MATH 113: Abstract Algebra

Jack Lipson

August 28, 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

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 $\overline{b}$ 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 $\mathscr{R}$.

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

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

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

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

Definition 3 (Equivalence Class)**.** Each cell $\overline{a}$ 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)**.** Equiva;ence calsses 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. Associativty of function compostion follows.

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

$*$	a	b	c
a	b	c	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:

($\mathscr{G}_1$) $*$ is associative.

($\mathscr{G}_2$) There exists a **unique** *identity* element e on G s.t. $e * x = x * e$ for all $x \in G$.

($\mathscr{G}_3$) 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 $*$.

($\mathscr{G}_4$) *(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.

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

$\square$

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 $1 = \zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}$.

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 respecitvely write $\mathbb{Z}_n$ and $\mathbb{R}_c$ to denote $[0, 1, \ldots, n-1]$ 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 *homorphism property*. If the function ϕ is NOT one-to-one, it is a homormorphism 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 $S \to S'$.

(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 $\phi \colon \mathbb{R} \to \mathbb{R}^+ \colon x \longmapsto e^x$ 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 $x \in Q$ for all $c \in \mathbb{Q}$, but this is not true for $\mathbb{Z}$ if, say, $c = 3$. This structural propery 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 $\phi\colon S \to S'$ is an isomorphism to $\langle S', *'\rangle$ then $\phi(e)$ is an identity element for $*'$ on S'.

Proof. Because an isomorphism exists from $S \to S'$, 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 arbitary 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 oxperation.

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 $\langle \mathbb{R}, -\rangle$.

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 ($\mathscr{G}_2$), each element of H has a unique inverse in H ($\mathscr{G}_3$), and H is closed under the binary operation of G (*optional* $\mathscr{G}_4$). To satisfy ($\mathscr{G}_1$), the binary operation on H must be associative s.t., for all $a, b, c \in H$, $(ab)c = a(bc)$. But this is clearly holds in G so ($\mathscr{G}_1$) is satisfied and H is a subgroup of G. □

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. □

Cont. on Page 58 in 7th ed

Cont. on Page 55 for copying lattice diagrams