Abstract Algebra - Fraleigh text, 2018

Trevor Klar

July 23, 2018

Contents

Note: If you find any typos in these notes, please let me know at trevor.klar.834@my.csun.edu. If you could include the page number, that would be helpful.

1 Groups and Subgroups

1.1 Binary Operations

Definition. A **binary operation** is a function $* : S \times S \to S$. For any $(a, b) \in S \times S$, we notate $*(a, b)$ as

$$a * b.$$

Note that since $*$ is a function, these two properties must hold:

- $*$ is well-defined on all S
- S is closed under $*$.

Definition. Let S be a set equipped with the operation $*$, and let $H \subseteq S$. We say H is **closed under** $*$ if

$$\text{for all } a, b \in H, \text{we also have } a * b \in H.$$

Definition. Let S be a set equipped with the operation $*$. If $H \subseteq S$ is closed under $*$, then

$$*|_H : H \times H \to H$$

is the **induced operation** of $*$ on H. Usually we suppress the notation for the induced operation.

Definition. A binary operation $*$ on a set S is **commutative** iff for all $a, b \in S$, we have

$$a * b = b * a.$$

Definition. A binary operation $*$ on a set S is **associative** iff for all $a, b, c \in S$, we have

$$(a * b) * c = a * (b * c).$$

1.2 Isomorphic Binary Structures

Definition. A **binary algebraic structure** is a set S equipped with a binary operation $*$, notated $\langle S, * \rangle$.

Definition. Let $\langle S, * \rangle$, $\langle S', *' \rangle$ be binary algebraic structures. An **isomorphism** of S with S' is a bijection $\phi : S \to S'$ such that for all $x, y, \in S$,

$$\phi(x * y) = \phi(x) *' \phi(y).$$

If such a map exists, then we say S and S' are **isomorphic** binary structures, and denote this as $S \cong S'$.

Definition. A **structural property** of a binary structure is one that must be shared by any isomorphic structure. An **algebraic property** is a structural property that is characterized in terms of the operation, i.e. associativity.

Definition. Let $\langle S, * \rangle$ be a binary structure. An element $e \in S$ is an **identity** of * if, for all $s \in S$,

$$e * s = s * e = s.$$

1.3 Groups

Definition. A **group** $\langle G, * \rangle$ is a binary structure (and thus is closed under *) such that:

$\mathscr{G}_1$: (Associativity) $*$ is associative,

$\mathscr{G}_2$: (Identity) There exists e an identity for $*$,

$\mathscr{G}_3$: (Inverse) For each $a \in G$, there exists $a' \in G$ which is an inverse of a, that is, $a * a' = e$, where e is the identity under $*$.

Definition. A group $\langle G, * \rangle$ is an **abelian** group if $*$ is commutative.

Theorem (Left and right cancellation laws). Let $\langle G, * \rangle$ be a group. Then for any $a, b, c \in G$,

$$\begin{array}{lrcl} \text{If} & a * b & = & a * c, \\ \text{then} & b & = & c, \end{array}$$

and

$$\begin{array}{lrcl} \text{If} & b * a & = & c * a, \\ \text{then} & b & = & c. \end{array}$$

Theorem. Let $\langle G, * \rangle$ be a group. For all $a, b \in G$, there exist unique $x, y \in G$ such that

$$a * x = b$$

and

$$y * a = b.$$

That is, all linear equations have unique solutions in G.

Theorem. The identity and inverse of a group are unique.

Corollary 1. Let $\langle G, *\rangle$ be a group. For all $a, b \in G$, we have

$$(a * b)' = b' * a'.$$

Definition. The **general linear group** of degree n is the following set of matrices equipped with matrix multiplication:

$$GL(n, \mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \,|\, A \text{ is invertible}\}$$

There is a similar group consisting of invertible linear transformations equipped with function composition:

$$GL(\mathbb{R}^n) = \{T \in \mathscr{L}(\mathbb{R}^n, \mathbb{R}^n) \,|\, T \text{ is invertible}\}$$

1.4 Subgroups

We will now dispense with the $\langle S, *\rangle$ notation unless necessary, and use the symbol $+$ along with juxtaposition to denote abstract "addition" and "multiplication" operations, respectively. Thus, $-a$ and a^{-1} mean exactly what you'd think: inverses of a additive and multiplicative group, respectively.

Definition. If G is a finite group, then the **order** $|G|$ of G is the number of elements in G.

Definition. Let $\langle G, *\rangle$ be a group.

If $H \subset G$ is closed under $*$, and $\langle H, *\rangle$ is itself a group, then H is a **subgroup** of G.

We write $H \leq G$ and $H < G$ to mean subgroup and proper subgroup, respectively.

1.5 Cyclic Groups and Generators

Theorem (Characterization of a subgroup). Let $\langle G, * \rangle$ be a group. $H \subset G$ is a subgroup of G iff:

- (Closure) H is closed under $*$,
- (Identity) The identity e of G is in H,
- (Inverse) For all $a \in H$, we have $a^{-1} \in H$.

Definition. Let G be a group, and let $a \in G$. Then

$$H = \{a^n | n \in \mathbb{Z}\}$$

is called the **cyclic subgroup** of G **generated by** a, and it is denoted as $\langle a \rangle$.

Observe, this includes a^{-1} (a's inverse) as well as $a^0 = e$ (the identity).

Theorem. Let G be a group, and let $a \in G$. Then,

- $\langle a \rangle$ is a subgroup of G, and
- every subgroup that contains a also contains $\langle a \rangle$.

Definition. Let $\langle a \rangle$ be a cyclic subgroup of a group G.
If $\langle a \rangle$ is finite, then the **order of** a is the order $|\langle a \rangle|$ of this cyclic subgroup.

If $\langle a \rangle$ is infinite, then we says that a is of **infinite order**.

Theorem. Every cyclic group is abelian.

Proof Let G be a cyclic group such that a is a generator of G. We will show that for any two $g_1, g_2 \in G$, we have that $g_1 g_2 = g_2 g_1$. Let $g_1, g_2 \in G$. Since a is a generator of G, there exists some $n, k \in \mathbb{Z}$ such that $a^n = g_1$ and $a^k = g_2$. Then,

$$\begin{aligned}
g_1 g_2 &= a^n a^k && \text{since } a \text{ is a generator} \\
&= \underbrace{(a)(a)\cdots(a)}_{n}\underbrace{(a)(a)\cdots(a)}_{k} && \text{by definition} \\
&= \underbrace{(a)(a)\cdots(a)(a)}_{k}\underbrace{(a)\cdots(a)}_{n} && \text{associative property} \\
&= a^k a^n \\
&= g_2 g_1
\end{aligned}$$

and we are done. ■

Division Algorithm for $\mathbb{Z}$ Given a number $n \in \mathbb{Z}$ and divisor $m \in \mathbb{Z}^+$, there exists a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}^+$ such that

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$

Theorem. Any subgroup of a cyclic group is cyclic.

Corollary. The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ for all $n \in \mathbb{Z}$.

Definition. Let $r, s \in \mathbb{Z}^+$. The generator d of the cyclic group

$$H = \{nr + ms : n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor** (gcd) of r and s.

Note: This means that if $\gcd(r, s) = d$, then there exist $n, m \in \mathbb{Z}$ such that

$$d = nr + ms.$$

Definition. Two positive integers are **relatively prime** if their gcd is 1.

Theorem. If r and s are relatively prime and r divides sm, then r divides m.

Proof Since r and s are relatively prime, then there exist $a, b \in \mathbb{Z}$ such that

$$1 = ar + bs.$$

Multiplying by m,

$$m = arm + bsm.$$

Since r divides sm, there exists some $k \in \mathbb{Z}$ such that $kr = sm$.So,

$$m = arm + bkr = (am + bk)r.$$

Thus, r divides m. ■

Definition. Addition Modulo n It's what you think.

$$h + k \mod n = \text{remainder}\big((h + k)/n\big)$$

Theorem. $\mathbb{Z}_n$ under addition mod n is a cyclic group.

Let G be a cyclic group with n elements generated by a.

$$f(x) = \sum_{n=0}^{\infty} \mathrm{proj}_{\sin(nx)} f = \sum_{n=0}^{\infty} \langle f(x), \sin(nx) \rangle \sin(nx)$$

2 More Groups and Cosets

2.1 Groups of Permutations

Definition. A **permutation** of a set A is a bijection $\phi : A \to A$.

Theorem. Let A be a nonempty set, and let S_A be the collection of all permutations of A.

Then S_A is a group under permutation multiplication.

Proof

- (Closure) True by definition.
- (Associative) Composition of functions is associative.
- (Identity) The identity function is a permutation.
- (Inverse) Permutations are bijections, and bijections are invertible.

■

Definition. Let A be a finite group of n elements. The group of all permutations on A is the **symmetric group on** n **letters**, denoted S_n.

Note that S_n has $n!$ elements.

Theorem (Cayley's Theorem). Every group is isomorphic to a group of permutations.

Proof Consider a group

	e	a	b	$\cdots$
e	e	a	b	$\cdots$
a	a	b	c	$\cdots$
b	b	c	d	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Consider ϕ such that $\phi(x) \mapsto$ (the row corresponding to x). Informally, one can see the row is the image of the image of the set in a permutation. ■

Definition (Regular representations). The function ϕ mapping each element of a group to the permutation corresponding to multiplication by that element is called the **left regular representation** and **right regular representation** (for left and right multiplication, respectively). i.e. for the group

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

the left representation is given as follows:

$$\lambda_e = \begin{pmatrix} e & a & b \\ e & e & a \end{pmatrix} \quad \lambda_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix} \quad \lambda_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$$

2.2 Orbits, Cycles, and the Alternating Groups

Definition. Let σ be a permutation of a sat A. The **orbits** of σ are the equivalence classes given by

$$a \sim b \text{ iff } b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}.$$

An orbit is called **nontrivial** if it has more than one element.

Definition. A permutation $\sigma \in S_n$ is a **cycle** if it has at most one nontrivial orbit. The **length** of a cycle is the number of elements in its nontrivial orbit.

Example. Consider the permutation

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1, 3, 5, 4).$$

This is a cycle of length 4, since it has only one nontrivial orbit.

Example. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 7, 5).$$

This is a not a cycle, since it has 3 nontrivial orbits.

Example. Consider the permutation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1, 3, 6)(1, 3, 2)(3, 4, 5) = (1, 6)(2, 3, 4, 5)$$

Note that the product of multiple cycles sometimes simplifies to a product of a smaller number of cycles, perhaps even becoming a cycle in the product. In this case, the product of 3 cycles produced a permutation with 2 nontrivial orbits, so it is not a cycle.

Theorem. Every permutation σ of a finite set is a product of a unique set of disjoint cycles (assuming the identity is not in the set).

Proof Let σ be a permutation of a finite set S. Let $B_1, B_2, \ldots, B_n$ be the orbits of σ (we know this set exists uniquely by construction, and is finite since S is finite). Then, consider the cycles

$$\mu_i(x) = \begin{cases} \sigma(x) & x \in B_i \\ x & \text{otherwise} \end{cases}.$$

Then, since all the orbits B_i are disjoint, then all the cycles μ_i are disjoint. Thus,

$$\prod_{i=1}^{n} \mu_i = \sigma,$$

and we are done. ■

Definition. A cycle of length 2 is a **transposition**.

Corollary. Any permutation of a finite set (with at least two elements) is a product of transpositions.

Proof Since any permutation is a product of disjoint cycles, it suffices to show that any cycle is a product of transpositions. Let

$$(a_1, a_2, \ldots, a_n)$$

be an arbitrary cycle. To see that it is a product of transpositions, compute

$$(a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2) = (a_1, a_2, \ldots, a_n)$$

and we are done. ■

Theorem. No permutation in S_n can be expressed as a product of both an even and an odd number of transpositions.

Proof First, note that we can multiply any permutation by the identity $\iota = (1, 2)(1, 2)$ to change the number of permutations, but this doesn't change the parity (evenness or oddness). Now, consider some permutation μ written as a product of disjoint nontrivial cycles, $\mu = B_1 B_2 \ldots B_n$; and let $\tau = (i, j)$ be some transposition.

Claim: The σ and ■

3 Index