Algebra

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

Kaedon Cleland-Host

October 3, 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 $a, b \in G$, $ab = ba$.

Definition 1.0.4. The **order** of a group G is the cardinality of the set.

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. $\square$

1.2 Subgroups

Definition 1.2.1. 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 1.2.2. A subgroup S of G is a **proper subgroup** if $S \neq G$ and $S \neq \{\mathbb{I}\}$.

Proposition 1.2.1. If H and K are subgroup of G, then $H \cap K$ is a subgroup.

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, $\mathbb{Z}a = S$. $\square$

Definition 1.2.3. For two integers $a, b \in \mathbb{Z}$ we sat that a **divides** b if $\frac{b}{a} \in \mathbb{Z}$ denoted $a|b$.

1.2.1 Greatest Common Divisor

Definition 1.2.4. The **greatest common divisor** of two integers $a, b \in \mathbb{Z}$ is the integer $d \in \mathbb{Z}$ such that

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} | n = ra + sb \forall r, s \in \mathbb{Z}\}$$

Proposition 1.2.2. Properties of the greatest common divisor Let $a, b \in \mathbb{Z}$, not both zero, and let d be the greatest common divisor. Then

1. There are integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$.

2. $d|a$ and $d|b$.

3. If $e \in \mathbb{Z}$ such that $e|a$ and $e|b$ then $e|d$.

Proof. 1. Immediately follows because $d \in \mathbb{Z}d$

2. Similarly, since $a, b \in \mathbb{Z}d$ we have $d|a$ and $d|b$.

3. Lastly, if $e|a$ and $e|b$ then $e|(ra + sb) \Rightarrow e|d$.

$\square$

Definition 1.2.5. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$.

Corollary 1.2.1.1. A pair $a, b \in \mathbb{Z}$ is relatively prime if an only if there are integers $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Corollary 1.2.1.2. Let p be a prime integer. If p divides a product ab if integers, then at least one of $p|a$ or $p|b$ holds.

1.2.2 Least Common Multiple

Definition 1.2.6. The **least common multiple** of two integers $a, b \in \mathbb{Z}$ is the integer $m \in \mathbb{Z}$ such that

$$\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$$

Proposition 1.2.3. Properties of least common multiple Let a, b be non-zero integers and let m be there least common multiple. Then

1. $a|m$ and $b|m$.
2. If $n \in \mathbb{Z}$ such that $b|n$ and $a|n$, then $m|n$.

Proof. Both statements follow from the definition. $\square$

Corollary 1.2.1.3. For $d = \gcd(a, b)$ and $m = $ lcma,b then $ab = dm$.

1.3 Cyclic Groups

Definition 1.3.1. Let G be a group and $x \in G$. The **cyclic subgroup** generated by x denoted $\langle x \rangle$ is

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots\}$$

Remark. For any subgroup S that contains x we have $S \subset \langle x \rangle$.

Definition 1.3.2. The **order of an element** $x \in G$ is the order of the group $\langle x \rangle$. This is the smallest positive integer n such that $x^n = 1$.

Proposition 1.3.1. Let $\langle x \rangle \subset G$ and consider the set $S = \{k \in \mathbb{Z} | x^k = 1\}$

1. The set S is a subgroup of $\mathbb{Z}^+$
2. $x^r = x^s$ $(r \geq s)$ if and only if $x^{r-s} = 1$.
3. If $S \neq \{0\}$, then $S = \mathbb{Z}n$ for some positive $n \in \mathbb{Z}$ and $\langle x \rangle = \{1, x^1, x^2, \dots, x^{n-1}\}$

Proposition 1.3.2. Let x be an element of finite order n in a group and let $k \in \mathbb{Z}$. Let $k = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

1. $x^k = x^r$
2. $x^k = 1$ if an only if $r = 0$.
3. The order of x^k is $n/\gcd(k, n)$.

Chapter 2

Homomorphisms

Definition 2.0.1. A **homomorphism** $\varphi : G \to G'$ is a map from a group G to a group G' such that for any $a, b \in G$ we have

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Proposition 2.0.1. Let $\varphi : G \to G'$ be a homomorphism

1. $\varphi(1) = 1$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ for any $a \in G$

Definition 2.0.2. A homomorphism $\varphi : G \to G'$ is **injective** if $\varphi(x) = \varphi(u) \Rightarrow x = y$

Definition 2.0.3. A homomorphism $\varphi : G \to G'$ is **surjective** if for every $b \in G'$, there exists $a \in G$ such that $\varphi(a) = b$.

Definition 2.0.4. A homomorphism is **bijective** if it is both injective and surjective. We call a bijective homomorphism an **isomorphism**.

Definition 2.0.5. An **automorphism** is an isomorphism $\varphi : G \to G$.

Definition 2.0.6. Let $\varphi : G \to G'$ be a homomorphism

1. The **kernal** of φ denoted $\ker(\varphi)$ is the set
$$\ker(\varphi) = \{a \in G | \varphi(a) = 1\}$$
2. The **image** of φ denoted $\mathrm{Im}(\varphi)$ is the set
$$\mathrm{im}(\varphi) = \{b \in G' | \exists a \in G, \varphi(a) = b\}$$

Corollary 2.0.0.1. A homomorphism $\varphi : G \to G'$ is injective if $\ker(\varphi) = \{1\}$

Corollary 2.0.0.2. A homomorphism $\varphi : G \to G'$ is surjective if $\mathrm{Im}(\varphi) = G'$

Proposition 2.0.2. Let $\varphi : G \to G'$ be a homomorphism the $\ker(\varphi)$ and $\mathrm{Im}(\varphi)$ are subgroups of G and G'

2.1 Relations and Partitions

Definition 2.1.1. A **Relation** of a set X is a subset of X^2. Conventionally written xRy rather than $(x, y) \in R$

2.1.2. Properties of Relation

1. **Reflexive** if xRx for all $x \in X$
2. **Transitive** if xRy and $yRz \Rightarrow xRz$
3. **Symmetric** if $xRy \Leftrightarrow yRx$

Definition 2.1.3. An **Equivalence Relation** is a relation that is Reflexive, Transitive, and Symmetric

Definition 2.1.4. A **partition** S of a set X is a set of subsets of X such that

1. S **covers** X, that is $X \subseteq \bigcup S$
2. S is **pairwise disjoint**, that is $\bigcap S = \emptyset$

Proposition 2.1.1. An **equivalence relation** on a set S uniquely determines a **partition**.

Definition 2.1.5. An **equivalence class** of an element $a \in S$ is the set S_a determined by a relation $\sim$ given by

$$S_a = \{b \in S | a \sim b\}$$

2.2 Cosets and Lagrange's Theorem

Definition 2.2.1. Let H be a subgroup of G. The **left coset** of H induced by an element $a \in G$ is the set

$$aH = \{ah | h \in H\}$$

The **right coset** of H induced by an element $a \in G$ is the set

$$Ha = \{ha | h \in H\}$$

Proposition 2.2.1. Let H be a subgroup of G. The left cosets partition G. The right cosets partition G.

Proof. Consider the equivalence relation on G given by

$$a \sim b \text{ if } b = ah \text{ for some } h \in H$$

To prove this is an equivalence relation we check the following properties

1. For $a \in G$, we have $a = a\mathbb{I}$ and we know $\mathbb{I} \in H$, so $\sim$ is reflective
2. For $a, b \in G$, if $b = ah$, then $a = bh^{-1}$ and since H is a subgroup we have $h^{-1} \in H$. Hence $\sim$ is symmetric.
3. For $a, b, c \in G$, if $b = ah$ and $c = bh'$ for some $h, h' \in H$, then $c = ahh'$ and $hh' \in H$ since H is a subgroup. Hence $\sim$ is transitive.

Therefore, from 2.1.1 the set of all left cosets of H partition G. □

Definition 2.2.2. For a subgroup H of G. The **index of** H **in** G denoted $[G : H]$ is the number of left cosets of H in G.

Lemma 2.3. All left cosets aH and all right cosets Ha of a subgroup H of a group G have the same order.

Lemma 2.4. Counting Formula. For a subgroup H of G we have

$$|G| = |H|[G : H]$$

Theorem 2.4.1. Lagrange's Theorem. Let H be a subgroup of a finite group G. The order of H divides the order of G.

Corollary 2.4.1.1. The order of an element of a finite group divides the order of the group.

Corollary 2.4.1.2. If G is a group of prime order then for $a \in G$ where $a \neq \mathbb{I}$, we have $G = \langle a \rangle$.

Corollary 2.4.1.3. If $\varphi : G \to G'$ is a homomorphism of finite groups then

$$|G| = |\ker(\varphi)||\text{Im}(\varphi)|$$

2.5 Normal Subgroups

Definition 2.5.1. A subgroup N of a group G is **normal** if for every $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Definition 2.5.2. The **conjugate** of $a \in G$ by $g \in G$ is gag^{-1}.

Proposition 2.5.1. For any homomorphism $\varphi : G \to G'$ the $\ker(\varphi)$ is a normal subgroup of G.

Definition 2.5.3. The **center** of a group G is the subgroup

$$Z = \{z \in G | zg = gz \text{ for all } g \in G\}$$

Corollary 2.5.0.1. The center of a group is a normal subgroup.

Lemma 2.6. G is abelian $\Leftrightarrow$ conjugation map is the identity

Proposition 2.6.1. Let $H \subset G$ be a subgroup. Then the following are equivalent

1. H is a normal subgroup.
2. For all $g \in G$, $gHg^{-1} = H$
3. For all $G \in G$, $gH = Hg$
4. Every left coset of H in G is a right coset of H in G.

Corollary 2.6.0.1. If a group G has just one subgroup of order n, then that subgroup is normal.

2.7 Modular Arithmetic

Example. For a choice of positive integer n, consider the equivalence relation on $\mathbb{Z}^+$ given by

$$a \sim b \text{ if } b - a \in \mathbb{Z}n$$

We represent elements in the n equivalence classes with

$$17 \in 2 \mod 5$$

Proposition 2.7.1. The index $[\mathbb{Z} : \mathbb{Z}n] = n$

Lemma 2.8. If $a' \in a \mod n$ and $b' \in b \mod n$, then

- $a' + b' \in a + b \mod n$
- $a'b' \in ab \mod n$

Definition 2.8.1. The group G/N is the set of left cosets of G by N together with the law of composition:

$$(aN)(bN) = (ab)N$$

Theorem 2.8.1. Correspondence Theorem Let $\varphi : G \to G'$ be a surjective homomorphism with kernal K. There is a bijective correspondence between subgroups of G' and subgroup of G that contain K.