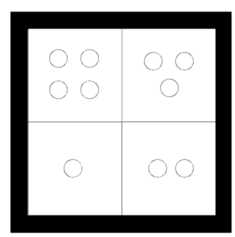
15-251
Great Theoretical Ideas in Computer Science

Algebraic Structures: Group Theory

Lecture 16, October 14, 2009

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

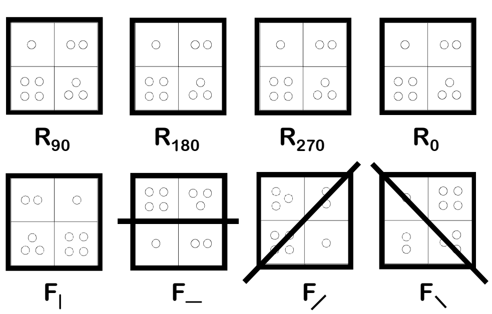
Rotating a Square in Space



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?

We will now study these 8 motions, called the symmetries of the square



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 $a \bullet b \in Y_{SQ}$?

	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

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, • 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 •(a,b) as "a • b"

Binary Operations

"•" is called a binary operation on Y_{SQ}

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

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 ♦ on a set S is associative if:

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

Examples:

Is f: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x,y) = xy + y$ associative?

$(ab + b)c + c = a(bc + c) + (bc + c)$? NO!

Is the operation • on the set of symmetries of the square associative? YES!

Commutativity

A binary operation ♦ on a set S is commutative if

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

Is the operation • on the set of symmetries of the square commutative? NO!

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

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 ♦ 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 ♦ 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

Groups

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

1. ♦ 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,♦) and ♦ 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,♦)
1. Check "closure" for (S,♦)
   (i.e, for any a, b in S, check a ♦ 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 + 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 + 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 + associative on Odds? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

Are the Odds closed under addition NO!

(Odds,+) is NOT a group

Examples

Is (Y_{SQ}, •) a group?

Is • associative on Y_{SQ}? YES!

Is there an identity? YES: R_0

Does every element have an inverse? YES!

(Y_{SQ}, •) is a group

Examples

Is $(Z_n,+)$ a group?

(Z_n is the set of integers modulo n)

Is + associative on Z_n? YES!

Is there an identity? YES: 0

Does every element have an inverse? YES!

$(Z_n, +)$ is a group

Examples

Is $(Z_n,*)$ a group?

(Z_n is the set of integers modulo n)

Is * associative on Z_n? YES!

Is there an identity? YES: 1

Does every element have an inverse? NO!

$(Z_n, *)$ is NOT a group

Examples

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

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

Is * associative on Z_n^* ? YES!

Is there an identity? YES: 1

Does every element have an inverse? YES!

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

And some properties…

Identity Is Unique

Theorem: A group has at most one identity element

Proof:

Suppose e and f are both identities of G=(S,♦)

Then f = e ♦ 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 ♦ e = b ♦ (a ♦ c) = (b ♦ a) ♦ c = c

Orders and generators

Order of a group

A group G=(S,♦) 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},♦) where e ♦ e = e

How many groups of order 2 are there?

	e	f
e	e	f
f	f	e

Generators

A set $T \subseteq S$ is said to generate the group G = (S,♦) 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,♦) if {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 (mod n) for $x,y \in \{1,\ldots,n\}$ and $x \neq y$

Then n | a(x-y)

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

Order of an element

If G = (S,♦), 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 $a^n = e$

The order of an element can be infinite!

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

What is the order of $F_{|}$ in Y_{SQ}? 2

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

Orders

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

For $(Z_n, +)$, recall that order(g) = n/GCD(n,g)

Orders

What about $(Z_n^*, *)$?

order$(Z_n^*, *) = \phi(n)$

What about the order of its elements?

Orders

What about $(Z_n^*, *)$?

order$(Z_n^*, *) = \phi(n)$

What about the order of its elements?

Non-trivial theorem:
There are $\phi(n-1)$ generators of $(Z_n^*, *)$

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)

BTW, what group did we apply the theorem to?

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

Groups and 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
and (Evens, +) is a subgroup.

Also, (Z, +) is a subgroup of (Z, +). (Duh!)

What about (Odds, +)?

Examples

$(Z_n, +_n)$ is a group and if k | n,
what about ({0, k, 2k, 3k, …, (n/k-1)k}, $+_n$) ?

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

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

Quick facts (identity)

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

Quick facts (inverse)

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

Lagrange's Theorem

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|.

Corollary: If x in G, then order(x) divides |G|.
Proof of Corollary:
Consider the set T_x = (x, x^2 = x ♦ x, x^3, …)
H = (T_x, ♦) is a group. (check!)
Hence it is a subgroup of G = (S, ♦).
Order(H) = order(x). (check!)

On to other algebraic definitions

Lord Of The 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
3. The distributive laws hold in R:

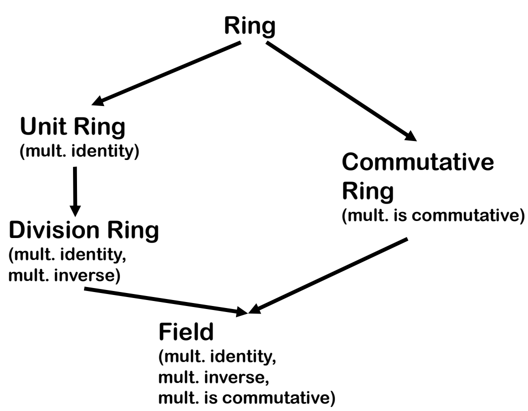
   (a + b) × c = (a × c) + (b × c)

   c × (a + b) = (c × a) + (c × b)

Examples:

Is (Z, +, *) a ring?

How about (Z, +, min)?



Fields

Definition:

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) × c = (a × c) + (b × c)

Examples:

Is (Z, +, *) a field?

How about (R, +, *)?

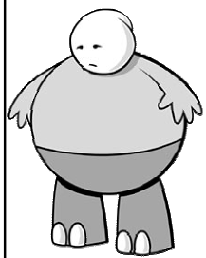
How about (Z_n, $+_n$, $*_n$)?

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…

Symmetries of the Square
Compositions

Groups
Binary Operation
Identity and Inverses
Basic Facts: Inverses Are Unique
Generators

Rings and Fields
Definition