &\implies n^2 \text{ is even} \\ &\implies n \text{ is even.} \end{aligned}$$

Thus the statement $r^2 = 2$ implies (m is even and n is even and m, n are not both even), which is false. The theorem follows. |||

3.46 Note.

When Plato (427?–347B.C.) wrote *The Laws*, he lamented that most Greeks at the time believed that all numbers were rational (i.e. that all lines are commensurable):

> ATHENIAN: My dear Cleinias, even I took a very long time to discover mankind's plight in this business; but when I did, I was amazed, and could scarcely believe that human beings could suffer from such swinish stupidity. I blushed not only for myself, but for Greeks in general.
>
> CLEINIAS: Why so? Go on, sir, tell us what you're getting at. ...
>
> ATHENIAN: The real relationship between commensurables and incommensurables. We must be very poor specimens if on inspection we can't tell them apart. These are the problems we ought to keep on putting up to each other, in a competitive spirit, when we've sufficient time to do them justice; and it's a much more civilized pastime for old men then draughts.
>
> CLEINIAS: Perhaps so. Come to think of it, draughts is not radically different from such studies.
>
> ATHENIAN: Well, Cleinias, I maintain that these subjects are what the younger generation should go in for. They do no harm, and are not very difficult: they can be learnt in play, and so far from harming the state, they'll do it some good[39, book vii,820].

However, when Aristotle (384-322 BC) wrote the *Priora Analytica*, he assumed that his reader was familiar with the proof of theorem 3.45 just given. The following quotation would not be understood by anyone who did not know that proof.

> For all who effect an argument *per impossible* infer syllogistically what is false, and prove the initial conclusion hypothetically when something impossible results from the assumption of its contradictory; e.g., that the diagonal of the square is incommensurate with the side, because odd numbers are equal to evens if it is supposed to be commensurate. One infers syllogistically that odd numbers come out equal to evens, and one proves hypothetically the incommensurability of the diagonal since a falsehood results through contradicting this.[4, 1-23, 41a, 23-31]

The meaning of the word "rational" has changed since the time of Euclid. He would have said that a line of length $\sqrt{2}$ was rational, but a rectangle of area $\sqrt{2}$ was irrational. The following quotation is from book X of *The Elements*[19, vol 3, p10, definitions 3 and 4].

> Let then the assigned straight line be called *rational*, and those straight lines which are commensurable with it, whether in length and in square or in square only, *rational*, but those which are incommensurable with it *irrational.*
>
> 4. And let the square on the assigned straight line be called *rational*, and those areas which are commensurable with it *rational*, but those which are incommensurable with it *irrational.*

3.47 Warning. An early commentator on Euclid (quoted in [19, vol III page1]) suggested that perhaps

> $\cdots$ everything irrational and formless is properly concealed, and, if any soul should rashly invade this region of life and lay it open, it would be carried away into the sea of becoming and be overwhelmed by its unresting currents.

3.48 Notation ($\mathbf{N}, \mathbf{Z}, \mathbf{Q}$.) We have defined natural numbers $\mathbf{N}_F$ in any field F, and we've seen that the natural numbers in $\mathbf{Z}_5$ and the natural numbers in $\mathbf{Q}$ are quite different. However, if F is an ordered field, then

$$\mathbf{N}_F = \{0, 1, 2, 3, 4, \cdots\}$$

where the list contains no repetitions, since when we add a new term to the list we get something greater than every element already in the list. Hence if F, G are two ordered fields then $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same". We will denote the natural numbers in an ordered field by $\mathbf{N}$, and call $\mathbf{N}$ "the natural numbers". Since we defined $\mathbf{Z}_F$ in terms of $\mathbf{N}_F$, and we defined $\mathbf{Q}_F$ in terms of $\mathbf{Z}_F$, the integers in any two ordered fields are "essentially the same" and the rationals in any two ordered fields are "essentially the same". We will denote the integers in any ordered field by $\mathbf{Z}$, and call $\mathbf{Z}$ "the integers".

$$\mathbf{Z} = \mathbf{N} \cup -\mathbf{N} = \{0, 1, -1, 2, -2, 3, -3, \cdots\}.$$

Similarly we will call the rational numbers in an ordered field $\mathbf{Q}$, and call $\mathbf{Q}$ "the rational numbers"

$$\mathbf{Q} = \left\{\frac{n}{m} : n, m \in \mathbf{Z},\ \ , m \neq 0\right\}.$$

3.49 Remark. One can define formally what it means to say $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same," and one can prove that if F, G are ordered fields, then $\mathbf{N}_F$ and $\mathbf{N}_G$ are "essentially the same" (e.g., see [35, page 35]).

However, one can also construct ordered fields F and G such that $\mathbf{N}_F$ and $\mathbf{N}_G$ are radically different! (see [41]) The reason that both of these apparently contradictory things can happen is that our definition of $\mathbf{N}_F$ involves looking at the set of all inductive subsets of F, and our vague notions of set and function are just too imprecise to deal with this delicate question. The two quoted contradictory results are proved using different set theories, which are not consistent with each other, but both of which are more or less consistent with everything we've used about sets.

3.3 Recursive Definitions.

Our definition of function $f: A \to B$ involved the undefined word "rule". If I define $f: \mathbf{N} \to \mathbf{N}$ by

$$f(n) = 2 \cdot n + 1 \text{ for all } n \in \mathbf{N}$$

the rule is perfectly clear. I will often want to define functions by "rules" of the following sort: $f: \mathbf{N} \to \mathbf{N}$ is given by

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1) \cdot f(n) \quad \text{for all } n \in \mathbf{N}. \end{cases} \tag{3.50}$$

It is not quite so clear that this is a rule, since the right side of (3.50) involves the function I am trying to define. However, if I try to use this rule to calculate $f(4)$, I get

$$\begin{aligned} f(4) &= 4 \cdot f(3) \\ &= 4 \cdot 3 \cdot f(2) \\ &= 4 \cdot 3 \cdot 2 \cdot f(1) \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \cdot f(0) \\ &= 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \qquad (3.51) \end{aligned}$$

and by this example, you recognize that (3.50) defines the familiar factorial function. In fact, I make this my definition of the factorial function.

3.52 Definition (Factorial function.) We define $f\colon \mathbf{N} \to \mathbf{N}$ by the rules.

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1) \cdot f(n) \quad \text{for all } n \in \mathbf{N}. \end{cases}$$

We call f the *factorial function*, and denote $f(n)$ by $n!$. By definition,

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1) \cdot n!. \end{cases}$$

I could use the same rule (3.50) to define a factorial function $\mathbf{Z}_5 \to \mathbf{Z}_5$. The calculation (3.51) shows that then

$$f(4) = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 24 = 4,$$

and

$$f(5) = 5 \cdot f(4) = 5 \cdot 4 = 0.$$

but in $\mathbf{Z}_5$, $5 = 0$ so I have $f(0) = 0$, contradicting $f(0) = 1$. So I see that (3.50) is *not* a “rule”. How do I know that (3.50) is a “rule” when considered as a function from $\mathbf{N} \to \mathbf{N}$?; i.e., how do I know that no contradiction arises when I use (3.50) to calculate values for $n \in \mathbf{N}$? I have decided not to worry about this question, and to treat definitions analogous to (3.50) where functions on $\mathbf{N}$ are defined by giving $f(0)$ explicitly, and expressing $f(n+1)$ in terms of n and $f(k)$ for values of $k \le n$, as valid “rules”. Such defintions are called definitions *by recursion*. A discussion of, and justification for definitions by recursion can be found in [27].

3.53 Definition (Powers.) Let F be a field, and let $a \in F$. Define a function

$$f_a\colon \mathbf{N} \to F$$

by

$$\begin{aligned} f_a(0) &= 1. \\ f_a(n+1) &= f_a(n) \cdot a \text{ for all } n \in \mathbf{N}. \end{aligned} \tag{3.54}$$

Thus,

$$\begin{aligned} f_a(4) &= f_a(3) \cdot a \\ &= f_a(2) \cdot a \cdot a \\ &= f_a(1) \cdot a \cdot a \cdot a \\ &= f_a(0) \cdot a \cdot a \cdot a \cdot a \\ &= 1 \cdot a \cdot a \cdot a \cdot a \\ &= a \cdot a \cdot a \cdot a. \end{aligned}$$

We denote the value of $f_a(n)$ by a^n. Then we can rewrite (3.54) as

$$\begin{cases} a^0 = 1 \\ a^{n+1} = a^n \cdot a \quad \text{for all } n \in \mathbf{N}. \end{cases}$$

Note that $0^0 = 1$ and $a^1 = a$.

3.55 Theorem. *Let F be a field and let $a \in F$. Then for all $p, n \in \mathbf{N}$,*

$$a^{p+n} = a^p \cdot a^n.$$

Proof: Define a proposition form P on $\mathbf{N}$ by

$$P(n) = \text{“for all } p \in \mathbf{N}(a^{p+n} = a^p \cdot a^n)\text{” for all } n \in \mathbf{N}.$$

Then $P(0)$ says “for all $p \in \mathbf{N}(a^{p+0} = a^p \cdot a^0)$” which is true, since both sides of the equation are equal to a^p. For all $n \in \mathbf{N}$,

$$a^{p+n} \cdot a = a^{(p+n)+1} = a^{p+(n+1)},$$

and

$$(a^p a^n) \cdot a = a^p(a^n a) = a^p a^{(n+1)}.$$

Hence for all $n \in \mathbf{N}$,

$$\begin{aligned} P(n) &\Longrightarrow \text{for all } p \in \mathbf{N}(a^{p+n} = a^p a^n) \\ &\Longrightarrow \text{for all } p \in \mathbf{N}((a^{p+n}) \cdot a = (a^p a^n) \cdot a) \\ &\Longrightarrow \text{for all } p \in \mathbf{N}(a^{p+(n+1)} = a^p a^{n+1}) \\ &\Longrightarrow P(n+1). \end{aligned}$$

By induction, $P(n)$ is true for all $n \in \mathbf{N}$, i.e.

$$\text{for all } n \in \mathbf{N}\Big(\text{for all } p \in \mathbf{N}(a^{p+n} = a^p a^n)\Big). \ \|$$

3.56 Exercise. Let F be a field, and let a, b be elements of F. Show that

$$(ab)^n = a^n b^n \text{ for all } n \in \mathbf{N}.$$

3.57 Exercise. Let F be a field and let $a \in F$. Show that

$$(a^n)^m = a^{(nm)} \text{ for all } m, n \in \mathbf{N}.$$

The following results are easy to show and we will assume them.

$$\begin{aligned} &0^{n+1} = 0 \text{ for all } n \in \mathbf{N}, (\text{ but } 0^0 = 1). \\ &1^n = 1 \text{ for all } n \in \mathbf{N}. \\ &a \neq 0 \Longrightarrow (a^n \neq 0 \text{ for all } n \in \mathbf{N}). \end{aligned}$$

3.58 Remark. Let F be a field, let $a \in F \backslash \{0\}$ and let $n \in \mathbf{Z}$. We know that $n = p - q$ where $p, q \in \mathbf{N}$. Suppose we also have $n = P - Q$ where $P, Q \in \mathbf{N}$.

$$\begin{aligned} n = n &\Longrightarrow p - q = P - Q \Longrightarrow p + Q = q + P \\ &\Longrightarrow a^{p+Q} = a^{q+P} \Longrightarrow a^p a^Q = a^q a^P \\ &\Longrightarrow \frac{a^p}{a^q} = \frac{a^P}{a^Q}. \end{aligned}$$

I need this remark for the following definition to make sense.

3.59 Definition (Integer powers.) Let F be a field. If $a \in F\backslash\{0\}$ and $n \in \mathbf{Z}$, we define

$$a^n = \frac{a^p}{a^q} \text{ where } n = p - q, \quad p, q \in \mathbf{N}.$$

Note that this definition of a^{-1} is consistent with our use of a^{-1} for multiplicative inverse. Also, this definition implies that

$$1^n = 1 \text{ for all } n \in \mathbf{Z}.$$

3.60 Theorem. *Let F be a field and let $a \in F\backslash\{0\}$. Then*

$$\textit{for all } m, n \in \mathbf{Z} \ \ (a^{m+n} = a^m \cdot a^n).$$

Proof: Let $m, n \in \mathbf{Z}$, and write

$$m = p - q, \quad n = r - s \text{ where } p, q, r, s \in \mathbf{N}$$

then $p + r \in \mathbf{N}$ and $q + s \in \mathbf{N}$ and

$$\begin{aligned} a^{m+n} &= a^{(p-q)+(r-s)} = a^{(p+r)-(q+s)} \\ &= \frac{a^{p+r}}{a^{q+s}} = \frac{a^p a^r}{a^q a^s} \\ &= \frac{a^p}{a^q} \cdot \frac{a^r}{a^s} = a^m \cdot a^n. \ \|\| \end{aligned}$$

3.61 Remark. If F is a field, and $a \in F \setminus \{0\}$, then by definition 3.59 we know that

$$a^{p-q} = \frac{a^p}{a^q} \text{ for all } p, q \in \mathbf{N}.$$

It follows from theorem 3.60 that $a^q a^{p-q} = a^p$ for all $p, q \in \mathbf{Z}$, and hence

$$a^{p-q} = \frac{a^p}{a^q} \text{ for all } p, q \in \mathbf{Z}.$$

3.62 Exercise. Let F be a field, and let $a, b \in F\backslash\{0\}$. Show that

$$(ab)^n = a^n b^n \text{ for all } n \in \mathbf{Z}.$$

3.63 Corollary (to Exercise 3.62) *Let F be a field, and let $a, b \in F \setminus \{0\}$. Then*

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} \textit{ for all } n \in \mathbf{Z}.$$

Proof: By exercise 3.62

$$\left(\frac{a}{b}\right)^n b^n = \left(\frac{a}{b}\cdot b\right)^n = a^n \text{ for all } n \in \mathbf{Z}.$$

If we multiply both sides of this equation by $(b^n)^{-1}$, we get

$$\left(\frac{a}{b}\right)^n b^n(b^n)^{-1} = a^n(b^n)^{-1},$$

i.e.

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.$$

3.64 Exercise. Let F be a field, and let $a \in F\backslash\{0\}$. Show that

$$(a^m)^n = a^{(mn)} \text{ for all } m, n \in \mathbf{Z}.$$

3.4 Summation.

3.65 Notation ($\mathbf{Z}_{\geq k}$.) Let $k \in \mathbf{Z}$. We define

$$\mathbf{Z}_{\geq k} = \{n \in \mathbf{Z}: n \geq k\}.$$

In particular $\mathbf{Z}_{\geq 0} = \mathbf{N}$.

3.66 Definition ($\sum\limits_{j=k}^{p} f(j)$) Let $k \in \mathbf{Z}$ and let $f: \mathbf{Z}_{\geq k} \to F$ be a function from $\mathbf{Z}_{\geq k}$ to a field F. Define a function $S: \mathbf{Z}_{\geq k} \to F$ by the rules

$$\begin{aligned} S(k) &= f(k) \\ S(n+1) &= S(n) + f(n+1) \text{ for all } n \in \mathbf{Z}_{\geq k}. \end{aligned}$$

Hence, for $k = 2$,

$$\begin{aligned} S(5) &= S(4) + f(5) \\ &= S(3) + f(4) + f(5) \\ &= S(2) + f(3) + f(4) + f(5) \\ &= f(2) + f(3) + f(4) + f(5). \end{aligned}$$

We denote $S(p)$ by $\sum\limits_{j=k}^{p} f(j)$ for all $p \in \mathbf{Z}_{\geq k}$. Thus,

$$\sum_{j=k}^{k} f(j) = f(k) \tag{3.67}$$

and

$$\sum_{j=k}^{n+1} f(j) = \left(\sum_{j=k}^{n} f(j)\right) + f(n+1).$$

The letter j in (3.67) has no meaning, and can be replaced by any symbol that has no meaning in the present context. Thus $\sum\limits_{j=3}^{5} f(j) = \sum\limits_{w=3}^{5} f(w)$.

3.68 Example.

$$\begin{aligned} \sum_{j=0}^{4} j^2 &= 0^2 + 1^2 + 2^2 + 3^2 + 4^2 = 30 \\ \sum_{j=-3}^{3} j &= (-3) + (-2) + (-1) + 0 + 1 + 2 + 3 = 0. \end{aligned}$$

3.69 Remark. I will sometimes write things like

$$\sum_{j=1}^{2} \frac{1}{3-j} = \frac{1}{3-1} + \frac{1}{3-2} = \frac{1}{2} + 1 = \frac{3}{2}$$

even though my definition of summation is not strictly applicable here (since $\dfrac{1}{3-j}$ is not defined for all $j \in \mathbf{Z}_{\geq 1}$).

There are many formulas associated with summation notation that are easily proved by induction; e.g., let f, g be functions from $\mathbf{Z}_{\geq k}$ to an ordered field F, and let $c \in F$. Then

$$\sum_{j=k}^{p} f(j) + \sum_{j=k}^{p} g(j) = \sum_{j=k}^{p} [f(j) + g(j)] \text{ for all } p \in \mathbf{Z}_{\geq k}.$$

$$c \sum_{j=k}^{p} f(j) = \sum_{j=k}^{p} (c \cdot f(j)) \text{ for all } p \in \mathbf{Z}_{\geq k}.$$

If $f(j) \geq g(j)$ for all $j \in \mathbf{Z}_{\geq k}$, then $\sum\limits_{j=k}^{p} f(j) \geq \sum\limits_{j=k}^{p} g(j)$ for all $p \in \mathbf{Z}_{\geq k}$.

$\sum\limits_{j=k}^{p} f(j) = \sum\limits_{j=k}^{q} f(j) + \sum\limits_{j=q+1}^{p} f(j)$ for all $q \in \mathbf{Z}_{\geq k}, p \in \mathbf{Z}_{\geq q+1}$.

We will assume these results.

3.70 Remark. Usually induction arguments are presented less formally than I have been presenting them. In the proof of the next theorem I will give a more typical looking induction argument. (I personally find the more formal version – where a proposition is actually named – easier to understand.)

3.71 Theorem (Finite geometric series.) *Let F be a field, and let $r \in F \backslash \{1\}$. Then for all $n \in \mathbf{N}$,*

$$\sum_{j=0}^{n} r^j = \frac{1-r^{n+1}}{1-r}. \tag{3.72}$$

Proof: (By induction.) When $n = 0$, (3.72) says $\sum\limits_{j=0}^{0} r^j = \dfrac{1-r}{1-r}$ which is true since both sides are equal to 1. Now suppose that (3.72) is true for some $n \in \mathbf{N}$. Then

$$\begin{aligned} \sum_{j=0}^{n+1} r^j &= \sum_{j=0}^{n} r^j + r^{n+1} = \frac{1-r^{n+1}}{1-r} + r^{n+1} \\ &= \frac{1-r^{n+1}+r^{n+1}(1-r)}{1-r} = \frac{1-r^{(n+1)+1}}{1-r} \end{aligned}$$

so

$$\sum_{j=0}^{n+1} r^j = \frac{1-r^{(n+1)+1}}{1-r}.$$

Hence, if (3.72) holds for some $n \in \mathbf{N}$, it also holds when n is replaced by $n+1$. By induction (3.72) holds for all $n \in \mathbf{N}$. |||

3.73 Remark. I will sometimes denote $\sum\limits_{j=1}^{n} f(j)$ by $f(1)+f(2)+\cdots+f(n)$. I am not going to give a formal definition for $\cdots$, and when you see $\cdots$ written in these notes it is usually an indication that a straightforward induction argument or a recursive definition is being omitted.

3.74 Remark. The previous proof was easy, but in order to use the induction proof, I needed to know the formula. Here I will indicate how one might discover such a formula. For each $n \in \mathbf{N}$, let $S_n = 1 + r + \cdots + r^n$. Then

$$(1 + r + \cdots + r^{n+1}) = (1 + r + \cdots + r^n) + r^{n+1} = S_n + r^{n+1} \tag{3.75}$$

and

$$(1 + r + \cdots + r^{n+1}) = 1 + r(1 + r + \cdots + r^n) = 1 + rS_n.$$

Hence

$$S_n + r^{n+1} = 1 + rS_n, \tag{3.76}$$

and it follows that

$$S_n(1 - r) = 1 - r^{n+1}$$

i.e.

$$S_n = \frac{1 - r^{n+1}}{1 - r}.$$

Here I have derived the formula (3.72). If you write out the argument from line (3.75) to line (3.76), without using $\cdots$s, and using only properties of sums that we have explicitly proved or assumed, you will probably be surprised at how many implicit assumptions were made above. However all of the assumptions can be justified in a straightforward way.

3.77 Theorem (Factorization of $a^{n+1} - r^{n+1}$.) *Let F be a field, and let a, r be elements of F. Then for all $n \in \mathbf{N}$,*

$$\begin{aligned}(a^{n+1} - r^{n+1}) &= (a - r)(\sum_{j=0}^{n} a^{n-j} r^j) \qquad (3.78)\\ &= (a - r)(a^n + a^{n-1}r^1 + a^{n-2}r^2 + \cdots + a^1 r^{n-1} + r^n).\end{aligned}$$

Proof: Let $n \in \mathbf{N}$. The formula (3.72) for a finite geometric series shows that

$$(1 - r^{n+1}) = (1 - r)\sum_{j=0}^{n} r^j \text{ for all } r \in F \setminus \{1\}. \tag{3.79}$$

This formula also holds when $r = 1$, since then both sides of the equation are equal to zero, so

$$(1 - r^{n+1}) = (1 - r)\sum_{j=0}^{n} r^j \text{ for all } r \in F. \tag{3.80}$$

This proves our formula in the case $a = 1$. When $a = 0$, equation (3.78) says

$$-(r^{n+1}) = (-r) \cdot r^n$$

which is true, so we will suppose that $a \neq 0$. Then by (3.80) we have

$$\begin{aligned} a^{n+1} - r^{n+1} &= a^{n+1}\left(1 - \left(\frac{r}{a}\right)^{n+1}\right) \\ &= a^{n+1}\left(1 - \frac{r}{a}\right)\sum_{j=0}^{n}\left(\frac{r}{a}\right)^{j} = a\left(1 - \frac{r}{a}\right)\left(a^n \sum_{j=0}^{n} \frac{r^j}{a^j}\right) \\ &= (a - r)\sum_{j=0}^{n} \frac{a^n}{a^j} r^j = (a - r)\sum_{j=0}^{n} a^{n-j} r^j \ \Vert \end{aligned}$$

3.81 Remark. The solution to the problem of "factoring" an expression depends on the field over which we are working. For example, if we work over $\mathbf{Z}_7$, then

$$x^2 + 5 = (x + 3)(x + 4),$$

whereas if F is an ordered field, then $x^2 + 5$ does not factor in the form $(x + a)(x + b)$, where a and b are in F. (If $x^2 + 5 = (x + a)(x + b)$ for all $x \in F$, then by taking $x = -a$ we would get $a^2 + 5 = 0$, which is false since $a^2 + 5 > 0$ in any ordered field.)

3.82 Exercise. Factor five of the following expressions into at least two factors. Assume that all numbers appearing in your factorization are rational.

a) $a^3 - b^3$.

b) $r^p - 1$. (Here $p \in \mathbf{Z}_{\geq 2}$.)

c) $a^3 + b^3$.

d) $a^4 + b^4$.

e) $x^6 - b^6$.

f) $x^6 + a^6$.

3.83 Entertainment. Let F be a field and let $r \in F\backslash\{1\}$. For all $n \in \mathbf{Z}_{\geq 1}$, let

$$T_n = r + 2r^2 + 3r^3 + \cdots + n \cdot r^n = \sum_{j=1}^{n} jr^j.$$

By looking at $T_{n+1} - r \cdot T_n$ and using the known formula (3.72), derive the formula

$$T_n = \frac{r}{(1-r)^2}\left(1 + nr^{n+1} - (n+1)r^n\right).$$

3.84 Exercise. Let

$$S_n = \sum_{j=1}^{n} \frac{1}{j(j+1)} \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{3.85}$$

Calculate the values for S_1, S_2, S_3, S_4. Write your answers as fractions in the simplest form you can. Then guess a formula for S_n, and prove that it is valid for all $n \in \mathbf{Z}_{\geq 1}$.

3.86 Exercise. Let

$$T_n = \sum_{j=1}^{n}(2j-1) \text{ for all } n \in \mathbf{Z}_{\geq 1}. \tag{3.87}$$

Calculate the values for T_1, T_2, T_3, and T_4. Then guess a formula for T_n, and prove that your guess is correct.

3.5 Maximum Function

3.88 Definition ($\max(p,q)$**.)** Let F be an ordered field, and let $p, q \in F$. We define

$$\max(p,q) = \begin{cases} p & \text{if } p \geq q \\ q & \text{if } p < q. \end{cases}$$

Then

$$\begin{aligned} p &\leq \max(p,q) \\ q &\leq \max(p,q). \end{aligned}$$

3.89 Definition ($\max\limits_{j\leq n\leq l} f(n)$.) Let F be an ordered field, let $j \in \mathbf{Z}$ and let $f\colon \mathbf{Z}_{\geq j} \to F$ be a function. Define $M\colon \mathbf{Z}_{\geq j} \to F$ by the rules

$$\begin{aligned} M(j) &= f(j) \\ M(n+1) &= \max\left(f(n+1), M(n)\right) \text{ for all } n \in \mathbf{Z}_{\geq j}. \end{aligned}$$

Hence, e.g., if $f(n) = (n-1)^2$,

$$\begin{aligned} M(0) &= f(0) = 1 \\ M(1) &= \max\left(f(1), M(0)\right) = \max(0,1) = 1 \\ M(2) &= \max\left(f(2), M(1)\right) = \max(1,1) = 1 \\ M(3) &= \max\left(f(3), M(2)\right) = \max(4,1) = 4. \end{aligned}$$

We write

$$M(l) = \max_{j\leq m\leq l} f(m)$$

where m is a dummy index, and we think of $M(l)$ as the largest of the numbers $\{f(j), f(j+1), \cdots, f(l)\}$. By definition

$$\max_{j\leq m\leq j} f(m) = f(j)$$

and

$$\max_{j\leq m\leq l+1} = \max\left(f(j+1), \max_{j\leq m\leq l} f(m)\right).$$

3.90 Notation ($\mathbf{Z}_{j\leq n\leq l}$.) Let $j, l \in \mathbf{Z}$ with $j \leq l$. Then

$$\mathbf{Z}_{j\leq n\leq l} = \{n \in \mathbf{Z}\colon j \leq n \leq l\}.$$

3.91 Theorem. *Let F be an ordered field, let $j \in \mathbf{Z}$ and let $f\colon \mathbf{Z}_{\geq j} \to F$ be a function. Then for all $l \in \mathbf{Z}_{\geq j}$,*

$$\textit{for all } p \in \mathbf{Z}_{j\leq m\leq l},\ f(p) \leq \max_{j\leq m\leq l} f(m). \tag{3.92}$$

Proof: Let P be the proposition form on $\mathbf{Z}_{\geq j}$ such that $P(l)$ is the proposition (3.92). Then $P(j)$ says

$$\text{for all } p \in \mathbf{Z}_{j\leq m\leq j},\ f(p) \leq \max_{j\leq m\leq j} f(m);$$

i.e.,

$$\text{for all } p \in \{j\},\ f(p) \leq f(j).$$

Hence $P(j)$ is true.

Now for all $l \in \mathbf{Z}_{\geq j}$,

$$\begin{aligned} P(l) &\implies \text{for all } p \in \mathbf{Z}_{j\leq m\leq l},\ f(p) \leq \max_{j\leq m\leq l} f(m) \\ &\implies \text{for all } p \in \mathbf{Z}_{j\leq m\leq l},\ f(p) \leq \max\Big(f(l+1), \max_{j\leq m\leq l} f(m)\Big) \\ &\qquad\qquad = \max_{j\leq m\leq l+1} f(m). \end{aligned}$$

We also have

$$f(l+1) \leq \max\Big(f(l+1), \max_{j\leq m\leq l} f(m)\Big) = \max_{j\leq m\leq l+1} f(m),$$

so

$$\begin{aligned} P(l) &\implies \text{for all } p \in \mathbf{Z}_{j\leq m\leq l} \cup \{l+1\},\ f(p) \leq \max_{j\leq m\leq l+1} f(m) \\ &\implies \text{for all } j \in \mathbf{Z}_{j\leq m\leq l+1},\ f(p) \leq \max_{j\leq m\leq l+1} \\ &\implies P(l+1). \end{aligned}$$

By induction, $P(l)$ is true for all $l \in \mathbf{Z}_{\geq j}$. |||

3.93 Note. The notation a^n for positive integer powers of a was introduced by Descartes in 1637[15, vol 1,p 346]. Both Maple and Mathematica denote a^n by `a^n`.

The notation $n!$ for the factorial of n was introduced by Christian Kramp in 1808[15, vol 2, p 66].

The use of the Greek letter Σ to denote sums was introduced by Euler in 1755[15, vol 2,p 61]. Euler writes

$$\Sigma x^2 = \frac{x^3}{3} - \frac{x^2}{2} + \frac{x}{6}.$$

The use of limits on sums was introduced by Augustin Cauchy(1789-1857). Cauchy used the notation $\sum\limits_{m}^{n}{}_{r} fr$ to denote what we would write as $\sum\limits_{r=m}^{n} f(r)$[15, vol 2, p 61].

In Maple, the value of $\sum\limits_{i=1}^{n} f(i)$ is denoted by `sum(f(i),i=1..n)` . In Mathematica it is denoted by `Sum[f[i],{i,1,n}]` .