Algebra

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

Kaedon Cleland-Host

December 15, 2021

Contents

Chapter 1

Group Theory

1.1 Groups

Definition 1.1.1. 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 1.1.2. 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 1.1.3. An **abelian group** is a group with a commutative law of composition. That is for any $a, b \in G$, $ab = ba$.

Definition 1.1.4. The **order** of a group G is the cardinality of the set.

Proposition 1.1.5. Cancellation Law For $a, b, c \in G$ if $ab = ac$ then $b = c$.

Proposition 1.1.6. 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.

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

Theorem 1.2.4. If S is a subgroup of $\mathbb{Z}^+$, then either

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

Definition 1.2.5. 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 1.2.6. 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 1.2.7. 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 $e|d$.

Definition 1.2.8. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$.

Corollary 1.2.9. 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 1.2.10. 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 1.2.11. 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 1.2.12. 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 $m|n$.

Corollary 1.2.13. For $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$ then $ab = dm$.

1.2.3 Cyclic Groups

Definition 1.2.14. 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 1.2.15. 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 1.2.16. 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 1.2.17. 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 $n/\gcd(k, n)$.

1.3 Homomorphisms

Definition 1.3.1. 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 1.3.2. 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 1.3.3. A homomorphism $\varphi : G \to G'$ is **injective** if $\varphi(x) = \varphi(u) \Rightarrow x = y$

Definition 1.3.4. 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 1.3.5. 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 $\text{Im}(\varphi)$ is the set

$$\text{im}(\varphi) = \{b \in G' | \exists a \in G, \varphi(a) = b\}$$

Corollary 1.3.6. A homomorphism $\varphi : G \to G'$ is injective if $\ker(\varphi) = \{1\}$

Corollary 1.3.7. A homomorphism $\varphi : G \to G'$ is surjective if $\text{Im}(\varphi) = G'$

Proposition 1.3.8. Let $\varphi : G \to G'$ be a homomorphism the $\ker(\varphi)$ and $\text{Im}(\varphi)$ are subgroups of G and G'

Definition 1.3.9. An **isomorphism** is a **bijective** homomorphism. A homomorphism is **bijective** if it is both injective and surjective.

Proposition 1.3.10. If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Definition 1.3.11. Two groups G and G' are **isomorphic** if there is an isomorphism $\varphi : G \to G'$.

Definition 1.3.12. An **automorphism** is an isomorphism $\varphi : G \to G$.

1.4 Cosets

Definition 1.4.1. 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 1.4.2. Let H be a subgroup of G. The left cosets partition G. The right cosets partition G.

Definition 1.4.3. 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 1.4.4. All left cosets aH and all right cosets Ha of a subgroup H of a group G have the same order.

Lemma 1.4.5. Counting Formula. For a subgroup H of G we have

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

Theorem 1.4.6. Lagrange's Theorem. Let H be a subgroup of a finite group G. The order of H divides the order of G.

Corollary 1.4.7. The order of an element of a finite group divides the order of the group.

Corollary 1.4.8. 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 1.4.9. If $\varphi : G \to G'$ is a homomorphism of finite groups then

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

1.5 Normal Subgroups

Definition 1.5.1. A subgroup N of a group G is **normal** if for every $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Proposition 1.5.2. For any homomorphism $\varphi : G \to G'$ the $\ker(\varphi)$ is a normal subgroup of G.

Proposition 1.5.3. 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 1.5.4. If a group G has just one subgroup of order n, then that subgroup is normal.

1.6 Quotient Groups

Definition 1.6.1. If $H \subset G$ is a subgroup. The **Quotient** is defined $G/H = \{\text{left cosets of } H\}$.

Proposition 1.6.2. If $H \subset G$ is a normal subgroup, then G/H is a group with law of composition $[aH][bH] = [abH]$.

Theorem 1.6.3. Correspondence Theorem Let $\varphi : G \to G'$ be a surjective homomorphism with kernal K. There is a bijective correspondence between subgroups of G' and subgroups of G that contain K.

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow G/K$$

1.7 Product Groups

Definition 1.7.1. If G and G' are groups, $G \times G'$ is the **product group** defined

$$G \times G' = \{(g, g')|g \in G, g' \in G'\}$$

with the law of composition

$$(a, a')(b, b') = (ab, a'b')$$

Proposition 1.7.2. Let G be a cyclic group of order mn where $\gcd(m, n) = 1$ then $G \equiv C_m \times C_n$.

Proposition 1.7.3. Let H, K be subgroups of a group G. Consider the multiplication map

$$f : H \times K \to G$$

given by $f(h, k) = hk$. Then

1. f is a homomorphism if an only if $kh = hk$ for all $h \in H$ and $k \in K$
2. f is injective if and only if $H \cap K = \{1\}$
3. if H is normal the image HK of f is a subgroup of G.

In particular, $G \cong H \times K$ under f if and only if $H \cap K = \{1\}$, $HK = G$ and K and H are both normal.

Proposition 1.7.4. The map $\pi : G \to G/N$ defined by $\pi(x) = [aN]$ such that $x \in aN$ is a surjective homomorphism with kernal N.

Theorem 1.7.5. First Isomorphism Theorem Let $\varphi : G \to G'$ be a surjective homomorphism and let N be its kernal.

$$G' \cong G/N$$

1.8 Group Actions

Definition 1.8.1. An **action** of a group G on a set S is a map

$$G \times S \to S$$

$$(g, s) \mapsto g * s$$

such that

1. $1 * s = s$ for all $s \in S$.
2. **Associativity**: $(gg') * s = g * (g * s)$ for all $g, g' \in G$ and $s \in S$.

Definition 1.8.2. Given an action of a group G on the set S, the **orbit** O_s of an element $s \in S$ is

$$O_s = \{gs \in S | g \in G\}$$

Definition 1.8.3. An action of G on S is **transitive** if $S = O_s$ for some $s \in S$.

Definition 1.8.4. The **stabilizer** G_s of an element $s \in S$ is

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

Proposition 1.8.5. Let G be a subgroup of a group G.

1. The action of G on G/H is transitive.
2. The stabilizer $G_{[H]}$ of $[H]$ is the subgroup H.

Theorem 1.8.6. textbfOrbit Stabilizer Theorem Let G be a group action on a set S. For any $s \in S$, there is a bijection

$$\epsilon : G/G_s \leftrightarrow O_s$$

$$[aG_s] \mapsto as$$

such that $\epsilon(g[C]) = g\epsilon([C])$ for all $g \in G$ and $[C] \in G/G_s$

Corollary 1.8.7. Let G be a group acting on a finite set S. Then for any $s \in S$

$$|G| = |O_s||G_s|$$

1.9 Conjugation

Definition 1.9.1. The **conjugate** of $a \in G$ by $g \in G$ is gag^{-1}.

Definition 1.9.2. The **conjugation action** is the action of a group G defined by $G \times G \to G$ with $(g, x) \mapsto gxg^{-1}$.

Lemma 1.9.3. G is abelian $\Leftrightarrow$ conjugation map is the identity

Definition 1.9.4. The **centralizer** of x is the stabilizer of x under conjugation.

$$Z(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$$

Definition 1.9.5. The conjugacy class of x is the orbit of x under conjugation.

$$C(x) = \{gxg^{-1} \in G | g \in G\}$$

Definition 1.9.6. The **center** of a group G is the subgroup

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

Corollary 1.9.7. The center of a group is a normal subgroup.

Corollary 1.9.8. Every centralizer contains the center.

Proposition 1.9.9. The Class Equation The orbits of of conjugation partition the group.

$$|G| = \sum_{\text{conjugacy classes } C} |C|$$

1.10 p-Groups

Definition 1.10.1. A $p-group$ is a group of order p^n for some prime p.

Proposition 1.10.2. The center of a p-group is non-trivial.

Theorem 1.10.3. Fixed Point Theorem LEt G be a p-group action on a finite set S If $|S|$ is not divisible by p, then there is a fixed point for the action of G on S.

Proposition 1.10.4. Every group of order p^2 is abelian.

Corollary 1.10.5. A group of order p^2 is either cyclic or a product of two cyclic groups

Definition 1.10.6. A subgroup $H \subset G$ of order p^e is called a **Sylow p-subgroup**.

Theorem 1.10.7. First Sylow Theorem A finite group whose order is divisible by a prime contains a Sylow p-subgroup.

Corollary 1.10.8. A group whose order is divisible by a prime p contains a Sylow p-subgroup.

Theorem 1.10.9. Second Sylow Theorem Let G be a finite group whose order is divisible by a prime p.

1. The Sylow p-subgroups of G are conjugate subgroups.
2. Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

Corollary 1.10.10. A group G has just one Sylow p-subgroup H if and only if H is normal.

Theorem 1.10.11. Third Sylow Theorem Let G be a finite group whose order $n = p^e m$, with p prime and p not dividing m. Let s be the number of Sylow p-subgroups of G. Then s divides m and $s \equiv 1 \mod p$.