Algebra

Xuzhe Xia

January 1, 2023

Contents

Chapter 1

Group Theory

Notation.

- **1** denote the identity element distinguish from 1.
- Denote u^{-1} the inverse of u.
- $a \cdot b$ can be written as ab for short.
- If r is finite, we write $r < \infty$.

1.0 Overview

1.1 Monoid

Definition 1 (Monoid). A *monoid* is a triple $(M, \cdot, \mathbf{1})$ in which

1. M is non-empty set,
2. $\cdot$ is an associate binary operation in M,
3. $\mathbf{1} \in M$, such that $\forall a \in M, \mathbf{1} \cdot a = a = a \cdot \mathbf{1}$.

Remark. $\mathbf{1}$ is unique.

Definition 2 (Monad; Semigroup).

- Dropping associativity of p from a monoid results a *monad*.
- Dropping identity element from a monoid results a *semigroup*.

Definition 3 (Submonoid). Let M be a monoid.
A subset N is *submonoid* of M if

- $\mathbf{1} \in N$,
- $\forall n_1, n_2 \in N$, $n_1 \cdot n_2 \in N$.

Remark.

- A submonoid is a monoid.
- A submonoid of a submonoid of M is a submonoid of M.

Example. Let $M(S)$ be a set of all transformation of S, $\cdot$ be the function composition, $\mathbf{1}$ be the identity transformation, then $(M(S), \cdot, \mathbf{1})$ is a monoid.

Definition 4 (Monoid of transformation). Let S be a set, and $M(S)$ be the set of transformation of S, then a submonoid of $M(S)$ is called a *monoid of transformation (of S)*.

Definition 5 (Order of monoid). The *order of a monoid* is its cardinality, denoted by $|M|$.

Remark. The order of the monoid of transformation of $S = \{1, 2, \cdots, n\}$ is n^n.

Definition 6 (Finite). A monoid is *finite* if it has finite order.

1.2 Group

Definition 7 (Invertible). An element u of a monoid M is said to be *invertible* if there exists $v \in M$ such that $uv = \mathbf{1} = vu$.
Such v is called the *inverse* of u.

Remark. Let M be a monoid. $\forall u \in M$, if u is invertible, then its inverse is unique.

Definition 8 (Group; Subgroup).

- A *group* G is a monoid all of whose elements are invertible.
- Let G be a group. A subset of G is a *subgroup of* G if it is a group.

Definition 9 (Group of units). The set of invertible elements of the monoid M is called the *group of unites of* M, denoted by $U(M)$.

Definition 10 (Symmetric group). Let S be a set.
The *symmetric group* of S is $U(M(S))$, the set of invertible transformation (bijection) of S.

Definition 11 (Permutation). Let $S = \{1, 2, \cdots, n\}$, a *permutation* of S is an element of the symmetric group S_n of S.

Proposition 1. The order of S_n is $n!$.

Definition 12 (Group of transformations / Transformation group; Permutation group).

- Let S be a set, and $G(S)$ be the symmetric group of S, then a subgroup of $G(S)$ is called a *group of transformations (of S)*.
- If S is finite, then we call the group of transformations of S the *permutation group (of S)*.

Definition 13 (Direct product). Let $M_1, M_2, \cdots, M_n$ be given monoids. The *direct product* $M = M_1 \times M_2 \times \cdots \times M_n$ *of the monoids* M_i is defined as $\{(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n) : a_i, b_i \in M_i\}$.

Remark. The direct product of monoids is still a monoid.

1.3 Isomorphism

Definition 14 (Isomorphism). Two monoids $(M, \cdot, \mathbf{1})$ and $(M', *, \mathbf{1}')$ are said to be *isomorphic* (denoted by $M \cong M'$) if there exists a bijective map $\eta : M \to M'$ such that:

$$\eta(\mathbf{1}) = \mathbf{1}', \qquad \eta(x \cdot y) = \eta(x) * \eta(y), \qquad \forall x, y \in M$$

Proposition 2. Isomorphism is an equivalence relation on all monoids.

Theorem 1 (CAYLEY'S THEOREM FOR MONOIDS AND GROUPS).

1. Any monoid is isomorphic to a monoid of transformations.
2. Any group is isomorphic to a transformation group.

Proof. Idea: Let $(M, \cdot, 1)$, we could set up an isomorphism of $(M, \cdot, 1)$ with a monoid of transformations of the set M itself. □

Corollary. Any finite group of order n is isomorphic to a subgroup of the symmetric group S_n.

1.4 Associativity and Commutativity

Associativity

Let $\{a_i\}$ be a finite sequence of elements of a monoid M.

Lemma 1. Define $\prod_1^n a_i$ by $\prod_1^1 a_i = a_1$, $\prod_1^{r+1} a_i = (\prod_1^r a_j)a_{r+1}$. Then

$$\prod_1^n a_i \prod_1^m a_{n+j} = \prod_1^{n+m} a_k.$$

Remark. For a given product $a_1 a_2 \cdot a_n$, the parentheses does not affect the result.

Definition 15 (Power).

- The *n-th power of* a is $a^n = a_1 a_2 \cdots a_n$ where all $a_i = a$.
- Define $a^0 = \mathbf{1}$.
- If a is invertible, then define $a^{-n} = a_1^{-1} a_2^{-1} \cdots a_n^{-1}$ where all $a_i^{-1} = a^{-1}$.

Remark.

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}, \qquad \forall m, n \in \mathbb{N}$$

If in addition a is invertible, then the above holds for all $m, n \in \mathbb{Z}$

Commutativity

Definition 16 (Commute). Elements a, b of a monoid M said to *commute* if $a \cdot b = b \cdot a$.

Definition 17 (Commutative monoid; Abelian group).

- A monoid is a *commutative monoid* if $\forall a, b \in M$, a, b commute.
- An *Abelian group* is a commutative group.

Definition 18 (Centralizer; Center). Let M be a monoid.

- Let $a \in M$, the *centralizer of* a, $C_M(a)$ is $\{b \in M : a, b \text{ commute}\}$.
- Let $A \subseteq M$, the *centralizer of* A, $C_M(A) = \bigcap_{a \in A} C_M(a)$.
- $C_M(M)$ is the *center* of M.

Remark.

- The centralizer $C_M(a)$, $C_M(A)$ of a monoid M is a submonoid of M.
- The centralizer $C_G(a)$, $C_G(A)$ of a group G is a subgroup of G.

Proposition 3. Let $a_1, a_2, \cdots, a_n \in M$ such that $a_i a_j = a_j a_i$ for all i, j.
Then the product $a_1 a_2 \cdots a_n$ is invariant under all permutations. In particular, if $ab = ba$, then

$$(ab)^m = a^m b^m \qquad \forall m \in \mathbb{N} \cup \{0\}$$

If in addition a, b are invertible, then the above holds for $m \in \mathbb{Z}$.

1.5 Generator

We can approach the definition of generator in two ways. One is through a non-constructive way:

Definition 19 (Generator). Let S be a subset of a monoid M (or a group G), and let $\{M_\alpha\}$ (or $\{G_\alpha\}$) be the set of all submonoids (or subgroup) of M (or G) which contain the set S. Then the *submonoid (or subgroup) generated by* S is

$$\langle S\rangle = \bigcap_\alpha M_\alpha \quad \left(\text{or} \quad \langle S\rangle = \bigcap_\alpha G_\alpha\right)$$

Another is through a constructive way:

Definition 20 (Generator). Let S be a subset of a monoid M (or a group G), then the *submonoid (or subgroup) generated by* S is

$$\langle S\rangle = \{\mathbf{1}, \prod_{i=1}^{n} s_i : s_i \in S, n \in \mathbb{N}\}$$

$$\left(\text{or} \quad \langle S\rangle = \{\mathbf{1}, \prod_{i=1}^{n} s_i : s_i \in S \vee s_i^{-1} \in S, n \in \mathbb{N}\}\right)$$

In the case where $\langle S\rangle = M$ (or G), we say S a set of *generators* of M (or G).

Remark. $\langle S\rangle$ is a submonoid (or subgroup) of M.

The **Definition 20** tells us that the submonoid generated by S is the smallest submonoid of M that contains S.

Proposition 4. Given $S \subseteq M$. Obtain $\langle S\rangle$ from the **Definition 20**, $\langle S\rangle'$ from the **Definition 21**, $\langle S\rangle = \langle S\rangle'$.

1.6 Cyclic group

Definition 21 (Cyclic group; Order of element)**.** Let G be a group and $a \in G$. The *cyclic group with generator* a is $\langle a \rangle$. The *order of* a, denoted by $o(a)$, is the order of $\langle a \rangle$.

Remark. Cyclic groups are Abelian.

Lemma 2.

1. A cyclic group of order infinite is isomorphic to $\mathbb{Z}$
2. A cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Theorem 2. Any two cyclic groups of the same order are isomorphic.

Theorem 3. Any subgroup of a cyclic group $\langle a \rangle$ is cyclic.

- If the order of $\langle a \rangle$ is infinite, then the order of its non-$\langle \mathbf{1} \rangle$ subgroup is also infinite, moreover, there exists a bijection from $\mathbb{N}$ to the set of subgroups of $\langle a \rangle$.
- If $\langle a \rangle$ is or order r, then the order of every subgroup of $\langle a \rangle$ is a divisor of r, and for every positive divisor q of r, $\langle a \rangle$ has one and only one subgroup of order q.

Corollary. Let $\langle a \rangle$ be a cyclic group of order $r < \infty$, and H is a subgroup of $\langle a \rangle$ of order $q|r$. Then $H = \{b \in \langle a \rangle : b^q = \mathbf{1}\}$.

Definition 22 (Exponent)**.** Let G be a finite group. The *exponent*, $\exp(G)$, of G is the smallest positive integer e such that $\forall x \in G, x^e = \mathbf{1}$.

Lemma 3. Let g and h be elements of an Abelian group G having finite relatively prime orders m and n respectively (that is, $\gcd(m, n) = 1$). Then $o(gh) = mn$.

Lemma 4. Let G be an Abelian group with finite number of generators (or called *finitely generated abelian group*), $g \in G$ of maximal order. Then $\exp(G) = o(g)$.

Theorem 4. Let G be an finitely generated abelian group. Then G is cyclic if and only if $\exp(G) = |G|$.

1.7 Cycle and Alternating group

Definition 23 (r-cycle)**.** An *r-cycle*, is a permutation of γ of $\{1, 2, \cdots, n\}$ such that permutes a sequence of r elements $i_1, i_2, \cdots, i_r \in \{1, 2, \cdots, n\}$ cyclically in the sense that:

$$\gamma(i_1) = i_2, \quad \gamma(i_2) = i_3, \cdots, \gamma(r_{r-1}) = i_r, \quad \gamma(i_r) = i_1$$

and leaves order elements unchange.
We denote it as $(i_1 i_2 \cdots i_r)$, and the *length* of it is r.

Definition 24 (Disjoint)**.** Two cycles γ, γ' are said to be *disjoint* if their symbols contains no common letters.

Proposition 5. An r-cycle γ is of order r.

Proposition 6. Two disjoint cycles commute under function composition.

Proposition 7. Let α be a product of disjoint cycles, that is

$$\alpha = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots (l_1 l_2 \cdots l_u)$$

Let $m = \text{lcm}(r, s, \cdots, u)$. Then m is the order of α.

Proposition 8. Every permutation of $\{1, 2, \cdots, n\}$ can be factored as a product of disjoint cycles. Apart from the commutation of these disjoint cycles, this factorization is unique.

Definition 25 (Transposition)**.** A 2-cycle is called a *transposition*.

Remark. An r-cycle, $(i_1 i_2 \cdots i_n) = (i_1 i_r) \cdots (i_1 i_3)(i_1 i_2)$, is a product of $r - 1$ transpositions.

Definition 26 (Sign of permutation)**.** Let σ be a permutation, and $C_1 \cdots C_r$ a product of disjoint cycles that factor σ. Let the length of C_i be l_i. Then the *sign* of σ is

$$\text{sign}(\sigma) = (-1)^{(l_1-1)+(l_2-1)+\cdots+(l_r-1)}$$

We say σ is even if $\text{sign}(\sigma) = 1$ and odd if $\text{sign}(\sigma) = -1$.

Lemma 5. Let (ab) be a transposition, and $(ac_1 \cdots c_h b d_1 \cdots d_k)$ be a $(h + k + 2)$-cycle. Then

$$(ab)(ac_1 \cdots c_h b d_1 \cdots d_k) = (bd_1 \cdots d_k)(ac_1 \cdots c_h)$$

and

$$(ab)(bd_1 \cdots d_k)(ac_1 \cdots c_h) = (ac_1 \cdots c_h bd_1 \cdots d_k)$$

Proposition 9. Let σ_1, σ_2 be permutations, then

$$\operatorname{sign}(\sigma_1\sigma_2) = \operatorname{sign}(\sigma_1)\operatorname{sign}(\sigma_2)$$

Corollary. If $\sigma \in S_n$ is a product of k transpositions, then $\operatorname{sign}(\sigma) = (-1)^k$

Proposition 10. Let σ be a permutation. Let $\tau_1 \cdots \tau_k$ and $\tau_1' \cdots \tau_l'$ be two factorizations of σ for which $\tau_1, \cdots, \tau_k, \tau_1', \cdots, \tau_l'$ are transpositions. Then $l \equiv k \pmod 2$.

Corollary. Even permutations form a subgroup of S_n (symmetric group of $\{1, 2, \cdots, n\}$). We call this subgroup the *alternating group of degree* n and is denoted by A_n.

Remark. $|A_n| = \frac{n!}{2}$

1.8 Lagrange's theorem

Let G be a group, $H \subseteq G$ be a subgroup, $g_1, g_2 \in G$. We define $g_1 \sim g_2$ if

$$\exists h \in H \text{ s.t. } g_2 = g_1 h$$

Remark. $\sim$ is an equivalence relation on G.

Definition 27 (Left coset). Equivalence classes for $\sim$ are called *left cosets* of H in G. The *left coset containing* g is

$$gH = \{gh : h \in H\}$$

The set of left cosets of H in G is denoted by G/H.
The order of G/H is denoted by $[G : H]$, called the *index of* H *in* G.

Lemma 6. Every coset gH has $|H|$ elements.

Theorem 5 (LAGRANGE'S THEOREM). Let G be a finite group, $H \subseteq G$ be a subgroup. Then

$$|G| = |H|\,[G : H] \tag{1.1}$$

in particular, $|H|$ divides $|G|$.

Corollary. Let G be a group, $g \in G$, take $H = \langle g \rangle$, then $|H|$ divides $|G|$.
If $|G|$ is prime, then $|H| = 1$ or $|G|$. If $|H| = |G|$, then $H = G$ and G is cyclic.

Corollary. G is finite, $g \in G$, then $g^{|G|} = 1$.

1.9 Normalizer

We want to define multiplication on coset, such that $g_1H \cdot g_2H$ is well-defined.

Definition 28 (Normal). Let G be a group, and $H \subseteq G$ be a subgroup. Then H is *normal* if $\forall g \in G$, $gHg^{-1} = H$.

Proposition 11. If H is normal in G, then $\forall g \in G$, $gH = Hg$.

Proof. $\forall h \in H$, $ghg^{-1} = h_1 \in H \Leftrightarrow gh_1 = h_1g$ for some $h_1 \in H$, which implies $gH \subset Hg$. □

This lead to an equivalent definition of *normal*.

Definition 29 (Normal). Let G be a group, and $H \subseteq G$ be a subgroup. Then H is *normal* if $\forall g \in G$, $gH = Hg$.

Note.

- $gH \subseteq G$ is a subset
- $gH \in G/H$ is an element

1.10 Group Action

1.10.1 Group Action

Definition 30 (Group Action). Let G be a finite group and X be a finite set.
An *action of G on X* is a homomorphism:

$$\varphi : G \to \text{ group of permutation of } X$$

Definition 31 (Conjugation). Let $X = G$, a conjugation of X by $g \in G$ is:

$$\varphi(g) : X \mapsto gXg^{-1}$$

Corollary. Conjugation is a group action.

Remark. Consider conjugation action φ,

1. $\text{kernel}(\varphi) = \{g \in G : \forall x \in X, gxg^{-1} = x\}$.
2. $\text{kernel}(\varphi) = Z(G)$
3. $\text{kernel}(\varphi) = G \Leftrightarrow G$ Abelian.

Observe. Once we have the definition of group action, we can ask two questions:

1. What other states in S are reachable from s? (orbits)
2. What are the group elements in G does not move s? (stabilizer)

1.10.2 Orbit

Definition 32. Consider G, X, φ
Define $x \sim y$ to be the relation satisfying:

1. $x, y \in X$
2. $\exists g \in G$ with $\varphi(g)x = y$

Intuition. $x \sim y$ iff there is a $g \in G$ that moves x to y, or there exists a permutation in the image $\varphi(G)$ containing a cycle $(\cdots xy \cdots)$.

Corollary. The above relation is an equivalent relation.

Proof. The symmetry and transitivity relies on the fact that φ is homomorphism.
Whole proof omitted. □

Definition 33 (orbit). The orbit of $x \in X$ is $[x]$.

Remark. $X = \bigsqcup$ orbits.

Example. $X = G$, consider the action: $\varphi : x \mapsto gx$, the only one orbit is X itself, because $\forall x, y \in X$, let $g = yx^{-1}$, clearly $gx = y$.

Definition 34 (Transitive action). Actions with only 1 orbit are called to be transitive.

Remark. Action $\varphi : x \mapsto gx$ is transitive.

Observe. Given a transitive action, we can get from any $x \in X$ to any $y \in X$.

Remark. Action $\varphi : x \mapsto gxg^{-1}$ is **not** transitive.

Example. Give G is Abelian, and the conjugation action φ,

$$x \sim y \Leftrightarrow \exists g \in G \text{ s.t. } gxg^{-1} = y \Leftrightarrow x = y$$

Therefore, the orbits are one element set.

Proposition 12. Consider conjugation action, if G is non-Abelian, then $x \sim y \Rightarrow o(x) = o(y)$.

Observe. Every orbit under conjugation action consist elements of the same order, which means that we can get at least one orbit for elements of the same order. (In general, the order of elements is not enough to specify orbits)

Definition 35 (Conjugacy class). The orbit under conjugation action $[x] = \{gxg^{-1} : g \in G\}$ is the conjugacy class.

Example. Let $H \subseteq G$, $X = G$, and H acts on X by translation: $\varphi : x \mapsto hx$, then the right coset $Hx = \{hx : h \in H\}$ is an orbit of x. Intuitively, G breaks into orbits, and each coset is an orbit.

Example. Let $H < G$, $X = G/H$ (Quotient group), and G acts on X by $\varphi : xH \mapsto g(xH)$, this action is **transitive** because that $\forall xH, yH \in X$, let $g = yx^{-1}$, clearly $g(xH) = gxH = yH$.

1.10.3 Stabilizer

Definition 36 (Stabilizer). Consider group action G on X, the *stabilizer of* $x \in X$ *under* G is

$$\text{stab}_G(x) = \{g \in G : gx = x\}$$

Proposition 13. $\text{stab}_G(x)$ is a subgroup of G.

Remark. Consider G acting on G by conjugation, $\text{stab}_G(x) = \{g \in G : gxg^{-1} = x\} = C_G(x)$

Proposition 14. Consider G acts transitively on X, then $\exists g \in G$ s.t. $gx = y$, and $\forall x, y \in X$,

$$\text{stab}_G(y) = g \cdot \text{stab}_G(x) \cdot g^{-1}$$

1.10.4 Equivalent of group actions

Definition 37 (Equivalent of group actions). Let $\varphi : G \to S_X$ ad $\phi : G \to S_Y$.
X is *equivalent* to Y as a set with action of G if there exists a bijection $f : X \to Y$ such that

$$\forall x \in X, f(\varphi(g)x) = \phi(g)(f(x))$$

Intuition.
$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \varphi(g)}\downarrow & & \downarrow{\scriptstyle \phi(g)} \\ X & \xrightarrow{f} & Y \end{array}$$

Theorem 6. If G acts on X transitively, then $\exists H < G$ such that X is **equivalent** to G/H as sets with action of G.

Proof. Construction of H from X: pick $x \in X$, let $H = \{g \in G : gx = x\}$, which by definition means $H = \text{stab}_G(x)$. We want to prove X is equivalent to G/H:
Consider $f : gH \mapsto gx$ □

Intuition.
$$\begin{array}{ccc} X & \xrightarrow{f} & G/H \\ {\scriptstyle \varphi(g)}\downarrow & & \downarrow{\scriptstyle \phi(g)} \\ X & \xrightarrow{f} & G/H \end{array}$$

Corollary. $|X| = |G/H| = [G : H] \Rightarrow |X| \big| |G|$

Corollary. $|\text{orbit}(x)| = [x] = |G/\text{stab}_G(x)| = [G : \text{stab}_G(x)]$

Corollary. Consider G acts on X, and the set of orbits under this action is $\{X_i\}$, then

$$|X| = \sum_i |X_i| = \sum_i |G/H_i|$$

Observe.

Proposition 15. Let G be a finite group, and $|G| = p^r$ where p is a prime and $r \geq 1$, then $Z(G) \neq \{1\}$.

Corollary. Suppose $|G| = p^2$, then G is Abelian.

Definition 38 (polynomial)**.**

$$f(x) = a_n x^n + \cdots + a_0$$
$$f(x) = \Pi(x - \alpha_i)$$

(in $\mathbb{C}$)