Copyright & License

Abstract Algebra I

Definition

set operations

Abstract Algebra I

Theorem

De Morgan's rules

Abstract Algebra I

Definition

surjective or onto mapping

Abstract Algebra I

Definition

injective or one–to–one mapping

Abstract Algebra I

Definition

bijection

Abstract Algebra I

Definition

composition of functions

Abstract Algebra I

Lemma

composition of functions is associative

Abstract Algebra I

Lemma

cancellation and composition

Abstract Algebra I

Definition

image and inverse image of a function

Abstract Algebra I

$$\begin{aligned} A \cup B &= \{x \mid x \in A \text{ or } x \in B\} \\ A \cap B &= \{x \mid x \in A \text{ and } x \in B\} \\ A - B &= \{x \mid x \in A \text{ and } x \notin B\} \\ A + B &= (A - B) \cup (B - A) \end{aligned}$$

`jasonu [remove-this] at physics dot utah dot edu`

The mapping $f : S \mapsto T$ is *onto* or *surjective* if every $t \in T$ is the image under f of some $s \in S$; that is, iff, $\forall\, t \in T, \quad \exists\, s \in S$ such that $t = f(s)$.

For $A,\, B \subseteq S$

$$\begin{aligned} (A \cap B)' &= A' \cup B' \\ (A \cup B)' &= A' \cap B' \end{aligned}$$

The mapping $f : S \mapsto T$ is said to be a *bijection* if f is both 1-1 and onto.

The mapping $f : S \mapsto T$ is *injective* or *one–to–one* (1-1) if for $s_1 \neq s_2$ in S, $f(s_1) \neq f(s_2)$ in T.

Equivalently:

$$f \text{ injective} \Longleftrightarrow f(s_1) = f(s_2) \Rightarrow s_1 = s_2$$

If $h : S \mapsto T, g : T \mapsto U$, and $f : U \mapsto V$, then,

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Suppose $g : S \mapsto T$ and $f : T \mapsto U$, then the *composition* or *product*, denoted by $f \circ g$ is the mapping $f \circ g : S \mapsto U$ defined by:

$$(f \circ g)(s) = f(g(s))$$

Suppose $f : S \mapsto T$, and $U \subseteq S$, then the *image* of U under f is

$$f(U) = \{f(u) \mid u \in U\}$$

If $V \subseteq T$ then the *inverse image* of V under f is

$$f^{-1}(V) = \{s \in S \mid f(s) \in V\}$$

$$f \circ g = f \circ \widetilde{g} \text{ and } f \text{ is 1–1} \Rightarrow g = \widetilde{g}$$

$$f \circ g = \widetilde{f} \circ g \text{ and } g \text{ is onto } \Rightarrow f = \widetilde{f}$$

Definition

inverse function

Abstract Algebra I

Lemma

properties of $A(S)$

Abstract Algebra I

Definition

order of a group

Abstract Algebra I

Lemma

properties of groups

Abstract Algebra I

Lemma

when is a subset a subgroup

Abstract Algebra I

Definition

$A(S)$

Abstract Algebra I

Definition

group

Abstract Algebra I

Definition

abelian

Abstract Algebra I

Definition

subgroup

Abstract Algebra I

Definition

cyclic subgroup

Abstract Algebra I

If S is a nonempty set, then $A(S)$ is the set of all 1–1 mappings of S onto itself.

When S has a finite number of elements, say n, then $A(S)$ is called the *symmetric group of degree* n and is often denoted by S_n.

Suppose $f : S \mapsto T$. An *inverse* to f is a function $f^{-1} : T \mapsto S$ such that

$$\begin{aligned} f \circ f^{-1} &= i_T \\ f^{-1} \circ f &= i_S \end{aligned}$$

Where $i_T : T \mapsto T$ is defined by $i_T(t) = t$, and is called the *identity function* on T. And similarly for S.

A nonempty set G together with some operator $*$ is said to be a *group* if:

1. If $a, b \in G$ then $a * b \in G$
2. If $a, b, c \in G$ then $a * (b * c) = (a * b) * c$
3. G has an identity element e such that $a * e = e * a = a \ \ \forall\, a \in G$
4. $\forall\, a \in G, \ \ \exists\, b \in G$ such that $a * b = b * a = e$

$A(S)$ satisfies the following:

1. $f, g \in A(S) \Rightarrow f \circ g \in A(S)$
2. $f, g, h \in A(S) \Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$
3. There exists an i such that $f \circ i = i \circ f = f$ $\forall f \in A(S)$
4. Given $f \in A(S)$, there exists a $g \in A(S)$ such that $f \circ g = g \circ f = i$

A group G is said to be *abelian* if $\forall\, a, b \in G$

$$a * b = b * a$$

The number of elements in G is called the *order* of G and is denoted by $|G|$.

A nonempty subset, H of a group G is called a *subgroup* of G if, relative to the operator in G, H itself forms a group.

If G is a group then

1. Its identity element, e is unique.
2. Every $a \in G$ has a unique inverse $a^{-1} \in G$.
3. If $a \in G$, then $(a^{-1})^{-1} = a$.
4. For $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$, where $ab = a * b$.

A *cyclic subgroup* of G is generated by a single element $a \in G$ and is denoted by (a).

$$(a) = \left\{a^i \mid i \text{ any integer}\right\}$$

A nonempty subset $A \subset G$ is a subgroup $\Leftrightarrow$ A is closed with respect to the operator of G and given $a \in A$ then $a^{-1} \in A$.

Lemma

finite subsets and subgroups

Abstract Algebra I

Lemma

subgroups under ∩ and ∪

Abstract Algebra I

Definition

equivalence relation

Abstract Algebra I

Definition

equivalence class

Abstract Algebra I

Theorem

equivalence relations partition sets

Abstract Algebra I

Theorem

Lagrange's theorem

Abstract Algebra I

Definition

index of a subgroup

Abstract Algebra I

Definition

order of an element in a group

Abstract Algebra I

Theorem

finite groups wrap around

Abstract Algebra I

Definition

homomorphism

Abstract Algebra I

Suppose H and H' are subgroups of G, then

- $H \cap H'$ is a subgroup of G
- $H \cup H'$ is **not** a subgroup of G, as long as neither H nor H' is contained in the other.

Suppose that G is a group and H a nonempty *finite* subset of G closed under the operation in G. Then H is a subgroup of G.
Corollary If G is a *finite* group and H a nonempty subset of G closed under the operation of G, then H is a subgroup of G.

If $\sim$ is an equivalence relation on a set S, then the *equivalence class* of a denoted $[a]$ is defined to be:

$$[a] = \{b \in S \mid b \sim a\}$$

A relation $\sim$ on elements of a set S is an *equivalence relation* if for all $a, b, c \in S$ it satisfies the following criteria:

1. $a \sim a$ reflexivity
2. $a \sim b \Rightarrow b \sim a$ symmetry
3. $a \sim b$ and $b \sim c \Rightarrow a \sim c$ transitivity

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. That is,

$$|G| = k\,|H|$$

for some integer k. The converse of Lagrange's theorem is not generally true.

If $\sim$ is an equivalence relation on a set S, then $\sim$ partitions S into equivalence classes. That is, for any $a, b \in S$ either:

$$[a] = [b] \quad \text{or} \quad [a] \cap [b] = \emptyset$$

If a is an element of G then the *order* of a denoted by $o(a)$ is the least positive integer m such that $a^m = e$.

If G is a finite group, and H a subgroup of G, then the *index* of H in G is the number of distinct right cosets of H in G, and is denoted:

$$[G : H] = \frac{|G|}{|H|} = i_G(H)$$

If G and G' are two groups, then the mapping

$$f : G \to G'$$

is a *homomorphism* if

$$f(ab) = f(a)f(b) \qquad \forall\, a, b \in G$$

If G is a finite group of order n then $a^n = e$ for all $a \in G$.

Definition

monomorphism, isomorphism, automorphism

Abstract Algebra I

Definition

kernel

Abstract Algebra I

Definition

normal subgroup

Abstract Algebra I

Definition/Theorem

factor group

Abstract Algebra I

Theorem

order of a factor group

Abstract Algebra I

Theorem

composition of homomorphisms

Abstract Algebra I

Theorem

kernel related subgroups

Abstract Algebra I

Theorem

normal subgroups and their cosets

Abstract Algebra I

Theorem

normal subgroups are the kernel of a homomorphism

Abstract Algebra I

Theorem

Cauchy's theorem

Abstract Algebra I

Suppose the mapping $f : G \to G'$ is a homomorphism, then:

- If f is 1–1 it is called a *monomorphism*.
- If f is 1–1 and onto, then it is called an *isomorphism*.
- If f is an isomorphism that maps G onto itself then it is called an *automorphism*.
- If an isomorphism exists between two groups then they are said to be *isomorphic* and denoted $G \simeq G'$.

Suppose $f : G \mapsto G'$ and $h : G' \mapsto G''$ are homomorphisms, then the composition of h with f, $h \circ f$ is also a homomorphism.

If f is a homomorphism from G to G' then the *kernel* of f is denoted by $\text{Ker} f$ and defined to be

$$\text{Ker} f = \{a \in G \mid f(a) = e'\}$$

If f is a homomorphism of G into G', then

1. $\text{Ker} f$ is a subgroup of G.
2. If $a \in G$ then $a^{-1}(\text{Ker} f)a \subset \text{Ker} f$.

A subgroup N of G is said to be a *normal subgroup* of G if $a^{-1}Na \subset N$ for each $a \in G$.

N normal to G is denoted $N \lhd G$.

$N \lhd G$ iff every left coset of N in G is also a right coset of N in G.

If $N \lhd G$, then we define the *factor group* of G by N denoted G/N to be:

$$G/N = \{Na \mid a \in G\} = \{[a] \mid a \in G\}$$

G/N is a group relative to the operation

$$(Na)(Nb) = Nab$$

If $N \lhd G$, then there is a homomorphism $\psi : G \mapsto G/N$ such that $\text{Ker}\psi = N$.

If G is a finite group and $N \lhd G$, then

$$|G/N| = \frac{|G|}{|N|}$$

If p is a prime that divides $|G|$, then G has an element of order p.

Theorem

first homomorphism theorem

Abstract Algebra I

Theorem

correspondence theorem

Abstract Algebra I

Theorem

second isomorphism theorem

Abstract Algebra I

Theorem

third isomorphism theorem

Abstract Algebra I

Theorem

groups of order pq

Abstract Algebra I

Definition

external direct product

Abstract Algebra I

Definition

internal direct product

Abstract Algebra I

Lemma

intersection of normal subgroups when the group is an internal direct product

Abstract Algebra I

Theorem

isomorphism between an external direct product and an internal direct product

Abstract Algebra I

Theorem

fundamental theorem on finite abelian groups

Abstract Algebra I

Let $\varphi : G \mapsto G'$ be a homomorphism which maps G onto G' with kernel K. If H' is a subgroup of G', and if $H' = \{a \in G \mid \varphi(a) \in H'\}$ then

- H is a subgroup of G
- $K \subset H$
- $H/K \simeq H'$

Also, if $H' \lhd G'$ then $H \lhd G$.

If $\varphi : G \mapsto G'$ is an onto homomorphism with kernel K then,

$$G/K \simeq G'$$

with isomorphism $\psi : G/K \mapsto G'$ defined by

$$\psi(Ka) = \varphi(a)$$

If $\varphi : G \mapsto G'$ is an onto homomorphism with kernel K and if $N' \lhd G'$ with $N = \{a \in G \mid \varphi(a) \in N'\}$ then

$$G/N \simeq G'/N'$$

or equivalently

$$G/N \simeq \frac{G/K}{N/K}$$

Let H be a subgroup of G and $N \lhd G$, then

1. $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G
2. $H \cap N \lhd H$
3. $H/(H \cap N) \simeq (HN)/N$

Suppose $G_1, \ldots, G_n$ is a collection of groups. The *external direct product* of these n groups is the set of all n–tuples for which the ith component is an element of G_i.

$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$$

The product is defined component–wise.

$$(a_1, a_2, \ldots, a_n)\,(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

If G is a group of order pq (p and q primes) where $p > q$ and $q \not| \, p-1$ then G must be cyclic.

If G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, then for $i \neq j, N_i \cap N_j = \{e\}$.

A group G is said to be the *internal direct product* of its normal subgroups $N_1, N_2, \ldots, N_n$ if every element of G has a unique representation, that is, if $a \in G$ then:

$$a = a_1, a_2, \ldots, a_n \text{ where each } a_i \in N_i$$

A finite abelian group is the direct product of cyclic groups.

Let G be a group with normal subgroups $N_1, N_2, \ldots, N_n$, then the mapping:

$$\psi : N_1 \times N_2 \times \cdots \times N_n \mapsto G$$

defined by

$$\psi((a_1, a_2, \ldots, a_n)) = a_1 a_2 \cdots a_n$$

is an isomorphism iff G is the internal direct product of $N_1, N_2, \ldots, N_n$.

Definition

centralizer of an element

Abstract Algebra I

Lemma

the centralizer forms a subgroup

Abstract Algebra I

Theorem

number of distinct conjugates of an element

Abstract Algebra I

Theorem

the class equation

Abstract Algebra I

Theorem

groups of order p^n

Abstract Algebra I

Theorem

groups of order p^2

Abstract Algebra I

Theorem

groups of order p^n *contain a normal subgroup*

Abstract Algebra I

Definition

p*–Sylow group*

Abstract Algebra I

Theorem

Sylow's theorem (part 1)

Abstract Algebra I

Theorem

Sylow's theorem (part 2)

Abstract Algebra I

If $a \in G$, then $C(a)$ is a subgroup of G.

If G is a group and $a \in G$, then the *centralizer* of a in G is the set of all elements in G that commute with a.

$$C(a) = \{g \in G \mid ga = ag\}$$

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$$

Let G be a finite group and $a \in G$, then the number of distinct conjugates of a in G is $[G : C(a)]$ (the index of $C(a)$ in G).

If G is a group of order p^2 (p prime), then G is abelian.

If G is a group of order p^n, (p prime) then $Z(G)$ is non–trivial, i.e. there exists at least one element other than the identity that commutes with all other elements of G.

If G is a group of order $p^n m$ where p is prime and $p \not| m$, then G is a p–Sylow group.

If G is a group of order p^n (p prime), then G contains a normal subgroup of order p^{n-1}.

If G is a p–Sylow group ($|G| = p^n m$), then any two subgroups of the same order are conjugate. For example, if P and Q are subgroups of G where $|P| = |Q| = p^n$ then

$$P = x^{-1}Qx \quad \text{for some } x \in G$$

If G is a p–Sylow group ($|G| = p^n m$), then G has a subgroup of order p^n.

Theorem

Sylow's theorem (part 3)

Abstract Algebra I

If G is a p–Sylow group ($|G| = p^n m$), then the number of subgroups of order p^n in G is of the form $1 + kp$ and divides $|G|$.