Textbook notes on Abstract Algebra

David Cardozo

April 5, 2015

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

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 1.1. *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 $f \restriction_A$

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!

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! $\square$

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. $\square$

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

11. To be asked also.

4 Subgroups

Definition 4.1. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e, $x, y \in H \implies x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$

Proposition 4.1. ***(The Subgroup Criterion)*** *A subset H of a group G is a subgroup if and only if:*

- *$H \neq \varnothing$, and*
- *for all $x, y \in H \implies x \cdot y^{-1} \in H$*

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proof. Suppose H is a subgroup of G, then is certain that (1) and (2) holds, since it contains the identity of G and the inverse of each of its elements and because H is closed under multiplication. It remains to show conversely that if H satisfies both (1) and (2), then $H \leq G$. Let x be any element in H. Let $y = x$ and apply property (2) to deduce that $1 = xx^{-1} \in H$ so H contains the identity of G. Then, again by (2), since H contains 1 and x, H contains the element $1x^{-1}$, that is$x^{-1} \in H$ and H is closed under taking inverses. Finally, if x and y are any two elements of H, then H contains x and y^{-1}, so by (2), H also contains $x(y^{-1})^{-1}$ that is xy Hence H is also closed under multiplication, which proves H is a subgroup of G. □

4.1 Centralizers and Normalizers, Stabilizers and Kernels

We introduce some important families of subgroups of an arbitrary group G.

Definition 4.2. Let A be any nonempty subset of G. Define

$$C_G(A) = \left\{g \in G | gag^{-1} = a \text{ for all } a \in A\right\}$$

This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A

Proposition 4.2. *The centralizer $C_G(A)$ is a subgroup.*

Proof. First we show that is nonempty. Let us observe that $1 \in C_G(A)$ since $1a1^{-1} = a$, so that $C_G(A) \neq \varnothing$. Now let $x, y \in C_G(A)$, so that $xax^{-1} = a$ and $yay^{-1} = a$, observe that since $yay^{-1} = a$, multiplying wisely in both left and right we have $y^{-1}ay = a$ so that $y^{-1} \in C_G(A)$ so now let us consider:

$$\begin{aligned} (xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a \end{aligned}$$

so that $C_G(A)$ is closed under product and taking inverses so that $C_G(A) \leq G$. □

In the special case that $A = \{a\}$ we write $C_G(a)$, observe that $a^n \in C_G(A)$ for all $n \in \mathbb{Z}$

Definition 4.3. Define $Z(G) = \{g \in G | gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the *center* of G.

Remark. The center of a group is a subgroup

Proof. The center of a group is an special case of the centralizer since $Z(G) = C_G(G)$ ☐

Definition 4.4. Define $gAg^{-1} = \left\{gag^{-1} | a \in A\right\}$. Define the **normalizer** of A in G to be the set $N_G(A) = \left\{g \in G | gAg^{-1} = A\right\}$.

Let us remark that if $g \in C_G(A)$ then $gag^-1 = a \in A$ so that $C_G(A) \leq N_G(A)$

4.2 Stabilizers and Kernels of Group Actions

We can indicate that the structure of G is reflected by the sets on which it acts, as follows: if G is a group acting on a set S and s is ome fixed element of S, the *stabilizer* of s in G is the set:

$$G_s = \{g \in G | g \cdot s = s\}$$

Exercise 1. Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G:

1. the kernel of the action,
2. $\{g \in G | ga = a\}$ this subgroup is called the *stabilizer* of a in G.

Solution.

- So let $G \circlearrowright A$, consider $\ker(G \circlearrowright A)$, we want to see that it is in fact a subgroup. First observe that is nonempty since $1 \cdot a = a$ for all $a \in A$ so that 1 belongs to the kernel, now let x, y belong to the kernel, observe that since y is in the kernel $y \cdot a = a$ for all $a \in A$. Now:

$$\begin{aligned} e \cdot s &= s \\ (g^{-1} \star g)s &= s \\ g^{-1} \cdot (g \cdot s) &= s \\ g^{-1} \cdot (s) &= s \end{aligned}$$

and we observe that g^{-1} belongs to the kernel, so that the set is closed under inverses, for multiplication let us observe:

$$\begin{aligned} (x \star y) \cdot s &= x \cdot (y \cdot s) \\ &= x \cdot (s) \qquad\qquad = s \end{aligned}$$

so that is closed under multiplication.

- As above, the same procedure holds but only for a member of s which does not changes the argument above.

Finally, we observe that the fact that centralizers, normalizers and kernels are subgroups is a special case of the facts that stabilizers and kernels of actions are subgroups. Let $S = \mathcal{P}(G)$, the collection of all subsets of G, and let G act on $\mathcal{P}(G)$ by *conjugation* $g \in G$ and $B \in \mathcal{P}(G), B \subset G$:

$$g : B \to gBg^{-1}$$

under this action, we see that the normalizer $(N_G(A))$ is precisely the stabilizer of A in G, $G_s = N_G(A)$, where $s = A \in \mathcal{P}(G)$, so that $N_G(A)$ is a subgroup of G.

Exercise 2. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $a, g \in G$ satisfy the axioms of a (left) group action.

Solution. So let $G \circlearrowright A$, and $A = G$ via: $g \cdot a = gag^{-1}$, let us observe that $1 \cdot a = 1a1^{-1} = a$ so that the first condition holds. Secondly, observe

$$x \cdot (y \cdot a) = x \cdot (yay^{-1}) \qquad = x(yay^{-1})x^{-1} \qquad = (xy)a(xy)^{-1}$$

so that the axioms for an actions are satisfied.

Next let the group $N_G(A)$ act on the set $S = A$ by conjugation, that is for all $g \in N_G(A)$ and $a \in A$

$$g : a \rightarrowtail gag^{-1}$$

Note that this does map A to A by the definition $N_G(A)$ and so gives an action on A. The Kernel of this action is precisely $C_G(A)$ hence $C_G(A) \leq N_G(A)$. Finally $Z(G)$ is the kernel of G action on $S = G$ by conjugation, so $Z(G) \leq G$

4.3 Cyclic Groups and Cyclic Subgroups

Definition 4.5. A group H is *cyclic* if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

In additive notation H is cyclic if $H = \{nx | n \in Z\}$. In both cases will write $H = \langle x \rangle$, we observe that $H = \langle x \rangle = \langle x^{-1} \rangle$ so that it may have more than one generator. **by the law of exponents cyclic groups are abelian**.

Proposition 4.3. *If $H = \langle x \rangle$, then $|H| = |x|$(where if one side of this equality is infinite, so is the other). More specifically:*

- *if $|H| = n < \infty$, then $x^n = 1$, and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and:*
- *if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.*

Proof. Let $|x| = n$ and consider the finite case. The elements $1, x, x^2, \dots, x^{n-1}$ are distinct because if $x^a = x^b$, with say $0 \leq a \leq b < n$, then $x^{b-a} = x^0 = 1$. Contrary to the hypothesis that n was the smallest positive power of x that equals 1. This H has at least n elements and it remains to show that these are all of them. Let x^t is any power of x, we use the Division Algorithm to write $t = nq + k$ where $0 \leq k < n$, so:

$$x^t = x^{nq+k} = x^{nq}x^k = 1x^k = x^k \in \left\{1, x, \dots, x^{n-1}\right\}$$

For the infinite case, observe then that no positive power of x is the identity. If $x^a = x^b$ for some a and b then $x^{a-b} = 1$, which contradicts our hypothesis. So we conclude that distinct power of x are distinct elements of H so $|H| = \infty$ $\square$

Observe that the calculations of distinct powers of a generator of a cyclic group of order n are carried out via arithmetic $\frac{\mathbb{Z}}{n\mathbb{Z}}$, the following reasoning proves that the groups are isomorphic.

Proposition 4.4. *Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m*

Proof. Consider $d = (m, n)$ by the Euclidean Algorithm there exists integers r, s for which $d = rm + sn$, and d is the greates common divisor of m and n. Thus:

$$x^d = x^{mr+ns} = x^{mr}x^{ns} = 1$$

This proves the first assertion. For the second assertion if $x^m = 1$, and let $n = |x|$. If $m = 0$, certainly $n \mid m$, so assume $m \neq 0$. Since some nonzero power of x is the identity, $n \leq \infty$. Let $d = (m, n)$ so by the same observation above:

$$x^d = 1$$

Since $0 < d \leq n$ and n is the smallest positive positive power of x which gives the identity, we must have $d = n$, that is, $n \mid m$ as asserted. $\square$

5 Direct and Semidirect Products and Abelian Groups

5.1 Direct Products

Definition 5.1. The **direct product** $G_1 \times G_2 \times \ldots \times G_n$ of the groups $G_1, G_2, \dots, G_n$ with operations $\star_1, \star_2, \dots, \star_n$, respectively, is the set of n-tuples $(g_1, \dots, g_n)$ where $g_i \in G_i$ with operation defined :

$$(g_1, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, \dots, g_n \star_n h_n).$$

Similarly:

Definition 5.2. The **direct product** $G_1 \times \ldots$ of the groups $G_1, G_2, \ldots$ with operations $\star_1, \ldots$ respectively, is the set of sequences $(g_1, g_2, \ldots)$ where $g_i \in G_i$ with operation defined componentwise:

$$(g_1, g_2, \ldots) \star (h_1, h_2, \ldots) = (g_1 \star_1 h_1, \ldots).$$

Proposition 5.1. *If $G_1, \ldots, G_n$ are groups, their direct product is a group of order $|G_1| \cdots |G_n|$ (if any G_i is infinite, so is the direct product).*

Proof. Prove that it is a group (each of the axiom of a group holds componentwise) and a counting argument should hold. □

Proposition 5.2. *Let $G_1, G_2, \ldots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$ be their direct product.*

1. *For each fixed i the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$ and arbitrary elements of G_i in position i is a subgroup of G isomorphic to G_i:*

   $$G_i \cong \{(1, 1, \ldots, 1, g_i, 1, \ldots, 1) | g_i \in G_i\}$$

   If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and:

   $$G/G_i \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

2. *For each fixed i define $\pi_i : G \to G_i$ by:*

   $$\pi_i((g_1, \ldots, g_n)) = g_i$$

   Then π_i is a surjective homomorphism with:

   $$\ker \pi_i = \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) | g_j \in G_j \text{ for all } j \neq i\}$$

   $$\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times G_n$$

3. *Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$*