Great Theoretical Ideas In Computer Science

Victor Adamchik
Danny Sleator

CS 15-251 Spring 2010

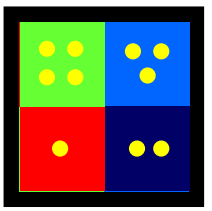
Lecture 16 Mar. 16, 2010 Carnegie Mellon University

Algebraic Structures: Group Theory

Today we are going to study the abstract properties of binary operations

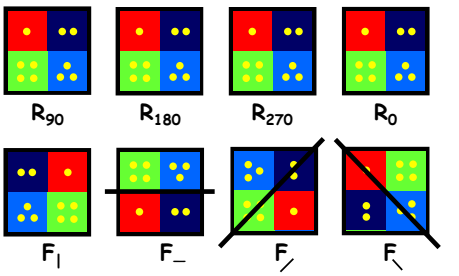
Groups
Subgroups
Rings
Fields

Rotating a Square in Space



Imagine we can pick up the square, rotate it in any way we want, and then put it back on the white frame

In how many different ways can we put the square back on the frame?



Symmetries of the Square

Y_{SQ} = { R_0, R_{90}, R_{180}, R_{270}, $F_|$, F_-, $F_/$, $F_\backslash$ }

Composition

Define the operation "•" to mean "first do one symmetry, and then do the next"

For example,

$R_{90} \bullet R_{180}$

means "first rotate 90° clockwise and then 180°"

$= R_{270}$

$F_| \bullet R_{90}$

means "first flip horizontally and then rotate 90°"

$= F_/$

Question: if $a,b \in Y_{SQ}$, does $a \bullet b \in Y_{SQ}$? **Yes!**

	R_0	R_{90}	R_{180}	R_{270}	$F_{\|}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_{\|}$	F_{-}	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_{\backslash}$	$F_{/}$	$F_{\|}$	F_{-}
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_{-}	$F_{\|}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	F_{-}	$F_{\|}$
$F_{\|}$	$F_{\|}$	$F_{/}$	F_{-}	$F_{\backslash}$	R_0	R_{180}	R_{90}	R_{270}
F_{-}	F_{-}	$F_{\backslash}$	$F_{\|}$	$F_{/}$	R_{180}	R_0	R_{270}	R_{90}
$F_{/}$	$F_{/}$	F_{-}	$F_{\backslash}$	$F_{\|}$	R_{270}	R_{90}	R_0	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\|}$	$F_{/}$	F_{-}	R_{90}	R_{270}	R_{180}	R_0

How many symmetries for n-sided body? 2n

$R_0, R_1, R_2, \ldots, R_{n-1}$

$F_0, F_1, F_2, \ldots, F_{n-1}$

$R_i R_j = R_{i+j}$ $R_i F_j = F_{j-i}$

$F_j R_i = F_{j+i}$ $F_i F_j = R_{j-i}$

Some Formalism

If S is a set, $S \times S$ is:

the set of all (ordered) pairs of elements of S

$S \times S = \{ (a,b) \mid a \in S \text{ and } b \in S \}$

If S has n elements, how many elements does $S \times S$ have? n^2

Formally, $\bullet$ is a function from $Y_{SQ} \times Y_{SQ}$ to Y_{SQ}

$\bullet : Y_{SQ} \times Y_{SQ} \rightarrow Y_{SQ}$

As shorthand, we write $\bullet(a,b)$ as "$a \bullet b$"

Binary Operations

"$\bullet$" is called a binary operation on Y_{SQ}

Definition: A binary operation on a set S is a function: $S \times S \rightarrow S$

Example:

The function $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by

$f(x,y) = xy + y$

is a binary operation on $\mathbb{N}$

Associativity

A binary operation $\bullet$ on a set S is associative if:

for all $a,b,c \in S$, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

Examples:

Is $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x,y) = x\,y + y$ associative? NO!

$(a\,b + b)\,c + c = a\,(b\,c + c) + (b\,c + c)$?

Is the operation $\bullet$ on the set of symmetries of the square associative? YES!

Commutativity

A binary operation $\blacklozenge$ on a set S is commutative if

For all $a,b \in S$, $a \blacklozenge b = b \blacklozenge a$

Is the operation $\bullet$ on the set of symmetries of the square commutative?

$R_{90} \bullet F_{|} \neq F_{|} \bullet R_{90}$

NO!

Identities

R_0 is like a null motion

Is this true: $\forall a \in Y_{SQ}$, $a \bullet R_0 = R_0 \bullet a = a$? **YES!**

R_0 is called the identity of $\bullet$ on Y_{SQ}

In general, for any binary operation $\blacklozenge$ on a set S, an element $e \in S$ such that for all $a \in S$,

$$e \blacklozenge a = a \blacklozenge e = a$$

is called an identity of $\blacklozenge$ on S

Inverses

Definition: The inverse of an element $a \in Y_{SQ}$ is an element b such that:

$$a \bullet b = b \bullet a = R_0$$

Examples:

R_{90} **inverse:** R_{270}

R_{180} **inverse:** R_{180}

$F_|$ **inverse:** $F_|$

Every element in Y_{SQ} has a unique inverse

	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_|$	F_-	$F_/$	$F_\backslash$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_\backslash$	$F_/$	$F_|$	F_-
R_{180}	R_{180}	R_{270}	R_0	R_{90}	F_-	$F_|$	$F_\backslash$	$F_/$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_/$	$F_\backslash$	F_-	$F_|$
$F_|$	$F_|$	$F_/$	F_-	$F_\backslash$	R_0	R_{180}	R_{90}	R_{270}
F_-	F_-	$F_\backslash$	$F_|$	$F_/$	R_{180}	R_0	R_{270}	R_{90}
$F_/$	$F_/$	F_-	$F_\backslash$	$F_|$	R_{270}	R_{90}	R_0	R_{180}
$F_\backslash$	$F_\backslash$	$F_|$	$F_/$	F_-	R_{90}	R_{270}	R_{180}	R_0

Group

A group G is a pair $(S,\blacklozenge)$, where S is a set and $\blacklozenge$ is a binary operation on S such that:

1. **$\blacklozenge$ is associative**

2. **(Identity) There exists an element $e \in S$ such that:**

   $e \blacklozenge a = a \blacklozenge e = a$, for all $a \in S$

3. **(Inverses) For every $a \in S$ there is $b \in S$ such that:**

   $a \blacklozenge b = b \blacklozenge a = e$

Commutative or "Abelian" Groups

If $G = (S,\blacklozenge)$ and $\blacklozenge$ is commutative, then G is called a commutative group

remember, "commutative" means

$a \blacklozenge b = b \blacklozenge a$ for all a, b in S

To check "group-ness"

Given $(S,\blacklozenge)$

1. Check "closure" for $(S,\blacklozenge)$
   (i.e, for any a, b in S, check $a \blacklozenge b$ also in S).
2. Check that associativity holds.
3. Check there is a identity
4. Check every element has an inverse

Some examples…

Examples

Is $(\mathbb{N},+)$ a group?

Is $\mathbb{N}$ closed under +? YES!

Is + associative on $\mathbb{N}$? YES!

Is there an identity? YES: 0

Does every element have an inverse? NO!

$(\mathbb{N},+)$ is NOT a group

Examples

Is $(Z,+)$ a group?

Is Z closed under +? YES!

Is + associative on Z? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$(Z,+)$ is a group

Examples

Is (Odds,+) a group?

Is Odds closed under +? NO!

Is + associative on Odds? YES!

Is there an identity? NO!

Does every element have an inverse? YES!

(Odds,+) is NOT a group

Examples

Is $(Y_{SQ}, \bullet)$ a group?

Is Y_{SQ} closed under $\bullet$? YES!

Is $\bullet$ associative on Y_{SQ}? YES!

Is there an identity? YES: R_0

Does every element have an inverse? YES!

$(Y_{SQ}, \bullet)$ is a group

the "dihedral" group D_4

Examples

Is $(Z_n, +_n)$ a group?

(Z_n is the set of integers modulo n)

Is Z_n closed under $+_n$? YES!

Is $+_n$ associative on Z_n? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$(Z_n, +_n)$ is a group

Examples

Is $(Z_n, *_n)$ a group?

(Z_n is the set of integers modulo n)

Is $*_n$ associative on Z_n? YES!

Is there an identity? YES: 1

Does every element have an inverse? NO!

$(Z_n, *_n)$ is NOT a group

Examples

Is $(Z_n^*, *_n)$ a group?

(Z_n^* is the set of integers modulo n that are relatively prime to n)

Is $*_n$ associative on Z_n^* ?YES!

Is there an identity? YES: 1

Does every element have an inverse? YES!

$(Z_n^*, *_n)$ is a group

Permutation Group

A permutation of a nonempty set S is a bijection f:S->S.

A set of all permutations of S is a group with respect to composition.

This group is called the symmetric group. When S={1,2,…,n}, the group is denoted S_n.

An element of S_n is represented by two-row form

Permutation Group

Composition: (read from right to left)

$$\begin{pmatrix}1234\\2413\end{pmatrix} o \begin{pmatrix}1234\\3412\end{pmatrix} = \begin{pmatrix}1234\\1324\end{pmatrix}$$

Composition of functions is associative.

The inverse element is obtained by reading the bottom row first

$$\begin{pmatrix}1234\\2431\end{pmatrix}^{-1} = \begin{pmatrix}1234\\4132\end{pmatrix}$$

Permutation Group

Theorem. If n>2, then S_n is non-commutative.

$$\begin{pmatrix}1234\\2413\end{pmatrix} o \begin{pmatrix}1234\\3412\end{pmatrix} = \begin{pmatrix}1234\\1324\end{pmatrix}$$

$$\begin{pmatrix}1234\\3412\end{pmatrix} o \begin{pmatrix}1234\\2413\end{pmatrix} = \begin{pmatrix}1234\\4231\end{pmatrix}$$

Some properties of groups…

Identity Is Unique

Theorem: A group has exactly one identity element

Proof:

Suppose e and f are both identities of $G=(S,\blacklozenge)$

Then $f = e \blacklozenge f = e$

We denote this identity by "e"

Inverses Are Unique

Theorem: Every element in a group has a unique inverse

Proof:

Suppose b and c are both inverses of a

Then $b = b \blacklozenge e = b \blacklozenge (a \blacklozenge c) = (b \blacklozenge a) \blacklozenge c = c$

Orders and generators

Order of a group

A group $G=(S,\blacklozenge)$ is **finite** if S is a finite set

Define $|G| = |S|$ to be the **order** of the group (i.e. the number of elements in the group)

What is the group with the least number of elements?

$G = (\{e\},\blacklozenge)$ where $e \blacklozenge e = e$

Theorem. The order of S_n is n!.

Generators

A set $T \subseteq S$ is said to generate the group $G = (S,\blacklozenge)$ if every element of S can be expressed as a finite product of elements in T

Question: Does $\{R_{90}\}$ generate Y_{SQ}? NO!

Question: Does $\{F_|, R_{90}\}$ generate Y_{SQ}? YES!

An element $g \in S$ is called a **generator** of $G=(S,\blacklozenge)$ if the set {g} generates G

Does Y_{SQ} have a generator? NO!

Generators For $(Z_n,+)$

Any $a \in Z_n$ such that GCD(a,n)=1 generates $(Z_n,+)$

Claim: If GCD(a,n) =1, then the numbers a, 2a, …, (n-1)a, na are all distinct modulo n

Proof (by contradiction):

Suppose $xa = ya \pmod n$ for $x,y \in \{1,\ldots,n\}$ and $x \neq y$

Then $n \mid a(x-y)$

Since GCD(a,n) = 1,
then $n \mid (x-y)$, which cannot happen

Order of an element

If $G = (S,\blacklozenge)$, we use a^n denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{n \text{ times}}$

Definition: The order of an element a of G is the smallest positive integer n such that $a^n = e$

What is the order of F_1 in Y_{SQ}? 2

What is the order of R_{90} in Y_{SQ}? 4

The order of an element can be infinite!
(if such n does not exist)

Example: The order of 1 in the group (Z,+) is infinite

Remember

order of a group G = size of the group G

order of an element g = (smallest n>0 s.t. $g^n = e$)

Orders

Consider the permutation $\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}$

$$\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}^2 = \begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}^4 = \begin{pmatrix}1&2&3&4&5\\1&2&4&5&3\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix}^6 = \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}$$

Orders

Theorem: If G is a finite group, then for all g in G, order(g) is finite.

Proof:

Consider $g, g\blacklozenge g, g\blacklozenge g\blacklozenge g = g^3, g^4, \ldots$

Since G is finite, $g^j = g^k$ for some $j < k$

Multiplying both sides by $(g^j)^{-1}$, we obtain

$e = g^{k-j}$

Remember

order of a group G = size of the group G

order of an element g = (smallest n>0 s.t. $g^n = e$)

g is a generator if order(g) = order(G)

Orders

What is order(Z_n, $+_n$)? n

For x in (Z_n, $+_n$), what is order(x)?

order(x) = n/GCD(x,n)

Proof. Let order(x)=m.
This means m x=0(mod n), or m x = q n
Let d = gcd(x,n), x = x_1 d, n = n_1 d.
where gcd(x_1,n_1)=1

$n_1 x = n_1 x_1 d = n x_1 = 0 \pmod n$, Thus, $m \leqslant n_1$
$mx=qn \Rightarrow mx_1 d=qn_1 d \Rightarrow mx_1=qn_1 \Rightarrow n_1 | mx_1 \Rightarrow n_1 | m$
Thus, $m \geqslant n_1$. We conclude, $m = n_1 = n/d$

Orders

order(Z_n^*, $*_n$)?

$\phi(n)$

For x in (Z_n^*, $*_n$), what is order(x)?

At most $\phi(n)$

Euler's theorem: $x^{\phi(n)} = 1 \pmod n$

Orders

Theorem: Let x be an element of G. The order of x divides the order of G

Corollary: If p is prime, $a^{p-1} = 1 \pmod p$
(remember, this is Fermat's Little Theorem)

G = (Z_p^*, *), order(G) = p-1

Subgroups

Subgroups

Suppose G = (S,♦) is a group.

If $T \subseteq S$, and if H = (T, ♦) is also a group, then H is called a subgroup of G.

Examples

(Z, +) is a group
(Evens, +) is a subgroup.

Is (Odds, +) a subgroup of (Z,+) ?

No! (Odds,+) is not a group!

Examples

$(Z_n, +_n)$ is a group and if k | n,
Is $(\{0, k, 2k, 3k, \ldots, (n/k-1)k\}, +_n)$ subgroup of $(Z_n, +_n)$?

Only if k is a divisor of n.

Is $(Z_k, +_k)$ a subgroup of $(Z_n, +_n)$?

No! it doesn't even have the same operation

Is $(Z_k, +_n)$ a subgroup of $(Z_n, +_n)$?

No! $(Z_k, +_n)$ is not a group! (not closed)

Subgroup facts (identity)

If e is the identity in G = (S, ♦),
what is the identity in H = (T, ♦)?

e

Proof: Clearly, e satisfies

$e \diamond a = a \diamond e = a$ for all a in T.

But we saw there is a unique such element in any group.

Subgroup facts (inverse)

If b is a's inverse in G = (S, ♦),
what is a's inverse in H = (T, ♦)?

b

Proof: Let a^{-1} is the inverse of a in G and let c is the inverse of a in H

Then, $c \diamond a = a \diamond c = e$ by previous slide

Moreover, we proved that a^{-1} is the unique.

Thus, $c \diamond a = e \Rightarrow c = a^{-1}$

Lagrange's Theorem

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

Lagrange's Theorem

Corollary: If x in G, then order(x) divides |G|.

Proof of Corollary:
Consider the set $T_x = (x, x^2, x^3, \ldots)$
$H = (T_x, \diamond)$ is a group. (check!)
Hence it is a subgroup of $G = (S, \diamond)$.
Order(H) = order(x). (check!)

On to other algebraic definitions

Rings

We often define more than one operation on a set

For example, in Z_n we can do both addition and multiplication modulo n

A ring is a set together with two operations

Definition:

A ring R is a set together with two binary operations + and ×, satisfying the following properties:

1. (R,+) is a commutative group
2. × is associative

Minimal requirements from "product"

3. The distributive laws hold in R:
   $(a + b) \times c = (a \times c) + (b \times c)$
   $c \times (a + b) = (c \times a) + (c \times b)$

Examples:

Is (Z, +, *) a ring?

Yes. (Z,+) is commutative group
* is associative
+ distributes over *

Is (Z, +, min) a ring?

No (Z,+) is commutative group
min is associative
but + does not distribute over min
$\min(1+3,2) \neq \min(1,2) + \min(3,2)$

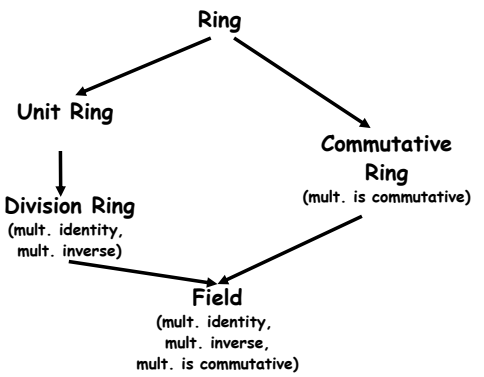
Examples:

(Set of mxn Z-valued matrices, +, *)?

Yes. It is commutative group with respect to +
* is associative
+ distributes over *

(Set of polynomials with real coefficients,+,*)?

Yes. It is commutative group with respect to +
* is associative
+ distributes over *



Fields

A field F is a set together with two binary operations + and ×, satisfying the following properties:

1. (F,+) is a commutative group
2. (F-{0},×) is a commutative group
3. The distributive law holds in F:
   $(a + b) \times c = (a \times c) + (b \times c)$

Examples:

Is (Z, +, *) a field?

No. (Z,*) not a group

How about (R, +, *)?

Yes.

How about $(Z_n, +_n, *_n)$?

Only when n is prime. $(Z_n, *_n)$ is a group only for prime n.

In The End…

Why should I care about any of this?

Groups, Rings and Fields are examples of the principle of abstraction: the particulars of the objects are abstracted into a few simple properties

If you prove results from some group, check if the results carry over to *any* group

Here's What You Need to Know…

Binary Operation
Identity and Inverses
Generators
Order of element, group

Groups
Subgroups
Rings and Fields