A First Course in Abstract Algebra

Samuel Lindskog

June 30, 2024

Definition 1.1 (Binary Operation)**.** A binary operation $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$.

Definition 1.2 (Closed Under)**.** Let $*$ be a binary operation on S and let H be a subset of S. The subset H is closed under $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the binary operation on H is the *induced operation* of $*$ on H.

Definition 1.3 (Commutative)**.** A binary operation $*$ on a set S is commutative iff $a * b = b * a$ for all $a, b \in S$.

Definition 1.4 (Associative)**.** A binary operation $*$ on a set S is associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Definition 1.5 (Binary Algebraic Structure)**.** A binary algebraic structure $\langle S, * \rangle$ is a set S together with a binary operation $*$ on S.

Definition 1.6 (Isomorphism)**.** Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An isomorphism of S with S' is a one-to-one function[1] ϕ mapping S onto S' such that:

$$\underbrace{\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } (x, y \in S).}_{\textit{homomorphism property}}$$

If such a function exists, then S and S' are isomorphic binary structures, which we denote by $S \simeq S'$

Definition 1.7 (Identity Element)**.** Let $\langle S, * \rangle$ be a binary structure. An element e of S is an identity element for $*$ if $e * s = s * e = s$ for all $s \in S$

Theorem 1.1 (Uniqueness of Identity Element)**.** A binary structure $\langle S, * \rangle$ has at most one identity element.

Theorem 1.2. Suppose $\langle S, * \rangle$ has an identity element e for $*$. If $\phi \; S \;\; \rightarrow \;\; S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\phi(e)$ is an identity element for the binary operation $*'$ on S'.

Definition 1.8 (Group)**.** A group $\langle G, * \rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:[2]

1. For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.
2. There is an element e in G such that for all $x \in G$, $e * x = x * e = x$.

[1] if no one-to-one function exists but the homomorphism property is satisfied, than phi is a homomorphism.

[2] A group G is *abelian* if its binary operation is commutative.

3. Corresponding to each $a \in G$, there is an element a' in G such that $a * a' = a' * a = e$.

Theorem 1.3. If G is a group with binary operation $*$, then the left and right cancellation laws hold in G.

Proof: Suppose $a * c = b * c$. It follows that $(a * c) * c^{-1} = (b * c) * c^-1$, and thus following the fact that group operations are associative, $a * e = b * e$ and $a = b$. □

Theorem 1.4. If G is a group with binary operation $*$, and if a and b are any elements of G, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.

Theorem 1.5. In a group G with binary operation $*$, there is only one element e in G such that $e * x = x * e = x$ for all x in G. Likewise for each a in G there is only one element a' in G such that $a' * a = a * a' = e$.[3]

[3] This follows trivially from the left and right cancellation laws.

Corollary 1.1. Let G be a group. Then for all $a, b \in G$, we have $(a * b)' = b' * a'$

Definition 1.9 (Structural Property)**.** A structural property of a binary structure is one that must be shared by any isomorphic binary structure.[4]

[4] For example, the cardinality of set S is a structural property of $\langle S, * \rangle$

Definition 1.10 (Semigroups and Monoids)**.** A *semigroup* is a set with an associative binary operation. A *monoid* is a semigroup what has an identity element.[5]

[5] Every group is a semigroup and a monoid.

Problem 1. Show that every group G with identity e such that $x * x = e$ for all $x \in G$ is abelian.

Proof: Suppose a, b are two elements in G, with $a \neq b$. Trivially, $(a * b) * (b * a) = e$. Because $x * x = e$ for all $x \in G$, it follows that $(a * b) * (a * b) = e$, so $a * b = b * a$.[6] □

[6] The associative axiom of groups introduces the existence of a set of factors for any one element in the group.

Problem 2. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists $n \in Z^+$ s.t. $a^n = e$.

Proof: Suppose $G = \{e\}$. Then $e^1 = e$. Suppose G has two or more elements, $n \in Z^+$, $a \in G$. Because G is finite, there are a finite number of elements in G that a^n can assume. It follows that there exists $k, j \in Z^+$ with $k < j$ such that $a^k = a^j$. Therefore there exists n such that $a^k * a^n = a^j$, from which follows $a^n = e$. □

Notation. In place of the notation of $a * b$, we can use $a + b$ to be read as "the sum of a and b", or ab to be read as "the product of a and b". As a convention, $a + b$ refers to commutative operations, while ab may be used if the operation may or may not be commutative. na refers to $a + \ldots + a$ repeated n times.

Definition 1.11 (Subgroup)**.** If a subset H of a group G is closed under the binary operation of G, and if H with the induced operation from G is itself a group, then H is a subgroup of G.[7]

[7] If H is a subgroup of G, this can be denoted $H \leq G$, or $H < G$.

Definition 1.12 (Improper and Proper Subgroups)**.** If G is a group, then 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. All other subgroups are nontrivial.

Definition 1.13 (Klein 4-group)**.**

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Theorem 1.6. 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 element e of G is in H
3. For all $a \in H$ it is true that $a^{-1} \in H$

Theorem 1.7. Let G be a group and let $a \in G$. Then

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

is the smallest subgroup of G that contains a.[8]

[8] Look at discreetmath notes for definitions. In this case, we are finding the r-smallest element of a partial order on $\mathscr{P}(G)$ pairing each subgroup containing a with all containing groups.

Definition 1.14 (Cyclic Subgroup)**.** Let G be a group and let $a \in G$. Then the subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of G is called the *cyclic subgroup of G generated by a*, and is denoted by $\langle a \rangle$.[9]

[9] Take note that n can be negative.

Definition 1.15 (Generator)**.** An element a of a group G generates G if $\langle a \rangle = G$.

Definition 1.16 (Cyclic Group)**.** A group G is cyclic if there is some element a in G that generates G.

Problem 3. Is a generator for a cyclic group unique?

Proof: No. Suppose G a group and $\langle a \rangle = G$. Because $a^n = (a^{-1})^{-n}$, we can clearly see $\langle a^{-1} \rangle = G$. □