8-1953

On The Treatment Of The Logical Basis Of The Principle Of Mathematical Induction With Some Applications

Theodore C. Smith

ON THE TREATMENT OF THE LOGICAL BASIS OF THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH SOME APPLICATIONS

SMITH

1953

ON THE TREATMENT OF THE LOGICAL BASIS OF THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH SOME APPLICATIONS

By

Theodore C. Smith

A Thesis in Mathematics Submitted in Partial Fulfillment
of the Requirements for the Degree of

Master of Science

in the

Graduate Division

of

Prairie View Agricultural and Mechanical College

Prairie View, Texas

August 19, 1953

ACKNOWLEDGEMENT

The writer wishes to acknowledge with thanks the assistance given him by his advisor, Mr. L. C. Marshall and Mr. L. K. Williams of the mathematical department in the preparation of this work.

TABLE OF CONTENTS

INTRODUCTION

A criticism which is often made of mathematics as a subject of study is that it involves nothing of observation, experimentation and induction as the terms are understood in the natural sciences. Whether or not this criticism is just is a debatable question, nevertheless the work of many investigators who helped to develop mathematical science reflects very clearly a constant use of a great deal of observation, experimentation and induction, that is the process of deriving a general conclusion from particular cases.

It is worthy to note that observation and experimentation in mathematics do not usually involve costly and complicated apparatus as is often the case with physics, astronomy and some other sciences. Pencil and paper are all that one needs, ordinarily, nevertheless they are true observations.

Investigations and experimentations in modern science suggest to us the following conjecture, namely, that the universe operates in a somewhat orderly manner. Clearly then, to understand thoroughly the nature of these operations we must first discover the various laws by which they are governed.

The object of the scientist is to examine critically natural phenomena in order to be able to predict and control the various natural processes. To that end mathematics has been a valuable asset, for it has made it possible for one to represent certain natural relationships quantitatively.

Indeed, to extend our mathematical knowledge, is to extend our knowledge of these physical inter-relationships.

But how shall we enlarge the nucleus of mathematical truths? While several methods of extending mathematical knowledge are open to us, in this paper we shall be concerned with but one of these methods - one which is both ancient and powerful, namely, the principle of mathematical induction.

The purpose of this paper then is:

1. To trace the development of those ideas seeking to justify the principle of mathematical induction,
2. To analyze its structure,
3. To give a logical justification for the use of this principle,
4. And finally to point to some areas in which the use of the principle of mathematical induction has been decisive.

The subsequent impact of the principle of mathematical induction on the advancement of science, therefore, becomes apparent.

A HISTORICAL NOTE ON THE DEVELOPMENT OF THE PRINCIPLE OF MATHEMATICAL INDUCTION

Cantor in his "Vorlesungen Uber Geschichte der Mathematik" states that Pascal was the originator of mathematical induction, but on being informed otherwise by G. Vacca, he submitted a note in 1575 correcting this mistake. Thus, the first discoverer of mathematical induction seems to be one Franciscus Maurolycus. This principle was used at the beginning of his work in demonstrating very simple propositions.

He first applied the principle to the proof of the statement:

If a is any number, then

$$a^2 + (2a + 1) = (a + 1)^2.$$

Using this result he proved that

$$1 + 3 + 5 + \ldots + (2a + 1) = (a + 1)^2.$$ [1]

Pascal repeatedly used the method of complete induction. In fact, the literature supports Cantor's argument that he borrowed the method from Maurolycus.

The following is an interesting example of Pascal's

---

[1]Bulletin of American Mathematical Society, Vol. 16 (70).

use of the method of complete induction:

The number of combinations of m things k at a time is to the number of combinations of m things k + 1 as k 1 is to n - k, or symbolically

$$mC_k : mC_{k+1} = (k + 1) : (m - k).$$

Proof: First part. By inspection the theorem is true for m equals 2, for then the only possible value of k and k + 1 are 1 and 2, respectively and

$$2C_1 : 2C_2 = 2 : 1.$$

Second part. Assume that the theorem is true for m equals q; that is assume

$$\text{(A)} \quad {}_qC_k : {}_qC_{k+1} = (k + 1) : q - k$$

for all positive integral values of k less than q. We show that

$$\text{(B)} \quad (q + 1)\, C_j : {}_{(q+1)}C_{j+1} = (j + 1) : q + 1 - j$$

for all positive integral values of j less than q+1.

(B) is obtained from (A) by replacing q in (A) by q + 1 and by using another letter for k to avoid confusion.

The well known relation

$$\text{(C)} \quad NC_r = N - 1 \cdot C_{r-1} + N - 1 \cdot C_r$$

is needed to prove that (B) follows from (A). By relations (A) the left hand member of (B) is equivalent to

$$\frac{{}_qC_{j-1} + {}_qC_j}{{}_qC_j + {}_qC_{j+1}} = \frac{\dfrac{{}_qC_{j-1}}{{}_qC_j} + 1}{1 + \dfrac{{}_qC_{j+1}}{{}_qC_j}} .$$

On applying relation (A) to the minor fractions ${}_qC_{j-1}/{}_qC_j$ and ${}_qC_{j+1}/{}_qC_j$ this becomes

$$\frac{\dfrac{j}{q - j + 1}}{1 + \dfrac{q - j}{j + 1}} = \frac{j + 1}{q - j + 1} . \qquad \text{Q. E. D.}$$

SOME THEORIES SEEKING TO JUSTIFY INDUCTION

Generalization is probably as old as human thought. In fact the tendency to rash generalizations would seem to be one of the original sins of mankind.[1]

Early thinkers like Aristotle attempted to check the tendency toward rash generalizations by setting up severe standards and insisting that the ideal of generalization is what is still known as "perfect induction," for example, generalization based upon an exhaustive examination of the whole countries or communities until they knew every citizen or member thereof. But then the ideal of perfect induction has made no impression on practical people, and has proved to be worthless as a guide to scientific people. In the vast majority of cases the classes of objects and events with which science is concerned are far too numerous to permit anything even distantly approaching exhaustive individual examination of all the members. All of the important inductions of science are those which were once called imperfect inductions, that is to say, generalization based on the examination of a bare sample of the whole class under investigation. Its great weakness has been and still is how to

---

[1]Encyclopedia Britannica, Vol. 12, p. 271.

excuse, or justify, such extensive generalization after the study of just a few instances. To this question various answers have been attempted, and the most important of them may now be considered briefly.

One answer, which is rather in favor among some of the more philosophical of contemporary men of science, is to the effect that there is really no justification for induction--that all induction, and all forecasts based on them, are just more or less sanguine adventures or speculations, and the fact that they do not always disappoint us is nothing short of a miracle.

Another answer given, and one that is much in favor among certain statisticians and other mathematically minded people, is based upon what is essentially of the artless induction by simple enumeration, the solution now under consideration bases itself on the calculus of probability, and correlates the reliability of the generalization with the number and kind of observation made. Each observed occurrence of an event in certain circumstances is treated as a point in favor of expecting its recurrence in a similar circumstance.

J. S. Mill[1] based all induction on the principle of the uniformity of nature, but his conception was not very satisfactory. For, on one hand he regarded this assumed

---

[1] _Ibid_., p. 272.

objective uniformity, as the ground of all induction, and on the other hand, he regarded it as being itself a very comprehensive induction based upon numerous other inductions each much more limited in scope. This ambiguous attempt to make the same principle at once the foundation and the proof of this whole structure of science has not been received with favor.

Perhaps the least unsatisfactory way of answering the general question as to the logical ground of induction, using this term in its widest sense for every attempt to trace order in nature, is along the following lines:[1]

The scientific search for order among natural phenomena would seem to assume the existence of order there. Science does not propose to invent it and at the same time to impose upon nature, but rather, if possible, only to discover it. This search does not necessarily presuppose a definite conviction that what is sought is actually there. One may look for what is hoped for or for what is deemed probable, as well as for what is definitely expected to be there. Moreover, to assume that there is some order in nature is not the same thing as to suppose that nature is orderly through and through.

After all the world is vast, and the field of

---

[1] Ibid., p. 272.

actual scientific investigation is comparatively limited, so it is always open to the man of science to select for his field of research some class of facts in which discovery of order looks fairly promising. On the whole, experience has shown that there is some order in nature, indeed sufficiently so to justify and encourage the continued search for more. Turning to the question of the ground of generalization more particularly, one must, in the first place, distinguish between those which rest on induction by simple enumeration only; and those which are based ultimately on one of the induction methods especially when these can be applied with some rigour, and not rather loosely. Induction based on simple enumeration and even statistical generalization must always be regarded with a measure of diffidence. They may indicate temporary or partial conjunctions rather than general connections. It is rather different in those cases in which the inductive methods have been applied.

AXIOMS OF MATHEMATICAL INDUCTION

The principle of mathematical induction is not a method of discovery, but rather a method of proving rigorously that which has already been discovered. Undoubtedly, it is one of the most fruitful methods in all of mathematics.

A theorem provable by complete induction involves a statement about an integer which we usually denote by n. The proof of a statement by the principle of mathematical induction is in two parts. The first part verifies the theorem for a special case. The second part of the proof is what has been called the argument from n to n + 1. It is the argument which justifies one in drawing a general conclusion from the special cases verified. For this reason it is called the induction argument. We submit the following so-called axioms of mathematical induction.

Let P(n) be a proposition involving the integer n. Assume:

(a) The proposition is correct for n equals 1.

(b) If k is any value of n for which the proposition is true, then the proposition is also true for the next value of n namely k + 1.

Then the proposition is true for all positive integral values of n.

Let us apply the method to the proof of the binomial theorem.

The Binomial Theorem

Theorem:

If n is any positive integer, then

$$(a + b)^n = a^n + \frac{n}{1!} a^{n-1}b + \frac{n(n-1)}{2!} a^{n-2}b^2 + \frac{n(n-1)(n-2)}{3!} a^{n-3}b^3$$

$$+ \frac{n(n-1)(n-2)(n-3)}{4!} a^{n-4}b^4 + \ldots$$

$$+ \frac{n(n-1)(n-2)\ldots(n-r+1)}{r!} a^{n-r}b^r + \ldots + b^n$$

Proof:

(A) For n = 1 we have $(a + b)^1 = a + b$. Thus the formula is true for n = 1.

(B) Assume that the formula is true for n = k. We must show that the formula is true for n = k + 1. The assumption that the formula is true for n = k is equivalent to the assumption that

$$(a + b)^k = a^k + C(k,1)a^{k-1}b + \ldots. + C(k,r-1)a^{k-r+1}b^{r-1}$$

$$+ C(k,r)a^{k-r}b^r + \ldots. + b^k,$$

where $C(n,r) = \dfrac{n(n-1)(n-2)(n-3) \ldots\ldots (n-r+1)}{r!}$.

To show that the formula is true for $n = k + 1$ is equivalent to proving that

$$(a + b)^{k+1} = a^{k+1} + C(k + 1,j)a^k b + \ldots + C(k + 1,r)a^{k-r+1}b^r$$

$$+ \ldots\ldots + b^{k+1}.$$

Consider the expansion

$$(1) \quad (a + b)^k = a^k + C(k,1)a^{k-1}b + \ldots$$

$$+ C(k,r-1)a^{k-r+1}b^{r-1} + \ldots + b^k$$

Multiplying both sides of (1) by $(a + b)$, we get

$$(2) \quad (a + b)^{k+1} = (a + b)(a^k + C(k,1)a^{k-1}b$$

$$+ \ldots + C(k,r-1)a^{k-r+1}b^{k-1} + b^r).$$

Consider the right member of (2), we examine a typical term in the product, say the term involving b^r. This will be the sum of two terms, the first being the product of a by the term involving b^r in (1), and the second term being the product of b by the term involving b^{r-1} in (1). These two products are $C(k,r)a^{k-r+1}b^r$ and $C(k,r-1)a^{k-r+1}b$ respectively. Thus their sum is $(C(k,r) + C(k,r-1))a^{k-r+1}b^r$.

But $C(k,r) + C(k,r-1) = C(k + 1,r)$. Therefore, the general term of the conclusion is $C(k + 1, r)a^{k-r+1}b^r$, as was required to show.

Consider the following example:

It is a well known fact that the formula P(n) equals $n^2 - n + 41$ will produce a value of P which is a prime number for all integrals values of n from n = 0 up to and including n = 40. But when n = 41, $P = 41^2 - 41 + 41$, and $P = 41^2$, which is not a prime number.[1] Since P(41) does not hold, one is justified in asking, can we assume P(k) prove P(k + 1) and conclude that P(n) is true for all n by the above set of axioms? If so, then the method is doomed to inconsistency, for the axioms themselves would be inconsistent. We shall show that this situation described above will never occur.

Principle of Finite Induction

Thus the preceding example suggests the need for establishing rigorously the principle of mathematical induction. We begin by introducing certain important definitions.

Definition: (1) A set of elements is a collection of elements having certain specified properties.

---

[1]Hart, William L. College Algebra, Revised Edition, D. C. Heath and Company, New York, 1938, p. 195.

We shall deal with the set of all positive integers.

Definition: (2) A set of numbers is said to be well-ordered if each of its non-empty subsets contains a smallest element. Thus, the positive integers form a well-ordered set. Our goal is to prove the principle of finite induction. We first prove two theorems.

Theorem I.

There is no integer between 0 and 1.

Proof:

We prove the theorem by contradiction.

Suppose there exists an integer C such that $0 < C < 1$. Then the class of all integers less than 1 is not empty. But the integers form a well-ordered set, hence there exists a smallest such integer. Call this integer m. Clearly m satisfies the inequality $0 < m < 1$.

Consider $0 < m < 1$. Since $m > 0$, we may multiply by m, thereby preserving the inequality. Therefore, we have the inequality $0 < m^2 < m$. Since m is an integer, so is m^2. But $0 < m^2$, that is, there is an integer less than m and which is in the set defined above. Obviously, this contradicts the choice of m. We are forced to admit, then, that there is no integer between 0 and 1.

Theorem II.

A set S of positive integers which includes 1 and which includes $n + 1$ whenever it includes n, includes every positive integer.

Proof:

Let J be the set of all positive integers.

Define $S' = J - S = J \cap cS$, where cS = set of all integers in J but not in S. It suffices to show that $S' = \emptyset$ (that is the empty set). Suppose $S \neq \emptyset$. Then there exists at least one element, say x, which is in S'. Now S' is a subset of J. J is well-ordered. This implies that S' has a least element, say m. Clearly $m \neq 1$ by hypothesis. Therefore $m > 1$. Then $m - 1 > 0$. Now $m - 1 < m$, hence by the choice of m, m - 1 is in S. We now apply the hypothesis to obtain that $(m - 1) + 1$ is also in S, that is, m is in S. This is a contradiction and we must have $S' = \emptyset$, i. e., $J - S = \emptyset$, that is $J = S$. Our theorem is therefore proved.

We are now in a position to state and prove the extremely important

Principle of Finite Induction

Theorem:

Let there be associated with each positive integer n a proposition P(n) which is either true or false.[1]

---

[1]Birkhoff and MacLane, A Survey of Modern Algebra, The Macmillan Company, New York, 1949, p. 11.

Suppose:

(a) P(1) is true,

(b) For all k, P(k) implies P(k + 1), then P(n) is true for all values of n.

Proof:

Let S be the set of those integers k for which P(k) is true (or false). By hypothesis 1 is in S and k in S implies k + 1 is in S.
Theorem II. applies to give that S = J, that is, P(k) holds for all positive integers. This proves our theorem.

As an illustration of a proof by finite induction we establish formally in any integral domain the general distributive law for any number n of summands,

$$a(b_1 + \dots + b_{k+1}) = ab_1 + \dots + ab_{k+1},$$

In any integral domain we have the associative law the simple distributive law and the property of closure which are valid. Thus, applying these laws, we have

$$\begin{aligned} a(b_1 + \dots + b_k + b_{k+1}) &= a\left[(b_1 + b_2 + + \dots b_n) + b_{k+1}\right] \\ &= a(b_1 + b_2 + \dots + b_k) + ab_{k+1} \\ &= ab_1 + \dots + ab_k + ab_{k+1}, \end{aligned}$$

where the first term on the right was reduced by the law which we have assumed for n = k. Thus, the law holds for n = k + 1, and by our induction principle it holds in general, that is, for all positive integral values of n.

The Second Principle of Finite Induction

The following generalized method of proof by induction is often useful.

Second Theorem of Finite Induction. [1]

Let there be associated with each positive integer n a proposition P(n).

Assume:

(a) For each m, P(k) is true for all $k < m$ implies the conclusion that P(m) is itself true, then P(n) is true for all values of n.

Proof:

Let S be the set of integers for which P(n) is false. Unless S is empty, it will have a first member say m. By the choice of m, P(k) will be true for all $k < m$, hence by hypothesis P(m) must itself be true, giving a contradiction. The only way out is to admit that S is empty, and this proves our theorem.

Now if $m = 1$, the set of all $k < 1$ is void so one must verify the theorem for $m = 1$ directly.

Transfinite Induction

The principle of finite induction was proved for the set of positive integers, which obviously form a denumerably infinite set. Indeed, investigations in mathematics

[1] *Ibid*., p. 12.

often require us to consider sets which do not form denumerable sets; for example, the set of all real numbers.

Can we derive a principle of mathematical induction which will be valid for non-denumerable sets as well?

We concern ourselves with this question presently. Accordingly, we state the so-called principle of Transfinite Induction. [1]

Let W be any non-denumerable set. Suppose W is well-ordered.

Assume T is a certain theorem such that:

(a) T is true for the first element of the set W,

(b) T is true for an element a of W, if it is true for every element preceding a.

Then T is true for every element of W.

Indeed, suppose that a certain theorem T satisfies conditions a and b, but that there exist elements of W for which it is not true. Let N be the set of all such elements. N will, therefore, be a non-null subset of a well-ordered set and so will have a first element say a. It follows from the definition of N that T must be true for every element x of W which is such that $x \prec a$; but by condition b, T must be true for a, which is contrary to the

---

[1] Sierpinski, W., General Topology, University of Toronto, Toronto, Canada, 1934, p. 231.

fact that a $\in$ N. The principle of transfinite induction for well-ordered sets is, therefore, proved.

Application to Number Theory

In the theory of numbers there are numerous examples of the use of mathematical induction in proving propositions involving a numerical function of n. Typical of these are the following two theorems:

Theorem I (due to Fermat)

If n is a prime number, and N is an integer not divisible by n, then $N^n - N$ is divisible by n. [1]

Denote $N^n - N$ by the functional symbol F(N).

Then $F(M + 1) - F(M) = (M + 1)^n - (M + 1) -$

$$(M^n + M) = nM^{n-1} + \frac{n(n-1)M^{n-2}}{2!} + \ldots + nM$$

upon expanding $(M + 1)^n$ by the Binomial Theorem.

The first and last terms are evidently divisible by n. Also $\frac{n(n-1)}{2!}$ is an integer, being a binomial coefficient, and is divisible by n, since 2 does not divide the prime n(n 2) otherwise the term M^{n-2} does not occur). In general, the coefficient $\frac{n(n-1) \ldots (n - r - 1)}{r!}$ of M^{n-r} occurs only when

---

[1]Dickson, L. E., College Algebra, John Wiley and Sons, New York, 1902, p. 102.

n r and is then an integer. Moreover, it is divisible by n since there is no factor in common with n and the denominator r! . In fact n is greater than r and hence cannot divide any factor of r!; while, inversely, no factor of r! can divide the prime n.

$$\therefore F(M + 1) = F(M) + \text{a multiple of } n.$$

Thus, if we assume that F(M) is divisible by n, so is F(M + 1). But $F(1) \equiv 0$. Hence F(2) is dividible by n; therefore also F(3), etc.

Definition (1) $\phi(m)$ is the number of integers less than m and relatively prime to m. In particular, for a prime integer p, $\phi(p) = p - 1$.

Definition (2) If $\frac{b}{a}$ is an integer, we say b is divisible by a and we write a/b.

Definition (3) For any three numbers a, b, m $a \equiv b \pmod{m}$ means a - b is divisible by m, or symbolically m/a-b.

Definition (4) Let a and m be relatively prime. Suppose:

(a) $a^e \equiv 1 \pmod{m}$

(b) $a^s \equiv 1 \pmod{m}$

implies $s > e$.

Then a is said to "belong" to the exponent e modulus m.

We now prove, Theorem II. If $e/\phi(p)$ where p is a prime, there are exactly $\phi(e)$ numbers which belong to e modulo p. [1]

Write the divisor of $\phi(p) = p - 1$ in order of magnitude

$$d_1 < d_2 < \dots < d_s,$$

where $d_1 = 1$ and $d_s = p - 1$. Evidently 1 is the only number which belongs to the exponent 1, and $\phi(1) = 1$. Hence, the theorem is true for the first divisor of the sequence.

Assume the theorem for every divisor in the set

$$d_1 < d_2 < \dots < d_{i-1} .$$

The congruence

$$x^{d_i} \equiv 1 \bmod p$$

has exactly d solutions. [2]

Each of these solutions belongs either to d_i or to some divisor of d_i less than d_i by the theorem that

If a belongs to e modulo m, and if $a^k \equiv 1 \bmod m$, then e/k. [3]

Denote by $\psi(d_i)$ the number of integers which belong to d_i.

---

[1] MacDuffie, C. C., Introduction to Abstract Algebra, John Wiley and Sons, New York, 1940, p. 35.

[2] *Ibid.*, p. 30.

[3] *Ibid.*, p. 34.

Then $\psi(d_i)$ is equal to d_i diminished by the number of integers which belong to the divisors of d_i less than d_i. But the divisors of d_i less than d_i are divisors of p - 1, and we assumed that the number of integers belonging to a number of d_i of this set was $\varphi(d)$. Hence

$$\psi(d_i) = d_i - \sum\phi(d_i),$$

the summation extending over all the divisors of d_i less than d_i. But by the theorem

If $d_1, d_2, \ldots d_r$ are the different divisors of m, then

$$(d_1) + (d_2) + \ldots + (d_r) = m,$$ [1]

we have,

$$d_i = \phi(d_i) + \sum\phi(d_i),$$

so that

$$\psi(d_i) = \phi(d_i).$$

Definitions by Induction

Some examples of definitions by induction:

Definition (1)

Positive integral exponents in any integral domain D may be treated by induction. If n is a positive integer,

---

[1]*Ibid.*, p. 35.

the power a^n stands for the product a x a x a ...x a to n factors. This can also be stated as a "recursive" definition[1]

$$a^1 = a, \quad a^{n+1} = a^n \times a^1 \quad \text{(any a in D)}$$

which makes it possible to compute any power a^{n+1} in terms of an already computed lower power a^n. From these definitions one may prove the usual laws for any positive integral exponents m and n as follows:

$$a^m a^n = a^{m+n},$$

$$(a^m)^n = a^{mn}, \qquad (ab)^m = a^m b^m.$$

For instance, the first law may be proved by induction on n. If n = 1, the law becomes $a^m \times a = a^{m+1}$, which is exactly the definition of a^{m+1}. Next, assume that the law is true for every m and for a given positive interger n = k, and consider the analogous expression $a^m a^{k+1}$ for the next larger exponent k + 1. One finds

$$a^m a^{k+1} = a^m(a^k a) = (a^m a^k)a = a^{m+k}a = a^{(m+k)+1}$$

by successive applications of the definition, the associative law, the induction assumption, and the definition. This gives the law for the case n = k + 1, and so completes the induction.

---

[1]Birkhoff and MacLane, op. cit., p. 112.

Definition (2)

The sum a + b of any two natural numbers a and b may be defined inductively. [1] We define a + 0 to be s, a + 1 to be the successor of a. This amounts to the introduction of the notation a + 1 for the successor of a. We complete our definition inductively by defining

$$a + (k + 1) = (a + k) + 1.$$

The intuitive application of this definition then states that to find the sum a + b of any two natural numbers a and b, in every case where $b \neq 0$ or 1, we use the formula above with k = 1,2 ... until we arrive at a + (k + 1) with k + 1 = b. This is, of course, not the elementary arithmetic process for finding sums. That process uses the concept of digit and an addition table of sums of the integers 1, 2, 3, 4, 5, 6, 7, 8, 9. However, that process is based upon the definition we have given above.

Definition (3)

Let G be an additive group and let j be the set of all integers. Define $0_j \cdot g = 0_g$ where $0_J = 0$ and 0_G is the zero of the additive group, G.

Define $1 \times g = g$. Let n be a positive integer.

---

[1] Albert, A. A., College Algebra, MacGraw-Hill Book Company, New York, 1946, p. 5.

Assume that we have defined ng, we may define

$$(n + 1)g = ng + g$$

Thus ng is defined for all positive n. If $n < 0$, we define $ng = -(-ng)$. Then for all $n \in J$, ng is well defined.

SUCCESSIVE APPLICATION OF THE PRINCIPAL OF MATHEMATICAL INDUCTION

The strength of the principle of mathematical induction is even more remarkable than we have suggested earlier. By applying the principle successively, we are sometimes able to verify the accuracy of statements involving several integral values. An example will illustrate.

Let J^+ be the set of all positive integers, and G and additive abelian group. Define $0_{J^+} g = g$. Define $(n + 1)g$ inductively.

Let it be desired to prove the following theorem:

If n J^+, m J^+, g G, where J^+ is the set of positive integers, then

$$(n + m)g = ng + mg.$$

We prove the theorem using double induction.

Let $n = 0$, $m = 1$.

Then $(0 + 1)g = (1)g = 0g + 1 \cdot g = 1 \cdot g = g$ by definition.

Now hold n fixed, and assume that the theorem is true for $k = m - 1$.

Consider

$$(0 + m)g = mg = og + mg.$$

Now

$$0g + mg = 0g + (m - 1)g + g$$
$$= (m - 1)g + g$$
$$= mg \text{ (by definition of } mg\text{)}.$$

Thus for all m and n = 0

$$(0 + m)g = 0g + mg.$$

Now hold m fixed. Let n = 1.

Then

$$(1 + m)g = (m + 1)g = mg + g$$
$$= g + mg \text{ (since } G \text{ is abelian)}.$$

Thus, the relation holds for n = 1.

Assume the relation is true for $k = (n - 1)$, $n \quad 1$.

We show that the relation holds for k = n.

We are to show that

$$(n + m)g = ng \quad \text{where } m \text{ is fixed.}$$

Consider

$$(n + m)g = [(n - 1) + (m + 1)]g$$
$$= (n - 1)g + mg + g)$$
$$= (n - 1)g + g + mg$$
$$= ng + mg.$$

Therefore the formula is true for all m and n in J^+.

More generally, let $P(n_1, n_2, \ldots n_k)$ be a numerical proposition of k variables whose truthfulness (or falsity) is to be established. We may resort to the method of successive application of mathematical induction:

Hold n_1, ... n_{k-1} fixed and use the principle of mathematical induction to prove that the proposition is true for all values of n_k. Then hold n_1, n_2, ... n_{k-2} and n_k fixed and prove the proposition true for all values of n_{k-1}. Continuing this way, we finally prove that the proposition is true for all values of x_2, ... x_k. Applying the principle once more, holding x_2, ... x_k fixed, we can prove that it is true for all values of x_1. Thus, the proposition has been established for all values of x_1 ... x_k, and thus holds in general.

A MATHEMATICAL PARADOX

To suggest the extent to which one must be careful in applying the principle of mathematical induction, we shall prove by mathematical induction that any two positive integers are equal.

Consider a series of statement $A_1, A_2, A_3, \ldots A_n$. Suppose A_1 is true and if A_k is true then A_{k+1} is true, then all A_n is true for all n.

Definition:

Let a and b be any two integers and suppose $a \neq b$.

The define $\max(a,b) =$ a or b depending on whichever is greater.

If $a = b$, then let $\max(a,b) = a = b$.

Statement A_r:

If $\max(a,b) = r$ then $a = b$

A_1 is true since if $\max(a,b) = 1$ then $a = b = 1$.

Assume :

A_r is true now let $\max(a,b) = r + 1$ (hyp of A_{r+1})

Let $\alpha = a-1, \beta = b-1$

then $\max(\alpha,\beta) = r$

$a = b$ (equation)

If $\max(a,b) = r+1$ then $a = b$ i.e., A_{r+1} is true.

Thus, if A_r is true so is A_{r+1}. So

the statements A_1, A_2, ... A_n are all true.

Now take any positive integers (a,b). Clearly max(a,b) = n (where n is some positive integer).

Since A_n is true and max(a,b) = n we have a = b.

The above argument is fallacious, for a fundamental assumption, namely, α and β are positive integers does not hold for a = b = 1.

CONCLUSION

Having established rigorously the principle of finite and transfinite induction, we can therefore apply the axioms of mathematical induction, knowing that we do not permit ourselves to derive logical inconsistences. This makes it possible for us to accept, without reservation, any mathematical truth which has resorted to this principle for its verification.

BIBLIOGRAPHY

Albert, A. A., College Algebra, McGraw-Hill Book Company, 1946, p. 5

Birkhoff, G., and MacLane, S., A Survey of Modern Algebra, The Macmillan Co., New York, 1949, pp. 11, 12

Bulletin of American Mathematical Society, Vol. 16, (70)

Dickson, L. E., College Algebra, John Wiley & Sons New York, 1902, p. 102

Encyclopedia of Britannica, Vol. 12, pp. 271, 272, 1946, Chicago

Hart, W. L., College Algebra, Revised Edition, D. C. Heath Company, New York, 1938, p. 195

MacDuffee, C. C., Introduction to Abstract Algebra, John Wiley & Sons, New York, 1940, pp. 30, 34, 35

Sierpinski, W., Introduction to General Topology, University of Toronto Press, Toronto, Canada, 1934, p. 231