Textbook notes on Abstract Algebra

David Cardozo

January 25, 2015

The following are notes based on the book *Abstract Algebra* by Dummit & Foote.

0.1 Basics

We shall use the notation $f : A \to B$, and the value of f at a is denoted $f(a)$, that is we shall apply our functions on the left). map is a synonymous of function. The set A is called the domain of f and B the codomain of f. The notation $a \rightarrowtail b$ if f is understood indicates that $f(a) = b$ The set

$$f(A) = \{b \in B | b = f(a), \text{ for some } a \in A\}$$

is a subset of B, called the **range** or **image** if f. Fir each subset C of B the set:

$$f^{-1}(C) = \{a \in A | f(a) \in C\}$$

consisting of the elements of A mapping into C under f the **preimage** or **inverse** image of C under f. For each $b \in B$, the preimage of $\{b\}$ under f is called the **fiber** of f over b. The fibers of f generally contain many elements since there may be many elements of A mapping to the element b.

If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by:

$$(g \circ f)(a) = g(f(a))$$

Some important terminologies: Let $f : A \to B$:

- f is **injective** if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$
- f is **surjective** if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$
- f is **bijective** or it is a bijection if it is both injective and surjective.
- f has a left inverse if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map.
- f has a right inverse if there is function $h : A \to B$ such that $f \circ h : B \to B$ is the identity map on B.

Proposition 1. *Let $f : A \to B$.*

- *The map f is injective if and only if f has a left inverse.*
- *The map f is surjective if and only if f has a right inverse.*
- *The map f is a bijection if and only if there exists $G : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.*
- *If A and B are finite sets with the same number of elements. then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.*

An important remark is that any function is surjective onto its range (by definition).

Lemma 1. *The map f is a bijection if and only if there exists $G : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.*

Proof. Suppose f is a bijection, i.e, f is both surjective and injective. That is, since it is surjective, there exist $g : B \to A$ such that

$$f \circ g = 1_B$$

. Since it is injective, there exist a $g' : B \to A$ such that

$$g' \circ f = 1_A$$

Now let us observe that $g = g'$. Take note that for any $b \in B$.

$$\begin{aligned} g(b) &= 1_A(g(b)) = (g' \circ f)(g(b)) \\ &= ((g' \circ f) \circ g)(b) = (g' \circ (f \circ g))(b) \\ &= (g' \circ 1_B)(b) \\ &= g'(b) \end{aligned}$$

□

Lemma 2. *If A and B are finite sets with the same number of elements. then $f : A \to B$ is bijective if and only if f is injective if and only if f is surjective.*

Proof. Suppose that f is an injective function, then $f(A) = |A|$, this is known as the **cardinality of Image of Injection** and is proven using induction, therefore the subset $f(A)$ of B has the same number of elements of B and so $f(A) = B$, so f is surjective, and this implies is a bijection. □

A **permutation** of a set A is simply a bijection from A to itself. If $A \subseteq B$ and $f : B \to C$, we denote the **restriction** of f to A by $f \restriction_A$

0.2 Properties of the Integers

- **Well Ordering of** $\mathbb{Z}$ If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$.
- If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say a divides b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case we write $a \mid b$, otherwise we write $x \nmid y$
- If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer d, called the **greatest common divisor** of a and b, satisfying:
  - $d \mid a$, and $d \mid b$, and
  - If $e \mid a$ and $e \mid b$, then $e \mid d$

  The notation for d will be (a, b), if it happens that $(a, b) = 1$, we say that a and b are relatively prime.
- If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer l, called the **least common multiple** of a and b satisfying:
  - $a \mid l$ and $b \mid l$, and
  - if $a \mid m$ and $b \mid m$, then $l \mid m$ (so that l is the least such multiple)
- **The Division Algorithm**: if $a, b \in \mathbb{Z}$ and $b \neq 0$, then there exist unique $q, r \in \mathbb{Z}$ such that:

  $$a = qb + r \quad \text{and} \quad 0 \leq r < |b|$$

  where q is the quotient and r is the remainder.
- **The Euclidean Algorithm** It produces the greatest common divisor of two integers.
- If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that:

  $$(a, b) = ax + by$$
- An element p of $\mathbb{Z}^+$ is called a prime if $p > 1$ and the only positive divisors of p are 1 and p.
- The **Fundamental Theorem of Arithmetic** If $n \in \mathbb{Z}$, $n > 1$, then n can be factored uniquely into the product of primes.
- The Euler $\phi -$ function is defined as: for $n \in \mathbb{Z}$ let $\phi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n, i.e., $(a, n) = 1$. For prime p, $\phi(p) = p - 1$, and more generally, for all $a \geq 1$ we have the formula:

  $$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$$

  The function ϕ is multiplicative in the sense that:

  $$\phi(ab) = \phi(a)\phi(b) \quad \text{if} \quad (a, b) = 1$$

PUT LINE HERE!

0.3 Exercises

3. Prove that if n is composite, then there are integers a and b such that n divides ab but n does not divide either a or b. **Solution** Since n is composite, then $n = ab$ with $a < n$ and $b < n$, in both cases, because n cannot divide a positive number smaller than itself, so that $n \mid n = n \mid ab$.

6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.

Lemma 3. *Every nonempty subset $S \neq \varnothing \subseteq \mathbb{Z}^+$ has a minimum.*

Proof. Let us define the set:

$$T = \left\{ n \in \mathbb{Z}^+ \cup \{0\} \,|n \leq s \text{ for all } s \in S \right\}$$

Since $S \neq \varnothing$, we have that $T \neq \mathbb{Z}^+$, this is given by the fact that if $s' \in S$, then $s' + 1 \notin T$. Observe that at most $0 \in T$ to be done! □

7. Prove that if p is a prime, then $\sqrt{p}$ is not a rational number

Proof. Suppose $\sqrt{p}$ is a rational number, in other words:

$$\sqrt{p} = \frac{a}{b} \quad \text{with} \quad (a, b) = 1$$

or equivalently:

$$b^2 p = a^2$$

so we can see that $p \mid a \cdot a$, and we can conclude that $p \mid a$, i.e., $a = kp$ for some integer p. returning to our previous expression, we have that:

$$b^2 p = k^2 p^2$$

so that:

$$b^2 = k^2 p$$

from which we conclude that $p \mid b$, but this is a contradiction since $(a, b) = 1$. Therefore, our assumption that $\sqrt{p}$ is a rational number must be wrong. □

8. Find a formula for the largest power of p which divides $n!$ `https://www.proofwiki.org/wiki/Factorial_Divisible_by_Prime_Power`