Peano Systems and the Whole Number System

Ronald C. Freiwald, Copyright © 2009
Washington University in St. Louis

We have a good informal picture about how the whole numbers work. By the whole number system we mean to the set $\omega = \{0, 1, 2, ...\}$, together with its rules for arithmetic and for handling inequalities (for example, if $a, b, c \in \omega$ and $a < b$, then $a + c < b + c$). Informally, we know a multitude of facts about behavior involving whole numbers. $+$, $\cdot$, $=$, $<$, and $\leq$. We also know how induction works.

Ultimately, we want to show how the whole number system can be described in terms of our foundation, set theory. We want to construct a system consisting of sets, ways to combine them ($+$, $\cdot$) and ways to compare them ($<$, $\leq$) so that the system "acts just like" the whole number system. As we have said several times, mathematicians don't care about what the whole numbers "really are." If we can use set theory to build a system that "acts just like ω", then all mathematicians can agree to call that system ω .

More carefully, what do we need to do? When have we got a system "that acts just like ω"? There are so many facts we know about the whole number system that we should build into this system of sets. There may even be about facts about ω that we don't know but that ought to be included. Our job seems like a hopeless task.

To make things more manageable, it would be very helpful if we had a short list of "the crucial properties" of ω – a list from which we can prove that the other important properties of ω must also inevitably be true. Then, if we can build a system of sets which has all "the crucial properties" of ω, then our new system will include the other important properties of ω automatically.

Fortunately, there is just such a short list – axioms developed by the mathematician Giuseppe Peano in 1889. The latter part of the 19th century, and the beginning of the20th, were an "age of rigor" for mathematics – a period when firm foundations for mathematics were being established. This project was felt to be intellectually necessary. For example, calculus had by then been around for a couple of centuries and seemed to work well – at least in skilled and sensitive hands. But there was clearly a lot of vagueness about why it worked. A lack of firm foundations for the number systems (partilcularly $\mathbb{R}$) was part of the problem.

We are going to look at the list of "Peano's Axioms" and try to indicate how all the informal properties of the whole number system ω follow from the properties in the list. There are many, many details to check. We will check some of the details to indicate how (with several additional lectures) all the details could be ironed out. In not doing everything, there is no attempt to "hide" something hard. Any material we leave out is truly just "more of the same."

Definition A Peano system $\mathcal{P}$ is a collection of objects with the following properties:

P1) There is a special object in $\mathcal{P}$ named "0."
$($*Although the name " 0" is intended to suggest "the whole number zero," we really know nothing about how the object called " 0" in a Peano system acts except for what is stated in (or deducible from) the remaining axioms.*

P2) For each object $x \in \mathcal{P}$, there is exactly one object in $\mathcal{P}$ called the successor of x (for short, we write x^+ to represent the successor of x).

P3) 0 is not the successor of any object in $\mathcal{P}$:

$$(\forall x \in \mathcal{P}) \ \ x^+ \neq 0$$

P4) Different objects in $\mathcal{P}$ have different successors :

$$(\forall x \in \mathcal{P})(\forall y \in \mathcal{P}) \ \ (x \neq y \Rightarrow x^+ \neq y^+)$$

P5) Suppose $A \subseteq \mathcal{P}$. If $0 \in A$ and if $(\forall x \in \mathcal{P})\,(x \in A \Rightarrow x^+ \in A)$ is true, then $A = \mathcal{P}$.

Note: In his 1889 book, Peano went so far as to also include a few other axioms about how " $=$ " behaves: for example,

$$(\forall x \in \mathcal{P}) \ \ x = x \ \ \textit{and}$$
$$(\forall x \in \mathcal{P})(\forall y \in \mathcal{P}) \ ((x = y) \ \Rightarrow (y = x))$$

Our point of view is that " $=$ " is a logical term meaning "is the same thing as" and that such assumptions about " $=$ " do not really need to be spelled out $-$ although doing so would certainly be harmless.

A Peano system is an "abstract system" : we are given no information whatsoever about what the "objects" in $\mathcal{P}$ "really are," and we have no information about how x^+ can be found for a given $x \in \mathcal{P}$. The only things we know about the objects in $\mathcal{P}$ and their successors is what the axioms P1-P5 say about their behavior. Of course, we can logically deduce (prove) new pieces of information about $\mathcal{P}$ (theorems) from those axioms.

Until a reasonable collection of theorems about a Peano system is built up to use, the proofs of theorems will usually rely on axiom P5 $-$ which we will refer to as the induction axiom in $\mathcal{P}$.

The challenge (and the amusement) of proving things about a Peano system is that we have so little, at the beginning, to work with. We have to fight for each little new fact. But the more things we prove, the more tools we have to work with and the easier it gets.

Notice that the informal whole number system, ω, obeys each of the axioms P1-P5 provided that

i) we interpret the objects x in $\mathcal{P}$ to be whole numbers, and
ii) we interpret "successor" x^+ to mean the whole number "$x + 1$."

Under this interpretation, ω is an example of a Peano system. Of course, axiom P5 is what we called the Principle of Mathematical Induction (PMI) in ω.

When we have an abstract system like $\mathcal{P}$ and we

i) interpret all the objects and operations in $\mathcal{P}$ (such as "successor") as representing certain concrete objects and operations, and

ii) all the assumptions about the objects/operations in the abstract system become true statements about the specific objects in the interpretation

then we say we have found a concrete model for the abstract system. Thus, ω is a model for the abstract Peano system $\mathcal{P}$.

Some Theorems About a Peano System $\mathcal{P}$

To illustrate dealing with an abstract system, we will prove some simple theorems about $\mathcal{P}$ that follow from P1-P5. (*The theorems follow logically from the axioms P1-P5. Because P1-P5 (as interpreted in the model ω), each theorem must also be true when interpreted the same way as as statement about ω . For example, see the italicized interpretation of Theorem 1 in the model ω.*)

Theorem 1 For all $x \in \mathcal{P}$, either $x = 0$ or $(\exists y \in \mathcal{P})\ x = y^+$ (that is, every nonzero x in $\mathcal{P}$ is a successor). (*Interpreted in the model ω, Theorem 1 says that for each nonzero whole number x, there is a whole number y such that $x = y + 1$.*)

Proof Let $A = \{x \in \mathcal{P} : x = 0$ or $(\exists y \in \mathcal{P})\ x = y^+\} = \{x \in \mathcal{P} : x = 0$ or x is a successor$\}$. We need to show (using P5) that $A = \mathcal{P}$.

i) By definition of A, $0 \in A$
ii) Suppose $x \in A$. Then $x^+ \in A$ because x^+ is a successor (namely, the successor of x).

By the induction axiom P5, we conclude that $A = \mathcal{P}$. ●

A corollary is a theorem that follows as a relatively quick and easy consequence of a previous theorem.

Corollary 2 If $x \in \mathcal{P}$ and $x \neq 0,$ then $(\exists!\, y \in \mathcal{P})\ x = y^+.$

Proof Theorem 1 gives that if $x \neq 0$, then $(\exists\, y \in \mathcal{P})\ x = y^+$

To show uniqueness, notice that if $x = y^+$ and $x = z^+,$ then $y^+ = z^+$, so $y = z$ (using the contrapositive of P4). •

Definition If $x = y^+$ in $\mathcal{P}$, we call y the predecessor of x.

Notice that the definition makes sense: we can say the predecessor because (from Corollary 2) there can't be more than one predecessor for x. Corollary 2 therefore says that each nonzero element x in $\mathcal{P}$ has a unique predecessor.

Theorem 3 For all $x \in \mathcal{P},\ x \neq x^+$ (*that is, no object x in $\mathcal{P}$ is its own successor*).

Proof Homework exercise

Theorem 4 *If $x \in \mathcal{P}$, then either $x = 0$ or x can be obtained from 0 by applying the successor operation to 0 a finite number of times.*

Proof *Let $A = \{x \in \mathcal{P} :\ x = 0$ or x can be obtained from 0 by applying the successor operation to 0 a finite number of times$\}$.*

$0 \in A$ *(by definition of A)*

Suppose $x \in A$. We prove that $x^+ \in A$.

If $x = 0,$ then $x^+ \in A$ because $x^+ = 0^+$ can be obtained by applying the successor operation just one time.

If $x \neq 0$, then (because $x \in A$) x can be obtained from 0 by a finite number of successor operations. But then one additional application of the successor operation produces x^+. Therefore $x^+ \in A$.

By the Induction Axiom P5), $A = \mathcal{P}$, which proves the theorem. •

Corollary 5 *If $x, y \in \mathcal{P}$ and $x \neq y$, then one of x or y can be obtained from the other by applying the successor operation a finite number of times.*

Proof *If one of x or y is 0 (say, $x = 0)$ then Theorem 4 says we can obtain y by applying the successor operation to x a finite number of times.*

If neither x nor y is 0, then (by Theorem 4) we can obtain both x and y by from 0 using the successor operation. Applying the successor operation to 0, we arrive first at (say) x; and then continuing to apply the successor operation an additional number of times produces y. ●

NOTE: *Theorem 4 and Corollary 5 are italicized because we will not use them in any proofs that come later. In fact a "purist" might object that if we are trying to formally develop a theory of Peano systems in order to define the system of whole numbers ω, then we should not be allowed to use an argument that involves doing something "a finite number of times" – objecting that we can't formally say what "a finite number of times" means until after we have defined the whole number system.*

Nevertheless, it seemed like it would be helpful to include the italicized results to help build up our intuitive picture of what a Peano system $\mathcal{P}$ "looks like" – as discussed in the next section.

See Theorem 13.

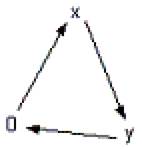
All Peano systems are “the same”

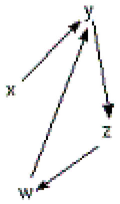
What does a Peano system “look like” ? We can get an idea with a schematic diagram in which an arrow “ $\rightarrow$ ” points to “the successor.” We start with 0, which has no predecessor:

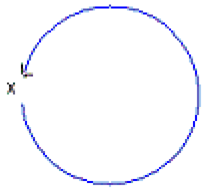
$$0 \rightarrow 0^{+} \rightarrow (0^{+})^{+} \rightarrow \ldots \quad \rightarrow x \rightarrow x^{+} \rightarrow \ldots$$

Theorem 4 tells us that every nonzero object $x \in \mathcal{P}$ appears in this diagram eventually, after applying the successor a sufficient number of times.

When we make the diagram, it will always “keep on going forward” – that is, there will never be any “backward loops” like







Which axiom says that the first loop is impossible? the second? Why is the third loop impossible ?

Thus we can informally picture a Peano system $\mathcal{P}$ as an “infinite linear chain” starting at its special element, 0:

$$0 \rightarrow 0^{+} \rightarrow (0^{+})^{+} \rightarrow \ldots \quad \rightarrow x \rightarrow x^{+} \rightarrow \ldots \text{ (and so on, forever)}$$

All Peano systems must look the same. The technical phrase for this is that all Peano Systems are isomorphic. To be a little more precise, this means that if we have two Peano systems $\mathcal{P}$ and $\boldsymbol{\mathcal{P}}$ (we use **boldface** for the second Peano system and its objects), then it is possible

i) to pair off all the elements of $\mathcal{P}$ with all the elements of $\boldsymbol{\mathcal{P}}$ in such a way that so that each object in one system has a unique "partner" in the other system.

ii) to do this not just with some "random" pairing, but to do it in such a way that 0 is paired with $\mathbf{0}$ and the pairing respects the successor operation: if $x \in \mathcal{P}$ is partnered with $\boldsymbol{x} \in \boldsymbol{\mathcal{P}}$, then x^+ (in $\mathcal{P}$) is partnered with $\boldsymbol{x}^{\boldsymbol{+}}$ (in $\boldsymbol{\mathcal{P}}$)) : in other words, "the successor of partner is the partner of the successor."

Our images of these systems would then look like this $-$ where vertical arrows indicate the "pairing":

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, leftrightarrow] & 0^+ \arrow[r] \arrow[d, leftrightarrow] & (0^+)^+ \arrow[r] \arrow[d, leftrightarrow] & \ldots \arrow[r] & x \arrow[r] \arrow[d, leftrightarrow] & x^+ \arrow[r] \arrow[d, leftrightarrow] & \ldots & \text{(and so on, forever)} \\
\mathbf{0} \arrow[r] & \mathbf{0}^{\mathbf{+}} \arrow[r] & (\mathbf{0}^{\mathbf{+}})^{\mathbf{+}} \arrow[r] & \ldots \arrow[r] & \boldsymbol{x} \arrow[r] & \boldsymbol{x}^{\boldsymbol{+}} \arrow[r] & \ldots & \text{(and so on, forever)}
\end{tikzcd}$$

A slightly different way to think of this isomorphic "pairing" is just to imagine that each object x in $\mathcal{P}$ has been "renamed" subject to the following rules:

i) 0 is renamed as $\mathbf{0}$
ii) if x is renamed as $\boldsymbol{x}$, then x^+ is renamed as $\boldsymbol{x}^{\boldsymbol{+}}$

From this point of view, the "second" Peano System $\boldsymbol{\mathcal{P}}$ is just the "same old stuff" but with new names.

This is an example of an important phenomenon. Sometimes different systems really are complete look-alikes: one is just the other with elements "renamed" in a way that respects the operations inside the system (e.g., "successor"). The systems are perfect "mirror images" of each other $-$ they have exactly the same structure. The words "structure" and "system" are a little vague, so we can't make a precise mathematical definition here. But here is an informal definition that may be useful to remember.

Informal Definition Suppose there is a "pairing (or renaming) rule" between two systems which pairs off all the objects in the two systems with each other in a one-for-one way. Suppose, moreover, that this pairing is done in a way that respects all the operations (like "successor", for example) in the systems. Then we say that the two structures are isomorphic and the "pairing rule" is called an isomorphism between the structures.

Note: “isomorphism” comes from two Greek words,

“isos”	*meaning*	*“equal” or “same”*
“morphe”	*meaning*	*“shape” or “form” or “structure”*)

To make the definition more precise, we would replace “pairing rule” with “a one-to-one, onto function” between the systems. But that additional precision needs to wait until we say more about functions, one-to-one functions, onto functions, etc.

Students who have already taken Math 309 (Matrix Algebra) should have seen the idea of “isomorphic systems” before – although the word “isomorphic” might not have been used. If V is a finite dimensional vector space with basis $\mathcal{B} = \{b_1, ..., b_n\}$, then V is isomorphic to (“looks just like”) the vector space $\mathbb{R}^n$. The “coordinate mapping” pairs off each vector $x \in V$ with a vector in $\mathbb{R}^n$, namely, $x \rightleftarrows (c_1, ..., c_n)$ where $c_1, ..., c_n$ are the coordinates of x with respect to the basis $\mathcal{B}$.)

This is sufficient detail for what we are going to do. We have argued that any two Peano systems are isomorphic, so that “<u>if you've seen one Peano system, you've seen them all</u>.”

> However, those who are interested are encouraged to also read this optional (indented) material. Unlike the more informal discussion, above, the following discussion makes no use of the “picture” and makes no use of the italicized results *Theorem 4* and *Corollary 5.* The “renaming” or “pairing” rule is defined inductively without any reference to the figures above.
>
> Define a “renaming” rule (function) $\boldsymbol{R}$ that pairs each element in $\mathcal{P}$ with a “unique partner” in the other Peano system $\boldsymbol{\mathcal{P}}$. The definition of $\boldsymbol{R}$ is done <u>inductively</u> (that is, using axiom P5):
>
> Let $\boldsymbol{R}(0) = \mathbf{0}$
> and, $\forall x \in \mathcal{P} \quad \boldsymbol{R}(x^+) = (\boldsymbol{R}(x))^+ \quad (*)$
>
> $(*)$ tells you how to find $\boldsymbol{R}(x^+)$ (an object in $\boldsymbol{\mathcal{P}}$) if you already know $\boldsymbol{R}(x)$ (an object in $\boldsymbol{\mathcal{P}}$). This defines $\boldsymbol{R}$ for every $x \in \mathcal{P}$:
>
> For example, the rule gives $\boldsymbol{R}(0) = \mathbf{0}$,
> $\boldsymbol{R}(0^+) = (\boldsymbol{R}(0))^+ = \mathbf{0}^+$,
> $\boldsymbol{R}((0^+)^+) = (\boldsymbol{R}(0^+))^+ = (\mathbf{0}^+)^+$, etc.
>
> More precisely, if we let $A = \{x \in \mathcal{P} : \boldsymbol{R}(x)$ is defined$\}$, then $0 \in A$ and if $x \in A$, then $x^+ \in A$ – so, by P5), $A = \mathcal{P}$.
>
> There are two important observations to make:

1) Different elements $x, y \in \mathcal{P}$ get assigned to different partners in $\boldsymbol{\mathcal{P}}$ – that is, if $x \neq y$, then $\boldsymbol{R}(x) \neq \boldsymbol{R}(y)$**.** To see this, we use induction.

Let $A = \{x \in \mathcal{P} : \ \forall y \ \ (y \neq x \ \Rightarrow \ \boldsymbol{R}(y) \neq \boldsymbol{R}(x) \ )\}$. We want to see that $A = \mathcal{P}$.

$0 \in A$: To see this, we need to check that if $y \neq 0$, then $\boldsymbol{R}(y) \neq \boldsymbol{R}(0) = \mathbf{0}$. In other words, we have to check that a nonzero y in $\mathcal{P}$ gets a nonzero partner in $\boldsymbol{\mathcal{P}}$.

Since $y \neq 0$, then (by Corollary 2) $y = z^{+}$ for some $z \in \mathcal{P}$. Therefore $\boldsymbol{R}(y) = \boldsymbol{R}(z^{+})$ $= (\boldsymbol{R}(z))^{+}$. That means that $\boldsymbol{R}(y)$ has a predecessor $\boldsymbol{R}(z)$ in $\boldsymbol{\mathcal{P}}$. But $\mathbf{0}$ has no predecessor in $\boldsymbol{\mathcal{P}}$ (by P3), so $\boldsymbol{R}(y) \neq \mathbf{0}$**.**

If $x \in A$, we must show that $x^{+} \in A$, that is: we must show that if $y \neq x^{+}$, then $\boldsymbol{R}(y) \neq \boldsymbol{R}(x^{+})$. We do this by showing the contrapositive: if $\boldsymbol{R}(y) = \boldsymbol{R}(x^{+})$, then $y = x^{+}$.

Suppose $\boldsymbol{R}(y) = \boldsymbol{R}(x^{+})$. Since $x^{+} \neq 0$ (by P3), $\boldsymbol{R}(x^{+}) \neq \boldsymbol{R}(0)$ (since $0 \in A$) so $y \neq 0$. Therefore y has a predecessor, say $y = z^{+}$.

Then $(\boldsymbol{R}(x))^{+} = \boldsymbol{R}(x^{+}) = \boldsymbol{R}(z^{+}) = (\boldsymbol{R}(z))^{+}$**.** By P4), we conclude that $\boldsymbol{R}(x) = \boldsymbol{R}(z)$. Since $x \in A$, this means that $x = z$. But then $y = z^{+} = x^{+}$.

Therefore, by P5), $A = \mathcal{P}$. ●

2) Every object in $\boldsymbol{\mathcal{P}}$ acquires a partner from $\mathcal{P}$. Again, we use induction. Let $\boldsymbol{A} = \{\boldsymbol{x} \in \boldsymbol{\mathcal{P}} : \ \boldsymbol{x} = \boldsymbol{R}(y) \text{ for some } y \in \mathcal{P}\}$. We need to show that $\boldsymbol{A} = \boldsymbol{\mathcal{P}}$.

$\mathbf{0} \in \boldsymbol{A}$ because $\mathbf{0} = \boldsymbol{R}(0)$

Suppose $\boldsymbol{x} \in \boldsymbol{A}$**.** Then $\boldsymbol{x} = \boldsymbol{R}(y)$ for some $y \in \mathcal{P}$. Therefore $\boldsymbol{R}(y^{+}) = (\boldsymbol{R}(y))^{+} = \boldsymbol{x}^{+}$. In other words, $\boldsymbol{x}^{+}$ is partnered with y^{+} from $\mathcal{P}$, so $\boldsymbol{x}^{+} \in \boldsymbol{A}$.

By P5), $\boldsymbol{A} = \boldsymbol{\mathcal{P}}$**.**

Putting observations 1) and 2) together, the rule $\boldsymbol{R}$ gives an exact pairing, one-for-one ($\boldsymbol{R}$ is a "one-to-one, onto function") between the all the objects in $\mathcal{P}$ and all those in $\boldsymbol{\mathcal{P}}$. By the definition of $\boldsymbol{R}$, the pairing respects the successor operation work in the two systems:

$$\boldsymbol{R}(x^{+}) = \boldsymbol{R}(x)^{+}$$

"the partner of the successor" $=$ "the successor of the partner"

More about a Peano System

We want to convince ourselves that a Peano system captures the essence of our informal system ω. Already, we have a "mental picture" and a few theorems which suggest that the objects in a Peano system are arranged just like the whole numbers. We want to see that we can define "addition," "multiplication," and " $<$ " between objects in a Peano system and that, when we're done, the result acts just like ω.

All Peano systems look alike, so let's begin by assigning some convenient names to the objects in a Peano system. After all, needing to write things like $0^{+++++++}$ becomes tedious.

There are lots of possible ways to name things. For example, some possibilities could be:

	0	0^{+}	0^{++}	0^{+++}	0^{++++}	0^{+++++}	0^{++++++}	... etc.
Naming System	œ	†	‡	¿	ð	€	ß	
Naming System	0	I	II	III	IV	V	VI	...
Naming System	0	1	10	11	100	101	110	...
Naming System	0	1	2	3	4	5	6	...

The point is that there are lots of ways to invent names for $0,\ 0^{+}, 0^{++}$, ...etc. It's important, here, to remember that however we decide to invent names for the objects in the Peano system, the names themselves don't give us any new information. But, keeping that in mind, we might as well use names are convenient and that remind us of how we hope the system is going to work. So we'll use the intuitively familiar symbols $0, 1, 2, 3, ...$ as in the fourth row of the table.

Caution For now, $0, 1, 2...$ are now just "marks on paper" $-$ the names we're giving objects in the Peano system. There's no more reason to say "1 plus 2 $=$ 3" than there is to say "† plus ‡ $=$ ¿" : both are just ways of saying (in different naming systems) that "0^{+} plus $0^{++} = 0^{+++}$" $-$ and in fact, the statement "0^{+} plus $0^{++} = 0^{+++}$" has no meaning yet at all because we haven't defined what "plus" means in a Peano system.

We cannot say $2 \cdot 2 = 4$, because (right now) that statement is just a new way of writing $0^{++} \cdot 0^{++} = 0^{++++}$ $-$ which, at the moment, has no meaning at all, because we haven't even defined what it means to "multiply" objects in a

Peano System.

We can, however, use these new names now to record things that we do already know. For example, the axioms for a Peano system now read:

P1) There is one special object named "0" in $\mathcal{P}$
P2) For each object $n \in \mathcal{P}$, there is exactly one object in $\mathcal{P}$ called its successor (and denoted n^+)
P3) 0 is not the successor of any object, that is, $(\forall n \in \mathcal{P})\ n^+ \neq 0$
P4) Different objects have different successors, that is

$$\forall m, \forall n \in \mathcal{P}\ (m \neq n \Rightarrow m^+ \neq n^+)$$

P5) Suppose $A \subseteq \mathcal{P}$. If $0 \in A$ and if

$$(\forall n \in \mathcal{P})\ \ (n \in A \Rightarrow n^+ \in A)$$

then $A = \mathcal{P}$.

Just because of how we named things, statements like these are true:

$0^+ = 1$ (i.e., 1 is the successor of 0) ,
$0^{++} = 1^+ = 2$,
$4^+ = 5$

If we had decided instead to use the naming system in the first row of the table, the following would be true:

œ$^+ =$ †
œ$^{++} =$ †$^+ =$ ‡
ð$^+ =$ €

The theorems we already proved, with the new naming system, can now be written:

Theorem 1 For all $n \in \mathcal{P}$, either $n = 0$ or $n = m^+$ for some $m \in \mathcal{P}$

Corollary 2 If $n \in \mathcal{P}$ and $n \neq 0$, then $n = m^+$ for a unique $m \in \mathcal{P}$.

Theorem 3 For all $n \in \mathcal{P}$, $n \neq n^+$

Theorem 4 *If $n \in \mathcal{P}$, then $n = 0$ or n can be obtained from 0 by applying the successor operation finitely often.*

Corollary 5 *If $m, n \in \mathcal{P}$ and $m \neq n$, then one of m and n can be obtained from the other by applying the successor operation finitely often.*

Defining Arithmetic in a Peano System

Addition Let $\mathcal{P}$ be a Peano system (in which we have named the elements $0, 1, 2, ...$).

First, we want to define addition: what does $m + n$ mean? For any given m in $\mathcal{P}$, the definition tells (using P5, the induction axiom) what it means to "add n, on the right, to m."

Definition A Suppose $m \in \mathcal{P}$. Define

i) $m + 0 = m$ and
ii) $\forall n \in \mathcal{P},\ \ (m + n^+) = (m + n)^+$

For any given $m,$ we can use P5) to show that $m + n$ has been defined for every n:

Suppose $m \in \mathcal{P}$. Let $A = \{n \in P : m + n$ is defined$\}$.

By i), $0 \in A$.

If $n \in A,$ then $m + n$ is defined. So then $m + n^+$ is also defined because ii) defines $m + n^+$ as the successor of $m + n$ in $\mathcal{P}$. Therefore $n^+ \in A$.

By P5), $A = \mathcal{P}$. ●

Example Suppose $m \in \mathcal{P}$. Then

$$\begin{aligned} m + 0 &= m && \text{(by definition Ai)} \\ m + 1 &= (m + 0^+) && \text{because "1" is the name we assigned to } 0^+ \\ &= (m + 0)^+ && \text{by Definition Aii} \\ &= m^+ && \text{by Definition Ai} \end{aligned}$$

(*Note: so it turns out, as a result of our definition of addition, that "add 1 to m" is the same thing as "take the successor of m."*)

In particular, if we let $m = 0,$ the preceding calculations show that

$$0 + 0 = 0$$
$$0 + 1 = 0^+ = 1$$
$$0 + 2 = (0 + 1)^+ = 1^+ = 2$$

If we let $m = 1$, we see that the preceding calculation shows that $1 + 1 = 1^+$, and the name we assigned to 1^+ is 2 : so $1 + 1 = 2$.

Similarly

$$2+1=2^+=3$$
$$3+1=3^+=4,$$

. etc.

$($*By convention, let's agree that we may also write* m^{++} *for* $(m^+)^+)$

$$\begin{aligned} m+2 &= (m+1^+) && \text{because “2” is the name we assigned to “}1^+\text{”} \\ &= (m+1)^+ && \text{by Definition Aii} \\ &= (m^+)^+ && \text{by the preceding example} \end{aligned}$$

Letting $m=1,2,...$ gives the specific facts

$$1+2=1^{++}=2^+=3$$
$$2+2=2^{++}=3^+=4$$

etc.

Similarly, for any $m,n,$ the recursive definition of addition lets us work backwards “deeper and deeper” until, with a lot of patience $-$ but only finitely many steps $-$ we eventually figure out the sum $m+n.$ For example, that $5+4=9$ $($*give a justification for each step*$)$:

$$\begin{aligned} 5+4 &= 5+3^+=(5+3)^+ = (5+2^+)^+=(5+2)^{++} \\ &= (5+1^+)^{++}=(5+1)^{+++}=(5+0^+)^{+++} \\ &= (5+0)^{++++}=5^{++++}=6^{+++}=7^{++}=8^+=9 \end{aligned}$$

From the definition of addition (Ai), we know that $m+0=m$ for any $m \in \mathcal{P}$. BUT that doesn't mean that we can say $0+m=m,$ because we haven't yet proved that addition in $\mathcal{P}$ is commutative. The next theorem is a first step in that direction.

Theorem 6 $(\forall n \in \mathcal{P})$ $0+n=n=n+0$

Proof Let $n \in \mathbb{N}$. We know $n+0=n$ by the Definition Ai) $-$ *that equation is included in Theorem 6 as contrast to* $0+n$. *It is the statement* $(\forall n \in \mathcal{P})\ 0+n=n$ *that we need to prove.* Let $A=\{n \in \mathcal{P}:\ 0+n=n\}$.

If $n=0$, then $0+0=0=0+0$, by Definition Ai). So $n=0 \in A$.

Suppose that $n \in A$. Then

$$\begin{aligned} 0+n^+ &= (0+n)^+ && \text{(by Definition Aii, with } m=0) \\ &= n^+ && \text{(because } n \in A) \end{aligned}$$

Therefore $n^+ \in A$.

By the induction axiom P5), $A = \mathcal{P}$. •

To prove that addition is commutative and associative, it's helpful to begin by proving a lemma.

Lemma 7 $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})\ m^+ + n = (m+n)^+ = m + n^+$

Proof We already know that $(m+n)^+ = m + n^+$ by the Definition Aii) – $m + n^+$ *included in Lemma 7 just as contrast to* $m^+ + n$. *It is the statement* $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})\ m^+ + n = (m+n)^+$ *that we need to prove.*

Let $m \in \mathcal{P}$. We need to show that $(\forall n \in \mathcal{P})\ m^+ + n = (m+n)^+$

Define $A = \{n \in \mathcal{P} :\ (m+n)^+ = m^+ + n\}$. We want to show that $A = \mathcal{P}$.

$(m+0)^+ = m^+ = m^+ + 0$ (using Definition Ai), so $0 \in A$

Suppose that $n \in A$. We need to show $n^+ \in A -$ that is, we need to show that $(m + n^+)^+ = m^+ + n^+$:

$$\begin{aligned} (m^+ + n^+) &= (m^+ + n)^+ && \text{(Definition Aii)} \\ &= (\,(m+n)^+)^+ && \text{(because } n \in A\text{)} \\ &= (\ m + n^+\ )^+ && \text{(Definition Aii)} \end{aligned}$$

By P5), $A = \mathcal{P}$. •

Theorem 8 a) $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})(\forall p \in \mathcal{P})\ \ m + (n+p) = (m+n) + p$
(*Addition is* *<u>associative</u>*.)

b) $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})\ \ m + n = n + m$
(*Addition is* *<u>commutative</u>*.)

Proof a) Suppose m, n be any objects in the Peano system $\mathcal{P}$. We need to show that

$$(\forall p \in \mathcal{P})\ \ m + (n+p) = (m+n) + p$$

Let $A = \{p \in \mathcal{P} :\ m + (n+p) = (m+n) + p\}$. We want to show that $A = \mathcal{P}$.

$$\begin{aligned} 0 \in A\text{:}\quad m + (n+0) &= m + n && \text{(by Definition Ai)} \\ &= (m+n) + 0 && \text{(by Definition Ai), again)} \end{aligned}$$

Suppose, for some p, that $p \in A$. We show that p^+ must be in A.

$$\begin{aligned} m+(n+p^+) &= m+(n+p)^+ && \text{(by Definition Aii)} \\ &= (m+(n+p))^+ && \text{(by Definition Aii, again)} \\ &= ((m+n)+p)^+ && \text{(because } p \in A) \\ &= (m+n)+p^+ && \text{(by Definition Aii, again)} \end{aligned}$$

Therefore $p^+ \in A$.

By P5), $A = \mathcal{P}$. •

b) Suppose $m \in \mathcal{P}$. We must show that $(\forall n \in \mathcal{P})\ \ m+n = n+m$.

Let $A = \{n \in \mathcal{P} :\ m+n = n+m\}$.

$m+0 = m$, by Definition Ai, and we proved in Theorem 6 that $0+m = m$. Therefore $0 \in A$.

Suppose that $n \in A$. We will show that n^+ must be in A.

$$\begin{aligned} m+n^+ &= (m+n)^+ && \text{(by Definition Aii)} \\ &= (n+m)^+ && \text{(because } n \in A) \\ &= n^+ + m && \text{(by Lemma 7)} \end{aligned}$$

Therefore $n^+ \in A$.

By P5), $A = \mathcal{P}$. •

Because addition is associative, we often write things like $m+n+p$ without parentheses, because it doesn't matter whether we interpret this as meaning $(m+n)+p$ or $m+(n+p)$.

<u>Summary</u>: We have defined addition ($+$) in $\mathcal{P}$. We have proved the necessary theorems to compute $m+n$ for any $m, n \in \mathcal{P}$. The addition we created turned out to be commutative and associative, and to have a "neutral" element, $0 :\ m+0 = 0+m = m$ for all $m \in \mathcal{P}$. In other words (as much as we can see, so far) addition in $\mathcal{P}$ behaves exactly like ordinary addition does in our infromal, intuitive system ω.

In ω, we can also multiply. So now we hope to define a multiplication operation in $\mathcal{P}$ that behaves just like multiplication in ω.

Multiplication

We also want to define multiplication in $\mathcal{P}$. We do that using addition and the successor operation. Then we need to look at some theorems about multiplication behaves in $\mathcal{P}$ and how multiplication is connected to addition.

We could try making a definition like

"$m \cdot n$ means the result of adding m to itself n times."

But this is an inconvenient way to put it because it doesn't give us a precise formula " $m \cdot n =$ ..." to work with: so what do we do?

> *We stop and look for motivation. Think about how multiplication works in the informal system ω. In ω, $m \cdot 0 = 0$, and, if you already know how to find $m \cdot n$, there is a formula telling you how to find $m \cdot (n+1)$, namely*
>
> $$m \cdot (n+1) = m \cdot n + m$$
>
> *We use this fact about the informal system ω, to inspire our definition of multiplication in the formal system $\mathcal{P}$. Of course, this makes it likely that multiplication in $\mathcal{P}$ will, in fact, act like multiplication in the informal system, ω. And that's what we want. We are trying to show how to create, from very simple assumptions, a formal system $\mathcal{P}$ that acts like ω, so we "build in" what we need to make the finished product be what we want it to be.*

Definition M Suppose $m \in \mathcal{P}$. We define

i) $m \cdot 0 = 0$ and
ii) for any $n \in \mathcal{P}$, $m \cdot n^+ = m \cdot n + m$

(*Sometimes we will just write "mn" for "$m \cdot n$."*)

Exercise: Suppose $m \in \mathcal{P}$. Verify (just as we did for addition) that $m \cdot n$ is defined for all $n \in \mathcal{P}$.

Example For any $m \in \mathcal{P}$,

$$m \cdot 1 = m \cdot 0^+ = m \cdot 0 + m = 0 + m = m$$
$$m \cdot 2 = m \cdot 1^+ = m \cdot 1 + m = m + m$$
$$m \cdot 3 = m \cdot 2^+ = m \cdot 1 + m = (m+m) + m$$

etc.

For example, $3 \cdot 1 = 3$

$3 \cdot 2 = 3 + 3 = 6$ (*using earlier work on addition*)

$$\begin{aligned} 4 \cdot 3 &= 4 \cdot 2^+ = 4 \cdot 2 + 4 = 4 \cdot 1^+ + 4 \\ &= (4 \cdot 1 + 4) + 4 \\ &= (4 \cdot 0^+ + 4) + 4 = ((4 \cdot 0 + 4) + 4) + 4 \\ &= ((0 + 4) + 4) + 4 = (4 + 4) + 4 \\ &= (\textit{using all the operations for computing sums})... \\ &= 8 + 4 = ... = 12 \end{aligned}$$

The next lemma gives a useful variation on the equations in Definition M. It is an analogue (for multiplication) of Lemma 7 (about addition).

Lemma 9 For all $m, n \in \mathcal{P}$,

a) $0 \cdot m = 0 = m \cdot 0$
b) $m^+ \cdot n = m \cdot n + n$

Proof Suppose $m \in \mathcal{P}$

a) $0 = m \cdot 0$ by Definition Mi). What we need to prove is that $0 \cdot m = 0$

Let $A = \{m \in \mathcal{P} : \ 0 \cdot m = 0\}$

$0 \in A$ because $0 \cdot 0 = 0$ (by Definition Mi)

Suppose $m \in A$. We will show that $m^+ \in A$.

$$\begin{aligned} 0 \cdot m^+ &= 0 \cdot m + 0 && \text{(by Definition Mii)} \\ &= 0 + 0 && \text{since } m \in A \\ &= 0 && \text{(by Definition Ai)} \end{aligned}$$

Therefore $m^+ \in A$.

By P5), $A = \mathcal{P}$. ●

b) Let $A = \{n \in \mathcal{P} : \ m^+ \cdot n = m \cdot n + n\}$

$$\begin{aligned} 0 \in A, \text{ because } m^+ \cdot 0 &= 0 && \text{(by Definition Mi)} \\ &= m \cdot 0 && \text{(by Definition Mi), again} \\ &= m \cdot 0 + 0 && \text{(by Definition Ai)} \end{aligned}$$

Suppose $n \in A$. We show that $n^+ \in A.$ To do this, we need to show that

$m^+ \cdot n^+ = m \cdot n^+ + n^+.$

$m^+ \cdot n^+ = m^+ \cdot n + m^+$	(by Definition Mii)
$= (m \cdot n + n) + m^+$	(because $n \in A$)
$= m \cdot n + (n + m^+)$	(by Theorem 8: addition is associative)
$= m \cdot n + (n + m)^+$	(by Definition Aii)
$= m \cdot n + (m + n)^+$	(by Theorem 8; addition is commutative)
$= m \cdot n + (m + n^+)$	(by Definition Aii)
$= (m \cdot n + m) + n^+$	(by Theorem 8: addition is associative)
$= m \cdot n^+ + n^+$	(by Definition Mii)

Therefore $n^+ \in A$.

By P5, $A = \mathcal{P}$. •

We can now prove a connection between addition and multiplication (the distributive rule) and see that multiplication is associative and commutative. For convenience, we agree to write mn for $m \cdot n$.

Theorem 10 $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})(\forall p \in \mathcal{P})$

a) $m(n+p) = mn + mp$ ($\cdot$ *and* $+$ *are connected by the distributive rule*)
b) $m(np) = (mn)p$ (*Multiplication is associative.*)
c) $mn = nm$ (*Multiplication is commutative.*)

Proof a) The proof of a) is an assigned problem in the homework. We assume a) in the arguments below.

b) Suppose $m, n \in \mathcal{P}$. We need to show that $(\forall p \in \mathcal{P})$ $m(np) = (mn)p$

Let $A = \{p \in \mathcal{P} : m(np) = (mn)p\}$. We want to show $A = \mathcal{P}$.

$0 \in A$ since $m(n \cdot 0) = m \cdot 0$	(by Definition Mi)
$= 0$	(by Definition Mi, again)
$= (mn) \cdot 0,$	(by Definition Mi, again)

Suppose, for some p, that $p \in A$. Then

$m(np^+) = m(np + n)$	(by Definition Mii)
$= m(np) + mn$	(by part a) of this theorem: the

distributive rule)

$= (mn)p + mn$ (because $p \in A$)

$= (mn)p^+$ (by Definition Mii)

Therefore $p^+ \in A$.

By P5, $A = \mathcal{P}$. •

c) Suppose $m \in \mathcal{P}$. We need to show that $(\forall n \in \mathcal{P})\ mn = nm$

Let $A = \{n \in \mathcal{P} : mn = nm\}$. We want to show $A = \mathcal{P}$.

$0 \in A$ because $m \cdot 0 = 0 = 0 \cdot m$ (by Lemma 9)

Suppose, for some n, that $n \in A$. Then

$mn^+ = mn + m$ (by Definition Mii)

$= nm + m$ (because $n \in A$)

$= n^+m$ (by Lemma 9)

Therefore $n^+ \in A$.

By P5, $A = \mathcal{P}$ •

Because multiplication is associative, we often write things like mnp without parentheses, because it doesn't matter whether we intended $(mn)p$ or $m(np)$.

Example An earllier example (with $m = 3$) showed that $m \cdot 3 = (m + m) + m$. We could also get this fact from addition and the distributive law:

$$(m + m) + m = (m \cdot 1 + m \cdot 1) + m \cdot 1$$

$$= m \cdot (1 + 1) + m \cdot 1 = (m \cdot 2) + m \cdot 1 = m(2 + 1) = m \cdot 3.$$

By the commutative law for multiplication, we can now say also that

$$m \cdot 3 = (m + m) + m = 3 \cdot m.$$

In the proofs that follow, we will now use the definitions of $+$ and $\cdot$ more freely (without always citing an explicit justification for each and every step). We will also freely use that multiplication are associative and commutative, and that the distributive law is true in $\mathcal{P}$. In some arguments, such as the proof of part c) of the following theorem, we use of results previously proven and don't need to use an induction in the argument.

Theorem 11 Suppose $m, n, c \in \mathcal{P}$.

a) If $m \neq 0$, then $m + n \neq 0$.

b) (Cancellation for $+$) If $m + c = n + c$, then $m = n$.
(If $c + m = c + n$, then $m + c = n + c$, so $m = n$. The theorem tells us that we can "cancel c on the left" , too.)

c) If $m \neq 0$ and $n \neq 0$, then $mn \neq 0$.

Note: We already proved in Theorem 8b) that addition is commutative. Therefore it doesn't matter in part a) whether the nonzero term, m, is on the left or the right: $m + n = n + m$: in words, 11a) merely says that the sum of two obejcts from $\mathcal{P}$ is not 0 if one of the objects is not 0.

Suppose $m + n = 0$. What can we conclude in $\mathcal{P}$?

Proof a) Suppose $m \neq 0$. Let $A = \{n \in \mathcal{P} : m + n \neq 0\}$.

$0 \in A$ because $m + 0 = m \neq 0$.

Suppose that $n \in A$. Then $m + n^+ = (m + n)^+ \neq 0$ (using P3).
Therefore $n^+ \in A$. By P5, $A = \mathcal{P}$. ●

b) This proof is an assigned exercise in the homework.

c) Suppose $m \neq 0$ and $n \neq 0$. We know that $n = k^+$ for some k (by Theorem 1), so $mn = mk^+ = mk + m$. Since $m \neq 0$, we conclude that $mn \neq 0$ (using part a) of this theorem). ●

(*Note: Part c) is done without using induction (P5). However, the proof uses other results (such as Theorem 1) that were proved using the induction axiom P5.*

Example For short, we can agree to write "n^2" for "$n \cdot n$", n^3 for "$(n \cdot n) \cdot n$", etc. Show that $(n+1)(n+2) = n^2 + 3n + 2$. (*Justify each step! Be sure that each "arithmetic calculation" is one that we justified.*)

$$\begin{aligned}
(n+1)(n+2) &= ((n+1) \cdot n) + (n+1) \cdot 2 = (n \cdot (n+1)) + 2 \cdot (n+1) \\
&= (n^2 + n \cdot 1) + (2 \cdot n + 2 \cdot 1) = (n^2 + n) + (2n + 2) \\
&= (n^2 + (n + 2n)) + 2 \\
&= (n^2 + n \cdot (1+2)) + 2 \\
&= (n^2 + n \cdot 3) + 2 \\
&= (n^2 + 3 \cdot n) + 2 \\
&= n^2 + 3 \cdot n + 2
\end{aligned}$$

(*Be sure you can justify each step*)

On the surface, it looks like we have shown, without induction, that

$$(\forall n \in \mathcal{P})\ \ (n+1)(n+2) = n^2 + 3n + 2$$

In fact, nearly every step in the calculations is justified by a theorem whose proof did use induction.

The truth is that a proof for any statement of the form

$$(\forall n \in \mathcal{P})\ P(n)$$

must depend on the induction axiom P5 (either in the proof itself, or in the proofs of earlier theorems that are used in the proof).

Defining an Ordering Relation in a Peano System

Finally, we can introduce an “ordering ” (denoted by $\leq$) in $\mathcal{P}$ with another definition.

Definition O Suppose $m, n \in \mathcal{P}$. We say $m \leq n$ iff $(\exists c \in \mathcal{P})\,(m + c = n)$.
We write $m < n$ iff $m \leq n$ and $m \neq n$.

Note: We also write $m \leq n$ as $n \geq m$: the two relations are understood to mean the same thing.
Similarly, the relations $m < n$ and $n > m$ are understood to mean the same thing.

Example For each $m \in \mathcal{P}$:

$0 + m = m$ so, by Definition O, $0 \leq m$

$m + 0 = m$ so, by Definition O, $m \leq m$.

Theorem 12 For all $m, n, p \in \mathcal{P}$:

a) $m \leq m$
b) if $m \leq n$ and $n \leq p$, then $m \leq p$.
c) if $m \leq n$ and $n \leq m$, then $m = n$.

Proof a) See the example, above.

b) If $m \leq n$, there is a c such that $m + c = n$, and
if $n \leq p$, there is a d such that $n + d = p$.
Therefore $m + (c + d) = (m + c) + d = n + d = p$,
so $m \leq p$.

c) If $m \leq n$, there is a c such that $m + c = n$, and
if $n \leq m$, there is a d such that $n + d = m$.

Since $m + c = n$,
$(m + c) + d = n + d = m$, so
$m + (c + d) = m = m + 0$.
Theorem 11b) lets us cancel the m and get $c + d = 0$.
But then, by Theorem 11a), $c = d = 0$.

Therefore $n = m + c = m + 0 = m$. •

Theorem 13 $(\forall m \in \mathcal{P})\,(\forall n \in \mathcal{P})\ (\,m \leq n$ or $n \leq m)$

Proof Let $m \in \mathcal{P}$. For this m, we need to show that $(\forall n \in \mathcal{P})\ (\,m \leq n$ or $n \leq m)$. Let $A = \{n \in \mathcal{P} :\ m \leq n$ or $n \leq m$ is true$\}$. We will show that $A = \mathcal{P}$.

The example above shows that $0 \leq m$, so $0 \in A$.

Suppose that $n \in A$. (*Since A is defined by a statement using "or", there are two cases to consider.*)

i) If $m \leq n$, then $\exists c \in \mathcal{P}$ such that $m + c = n$. In that case, $m + c^+ = (m+c)^+ = n^+$ so $m \leq n^+$ and therefore $n^+ \in A$.

ii) If $n \leq m$, then $\exists c \in \mathcal{P}$ such that $n + c = m$.

If $c = 0$, then $n = m$, so $m + 1 = m^+ = n^+$, which means that $m \leq n^+$, so $n^+ \in A$.

If $c \neq 0$, then c has a predecessor d in $\mathcal{P}$: $c = d^+$.
Then $n^+ + d = n + d^+$ (by Lemma 7)
$= n + c = m$, so $n^+ \leq m$
and therefore $n^+ \in A$.

In both cases, $n^+ \in A$.

Therefore, by P5, $A = \mathcal{P}$. ●

Note: Corollary 5 in the "Peano Systems" notes was printed in italics because it seemed to involve some questionable reasoning. Theorem 13 is a correct, rigorous version of what Corollary 5 was trying to say: if $m \neq n$, then "one of these two objects in $\mathcal{P}$" = "the other object + c" and, as we have seen in several examples, "adding c" turns out to be the same as repeated applications of the successor operation.

Corollary 14 $(\forall m \in \mathcal{P})(\forall n \in \mathcal{P})\ (\,m < n$ or $m = n$ or $m > n)$

Proof By Theorem 13**,** we know $m \leq n$ or $m \geq n$. If $m \neq n$, then (by definition of $<$), we know that $m < n$ or $m > n$. ●

Theorem 15 (Cancellation for multiplication) If $m, n, p \in \mathcal{P}$ and $p \neq 0$ and $mp = np$, then $m = n$.

(*Since multiplication is commutative, if $pm = pn$, then $mp = np$ so $m = n$. Therefore theorem tells us that we can also cancel a nonzero factor of p on the left.*)

Proof Homework exercise.

Finally, we want to check that the "order relation" $\leq$ interacts nicely with addition and multiplication (*just as* $\leq$, +, *and* $\cdot$ *interact nicely in the informal system* ω.) For example,

Theorem 16 Suppose $m, n, p \in \mathcal{P}$ and that $m \leq n.$ Then

a) $m + p \leq n + p$

b) $mp \leq np.$

Proof a) Since $m \leq n$, there is a $c \in \mathcal{P}$ such that $m + c = n.$ Then

$$(m + c) + p = n + p, \text{ so}$$
$$(m + p) + c = n + p, \text{ so}$$
$$m + p \leq n + p. \quad \bullet$$

b) This is an assigned problem in the homework.

Exercise Suppose that $x \leq y.$ Then there is a c in $\mathcal{P}$ for which $x + c = y.$
Prove that c is unique.

(*Hint: Assume that alsao* $x + d = y.$ *Compare* c *and* $d.$)

Looking Back and Looking Forward

A formal mathematical system refers to some collection of "objects," some axioms that describe exactly how the objects behave, and the body of definitions and theorems that grows out of the axioms. A Peano system, its associated definitions and theorems, is an example of a formal mathematical system.

An informal mathematical system is a not very precise term. It's everyday usage for a bunch of related mathematical definitions and facts that we know: for example, you might describe what you know (or what we all together know) about calculus as an informal mathematical system.

Another example would be our system of whole numbers, ω, together with all its algebra involving $+ \, . \, \cdot$, and $\leq$. We have been taking the point of view that the system of whole numbers, ω, is an informal system that (somehow) we seem to know a lot about. We want to create a formal system that acts just like this informal system. The notion of a Peano system seems like a good start in this direction.

We believe that the Peano Axioms P1-P5 are true statements about the informal system, ω when we interpret the "objects" in a Peano system $\mathcal{P}$ to be whole numbers, and interpret successor in $\mathcal{P}$ to mean "the next whole number." Based on what we know informally, it seems like the informal system ω is a specific model for a Peano system.

The theorems that we proved for a Peano system $\mathcal{P}$ also turn out to be true when they are interpreted as being statements about whole numbers. This is just what one would expect: if the axioms of $\mathcal{P}$ are true when interpreted as statements about whole numbers, then all the logical consequences of those axioms (theorems) will also be true about whole numbers.

Mathematicians don't care (unless they are becoming philosophers) what whole numbers "really are" – how they behave is what counts. Because a formal abstract Peano system seems to behave just like the informal system ω, mathematicians can agree to define ω as a Peano system.

So can we just say "ω is a Peano system" and be done? There are two things more to consider. The first is easy to settle, and the second needs a little more work:

> i) Which Peano system is ω? Are there many Peano systems? Even if there are, it doesn't matter: we argued earlier in these notes that "all Peano systems behave exactly alike." If behavior is what counts, one Peano system is as good for the definition of ω as another. If it doesn't matter much which particular Peano system we define ω to be – although it might convenient to settle on one particular Peano system.
>
> ii) But are there any Peano systems at all? Can we describe one?

> (*We can't really give ω as an example: ω is just an informal mathematical system for which we are trying to find a formal definition.*) Can we somehow create a particular Peano system for which we can then agree to say, by definition, that this particular Peano system is ω ?

What would we use to create a specific Peano system? Because set theory is supposed to be the foundation for mathematics, we try to build a Peano system in which the objects are sets: they are the most fundamental objects mathematics has. So we will try to create

> i) a collection $\mathcal{P}$ whose members are sets, and
>
> ii) an operation in $\mathcal{P}$ that takes a given set in $\mathcal{P}$ and creates in $\mathcal{P}$ a new set (denoted x^+ and called the "successor of x").

and to do this in a way that makes axioms P1)-P5) true.

If we can pull this off, we will have a specific, concrete Peano system, one built out of sets). Like any Peano system, this one will behave just like the informal system ω . Then we can make a definition – formally, once and for all – that this particular Peano system is officially the system of whole numbers. The objects (sets) in $\mathcal{P}$ will be called the whole numbers – so that (officially) every whole number is some set.

At the risk of being repetitive, let's notice: suppose we can create such a $\mathcal{P}$.

> i) We are not claiming to have proved that ω is $\mathcal{P}$ – it makes no sense to prove a definition. But defining the whole number system to be this Peano system $\mathcal{P}$ does give us a formal system which behaves, as best we can judge, just like the informal system ω that we started with and which we were trying to "formalize."
>
> ii) There might be other ways for someone to get a system that behaves "just like the informal system ω, " and the person might officially define that system instead to be ω. For philosophical or aesthetic reasons, the person might prefer a different approach and definition. But mathematically, the choice really doesn't matter: how the whole numbers behave is what does matter mathematically. Therefore mathematicians can all agree to live with whatever particular formal definition for ω is chosen.

Getting a Peano system of sets

We want to construct a collection of sets, together with a “successor set” operation inside the collection, that turns out to be a Peano system.

The idea of a “successor set” came up earlier in a homework exercise and it turns out to be exactly what we will need. Here is the definition again.

Definition For any set x, $x^+ = x \cup \{x\}$. The set x^+ is called the successor of x.

Notice that

i) The successor set x^+ contains for its elements: all the elements that were in the set x, together with one additional $\{x\}$.

$x \subseteq x^+$ is always true

$x \in x^+$ is always true

x^+ always contains exactly one more element than x.

ii) $\{a, b\}^+ = \{a, b\} \cup \{\ \{a, b\}\} = \{a, b, \{a, b\}\}$

$\mathbb{R}^+ = \mathbb{R} \cup \{\mathbb{R}\}$

Example

$\emptyset$

$\emptyset^+ \quad = \emptyset \cup \{\emptyset\} \quad = \{\emptyset\}$

$\emptyset^{++} \quad = \{\emptyset\}^+ \quad = \{\emptyset\} \cup \{\{\emptyset\}\} \quad = \{\emptyset, \{\emptyset\}\}$

$\emptyset^{+++} \quad = \{\emptyset,\ \{\emptyset\}\}^+ \quad = \{\emptyset,\ \{\emptyset\}\} \cup \{\{\emptyset,\ \{\emptyset\}\}\} \quad = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$

$\vdots$

and so on.

Definition Suppose I is a set (collection) of sets. I is called an inductive set if

a) $\emptyset \in I$, and
b) if $x \in I$, then $x^+ \in I$.

We ask: are there any inductive sets? Informally, it seems like there should be. For example, you can imagine the set

$$I = \{\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \ ...\}$$

However, this "example" of an inductive set I – even though its suggestive – seems little vague if we're trying to be careful. This set is only inductive because it is described very casually using "..." – the mathematical equivalent of "etc., etc., etc."

> If we tried to be more precise about writing down a definition for this set I, we'd try to write something like
>
> $$I = \{z \in U : *** \}$$
>
> and this highlights a couple of problems:
>
> > i) What can the universe Ube? Informally we'd like to say that the z's are chosen from $U =$ the "set of all sets." But the idea of a "set of all sets" quickly leads to contradictions (similar to Russell's Paradox).
> >
> > ii) Even if we had a good choice for U, what would the description $***$ be?
> >
> > The set I suggested above appears to contain the empty set together with successors of any sets already in I : that is
> >
> > $$I = \{z \in U : z = \emptyset \text{ or } (\exists w \in I)\, z = w^+\}$$
> >
> > But this is a self-referential definition – the members of I members are described in terms of I ! This also can lead to paradoxes like Russell's Paradox.

To decide what to do, we need to a brief look at the axioms for set theory itself. These axioms are "as deep down as we can ever go"because set theory, we have agreed, is to be the very foundation for all mathematics. In other words, all mathematics should flow from the axioms for set theory.

Axiomatic (formal) set theory is a system of objects (called sets) and a relation (denoted by " $\in$ ") between some of these objects. We know nothing about these objects except

that they behave according to the rules described in a certain set of ten axioms $-$ called the ZFC axioms ($=$ the “Zermelo-Fraenkel-with-Choice” axioms$)$.
(*Of course, these axioms were chosen in the first place to describe a formal system that would behave, as best we can tell, “just like” naive (informal) set theory.*)

A careful study of the ZFC Axioms, and the theorems that can be proved from them, is a whole field of study in itself, usually called “Axiomatic Set Theory.” In order to get the flavor, there follows a partial list of the axioms; it omits some of the more technical axioms that we don't need to think about. . (*The quantifiers in these axioms apply to the “universe” of sets – so* $(\forall x)$ *means “for all sets* x*”, etc. Convince yourself that the English translations given below are correct.*)

Axioms for Set Theory: Zermelo-Fraenkel-with-Choice (ZFC)

ZFC1 $\forall x \forall y \; (\forall z \; (z \in x \Leftrightarrow z \in y) \;\; \Leftrightarrow \;\; x = y)$

" Two sets are equal iff they have the same members. "

ZFC2 $\exists x \forall y \; (y \notin x)$

" There is a set with no members (an empty set). "

If "two" sets both have no members, then they certainly have the same members (none at all !) so, by ZFC1, they are the same set. In other words, the first theorem of ZFC could be "there is exactly one empty set." So, for convenience, we can give it a name: $\emptyset$

ZFC3 $\forall x \forall y \; (\exists z \forall u \; (u \in z \Leftrightarrow (u = x \vee u = y)))$

" If x and y are sets, then there is a set $z = \{x, y\}$" – in other words, two sets can be "paired" to create a new 2-element set.

ZFC4 $\forall x \exists y \; (\forall z \; (z \in y \Leftrightarrow \exists b \; (z \in b \wedge b \in x)))$

" For any set x, there is a set y consisting of the members of the members of x."

We can agree to give this set y a name: $\bigcup x$

ZFC5 $\forall x \exists y \, (\forall z \, (z \in y \; \Leftrightarrow (\forall w \, (w \in z \Rightarrow w \in x))))$

If we agree to <u>define</u> "$z \subseteq x$" to be shorthand for $\forall w \, (w \in z \Rightarrow w \in x)$ *Then ZFC5 could be written* $\forall x \exists y \; (\forall z \; (z \in y \; \Leftrightarrow z \subseteq x))$. *That is, axiom ZFC5 says "every set x has a power set y."*

ZFC6 $\exists I \; (\emptyset \in I \wedge (\forall y \; (y \in I \Rightarrow y^{+} \in I)))$

There exists an inductive set.

plus 4 other more technical axioms (omitted) : ZFC7, ZFC8, ZFC9, ZFC10 (AC)

The axiom ZFC10 is called the <u>Axiom of Choice (AC)</u>. It causes some <u>philosophical</u> controversy among those mathematicians who worry about foundations of mathematics, so <u>a few</u> mathematicians omit it from the list. If AC is omitted, then axioms 1-9 are referred to as the "ZF" axioms. But the 10-axiom system ZFC is the axiom system most mathematicians would use for set theory (and therefore to develop all of mathematics).

We might say a little about the Axiom of Choice later in the course.

We have taken a naive (informal) approach to set theory and will continue to do so. But everything that we have done (or will do) with sets can be justified by theorems provable from the ZFC axioms. For our purposes, we mentioned the ZFC axioms for two reasons.

First, because we were looking for an inductive set. The ZFC axioms guarantee that an inductive set exists. Moreover, we can infer that ZFC6 was probably included as an axiom for set theory because it's not possible (using the other axioms) to prove that an inductive set must exist: if you want set theory to have inductive sets (and our intuition expects that it should) then you have to build-in an axiom to somehow make that happen.

Second, the ZFC axioms are important. They are the basis for set theory which, in terms, can be used as a foundation for mathematics. Every math major should see what some of these axioms are like, just to get an idea of what all mathematics is built on.

To return to the question we were asking: we are convinced (informally) that set theory should contain an inductive set. Based on the axioms, we assume that there is at least one inductive set and proceed from there.

Definition I* Choose an inductive set I and define

$$S = \{x \in I : \ x \in J \text{ for every inductive set } J\} \qquad (*)$$

By definition, $S \subseteq I$. In fact the definition tells us even more – that S is a subset of every inductive set J (*Check! What does $S \subseteq J$ mean?*). Therefore you could think of describing S by the equation $S = \bigcap\{J : J \text{ is an inductive set}\}$.

> *As a matter of fact, one can prove from the ZFC Axioms that there are many different inductive sets. But*
>
> *i) The definition (*) of S would make sense even if there were only one inductive set, I.*
>
> *ii) If a different inductive set I' were chosen to use in definition (*), then we would still get the very same set S – because in both cases $S = \bigcap\{J : J \text{ is an inductive set}\}$*

S is an intersection of inductive sets, but we can't assume just assume that makes S itself an inductive set. However, the next theorem settles that question.

Theorem 17 S is an inductive set.

Proof a) $\emptyset$ is in every inductive set J, so $\emptyset \in S$.

b) Suppose $x \in S$. Then (by definition of S) x is a member of every inductive set J. Therefore x^+ is also a member of every inductive set J (by definition of "inductive set"). Hence $x^+ \in S$.

Therefore S is inductive. •

Since $S \subseteq J$ for every inductive set J, and because Theorem 17 tells us that S itself is an inductive set, we can now say that S is the <u>smallest</u> <u>inductive</u> <u>set</u>. In particular this means that

$$\emptyset \in S; \text{ therefore } \emptyset^+ \in S; \text{ therefore } \emptyset^{++} \in S; \text{ therefore } \emptyset^{+++} \in S; \text{ and so on.}$$

Caution: We are using the same notation x^+ for "successor of a set x" as we used for "successor" in a Peano system. But don't let the notation deceive: we have no right to assume that the successor operation for sets obeys the rules axioms P1-P5. We need to check whether that is true.

Definition $0 = \emptyset$ (*We are simply agreeing that* 0 *will be another name for* $\emptyset$.)

What can we say about S and the successor operation?
Since $0 = \emptyset \in S$, we now have

P1: There is a special object in S named 0.
(0 *is the set* $\emptyset$.)

Because S is and inductive set, the successor set x^+ for each set x in S is also in S. Therefore

P2: For every object $x \in S$, there is a successor x^+ in S.

For any set x, we have that $x \in x \cup \{x\} = x^+$, so $x^+ \neq \emptyset$.
So

P3: For all $x \in S$, $x^+ \neq 0$ $(= \emptyset)$

Suppose $A \subseteq S$, and suppose that

i) $0 \; (= \emptyset) \in A$, and
ii) $(\forall x \in S)\,(x \in A \Rightarrow x^+ \in A)$

These assumptions i) and ii) about A say that A is an inductive set. But $A \subseteq S$ and S is the <u>smallest</u> inductive set, so $A = S$. This shows that

P5: Suppose $A \subseteq S$:
i) if $0 \; (= \emptyset) \in A$, and
ii) if $(\forall x \in \omega)\,(x \in A \Rightarrow x^+ \in A)$

then $\boldsymbol{A = S}$.

At this point we have almost shown that S, with the successor set operation, forms a Peano system. But we still P4: that if $x, y \in S$ and $x \neq y$, then $x^+ \neq y^+$. This takes a little more work.

We will be using here another definition introduced earlier in the homework.

Definition A set k is called <u>transitive</u> iff $(\forall x)(\forall y)\ (x \in y \in k \Rightarrow x \in k)$
(*Less formally, x is transitive if "every member of a member of k is a member of k.*"

For example $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ is transitive but $\{\emptyset, \{\{\emptyset\}\}\}$ is <u>not</u> transitive.

Theorem 18 For any set A, the following are equivalent:

i) A is transitive
ii) $\bigcup A \subseteq A$
iii) $a \in A \Rightarrow a \subseteq A$
iv) $A \subseteq \mathcal{P}(A)$

Proof This theorem was an exercise in homework. (For Spring 2009, see the HW 5 solutions online if you're uncertain about the proof.) $\bullet$

Theorem 19 If k is a transitive set, then $k = \bigcup(k^+)$.

Remember: $\bigcup(k^+)$ just means the "set of all members of the sets that are in the collection k^+."

For example, if $k = \{\emptyset, \{\emptyset\}\}$, then $k^+ = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\}$
$= \{\emptyset, \{\emptyset\}, \{\{\emptyset, \{\emptyset\}\}\}$ so $\bigcup k^+ = \emptyset \cup \{\emptyset\} \cup \{\emptyset, \{\emptyset\}\} = \{\emptyset, \{\emptyset\} = k$.

Proof i) Suppose $x \in \bigcup(k^+)$. Then $x \in z$, where $z \in k^+ = k \cup \{k\}$.

if $z \in k$, then $x \in z \in k$ so $x \in k$ <u>because</u> k is assumed to be transitive
if $z \in \{k\}$, then $z = k$ so $x \in k$

Either way, we have $x \in k$. Therefore $\bigcup(k^+) \subseteq k$.

ii) Suppose $x \in k$. Since $k \in k^+$, $x \in \bigcup(k^+)$. Therefore $k \subseteq \bigcup(k^+)$.

Hence $\bigcup(k^+) = k$. $\bullet$

Alternate Proof (*a little slicker: think about each step*) $\bigcup(k^+) = \bigcup\,(k \cup \{k\})$ $= \bigcup k\, \cup k$. Since k is transitive, $\bigcup k \subseteq k$ (using $A = k$ in Theorem 18). Therefore $\bigcup k \cup k = k$. •

Corollary 20 If k is a transitive set, then k^+ is also transitive.

Proof For any set $k,\ k \subseteq k^+$. Suppose k is transititve. By Theorem 19, $\bigcup(k^+) = k \subseteq \mathrm{k}^+$. B y Theorem 18 (with $A = k^+$), k^+ is transitive. •

The next theorem gives us lots of examples of transitive sets.

Theorem 21 If $k \in S,$ then k is transitive.

Proof We use the fact that P5 is true in the set S. Let $A = \{k \in S : k \text{ is transitive}\}$.

i) $0\,(= \emptyset)$ is transitive, so $0 \in A$.

ii) Assume $k \in A$. Then k is transitive so, byCorollary 20, k^+ is transitive. Therefore $k^+ \in A$.

By P5, $A = S$. •

Now we can finally show that the remaining Peano axiom, P4, is true in the set S.

Theorem 22 ($=$ **P4** for S) Suppose $x, y \in S$. If $x \neq y$, then $x^+ \neq y^+$.

Proof (*We will prove the contrapositive.*) Since x^+ and y^+ are in S, they are transitive sets (by Theorem 21). So if $x^+ = y^+$, then Theorem 19 gives us that $x = \bigcup x^+ = \bigcup y^+ = y$ •

We have now achieved the objective. The set S, as given in Definition I*, with the set successor operation, is a specific Peano system (built out of sets). We will choose this specific Peano system S for our definition of the whole number system ω .

Definition The set ω of whole numbers is defined to be the set S (as given in Definition I*). A whole number is any member of the set ω .

Names for the whole numbers

We can name the objects in ω using the same system we used for any abstract Peano system:

Member of ω (set)	Name
$\emptyset$	0
$\emptyset^{+} = \{\emptyset\}$	1
$\emptyset^{++} = \{\emptyset\}^{+} = \{\emptyset, \{\emptyset\}\}$	2
$\emptyset^{+++} = \{\emptyset, \{\emptyset\}\}^{+} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$	3
$\vdots$	

Thus, in our official definition of ω, the whole numbers really certain <u>sets</u> $-$ sets that have been given the names $0, 1, 2, \ldots$.

<u>Some interesting (amusing?) observations show up in this list</u>:

i) $0 = \emptyset$
$1 = \{\emptyset\} = \{0\}$
$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$

The pattern suggests a theorem (which we won't take the time to prove): <u>every whole number is the set of preceding whole numbers</u> !

ii) $\emptyset \in \{\emptyset\} \in \{\emptyset, \{\emptyset\}\} \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \in$ ..., in other words

$$0 \in 1 \quad \in \quad 2 \quad \in \quad 3 \quad \in \ ..$$

Also, for example, $0 \in 3$ and $2 \in 3$. If you continued the list of successors and names, you would keep observing the pattern:

$$m < n \text{ (as defined in a Peano system)} \Leftrightarrow m \in n$$

That is also a theorem that can be proved.

Definition n is called a <u>natural number</u> if $n \in \omega$ and $n \neq 0$. The set of natural numbers $\mathbb{N}$ is defined to be the set $\omega - \{0\}$.

Therefore, natural numbers are also officially defined as sets.

<u>Conclusion</u>: Having done all this, the point is <u>not</u> that in the future you should always be thinking of the whole numbers as sets. In fact, you usually should think of the whole numbers the way you always have.

The "big picture" items that are important are:

1) There is a very small collection of axioms (P1-P5) from which all aspects of the whole number system (including arithmetic and rules for inequalities) can be carefully and systematically proven, and that

2) the whole numbers, and their arithmetic, <u>can</u> be "built" from set theory – in accordance with the view the sets should be a foundation for everything we need in mathematics.

We will see soon that the set of integers can be built from the set of whole numbers (sets) – so each integer will turn out to be a set. The set of rationals can then be built from the set of integers – so each rational number will turn out to be a set ; and so on.