Algebra

from the context of the course
MTH 418H: Honors Algebra

Kaedon Cleland-Host

September 12, 2021

Contents

Chapter 1

Groups

Definition 1.0.1. A **law of composition** is a map $S^2 \to S$.

Remark. We will use the notation ab for the elements of S obtained as $a, b \to ab$. This element is the product of a and b.

Definition 1.0.2. A **group** is a set G together with a law of composition that has the following three properties:

1. **Identity** There exists an element $1 \in G$ such that $1a = a1 = A$ for all $a \in G$.
2. **Associativity** $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. **Inverse** For any $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 1.0.3. An **abelian group** is a group with a commutative law of composition. That is for any $a, b \in G$, $ab = ba$.

1.1 Inverses

Definition 1.1.1. A **left inverse** of $a \in S$ is an element $l \in S$ such that $la = 1$.

Definition 1.1.2. A **right inverse** of $a \in S$ is an element $r \in S$ such that $ar = 1$.

Proposition 1.1.1. If $a \in S$ has a left and right inverse $l, r \in S$ then $l = r$ and are unique.

Proof. Immediately, $la = 1$, $lar = r$, $l = r$. Now, Let $a_1^{-1}, r_2^{-1} \in S$ both be inverse of $a \in S$ We have $a_1^{-1}a = 1$, $a_1^{-1}aa_2^{-1} = a_2^{-1}$, $a_1^{-1} = a_2^{-1}$. □

Proposition 1.1.2. Inverses multiply in reverse order: $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

$$(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aa^{-1} = 1$$
$$b^{-1}a^{-1}(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$$

□

Proposition 1.1.3. Cancellation Law For $a, b, c \in G$ if $ab = ac$ then $b = c$.

Proof.

$$ab = ac$$
$$a^{-1}ab = a^{-1}ac$$
$$b = c$$

□

Remark. Law of cancellation may not hold for non-invertible elements.

Proposition 1.1.4. Let S be a set with an associative law of composition and an identity. The subset of elements of S that are invertible forms a group.

Proof. Let G denote the subset consisting of the invertible elements in S.

1. Closure: Let $a, b \in G$. By definition, they must have inverses $a^{-1}, b^{-1} \in G$. Note that, $ab, b^{-1}a^{-1} \in S$. Now since $abb^{-1}a^{-1} = b^{-1}a^{-1}ab = 1$, ab is invertible and hence $ab \in G$.
2. Identity: Since $1 \in S$ and $11 = 11 = 1$ it is invertible so therefore $1 \in G$.
3. Inverse: Immediately by definition every elements in G is invertible.

Therefore G is a group. □

1.2 Symmetric Groups and Subgroups

Definition 1.2.1. A **Symmetric Group** denoted S_n is the set of unique bijections on the set $\{1, \ldots, n\}$. With function composition as the law of composition.

Remark. This is equivalent to the set of all permutations.

To denote the elements of a symmetric group we use a parentheses with element of the set $\{1, \ldots, n\}$ in the parentheses. Where the first elements maps the next one and the last element maps to the first one. Any elements not included map to themselves.

Example. Consider the elements $1, x, y \in S_n$ where $1 = ()$, $y = (1, 2)$, and $x = (1, 2, 3)$. Immediately we have

$$y^2 = 1$$

$$x^3 = 1$$

Through the cancellation law we find that the following elements are distinct and since $|S_n| = n!$ we have

$$S_3 = \{1, x, x^2, y, yx, yx^2\}$$

Definition 1.2.2. A group H is a **Subgroup** of G if H is subset of G, H has the same law of composition as G, and H is also a group. In other words H a group if it is a subset of G with the following properties:

1. **Closure** $a, b \in H$ then $ab \in H$.
2. **Identity** $1 \in H$.
3. **Inverse** For all $a \in H$, $a^{-1} \in H$.

Definition 1.2.3. A subgroup S of G is a **proper subgroup** if $S \neq G$ and $S \neq \{\mathbb{I}\}$.

Theorem 1.2.1. If S is a subgroup of $\mathbb{Z}^+$, then either

- $S = \{0\}$
- $S = \mathbb{Z}a$, where a is the smallest elements of S.

Proof. Let S be any subgroup of $\mathbb{Z}^+$ If $S = \{0\}$, the statement holds. Otherwise $S \neq \{0\}$. There exists a nonzero integer $n \in S$. If $n \in S$ then $-n \in S$ so S contains a positive integer. Let a be the smallest positive integer in S. Let $(j)a$ denote adding a to itself j times. Since $a \in S$, we have $(2)a \in S$. Now for any $k \in \mathbb{N}$ we see that $(k + 1)a = ka + a \in S$. So, by induction $ka \in S$ for all $k \in \mathbb{N}$. Now it follows that $-ka \in S$ and clearly $0 \in S$. Therefore, $\mathbb{Z}a \subset S$. For any $n \in S$ use division to write $n = qa + r$ for some integers r, q with $0 \leq r < a$. We know $n \in S$ and $qa \in S$. Hence $r = n - qa \in S$. Now since a is the smallest integer, we have $r = 0$. Hence, $n = qa \in \mathbb{Z}a$ and $S \subset \mathbb{Z}a$. Therefore, $\mathbb{Z}a = S$. $\square$