Mr G's Little Book on

Axiomatic Systems and Fundamental Theorems

Axiomatic Systems,

Branches of mathematics start with the axioms – assumed to be a consistent set of unprovable “truths”. Gödel proved that any axiomatic system powerful enough to contain ordinary arithmetic cannot be both **consistent** and **complete**.

He demonstrated that powerful axiomatic systems can create further axioms that cannot be proved within the system. This means the axiom or its negation can be added to the original system. In this sense all (sufficiently powerful) axiomatic systems are incomplete. That means there are some mathematical problems that can’t be solved but we don’t know which ones they are.

A long standing favourite was “Fermat’s Last Theorem” but after a few hundred years of continuous effort it was eventually cracked.

Godel also proved that **if** you could demonstrate a set of axioms to be consistent then they are inconsistent. This is because you can prove anything in an inconsistent system so if you’ve just proved something within your system that can’t be proved then your system must be faulty.

Whether the axioms are actually true or not is another issue. Truth and provability are different concepts. Amateurs try to extend this concept to any axiomatic system – such as Laws of Justice. But these systems are insufficiently powerful to be considered incomplete.

Peano’s Axioms of Arithmetic

- 1 is a natural number
- Every natural number has a successor
- 1 is not the successor of any natural number.
- Two numbers whose successors are equal are also equal.

  (alternatively just say different numbers have different successors)
- If something is true for an unspecified natural number and its successor and also for 0 then it’s true for all natural numbers.

The first four axioms set up the number system leaving the somewhat problematic fifth axiom (proof by induction). Most secondary students when shown proof by induction feel that some trickery sleight of hand has taken place. This is because you've proved something by an axiom that is assumed true (or at least consistent with the first four axioms).

By Gödel's incompleteness theorem there must exist further axioms. The only currently known example is the Continuum Hypothesis This states that there is no cardinal number κ

$$\aleph_0 < \kappa < 2^{\aleph_0}$$

or put another way $\aleph_1 = 2^{\aleph_0}$

The continuum hypothesis can also be stated as: there is no subset of the real numbers, which has cardinality strictly between that of the reals and that of the integers. It is from this that the name comes, since the set of real numbers is also known as the continuum. Whether this is actually true or not is another matter (though mathematicians lean toward the assumption it is true).

Axioms of Arithmetic

Having established the integers, the number system can be developed to the realm of Real Numbers. Some of these aren't strictly "axioms" because they can be derived from Peano's Axioms through the process of Propositional Calculus. However it is convenient to treat them as fundamental truths not requiring proof.

- **Closure Axiom**

  a + b and ab are unique and real for a,b real

- **Identity Axiom**

  For addition a + 0 = a

  For multiplication a.1 = a

- **Inverse Additive Axiom**

  For addition a + (- a) = 0

  For multiplication a + (1/a) = 1

- **Commutative Axiom**

  For addition a + b = b + a

  For multiplication a.b = b.a

- **Associative Axiom**

  For addition

  (a + b) + c = a + (b + c)

  For multiplication (a.b).c = a.(b.c)

- **Distributative Axiom**

  a (b + c) = a.b + a.c

Zermelo-Fraenkel's Set Theory Axioms

In the following will we use two undefined terms, '*set*' and '*member of* '.

- **Axiom of extensibility**: Two sets with equal members are equal. This states that sets are uniquely defined by their members.

- **Axiom of the empty set** : There is a set that contains nothing. This is called the empty set. This set is written {}.

- **Axiom of unordered pairs** : For any two sets there is a third set that contains those two sets and only those two sets. If A and B are two different sets then we can construct a third set {A,B} containing A and B and only A and B.

- **Axiom of union** : If set A is a set of sets, there is a set B that contains the union of the sets that are members of A.

- **Axiom of infinity** : There exist at least one infinite set. The axiom is needed to form the set of all natural numbers because the previous axioms are not powerful enough to do this. This axiom is similar to the axiom of induction.

- **Axiom of replacement** : If F(x,y) is a formula such that for any x in A, there is a unique y, then there is a set B such that y belongs to it if and only if there is a x in A such that F(x,y) is true.

- **Axiom of the power set** : For any set A there is a set B that includes every subset of A. This set is called the power set of A and is written P(A), which unfortunately looks a bit like probability.

Using these it can be shown that the Peano's axioms hold under a suitable interpretation of 'successor' and 'natural number'. This used to be meaningless to me but the more I read it the more it starts to make some sort of sense.

There is a further axiom called the **Axiom of Choice**. Tarski and Barnard believed the axiom was false so they assumed it true and "proved" the most outlandish possibility – that you could cut up an orange into no less than seven pieces and rearrange them to make an object twice as big (repeating the process ad infinitum). Unfortunately the message the rest of the world's mathematicians got was "my word, isn't maths amazing" so the axiom of choice is still assumed to be true and fortunate for people who like oranges.

Cohen has proved that the axiom of choice is consistent with ZF set theory but also independent – which presumably means you could choose its negation and still have a consistent set theory.

For the record I should mention there is also the **Axiom of Regularity** which prohibits a whole set being a member of itself. Some say this is the least useful of the Zermelo-Fraenkel's Set Theory.

Axioms of Probability

The Fundamental Theorem or The Law of Large Numbers

The average of the results obtained from a large number of trials should be close to the expected value and will tend to become closer as more trials are performed.

Axioms

Kolmogorov defined the three axioms of probability as

- The probability of an event is represented by a real number between 0 and 1.
- The probability that some elementary event in the entire

sample set will occur is 1. More specifically, there are no elementary events outside the sample set.

This is often overlooked in some mistaken probability calculations; if you cannot precisely define the whole sample set, then the probability of any subset cannot be defined either.

- The probability of an event set which is the union of other disjoint subsets is the sum of the probabilities of those subsets. If there is any overlap among the subsets this relation does not hold.

In probability notation the arithmetic sign + was used for OR and x for AND which is the reverse of what might be naively expected. (+ more associated with AND). This is because probability and arithmetic are based on different axiomatic systems.

In modern terminology AND is represented by intersection $\cap$ (the intersection of two sets in a Venn diagram) and OR represented by $\cup$ (union of two sets in a Venn diagram).

Lemmas in probability

From the Kolmogorov axioms one can deduce other useful rules for calculating probabilities:

OR

P(A OR B) = P (A) + P(B) – P(A AND B)

$(P(A \cup B) = P(A) + P(B) - P(A \cap B)$

That is, the probability that A *or* B will happen is the sum of the probabilities that A will happen and that B will happen, minus the probability that A *and* B will happen.

This also follows immediately from the Venn diagram.

The inclusion-exclusion principle is that. $P(\Omega - E) = 1 - P(E)$

That is, the probability that any event will *not* happen is 1 minus the probability that it will.

Conditional Probability

Define conditional probability as P(B/A) as probability B given A has happened.

Assume that P(B/A) is some proportionality of (P(A $\cap$ B) and setting B=A immediately gives

$(P(A \cap B) = P(A) . P(B/A)$

AND

It then follows that A and B are independent if and only if $(P(A \cap B) = P(A) . P(B)$

Euclid's Axioms of Geometry

1. For every point P and every point Q not equal to P there exists a unique line that passes through P and Q.

2. For every segment AB and for every segment CD there exists a unique point E such that B is between A and E and segment CD is congruent to segment BE.

3. For every point O and every point A not equal to O there exists a circle with center O and radius OA.

4. All right angles are congruent to each other.

5. For every line *l* and for every point P that does not lie on *l* there exists a unique line *m* through P that is parallel to *l*.

There are flaws in Euclid's axioms – principally that he doesn't define the concepts of a point and a line. The fifth axiom gave mathematicians centuries of work, trying to derive it from the first four without success. The solution was to assume its negation (either none or many lines) with immediately gives curved geometries. (elliptic and hyperbolic)

Euclid also takes certain common notions. I term these Axioms of logic but I suppose many would laugh at this.

Common Notions

1. Things which are equal to the same thing are also equal to one another.

2. If equals be added to equals, the wholes are equal.

3. If equals be subtracted from equals, the remainders are equal.

4. Things which coincide with one another are equal to one another.

5. The whole is greater than the part.

Theorems of Propositional Calculus

These are the theorems according to Hofstadter.

The symbols of propositional calculus are

< > P Q R … ‘ ∧ ∨ ⊃ ¬ [ ]

- ⊃ If then / implies
- ¬ negation
- ∨ OR (cf addition)
- ∧ AND (cf multiplication)

Joining Rule

If P and Q are theorems then < P ∧ Q> is a theorem

Separation Rule

If < P ∧ Q > is a theorem then both P and Q are theorems.

Double Tilde Rule

¬ ¬ can be deleted from any theorem.

Deduction Theorem (the Fantasy Rule)

If Q can be derived when P is assumed to be a theorem then < P ⊃ Q > is a theorem.

Carry Over Rule

Inside a deduction any theorem from a “reality” on a level higher can be used.

Rule of Detachment (modus ponendo ponens)

If P and $< P \supset Q >$ are both theorems then Q is a theorem.

Contrapositive Rule

$< P \supset Q >$ and $< \neg Q \supset \neg P >$ are interchangeable

"If it's Friday then tomorrow's Saturday" means the same as "If it's not Saturday then yesterday wasn't Friday"

De Morgan's Rule

$< \neg P \wedge \neg Q >$ and $\neg < P \vee Q >$ are interchangeable

"The flag is not moving and the wind is not blowing" means the same as "It is not true that either the flag is moving or the wind is blowing"

The Switcheroo Rule (modus tollendo ponens)

$< P \vee Q >$ and $< \neg P \supset Q >$ are interchangeable.

"Turn left or turn right" means the same as "If you don't turn left then turn right".

Other Fundamental Theorems

Branches of mathematics have fundamental theorems.

Here are the ones I am reasonable familiar with.

Fundamental Theorem of Algebra

Every polynomial equation of degree n with complex coefficients has n complex roots. I have produced a separate paper on this.

Fundamental Theorem of Arithmetic

Every natural number is either prime or can be uniquely factored as a product of primes in a unique way (except 1).

That 28 = 2 x 2 x 7 and no other combination of primes gives this product is not self-evident. So prime numbers are the building blocks, so to speak the bones, out of which the set of natural numbers is built. This is not always true for partial integer number sets.

The Fundamental Theorem of Calculus

Let f be some continuous function defined in closed interval [a,b] and define F as

$$F(x) = \int_a^b f(t)\,dt$$

Then $F'(x) = f(x)$

This is saying that the summation under a curve (the integration) is the inverse of differentiation.

Summary

There are many other fundamental theorems in many branches of mathematics

They generally fall into two groups

- self evidently obvious or
- totally incomprehensible.

Also available in this series is

- On My TI Calculator what's the difference between Sx and σx?

  It's not what I thought for the first 40 years of the scientific calculator

- Beyond Pascal – Multinomials and Dice Throwing

  How a lower set exercise in dice throwing led to the discovery of multinomials

- Conditional Probability and Bayes Theorem

  An investigation into the pitfalls of medical screening

- Hypercomplex Numbers

  Instead of making $i^2 = -1$ as in complex numbers what if we just make $i^2 = 1$

- Propositional Calculus

  Sherlock Holmes was the great <u>inductive</u> detective but not infallible

- The Harmonic Triangle

  How investigating harmonic triangles led to the discovery of a universal series summation formula