Abstract 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 $a|b$.

1.2.6 Greatest Common Divisor

Definition 1.2.7. 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 1.2.8. 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 1.2.9. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$.

Corollary 1.2.10. 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 1.2.11. 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.

1.2.12 Least Common Multiple

Definition 1.2.13. 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 1.2.14. 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 1.2.15. For $d = \gcd(a, b)$ and $m = \mathrm{lcm}(a, b)$ then $ab = dm$.

1.2.16 Cyclic Groups

Definition 1.2.17. 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 1.2.18. 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 1.2.19. 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 1.2.20. 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 $\mathrm{Im}(\varphi)$ is the set

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

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 $\mathrm{Im}(\varphi) = G'$

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

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

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 $s \equiv 1 \mod p$.

Chapter 2

Ring Theory

2.1 Rings

Definition 2.1.1. A **ring** R is a set with two laws of composition denoted $+$ and $\times$ that satisft the following axioms:

1. (R,+) is an abelian group, with identity denoted 0.
2. Multiplication on R is commutative and associative, with identity element denoted 1.
3. **Distributivity** For all $a, b, c \in R$, we have $a(b + c) = ab + ac$.

Definition 2.1.2. A **subring** H is a subset of a ring R containing 1 such that H is closed under multiplication and $(H, +)$ is a subgroup of $(R, +)$.

Corollary 2.1.3. A subset H of a ring R is a subring if and only if H is closed under addition, subtraction, and multiplication and contained the element 1.

Definition 2.1.4. A **unit** of a ring is an element with a multiplicative inverse.

Definition 2.1.5. A **field** is a ring F where every nonzero element is a unit.

Proposition 2.1.6. Let R be a ring. $0 = 1$ in R if and only if R is the zero ring.

2.1.7 Polynomial Rings

Definition 2.1.8. A **polynomial** with coefficients $a_i \in R$ in a ring R is a finite linear combination of powers of x^i

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Definition 2.1.9. The **degree** of a polynomial f is the largest n such that $a_n \neq 0$.

Definition 2.1.10. A polynomial f is **monic** if $a_n = 1$ where $n = \deg f$.

Definition 2.1.11. For a ring R the **polynomial ring** denoted $R[x_1, \ldots, x_r]$ is the ring of polynomials constructed from linear combinations of powers of the variables $x_1, \ldots, x_r$.

Proposition 2.1.12. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ be sets of variables. There is a unique isomorphism

$$R[x, y] \to R[x][y]$$

which is the identity on R and sends $x \mapsto x$, $y \mapsto y$.

2.2 Ring Homomorphisms

Definition 2.2.1. A **ring homomorphism** $\varphi : R \to R'$ is a map such that for all $a, b \in R$

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$
3. $\varphi(1) = 1$

Definition 2.2.2. A **ring isomorphism** is a bijective ring homomorphism.

Proposition 2.2.3. Substitution principle Let $\varphi : R \to R'$ be a ring homomorphism, and consider the polynomial ring $R[x_1, \ldots, x_n]$. For any elements $a_1, \ldots, a_n \in R'$ there is a unique homomorphism $\psi : R[x_1, \ldots, x_n] \to R'$ such that

1. $\psi(c) = \varphi(c)\ \forall c \in R$.
2. $\psi(x_i) = a_i$

Definition 2.2.4. The **kernel** of φ is the set

$$\ker \varphi = \{s \in R | \varphi(s) = 0\}$$

2.3 Ideals

Definition 2.3.1. An **ideal** I of a ring R is a nonempty subset of R such that I is closed under addition and if $s \in I$ and $r \in R$ then $rs \in I$.

Definition 2.3.2. A **principle ideal** generated by an element $a \in R$ in a ring R is the ideal

$$(a) = aR = Ra = \{ra | r \in R\}$$

Definition 2.3.3. An ideal is **proper** if it is neither $\{0\}$ nor R.

Definition 2.3.4. An **ideal generated by** a set of elements $a_1, \ldots, a_n \in R$ in a ring R is the ideal

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n | r_1, \ldots, r_n \in R\}$$

Proposition 2.3.5. The kernel of a ring homomorphism is an ideal.

Proposition 2.3.6. The only ideals of a ring R are (0) and (1) if an only if R is a field.

Corollary 2.3.7. Every homomorphism $\varphi : F \to R$ from a field F to a ring R is injective.

Proposition 2.3.8. The ideals in $\mathbb{Z}$ are the principle ideals $(a) = a\mathbb{Z}$ for $a \in \mathbb{Z}$.

Proposition 2.3.9. The ideals in $F[x]$ (where F is a field) is a principle ideal generated by a unique monic polynomial of lowest order.

2.4 Quotient Rings

Definition 2.4.1. The **quotient ring** R/I where I is and ideal of the ring R is the ring of cosets of I.

Theorem 2.4.2. There is a unique rings structure on the set R/I such that $\pi : R \to R/I$ given by $a \mapsto [a + I]$ is a ring homomorphism with kernel I.

Theorem 2.4.3. First Isomorphism Theorem Let $f : R \to R'$ be a surjective ring homomorphism with kernel K. Then there is a unique isomorphism $\bar{f} : R/K \to R'$.

Theorem 2.4.4. Correspondence Theorem Let $\varphi : R \to R'$ be a surjective ring homomorphism with kernel K. There is a bijective correspondence

$$\{\text{ideals of } R \text{ that contain } K\} \leftrightarrow \{\text{ideals of } R'\}$$

2.5 Maximal Ideals

Definition 2.5.1. A **maximal ideal** M of a ring R is an ideal such that $M \neq R$ and there are not ideals I such that $M \subsetneq I \subsetneq R$.

Proposition 2.5.2.

1. For an surjective ring homomorphism $\varphi : R \to R'$ with kernel K. The image R' is a field if and only if K is a maximal ideal.
2. An ideal I of a ring R is maximal if and only if R/I is a field.
3. The zero ideal of a ring R is maximal if and only if R is a field.

Proposition 2.5.3. The maximal ideals of $\mathbb{Z}$ are the ideals (p) where p is prime

Proposition 2.5.4. The maximal ideals of $F[x]$ where F is a field are the principle ideals generated by monic irreducible polynomials.

Theorem 2.5.5. Hilbert's Nullstellensatz There is a bijective correspondence

$$\{\text{points in } \mathbb{C}^n\} \leftrightarrow \{\text{maximal ideals in } \mathbb{C}[x_1, \ldots, x_n]\}$$

2.6 Algebraic Geometry

Definition 2.6.1. A point $p = (a_1, \ldots, a_n)$ of $\mathbb{C}^n$ is a **zero** of a polynomial $f(x_1, \ldots, x_n)$ if $f(a_1, \ldots, a_n) = 0$.

Definition 2.6.2. The **common zeros** of the set S are the points in $\mathbb{C}^n$ at which all the polynomials in S are zero.

Definition 2.6.3. A subset V of $\mathbb{C}^n$ is an **algebraic variety** if V is the set of common zeros of a finite number of polynomial in $\mathbb{C}[x_1, \ldots, x_n]$.

Theorem 2.6.4. Let $I = (f_1, \ldots, f_r)$ be an ideal of $\mathbb{C}[x_1, \ldots, x_n]$ and let V be the variety in $\mathbb{C}^n$ of common zeros of $f_1, \ldots, f_r$. Then the points of V are in bijective correspondence with the maximal ideals of the quotient ring $R = \mathbb{C}[x_1, \ldots, x_n]/I$.

Theorem 2.6.5. Let R be a ring. Every ideal I of R with $I \neq R$ is contained in a maximal ideal.

Corollary 2.6.6. The only ring having no maximal ideals is the zero ring

Corollary 2.6.7. If a system of polynomial equations $f_1, \ldots, f_r = 0$ in n variables has no solution in $\mathbb{C}^n$, then there exists $g_1, \ldots, g_r \in \mathbb{C}[x_1, \ldots, x_n]$ such that

$$1 = \sum g_i f_i$$

Definition 2.6.8. The field $\mathcal{F} = \mathbb{C}(t)$ is the set of equivalence classes of fractions f/g, where $f, g \in \mathbb{C}[t]$ and $g \neq 0$, where f/g and f'/g' are equivalent if there exists $q \in \mathbb{C}[t]$ such that $f = qf'$ and $g = qg'$.

Proposition 2.6.9. Let $h(t, x)$ and $f(t, x)$ be nonzero elements of $\mathbb{C}[t, x]$. Suppose that h is not divisible by any polynomial of the form $t - \alpha$. If h divides f in $\mathcal{F}[x]$ then h divides f in $\mathbb{C}[t, x]$.

Theorem 2.6.10. Two nonzero polynomials $f(t, x)$ and $g(t, x)$ have only finitely many common zeros in $\mathbb{C}^2$, unless they can a common nonconstant factor in $\mathbb{C}[t, x]$