An Introduction to Proof-based Mathematics

Harvard/MIT ESP: Summer HSSP

Isabel Vogt

Syllabus

1. **Logistics**

   Class dates: July 10th, 2011 - August 21st, 2011
   MIT Building 4, Room 153
   My email adress: ivogt@college.harvard.edu

2. **Course Description**

   This course will strive to provide an introduction to the fields of abstract algebra, finite geometry, and number theory which rely upon the mathematical cornerstone of proving theorems. In the process of learning about these interesting areas of math seldom touched upon in high school we will cultivate proof strategies.
   The course will be structured with 45 minutes of interactive lecture-style presentation of material, 30 minutes of mediated group work on proving theorems, and then 45 minutes of lecture to wrap up. I plan on showing a couple of interesting mathematical video clips in class.
   There is no required homework in the class, but I will be giving out a few optional "challenge problems" each week. These will be fun extrapolations on class material that will focus less on enforcing what was taught that week, and more on pushing you to make interesting connections of your own. These are, again, entirely optional, but I will hand out solutions to those of you who choose to do them the next week.

3. **Weekly Breakdown**

   - **July 10th**: Introductions, mathematical nomenclature and negation, constructing proofs, finite and infinite sets, binary operations
   - **July 17th**: Introduction to groups: group axioms, permutations, group order, cyclic groups, Abelian groups
   - **July 24th**: Isomorphisms, subgroups, group automorphism, symmetry groups
   - **July 31st**: Fields: field axioms, finite fields, $\mathbb{Z}_p$, field extensions

- **August 7th**: Finite Geometry: finite affine geometry, arithmetic in finite geometry
- **August 14th**: Elementary Number Theory: properties of integers, factorization, primes, congruences, Fermat's little theorem
- **August 21st**: Congruences continued, Selected diophantine equations, Chinese remainder theorem, Fermat's last theorem

4. **LaTeX**

   LaTeX is a user-friendly typesetting software especially designed to typeset math. I highly recommend downloading LaTeX and learning it. I am happy to help anyone create their first documents.

   LaTeX can be downloaded for free:

   - Windows Users: MikTex: http://miktex.org/
   - Mac Users: MacTex: http://www.tug.org/mactex/

   I will provide the LaTeX source for all of the documents I give you, so feel free to copy and reproduce any of my code in making your own LaTeX documents.

5. **Supplementary Texts**

   There is no text in this class, however, if you should feel you would succeed better with a text to supplement class lectures, I highly recommend the following two books

   - A First Course in Abstract Algebra by Fraleigh
   - The Higher Arithmetic by Davenport

An Introduction to Proof-based Mathematics

Harvard/MIT ESP: Summer HSSP

Isabel Vogt

Class 1: Preliminaries and Set Theory

Class Objectives

- Sets and Feilds
- Mathematical Nomenclature
- Negation
- Proof Construction
  - Direct proof
  - Indirect proof (by contradiction)
  - Contraposition
  - Induction
  - Equivalence
- Finite and Infinite Sets
- Cardinality
- The Cantor Set

1. **Sets**

Definition: A set is a well-defined collection of objects called **elements** of the set.

The set of letters in our standard alphabet is defined to be:
$A = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$

If an object is in the set, it is said to be an element of the set, represented by the symbol $\in$

For example: $j \in A$, $\flat \notin A$

This set is said to be **well-defined** as any object can definitively be said to either be an element of the set A or not.

The Null Set $\emptyset = \{\}$

A set may be defined by specifying all of its elements, or a rule by which to determine if a given object is an element of that set as in:
$A = \{\text{HSSP students} \mid \text{HSSP student is enrolled in M4767}\}$

This is read "A is the set of all HSSP students such that the HSSP student is enrolled in M4767"

What is another name for this set?

Examples of Common Sets

$\mathbb{N} = \{0, 1, 2, 3, 4, ...\}$

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$

$\mathbb{Q} = \{x \mid x = \frac{p}{q}, p, q, \in \mathbb{Z}, q \neq 0\}$

2. **Fields**

Fields are relatively difficult to define precisely without talking about groups, so we will return to fields more deeply in about 3 weeks.

A field is a set over which the usual rules of arithmetic we are familiar with hold.

The field axioms are:

(a) Addition is commutative: $a + b = b + a$.

(b) Addition is associative: $(a + b) + c = a + (b + c)$.

(c) Additive identity: $\exists 0$ such that $\forall a \in F, 0 + a = a + 0 = a$.

(d) Additive inverse: $\forall a \in F, \exists -a$ such that $-a + a = a + (-a) = 0$.

(e) Multiplication is associative: $(ab)c = a(bc)$.

(f) Multiplication is commutative: $ab = ba$.

(g) Multiplicative identity: $\exists 1$ such that $\forall a \in F, 1a = a$.

(h) Multiplicative inverse: $\forall a \in F - \{0\}, \exists a^{-1}$ such that $a^{-1}a = 1$.

(i) Distributive law: $a(b + c) = ab + ac$.

The sets over which we normally carry out arithmetic are thus **fields**. It is this property that allows us to build up the algebra we take for granted!

For a taste of things to come:

In the finite field $\mathbb{Z}_5$, $4 * 4 = 1$

We are able to solve linear system of equations because they are associated with fields.

The equation $x^3 + y^3 = z^3$ has no solutions over the field $\mathbb{Z}$ where it clearly has solutions over the field $\mathbb{R}$

3. **Useful Math Jargon and Negation**

Okay! Now it is time to start really getting into formal math notation! I know, what you have all been waiting for!

Useful Math Symbols

- $\in$ (is an element of)
- $\{a|p(a)\}$ (set of a for which $p(a)$ is true)
- $\forall$ (for all)
- $\exists$ (there exists)

A Bumper Sticker: "For every upside-down A there is a backwards E"

Negation

The negation of "$\forall x, P(x)$ is true" is "$\exists x$, for which $P(x)$ is not true."

The negation of "$\exists x$, for which $P(x)$ is true" is "$\forall x, P(x)$ is not true."

This stems from the idea that in order to prove something true for elements of a certain set, you must show it for **all** elements of the set. Yet to disprove something, you must only demonstrate a counter-example.

When negating a statement, also bear in mind that

The negation of "P and Q are true" is "either P or Q is not true."

The negation of "either P or Q is true" is "both P and Q are not true."

Examples:

Negate:
$\forall \epsilon > 0, \forall x_1 > 0, \exists \delta > 0$ such that $\forall x_2 > 0, |x_1 - x_2| < \delta$ implies $|f(x_1) - f(x_2)| < \epsilon$

A statement is true if its negation is false. This leads to the (commonsense-wise absurd) statement dreamed up by John Hubbard: "All 11-legged alligators are orange with blue spots"!!

Negate the above statement:

Why must this be true?

This may be the single most important thing you learn. You will see how important this "11-legged alligator" argument is!

4. **A Process of Abstraction**

Statements to be proved must be formulated in mathematical terms in a process of abstraction that gives concrete constraints with which to work.

Examples:

Informal: The number about which I am thinking is divisible by 3.

Formal:

Informal: Given two sticks of any size, some multiple of the smaller of the two will always yield a length larger than the larger of the two.

Formal:

Informal: If you have more pigeons than holes, at least one hole has more than one pigeon in it.

Formal:

Informal: Every square has either no remainder or a remainder of 1 upon division by 3

Formal:

Now we have the tools to begin exploring proof strategies!

5. **Infinitely Many Prime Numbers**

We will begin by proving the key result in number theory that there are infinitely many prime numbers. This will illustrate some key components of a proof which will be useful in future.

Prime Number: A number p is prime if and only if it is only divisible by 1 and p

The Fundamental Theorem of Arithmetic: Every natural number has a unique factorization into prime factors.

---

6. **Types of Proofs**

   (a) Direct Proof

   RTP: If A, then B

   Method:

   - Begin with A
   - Carry out logical, deductive steps
   - Reach the conclusion B

   Example:

   RTP: If $a, b \in \mathbb{R}, a < b$, then $a < \frac{a+b}{2}$

(b) Indirect Proof (Proof by Contradiction)

It is often easier to prove something indirectly rather than directly.

RTP: If A, then B

Method:

- Given A
- Assume not B
- Carry out logical, deductive steps
- Reach a contradiction
- Therefore the assumption must be false, and A implies B

Example:

RTP: If $a, b \in \mathbb{R}, a < b$, then $a < \frac{a+b}{2}$

(c) Proof by Contraposition

This proof is very similar to proof by contradiction, but subtly different.

Statement: If A, then B
Inverse: If B, then A
Converse: If not A, then not B
Contrapositive: If not B, then not A

Which of these are logically equivalent?

RTP: If A, then B

Method:

- Assume not B
- Carry out logical, deductive steps
- Reach the conclusion not A

Example:

RTP: For $a, b \in \mathbb{R}$, if ab is irrational, then either a or b is irrational

(d) Proof by Induction

I like to think of this as the "staircase argument"

This is the logical equivalent of proving the statement "and so on..."

The goal is to prove a statement $P(n), \forall n \in A$, for some set A (usually $\mathbb{Z}^+$)

Method:

- Base case: prove $P(n)$ for some beginning value of n (usually $n = 1$)
- Inductive Hypothesis: Assume $P(k)$ is true for some $n = k$
- Prove $P(k + 1)$ using the inductive hypothesis

Steps 2 and 3 combine to say, if you are on one step of the staircase, the next step is always true.
Step 1 initializes the process of "climbing the staircase" at some base case.

Example:
RTP: The sum of the first n odd numbers is n^2

RTP: Let $x \in \mathbb{R}$ with $x > -1$ and $x \neq 0$. Show that $(1+x)^n > 1+nx$ holds for every $n \in \mathbb{Z}^+, n \geq 2$

(e) Equivalence

In order to prove "if and only if" statements, one must show implication in **both** directions.

RTP A if and only if B

Method:

- Show A implies B
- Show B implies A

Generally, one direction is very easy to show, the other is challenging.

This is often seen in proving two sets are equal.

In order to prove $A = B$, one must show $A \subset B, B \subset A$

Example

RTP $(n+2)^2 - n^2$ is a multiple of 8 if and only if n is odd

7. **Cardinality**

The cardinality of a set is a measure of the size of a set.

For a finite set of n elements, the cardinality is merely n

The formal definition relies upon bijections

A **bijection** is a function which is invertible, ie it is both one-to-one (injective) and onto (surjective).

Function:

Injective Function:

Surjective Function:

Bijective Function:

Formal definition of finite cardinality: A set X has cardinality n if $\exists$ a bijection f between X and $\{1, 2, 3, ..., n\}$

A set X is **countable infinite** if $\exists$ a bijection f between X and $\mathbb{N} = \{0, 1, 2, 3, ...\}$

RTP: The set $\mathbb{Q}^+$ is countably infinite

RTP: The set $\mathbb{R}$ is uncountable infinite

8. **The Ternary Cantor Set**

The ternary Cantor set is formed by taking the closed line segment $[0, 1]$ and first removing the middle $\frac{1}{3}$ open set $(\frac{1}{3}, \frac{2}{3})$. Then the middle thirds of the remaining closed sets are then removed. This process is repeated to infinity, generating the classic fractal pattern.

Cardinality of the Cantor Set:

We can also determine the length of the Cantor set using the simply found sum of the geometric series of the removed pieces.

The first piece removed is length $\frac{1}{3}$ the second piece removed is size $(\frac{2}{3})(\frac{1}{3})$, the third piece is of size $(\frac{4}{9})(\frac{1}{3})$ and so on.

Total length removed $= \frac{1}{3} + \frac{2}{9} + \frac{4}{27} + ... = \Sigma_{i=0}(\frac{1}{3})(\frac{2}{3})^i = 1$

Something look strange to you? Perhaps the fact that there are uncountably infinite numbers in a set with length 0!?!

This consistently surprising result has come to be termed 'Cantor dust'!

9. **Challenge Problems**

An Introduction to Number-Set, Finite Topology

In finite topology, we start with a finite set X and single out some of its subsets as "open sets." The only requirement on a topology is that the collection of open sets satisfies the following rules (axioms)

- The empty set and the set X are both open.
- The union of two open sets is open. (In general, the union of an infinite number of sets must also be open, but this is irrelevant in the finite case.)
- The intersection of two open sets is open.

We can construct a topology by starting with a collection of sets that are required to be open, called a "subbasis" for the topology.

Taking all possible intersections of sets in the subbasis gives a "basis" for the topology.

Taking all possible unions of sets in the basis gives the complete list of open sets.

A concrete example:

Suppose that we start with $X = \{123456\}$ and choose a subbasis consisting of $\{123\}$, $\{245\}$, and $\{456\}$.

- Find all the other sets that must be open because of the intersection axiom and the empty-set axiom.

- Find all the other sets that must be open because of the union axiom and the axiom that set X is open.

- We now have the smallest collection of open sets that satisfies the axioms and includes the subbasis.

- What is the smallest legal collection of open sets?

- What is the largest legal collection of open sets?

10. A Web-site model for finite topology

    A model for a set of axioms is a set of real-world objects that satisfy the axioms. As a model for finite topology, consider a Web site of six pages, linked together as follows:

    $2 \to 1$, $2 \to 3$
    $1 \to 3$
    $3 \to 1$

    $4 \to 5$, $4 \to 6$
    $5 \to 4$, $5 \to 6$

    Drawing a model will help you to better visualize this.

    In this model, an "open set" is defined by the property that no page in the set can be reached by a link from outside the set. We need to show that this definition is consistent with the axioms for open sets. Let L denote the set of links. For example, $2 \to 1$ is an element of L.

    - Express with quantifiers the condition for a set Y not to be open and negate it to get the condition for a set Y to be open.

      Not open:

      Open:

    - Use an "11-legged alligator" argument to prove that in this model, the empty set is open.

    - Use an "11-legged alligator" argument to prove that in this model, the set X is open.

- Prove by contradiction that the union of two open sets is open.
  If $A \cup B$ is not open,

- Prove that the intersection of two open sets is open.