15-251

Great Theoretical Ideas in Computer Science

Algebraic Structures: Group Theory

Lecture 15 (October 12, 2010)

Number Theory

Naturals	Integers	Z_n
closed under +	closed under +	closed under $+_n$
a+b = b+a	a+b = b+a	$a +_n b = b +_n a$
(a+b)+c = a+(b+c)	(a+b)+c = a+(b+c)	$(a +_n b) +_n c = a +_n (b +_n c)$
a+0 = 0+a = a	a+0 = 0+a	$a +_n 0 = 0 +_n a$
	a+(-a) = 0	$a +_n (-a) = 0$

Number Theory

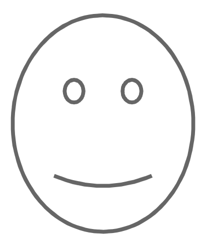
Matrices	Integers	Z_n
closed under +	closed under +	closed under $+_n$
A+B = B+A	a+b = b+a	$a +_n b = b +_n a$
(A+B)+C = A+(B+C)	(a+b)+c = a+(b+c)	$(a +_n b) +_n c = a +_n (b +_n c)$
A+0 = A	a+0 = 0+a	$a +_n 0 = 0 +_n a$
A+(-A) = 0	a+(-a) = 0	$a +_n (-a) = 0$
closed under *	closed under *	closed under $*_n$
ditto	(a+b)*c = a*c+b*c	ditto
ditto (AB ≠ BA)	1/a may not exist	ditto

Number Theory

Invertible Matrices ∪ {0}	Rationals	Z_n (n prime)
closed under +	closed under +	closed under $+_n$
A+B = B+A	a+b = b+a	$a +_n b = b +_n a$
(A+B)+C = A+(B+C)	(a+b)+c = a+(b+c)	$(a +_n b) +_n c = a +_n (b +_n c)$
A+0 = 0+A	a+0 = 0+a	$a +_n 0 = 0 +_n a$
A+(-A) = 0	a+(-a) = 0	$a +_n (-a) = 0$
closed under *	closed under *	closed under $*_n$
ditto	(a+b)*c = a*c+b*c	ditto
ditto	1/a exists if $a \neq 0$	ditto

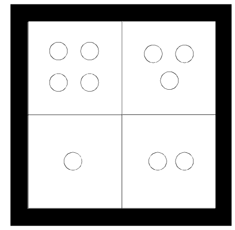
Abstraction: Abstract away the inessential features of a problem

=



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

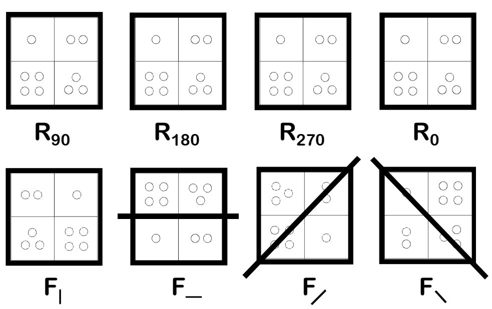
Rotating a Square in Space



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˚"

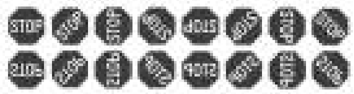
$= R_{270}$

$F_{|} \bullet R_{90}$ means "first flip horizontally and then rotate 90˚"

$= F_{/}$

Question: if $a,b \in Y_{SQ}$, does $a \bullet b \in Y_{SQ}$? 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, • 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 $\mathbb{N}$

$g(x,y) = \sqrt{x+y}$

implicitly contains "closure"

Associativity

A binary operation ♦ on a set S is associative if:

for all a,b,c∈S, (a♦b)♦c = a♦(b♦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∈S, a ♦ b = b ♦ 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 • 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 ♦ a = a ♦ 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}

$F_{\vert}$ inverse: $F_{\vert}$

Every element in Y_{SQ} has a unique inverse

	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	$F_{\_}$	$F_{/}$	$F_{\backslash}$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	$F_{\_}$	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_{\backslash}$	$F_{/}$	$F_{\vert}$	$F_{\_}$
R_{180}	R_{180}	R_{270}	R_0	R_{90}	$F_{\_}$	$F_{\vert}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	$F_{\_}$	$F_{\vert}$
$F_{\vert}$	$F_{\vert}$	$F_{/}$	$F_{\_}$	$F_{\backslash}$	R_0	R_{180}	R_{90}	R_{270}
$F_{\_}$	$F_{\_}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	R_{180}	R_0	R_{270}	R_{90}
$F_{/}$	$F_{/}$	$F_{\_}$	$F_{\backslash}$	$F_{\vert}$	R_{270}	R_{90}	R_0	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	$F_{\_}$	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:

S is closed under ♦

1. ♦ is associative
2. (Identity) There exists an element $e \in S$ such that:
   e ♦ a = a ♦ e = a, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: a ♦ b = b ♦ a = e

Commutative or "Abelian" Groups

If G = (S, ♦) and ♦ is commutative, then G is called a commutative group

remember,
"commutative" means
a ♦ b = b ♦ 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 $\mathbb{N}$ 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}, •) a group?

Is Y_{SQ} closed under •? YES!

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

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

$\mathbb{Z}$	(Z, *)	No inverses…
$\mathbb{Q}$ the rationals	(Q, *)	Zero has no inverse…
	(Q \ {0}, *)	Yes

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:
   $e ♦ a = a ♦ e = a$, for all $a \in S$

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

Some properties of groups…

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 □

⇒ exactly one identity

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

□

Cancellation

Theorem: If a ♦ b = a ♦ c, then b = c

Proof: $(a^{-1}) \diamond (a \diamond b) = (a^{-1}) \diamond (a \diamond c)$

$\Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$

$\Rightarrow e \circ b = e \circ c$

$\Rightarrow b = c$

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

	e	f
e	e	f
f	f	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Generators

A set T ⊆ S is said to generate the group G = (S,♦) if every element of S can be expressed as a finite "sum" of elements in T

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

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

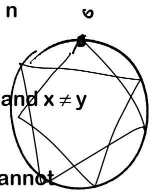
An element g ∈ S is called a generator of G=(S,♦) if the set {g} generates G

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 (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^t denote $\underbrace{(a \blacklozenge a \blacklozenge \ldots \blacklozenge a)}_{t \text{ times}}$

Warning: Potential Confusion

If G = $(Z_n, +)$, this means " a^t " denotes $\underbrace{(a + a + \ldots + a)}_{t \text{ times}}$ = t*a mod n

If G = $(Z_n^*, *)$, " a^t " now denotes a^t mod n

Please be careful when using notation " a^t " !

Order of an element

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

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

Remember

order of a group G = size of the group G

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

Orders

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

Proof: Consider g, g♦g, g♦g♦g = g^3, g^4, …

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

$\Rightarrow g^j = g^j \blacklozenge g^{k-j}$

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

$\Rightarrow e = g^{k-j}$

Remember

order of a group G = size of the group G

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

Thm g is a generator of group G
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)

Orders

order(Z_n^*, $*_n$)? $\phi(n)$

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

Danny's Thm
order(x) | $\phi(n)$
Exercise

At most $\phi(n)$

(Euler's theorem)

$\forall a \in \mathbb{Z}_n^*$ $a^{\phi(n)} \equiv 1 \pmod{n}$

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)

What group did we use for the corollary?

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

order(x) | p-1 $\Rightarrow$ $x^{p-1} \equiv 1 \pmod{p}$

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.
In fact, (Multiples of k, +) is also a subgroup.

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

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

Examples

$(Z_n, +_n)$ is a group and if $k \mid n$,
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

$e ♦ a = a ♦ e = a$ 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 c be a's inverse in H.

Then $c ♦ a = e$
$\Rightarrow c ♦ a ♦ b = e ♦ b$
$\Rightarrow c ♦ e = b$
$\Rightarrow c = b$

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 $T_x = (x, x^2 = x ♦ x, x^3, \ldots)$
$H = (T_x, ♦)$ is a group. (check!)
Hence it is a subgroup of G = (S, ♦).
Order(H) = order(x). (check!)

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.

Curious (and super-useful) corollary:

If you can show that H is a subgroup of G
and $H \neq G$
then |H| is at most ½ |G|

"Right" way of looking at primality testing

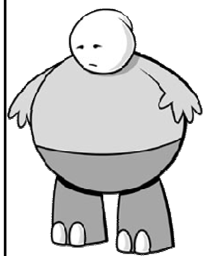
Fermat: if n prime, then $a^{n-1} = 1 \pmod n$
for all $0 \le a \le n$.

Suppose the converse was also true:
"if n composite, then exists g with $0 < g < n$.
$g^{n-1} \neq 1 \pmod n$"

Then consider "bad elements" for this n:
elements b such that $b^{n-1} = 1 \pmod n$

Bad elements form a subgroup of Z_n $\Rightarrow$ |Bad| < ½ n
Picking random element, it is good with probability ½.

Sadly, converse not true. Fixing that gives Miller-Rabin.



Here's What You Need to Know…

Symmetries of the Square
- Compositions

Groups
- Binary Operation
- Identity and Inverses
- Basic Facts: Inverses Are Unique
- Generators
- Order of element, group

Subgroups
- Lagrange's theorem