Math 403. Fall 2011
UMD

Lecture 4. Groups

Def Let M be a set. A binary operation on M is a map $*: M \times M \to M$.

Ex ① $M = \mathbb{Z}$, $+: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $(a,b) \mapsto a+b$ is a binary operation

② $M = \mathbb{Z}$, $\cdot: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $(a,b) \mapsto ab$ is another.

③ $M = \{1, 2, \ldots, n\}$ for $n \in \mathbb{Z}_+$. Then $M \times M$ has n^2 elements. To define a map $\phi: M \times M \to M$, for each element of $M \times M$, you have to pick one element of M to send it to. So there are $(n^2)^n = n^{2n}$ binary operations on M, most are uninteresting.

Notational Conventions ① An ordered pair $(M, *)$ where M is a set and $*$ is a binary operation on M is called a magma. There aren't too interesting, so you won't have the term to much.

② If $(M, *)$ is a magma, then we usually like to write the operation as $(m,n) \mapsto m * n$ instead of $(m,n) \mapsto *(m,n)$.

③ If $*$ is assumed known, we just say M is a magma instead of $(M, *)$ is a magma.

Or we say M is a magma with the operation $*$.

Ex $\mathbb{Q}$ is a magma with the operation

$a * b = ab^2$.

(4) Sometimes we get sick of writing $*$ and we just write mn instead of $m*n$.

Def Let M be a magma with operation $(m,n) \mapsto mn$. We say that

(1) M is associative if for all $a,b,c \in M$

$$(ab)c = a(bc)$$

(2) M is commutative (or abelian) if for all $a,b \in M$

$$ab = ba$$

(3) An element $e \in M$ is an identity element if $\forall$ $a \in M$, $em = me = m$.

Ex (1) Let $M = M_2(\mathbb{R})$ be the set of 2×2 matrices with real coefficients.

Define an operation $\circ$ on M by

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \circ \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + \\ & \end{pmatrix}$$

Then M is associative.

It has a identity element $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(2) Let $M = M_{2\times 2}(\mathbb{R})$ by with the binary operation

$(X,Y) \mapsto [X,Y] = X \circ Y - Y \circ X$. (This is called the Lie Bracket.). Then M is not associative

$$O = \left[\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}\right], \begin{pmatrix}0&1\\0&0\end{pmatrix}\right]$$

$$\left[\begin{pmatrix}1&0\\0&0\end{pmatrix}, \left[\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}\right]\right] = \left[\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}\right] = \begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

Def A magma M is called a monoid if it is associative and has a unit e

Prop Let M be a magma. If e, e' are id elements in M, then $e = e'$.

Pf $e = e'e$ since e' is an identity element

$= e'$ since e is an identity element.

Def A magma M is called a monoid if it is associative and has a unit element.

Ex (a) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ with binary op $(a,b) \mapsto a+b$ is a monoid. The unit element is 0.

(b) $\mathbb{N} = \{0, 1, 2, \ldots\}$ with binary op $(a,b) \mapsto ab$ is also a monoid. The unit element is 1.

(c) $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$ with binary op $(a,b) \mapsto ab$ is again a monoid. The unit element is 1.

(d) $\mathbb{Z}_+$ with binary op $(a,b) \mapsto a+b$ is not a monoid. No unit element. It is an associative magma.

Prop Let X be a set and set $E(X) = \{f : X \to X\}$. Define a binary op on $E(X)$ by $(f,g) \mapsto f \circ g$. Then $E(X)$ is a monoid with id_X as unit.

Pf We proved associativity and that $\mathrm{id}_X \circ f = f \circ \mathrm{id}_X$ already.

Prop 1 $E(X)$ is commutative $\iff$ X has fewer than 2 elements.

Pf If $X = \emptyset$ or $\{1\}$ then $E(X) = \{\mathrm{id}\}$. So clearly $E(X)$ is commutative. Otherwise $E(X) = \{\mathrm{id}_X\}$. Suppose x_1, x_2 are two distinct elements of X. Define $f, g \in E(X)$ by

$$f(x) = x_1 \quad \text{for all } x \in X$$

$$g(x) = \begin{cases} x_2 & x = x_1 \\ x_1 & x \neq x_1 \end{cases}$$

Then $f \circ g(x_1) = f(x_2) = x_1$

$g \circ f(x_1) = g(x_1) = x_2$.

So $f \circ g \neq g \circ f$.

Prop $M_2(\mathbb{R})$ is not commutative under matrix multiplication.

Pf $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Def Let M be a monoid. An element $u \in M$ is a **unit** if there exists $v \in M$ st $uv = vu = e$. (where e is the identity element). We write $M^\times = \{u \in M : u \text{ is a unit}\}$.

Prop Suppose $u \in M^\times$. Then if $v_1 u = u v_2 = e$ we have $v_1 = v_2$.

Pf $v_1 = v_1 e = v_1(u v_2) = (v_1 u) v_2 = e v_2 = v_2$.

Cor If $u \in M^\times$ then there exists a unique $v \in M$ st $uv = e$. For this v we have $vu = e$ as well.

Pf Suppose $u \in M^\times$. Then $\exists$ a v st $vu = uv = e$. If $v_1 u = e$ then $v_1 = v$.

Def If $u \in M^\times$ we write u^{-1} for the element of M st

$u u^{-1} = u^{-1} u = e$.

Exception If M is commutative and the op is written $+$ then we write $-u$ instead of u^{-1}.

Ex ① In $\mathbb{Q}$ with binary op $(a,b) \mapsto ab$ we have $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$. $3^{-1} = \frac{1}{3}$.

② In $\mathbb{Z}$ with binary op $(a,b) \mapsto a+b$ the inverse of 3 is -3.

③ In $\mathbb{Z}$ with op $(a,b) \mapsto ab$ we have $\mathbb{Z}^\times = \{\pm 1\}$.

$(-1)^{-1} = -1$.

Def A group is a monoid G st $G^\times = G$.

Prop Let $(G, *)$ be a mugma. Then G is a gp $\Leftrightarrow$

- $(a*b)*c = a*(b*c) \quad \forall a,b,c \in G$
- $\exists e \in G$ st $\forall a \in G$, $a*e = e*a = a$
- $\forall a \in G \ \exists a^{-1} \in G$ st $a a^{-1} = a^{-1} a = e$.

Pf Just check the defs.

Ex ① $(\mathbb{Z}, +)$ is a group. In fact abelian.

② $(\mathbb{Z}/n, +)$ also a group.

- $[n] + [-n] = [0]$ so the inverse
- $[0] + [n] = [n] + [0] - [n]$

Prop Let M be a monoid. Then for any $a, b \in M^\times$, $ab \in M^\times$ and $a^{-1} \in M^\times$. Consequently, $M^\times$ with the binary op inherited from M to $M^\times \times M^\times \to M^\times$ by $(a,b) \mapsto ab$ is a group.

Pf Take $a, b \in M^*$. Then

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1})$$
$$= a(ea^{-1}) = aa^{-1} = e$$

$$\Rightarrow \boxed{(ab)^{-1} = b^{-1}a^{-1}}$$

$$\Rightarrow ab \in M^\times.$$

$a^{-1}a = e \Rightarrow (a^{-1})^{-1} = a$. $\therefore a^{-1} \in M^\times$.
"
aa^{-1}

The product on $M^\times$ is clearly associative, so

We have $e \in M^\times$ since $ee = e \Rightarrow e^{-1} = e$.

The product in $M^\times$ clearly on. $\therefore M^\times$ is a grp.

Def

Prop Let X be a set. Then $E(X)^X = \{f : X \to X \mid f \text{ is 1-1 onto}\}$, & $E(X)^X$ is a gp. Call it $A(X)$, the group of automorphisms of the set X.

pf Suppose $f: X \to X$ 1-1 onto. Then $\exists\ g: X \to X$ s.t. $f \circ g = g \circ f = id_X$. & $f \in E(X)^X$. Conversely, suppose $f \in E(X)$ onto $\exists\ g \in E(X)$ s.t. $f \circ g = g \circ f = id_X$. Then, for $x \in X$

$$x = id_X(x) = f \circ g(x) = f(g(x))$$

$\Rightarrow f$ is onto.

And for $x, y \in X$

$$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow id_X(x) = id_X(y)$$

$$\Rightarrow x = y.$$

So f is 1-1.

Def $S_n = A(\{1, \ldots, n\})$. Called the symmetric group.

Notation for elements of $E(\{1,\dots,n\})$.

Let's write $\lceil a_1, a_2, \dots, a_n \rceil$ for the element of $E(\{1,\dots,n\})$ such that

$$\lceil a_1 \dots a_n \rceil(k) = a_k.$$

So

$S_1 = \{ \lceil 1 \rceil \}$

$S_2 = \{ \lceil 12 \rceil, \lceil 21 \rceil \}$ with following mult table

$\lceil 12 \rceil$	$\lceil 12 \rceil = (12)$
$\lceil 12 \rceil$	$\lceil 21 \rceil = \lceil 21 \rceil$
	$= \lceil 21 \rceil \lceil 12 \rceil$
~~$\lceil 12 \rceil \lceil 12 \rceil$~~	$\lceil 21 \rceil \lceil 21 \rceil = \lceil 12 \rceil$

S_3

	b
a	ab

	$\lceil 123 \rceil$	$\lceil 132 \rceil$	$\lceil 213 \rceil$	$\lceil 231 \rceil$	$\lceil 312 \rceil$	$\lceil 321 \rceil$
$\lceil 123 \rceil$	$\lceil 123 \rceil$	$\lceil 132 \rceil$	$\lceil 213 \rceil$	$\lceil 231 \rceil$	$\lceil 312 \rceil$	$\lceil 321 \rceil$
$\lceil 132 \rceil$	$\lceil 132 \rceil$	$\lceil 123 \rceil$	$\lceil 312 \rceil$	$\lceil 321 \rceil$		
$\lceil 213 \rceil$	$\lceil 213 \rceil$	$\lceil 231 \rceil$				
$\lceil 231 \rceil$	$\lceil 231 \rceil$					
$\lceil 312 \rceil$	$\lceil 312 \rceil$					
$\lceil 321 \rceil$	$\lceil 321 \rceil$					

Now $\lceil 132 \rceil \lceil 213 \rceil = \lceil 312 \rceil$ $\neq$ $\lceil 231 \rceil$ So not commutative.

$\lceil 213 \rceil \lceil 132 \rceil =$

Prop Let A be an associative magma and $a \in A$. Define a function $\mathbb{Z}_+ \to A$ ~~inductively by setting~~ written $n \mapsto a^n$ inductively by setting $a^1 = a$, $a^n = a(a^{n-1})$ for $n > 1$. Then, for all $n, m \in \mathbb{Z}_+$,

$$a^{n+m} = a^n a^m.$$

Pf Induct on n. For $n = 1$, we have

$$a^{1+m} = a\, a^m$$

by definition. So the result holds. Suppose the result holds for ~~all~~ $k < n$, and $n > 1$,

$$\begin{aligned} a^{n+m} &= a\, a^{n+m-1} && \text{by def} \\ &= a\, a^{(n-1)+m} \\ &= a(a^{n-1} a^m) && \text{by inductive hypothesis} \\ &= (a\, a^{n-1})\, a^m && \text{by associativity} \\ &= a^n a^m && \text{by def.} \end{aligned}$$

Prop Suppose G is a group and $g \in G$. For each $n \in \mathbb{Z}$ define

$$g^n = \begin{cases} g^n & \text{if } n > 0 \\ e & \text{if } n = 0 \\ (g^{-n})^{-1} & \text{if } n < 0, \end{cases}$$

using previous def.

Then $g^{n+m} = g^n g^m$.