

MATH 113: Abstract Algebra

Jack Lipson

September 5, 2023

Contents

0	A Few Preliminaries	2
0.1	Sets and Equivalence Relations	2
1	Introduction to Groups	4
1.1	Binary Operations	4
1.2	Groups	4
1.3	Isomorphic Binary Structures	6
1.4	More on Groups and Subgroups	7
1.5	Cyclic Groups	8
1.6	Generating Sets and Cayley Digraphs	11

Chapter 0

A Few Preliminaries

0.1 Sets and Equivalence Relations

Note. \mathbb{R}^* and \mathbb{C}^* represent the set of all nonzero real and complex numbers. Zero is excluded from $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$.

Note. When a set contains an element b that's algebraically or arithmetically equivalent to another element(s), our set can be partitioned into subsets \bar{b} which denote all entitites equivalent to b . e.g. $\frac{2}{3} = \frac{4}{6}$.

Definition 1 (Parititon). A *partition* of a set is a decomposition of the set into subsests s.t. every element is in exactly one subset, or *cell*.

Definition 2 (Equivalence Relation). For a nonempty set S , \sim is an equivalence relation between elements of S if for all $a, b, c \in S$, (S, \sim) satisfies:

1. (Reflexive) $a \sim a$.
2. (Symmetric) $a \sim b \Rightarrow b \sim a$.
3. (Transitive) $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Non-equivalence relations usually use \mathcal{R} .

Note. All relations \mathcal{R} are defined as $\{(a, b) \text{ for } a \in A, b \in B \mid a \mathcal{R} b\} \subseteq A \times B$. For equivalence relations, $\sim \subseteq S \times S$.

Remark (Natural Parition). \sim yields a natural partition of S : $\bar{a} = \{x \in S \mid x \sim a\}$ for all $a \in S$.

Explanation. For any $a \in S$, $a \in \bar{a}$. So each element of S is in at least one cell. To show that a is in exactly one cell, let $a \in \bar{b}$ as well. We must show

$\bar{a} = \bar{b}$. \Rightarrow : If $x \in \bar{a}$ then $x \sim a$. From our assumption $a \sim b$ so by (3), $x \sim b$ so $x \in \bar{b}$ thus, $\bar{a} \subseteq \bar{b}$. \Leftarrow : If $x \in \bar{b}$, $x \sim b$. From our assumption, $a \sim b$ so, by (2), $b \sim a$ meaning $x \sim a$ via (3) implying $x \in \bar{a}$ s.t. $\bar{b} \subseteq \bar{a}$. This completes the proof.

Definition 3 (Equivalence Class). Each cell \bar{a} in a natural partition given by an equivalence relation is called an equivalence class.

Definition 4 (Congruence Modulo n). Let h, k be distinct integers and $n \in \mathbb{Z}^+$. We say h congruent to k modulo n , written $h \equiv k \pmod{n}$ if $n \mid h - k$ s.t. $h - k = ns$ for some $s \in \mathbb{Z}$.

Definition 5 (Residue Classes Modulo). Equivalence classes for congruence modulo n are *residue classes modulo n* .

Remark. Each residue class modulo $n \in \mathbb{Z}^+$ contains an infinite number of elements.

Definition 6 (Irreducible). An irreducible polynomial $h(x)$ is one that cannot be factored into polynomials in $\mathcal{P}(\mathbb{R})$ all of lower degree than $h(x)$.

Chapter 1

Introduction to Groups

1.1 Binary Operations

Definition 7 (Binary Operation). A *binary operation* $*$ on a set S is a rule that assigns to each ordered pair (a, b) of elements of S another element of S generally denoted $a * b$ or formally $*(a, b)$. To be *well-defined*, $*$ must assign a value to every possible $a * b$.

Definition 8 (Closure under $*$). A set S is *closed under $*$* if for all $a, b \in S$, $a * b \in S$. If a subset H of S is also closed under $*$, this is referred to as the *induced operation $*$ on H* .

Definition 9 (Commutative Operation). A binary operation $*$ on a set S is *commutative* iff $a * b = b * a$ for all $a, b \in S$.

Definition 10 (Associative operation). A binary operation $*$ on a set S is *associative* iff $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Note. Associativity of function composition follows.

Remark. A binary operation on a set, typically finite, can be represented as follows:

$*$	a	b	c
a	b	b	b
b	a	c	b
c	c	b	a

1.2 Groups

Definition 11 (Group). A group $\langle G, * \rangle$ is a set G combined with a binary operation $*$ on G which satisfies the following axioms:

- (\mathcal{G}_1) $*$ is associative.
- (\mathcal{G}_2) There exists a **unique identity** element e on G s.t. $e * x = x * e$ for all $x \in G$.
- (\mathcal{G}_3) For each $a \in G$, there exists an $a' \in G$ s.t. $a' * a = a * a' = e$. This a' is called the *inverse* of a with respect to the operation $*$.
- (\mathcal{G}_4) (optional if part of binary operation definition) G is closed under $*$.

Theorem 1 (Left/Right Cancellation). If G is a group with binary operation $*$, then the *left and right* cancellation laws hold s.t. $a * b = a * c \Rightarrow b = c$ and $b * a = c * a \Rightarrow b = c$ for all $a, b, c \in G$.

Proof. The right cancellation proof is identical to that below.

$$\begin{array}{ll}
 a * b = a * c & \because \text{by supposition} \\
 a' * (a * b) = a' * (a * c) & \because \text{inverse axiom.} \\
 (a' * a) * b = (a' * a) * c & \because \text{associativity axiom} \\
 e * b = e * c & \because \text{inverse axiom} \\
 b = c & \square \text{ identity axiom}
 \end{array}$$

□

Theorem 2. Trivially, in a group G , $(ab)' = b'a'$ for all $a, b \in G$.

Remark. Note that the solutions x, y to $a * x = b$ and $y * a = b$ have unique solutions in G for any $a, b \in G$. Similarly, e is unique.

Note (Idempotent for $*$). An element x of S is *idempotent* for $*$ if $x * x = x$. This is always in the identity element.

Definition 12 (Abelian Group). A group G is *abelian* if its binary operation is commutative.

Definition 13 (Roots of Unity). Call the elements of the set $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$ the n^{th} roots of unity, usually listed as $1 = \zeta^0, \zeta^1, \zeta^2, \dots, \zeta^{n-1}$.

Remark. Let the unit circle $U := \{z \in \mathbb{C} \mid |z| = 1\}$. Clearly, for any $z_1, z_2 \in U$, $|z_1 z_2| = |z_1| |z_2| = 1$ such that $z_1 z_2 \in U$ implying U is closed under \cdot . Note then that $\langle U, \cdot \rangle \simeq \langle R_{2\pi}, +_{2\pi} \rangle$. Similarly, $\langle U_n, \cdot \rangle \simeq \langle \mathbb{Z}_n, +_n \rangle$ for $n \in \mathbb{Z}^+$.

Definition 14 (Addition Modulo n). We respectively write \mathbb{Z}_n and \mathbb{R}_c to denote $[0, 1, \dots, n-1]$ and $[0, c]$. Addition modulo n/c is written $+_n$ or $+_c$.

1.3 Isomorphic Binary Structures

Definition 15 (Binary Algebraic Structures). For two *binary algebraic structures* $\langle S, * \rangle$ and $\langle S', *' \rangle$ to be structurally alike, we would need a one-to-one correspondence between the elements $x \in S$ and $x' \in S'$ s.t. if $x \leftrightarrow x'$ and $y \leftrightarrow y'$ then $x * y \leftrightarrow x' *' y'$.

Remark (Homomorphism Property). This last condition is called the *homomorphism property*. If the function ϕ is NOT one-to-one, it is a homomorphism only.

Definition 16 (Isomorphism). An *isomorphism* of S with S' is a one-to-one function ϕ mapping S onto S' such that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$.

If such a map exists, S and S' are called *isomorphic binary structures* denoted $S \simeq S'$.

Note (Show Binary Algebraic Structures are Isomorphic).

(Step 1) Define the function ϕ which defines $\phi(s)$ for all $s \in S$ and gives the isomorphism from $S \rightarrow S'$.

(Step 2) Show ϕ is one-to-one.

(Step 3) Show ϕ is onto.

(Step 4) Show $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$.

Example. Take the isomorphism $\phi: \mathbb{R} \rightarrow \mathbb{R}^+: x \mapsto e^x$ from $\langle \mathbb{R}, + \rangle$ to $\langle \mathbb{R}^+, \cdot \rangle$. Clearly, $\forall x \in \mathbb{R}, \phi(x) \in \mathbb{R}^+$ and ϕ is bijective. Last, for $x, y \in \mathbb{R}$, $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x) \cdot \phi(y)$.

Definition 17 (Structural Property). A structural property is any property of a binary structure that is invariant to any isomorphic structure. These, like cardinality, are used to show no such isomorphism exists between structures.

Example. Although $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ both have cardinality \aleph_0 and have many one-to-one functions between them, the equation $x + x = c$ has a solution $x \in \mathbb{Q}$ for all $c \in \mathbb{Q}$, but this is not true for \mathbb{Z} if, say, $c = 3$. This structural property distinguishes these binary structures and thus they are

not isomorphic under the usual addition.

Theorem 3. Suppose $\langle S, * \rangle$ has an identity element e for $*$. If $\phi: S \rightarrow S'$ is an isomorphism to $\langle S', *' \rangle$ then $\phi(e)$ is an identity element for $*'$ on S' .

Proof. Because an isomorphism exists from $S \rightarrow S'$, for any element $s' \in S'$, there exists exactly one element $s \in S$ s.t. $\phi(s) = s'$. By the definition of an isomorphism $s' = \phi(s) = \phi(s * e) = \phi(s) *' \phi(e) = s' *' \phi(e)$ for an arbitrary element s' of S . This implies $\phi(e)$ is the identity element for S' . \square

1.4 More on Groups and Subgroups

Definition 18 (Semigroup). A semigroup is an algebraic structure combining a set with an associative binary operation.

Definition 19 (Monoid). A monoid is a semigroup that has an identity element corresponding to its binary operation.

Definition 20 (Subgroup). If a subset H of a group G is closed under the binary operation of G and is itself a group, H is a *subgroup* of G . This is denoted $H \leq G$. $H < G \Rightarrow H \neq G$.

Example. $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$, but $\langle \mathbb{Q}, \cdot \rangle$ is *not* a subgroup of $\langle \mathbb{R}, \cdot \rangle$.

Definition 21 (Proper and trivial subgroups). If G is a group, the subgroup consisting of G itself is the *improper subgroup* of G . All other subgroups are *proper subgroups*. The subgroup $\{e\}$ is the *trivial subgroup* of G and all other subgroups are nontrivial.

Theorem 4. A subset H of a group G is a subgroup of G if and only if:

1. H is closed under the binary operation of G .
2. the identity e of G is in H .
3. for all $a \in H$, $a^{-1} \in H$ also.

Proof. \Rightarrow : Let H be a subgroup of G . By definition, H is closed under G 's binary operation (1). H must have an identity element because it is a group. Because $a * x = a$ and $y * a = a$ have unique solutions, H 's identity element must be the same in H group as G group (2). (3) is trivial because H is a group.

\Leftarrow : Let (1), (2), (3) be true. Then H has a unique identity element on its binary operation (\mathcal{G}_2), each element of H has a unique inverse in H (\mathcal{G}_3),

and H is closed under the binary operation of G (*optional* \mathcal{G}_4). To satisfy (\mathcal{G}_1) , the binary operation on H must be associative s.t., for all $a, b, c \in H$, $(ab)c = a(bc)$. But this clearly holds in G so (\mathcal{G}_1) is satisfied and H is a subgroup of G . \square

1.5 Cyclic Groups

Theorem 5. Let G be a group and $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and the *smallest* subgroup of G that contains a .

Proof. Let's first check H is indeed a subgroup of G . (1) For any $r, s \in \mathbb{Z}$, $a^r * a^s = \overbrace{(a * \dots * a)}^{a \text{ } r \text{ times}} * \overbrace{(a * \dots * a)}^{a \text{ } s \text{ times}} = a^{r+s} \in H$ so we have closure. (2) Let $e := a^0 \in H$ so for all $r \in \mathbb{Z}$, $a^r * a^0 = a^r$. (3) For all $r \in \mathbb{Z}$, $a^r \in H$ so $\exists a^{-r} \in H$ such that $a^r * a^{-r} = a^0 = e$. Thus, $H \leq G$.

Next, to show it's the smallest possible subgroup, just take the set $\{a\}$. To have closure, we must add $a^n \forall n \in \mathbb{Z}^+$. To have inverses, we must have a^{-n} so our set becomes $\{a^n \mid n \in \mathbb{Z} \setminus \{0\}\}$. To have an identity, we must have a^0 and this completes the proof. \square

Definition 22 (Cyclic Subgroup of G). For any $a \in G$, define $\langle a \rangle$ to be the set $\{a^n \mid n \in \mathbb{Z}\}$. This is called the *cyclic subgroup of G generated by a* . An element a of a group G *generates* G and is a *generator for G* if $\langle a \rangle = G$.

Definition 23 (Cyclic Group). A group is *cyclic* if there is some element a in G that generates G .

Example. $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$ so \mathbb{Z}_4 is cyclic and both 1 and 3 are generators.

Example. The group $\langle \mathbb{Z}, + \rangle$ is a cyclic group generated ONLY by 1 and -1.

Remark (Subgroup Diagrams). Lattice, or *subgroup diagrams*, can be drawn such that lines run down from a group G to a group H if $H < G$.

Example. Take two group structures of order 4: \mathbb{Z}_4 and the Klein 4-group *Viererguppe* defined as follows:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

 $\mathbb{Z}_4 :$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

 $V :$

\mathbb{Z}_4
 \downarrow
 $\{0, 2\}$
 \downarrow
 $\{0\}$

V
 $\swarrow \quad \downarrow \quad \searrow$
 $\{e, a\} \quad \{e, b\} \quad \{e, c\}$
 $\swarrow \quad \downarrow \quad \searrow$
 $\{e\}$

We can map these as: $\{0\}$ and $\{e\}$.

Definition 24 (Order). If the cyclic subgroup $\langle a \rangle$ of G is finite, we say the *order* of a is the order $|\langle a \rangle|$. Otherwise, a is of *infinite order*.

Theorem 6. Every cyclic group is abelian.

Theorem 7 (Division Algorithm for \mathbb{Z}). If $m \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$, then there exist unique integers q, r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

Proof. From the archimedean property, there is a unique q such that $qm \leq n < (q+1)m$. Then, $0 \leq r = n - mq < m$ is unique. We regard q and r as the quotient and nonnegative remainder respectively when n is divided by m . \square

Theorem 8. A subgroup of a cyclic group is cyclic.

Proof. Take a cyclic group G with subgroup H . If $H = \langle e \rangle$ then H is cyclic and the proof is complete.

Otherwise, $H \neq \langle e \rangle$ so there exists $b \in H, b \neq e$. Because G is cyclic, there must exist $a \in G$ such that a generates G , i.e. for all $n \in \mathbb{Z}^+$, a^n spans every value of G including every element of H . Let $c := a^m$ where m is the least positive integer such that $c \in H$. Now, for all $b \in H$, take n such that $b = a^n$. From division algorithm, there exist integers q, r such that $n = mq + r$ so $a^n = a^{mq+r} = (a^m)^q a^r$ which implies, because $a^m \in H$ and H is a group so $a^{-m} \in H$, $a^n(a^m)^{-q} = a^r$. H is a group so this implies $a^r \in H$. Because $0 \leq r < m$ and m is the least positive integer such that $a^m \in H$, $r = 0$ such that $n = mq$ for all $b = a^n = (a^m)^q \in H$. $\langle c \rangle = H$ so H is cyclic. \square

Definition 25 (Greatest Common Divisor). The positive generator d of the cyclic group $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ under addition is called the *greatest common divisor* of r and s , written $d = \gcd(r, s)$.

Definition 26. Two integers are *relatively prime* if their gcd is 1.

Theorem 9. Let G be a cyclic group with generator a . If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n , then G is instead isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof. Take the following two cases. **Case 1:** For all positive integers m , $a^m \neq e$. Suppose $a^h = a^k$ and $h > k$. Thus, $a^h a^{-k} = a^{h-k} = e$ which contradicts our assumption. Therefore, each element of G can be uniquely expressed as a^m for a unique $m \in \mathbb{Z}$. The map $\phi : G \rightarrow \mathbb{Z}$ defined as $\phi(a^i) = i$ is then well-defined and bijective on \mathbb{Z} . Last, $\phi(a^i a^j) = \phi(a^{i+j}) = i+j = \phi(a^i) + \phi(a^j)$ so the homomorphism property is satisfied and ϕ is an isomorphism to $\langle \mathbb{Z}, + \rangle$.

Case 2: $a^m = e$ for some $m \in \mathbb{Z}^+$. Let n be the smallest positive integer so $a^n = e$. If $s \in \mathbb{Z}$ and $s = q + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = a^r$. Like in case 1, if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h-k < n$ contradicting our assumption that n is the smallest positive integer possible. Hence, $a^0, a^1, a^2, \dots, a^{n-1}$ are all distinct and comprise all elements of G . We can then make the map $\psi : G \rightarrow \mathbb{Z}_n$ defined by $\psi(a^i) = i$ for $i = 0, 1, \dots, n-1$ is well-defined and bijective on \mathbb{Z}_n . Also, because $a^n = e$, $a^i a^j = a^k$ whenever $k = i +_n j$. Therefore, $\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j)$ satisfying the homomorphism property so ψ is an isomorphism to $\langle \mathbb{Z}_n, +_n \rangle$. \square

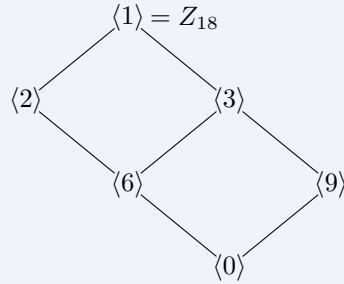
Theorem 10. Let G be a cyclic group generated by a with n elements. Let $b \in G$ and $b = a^s$. Then, b generates a cyclic subgroup H of G containing n/d elements where d is the greatest common divisor of n and s . Also, $\langle a^s \rangle = \langle a^n \rangle \Leftrightarrow \gcd(s, n) = \gcd(t, n)$.

Proof. We already know b generates a cyclic subgroup H of G . And that because it is finite, it has only as many elements as the smallest power m of b so $b^m = e$. This and $b = a^s$ implies $(a^s)^m = e$ if and only if n divides ms because $a^n = e$ because G is of finite order n . Let $d = \gcd(n, s)$ such that we want to find the smallest m so $\frac{ms}{n} = \frac{m(s/d)}{(n/d)}$ is an integer. This implies (n/d) divides m so the smallest m we can pick is n/d . Thus, H has order n/d .

We know G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$ so taking cyclic subgroup $\langle d \rangle$ of \mathbb{Z}_n where d divides n implies $\langle d \rangle$ has n/d elements and contains all positive integers m less than n such that $\gcd(m, n) = d$. Thus, there is only one subgroup of \mathbb{Z}_n of order n/d . It immediately follows that $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$. \square

Corollary. If a is a generator of a finite cyclic group G of order n , then the other generators of G are the elements of the form a^r , where r is relatively prime to n .

Example. For instance, we can easily derive that the subgroup diagram for



Z_{18} looks like:

1.6 Generating Sets and Cayley Digraphs

Example. The Klein 4-group $V = \{e, a, b, c\}$ is generated by $\{a, b\}$ since $ab = c$. It is similarly generated by $\{a, c\}$, $\{b, c\}$, and $\{a, b, c\}$.

Theorem 11. The intersection of some subgroups H_i of a group G for $i \in I$ is again a subgroup of G where I is the set of indices.

Proof. First, closure. For any $a, b \in \bigcap_{i \in I} H_i$, because each H_i has closure, $a, b \in H_i \Rightarrow ab \in H_i$ so $ab \in \bigcap_{i \in I} H_i$. Similarly, because the identity element of G is in H_i for all $i \in I$, $e \in \bigcap_{i \in I} H_i$. Last, for all $a \in \bigcap_{i \in I} H_i$, because H_i is a group, $a^{-1} \in H_i$. Thus, for any $a \in \bigcap_{i \in I} H_i$, $a \in H_i$ for all i so $a^{-1} \in H_i$ for all i so $a^{-1} \in \bigcap_{i \in I} H_i$. \square