Math 322, lecture 6, 26/9/2017

II. Groups and Homomorphisms

§1. Definitions & Examples

Def: A group is a pair $(G, \cdot)$ where G is a set, $\cdot : G \times G \to G$ is a binary operation and:

(1) Associativity: $\forall x, y, z \in G.\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

(2) Neutral element: $\exists e \in G : \forall x \in G : ex = x$.

(3) Left inverse: $\forall x \in G\ \exists \bar{x} \in G : \bar{x}\, x = e$

(If, in addition, we have $\forall x, y \in G\ \ x \cdot y = y \cdot x$, we say G is commutative or abelian)

Fix a group G.

Lemma: (1) $\bar{x}$ is a two-sided inverse: $x\bar{x} = e$ as well

(2) e is a two-sided identity: $xe = x$ as well

(3) the identity and inverse are unique

(4) $\bar{\bar{x}} = x$.

Pf: For any x we have

$$\bar{x} = e\bar{x} = (\bar{x}x)\bar{x} = \bar{x}(x\bar{x}).$$

multiply both sides on the left by $\bar{\bar{x}}$ to get:

$$e = \bar{\bar{x}}\,\bar{x} = \bar{\bar{x}}(\bar{x}(x\bar{x})) = (\bar{\bar{x}}\,\bar{x})(x\bar{x}) = e(x\bar{x}) = x\bar{x}.$$

(2) For any x we have $xe = x(\bar{x}x) = (x\bar{x})x = ex = x$.
(part (1))

(3) Let e' be another left identity.

Then $e = e'e = e'$ (e is a right identity.)

(e is a left identity)

Let $\bar{x}'$ be another left inverse:

$$\bar{x}'x = e$$

mult by $\bar{x}$ on right. Get:

$$\bar{x}' = \bar{x}'e = \bar{x}'(x\bar{x}) = (\bar{x}'x)\bar{x} = e\bar{x} = \bar{x}.$$

(4) Have $\bar{\bar{x}}\bar{x} = e = x\bar{x}$. By uniqueness of left inverse of $\bar{x}$, $\bar{\bar{x}} = x$.

Notation: write x^{-1} for $\bar{x}$.

Remark: $ex = x$ for one x is enough to force $e' = e$

Cor: If $xy = xz$ or $yx = zx$ then $y = z$.

Pf: mult by x^{-1}. (e.g. if $xy = xz$ then $x^{-1}(xy) = x^{-1}(xz)$, $(x^{-1}x)y$, ey, y; $(x^{-1}x)z$, ez, z)

Cor: If $x \cdot x = x$ then $x = e$.

Examples: (a) the trivial group

$\cdot$	e
e	e

(1) $\mathbb{Z}$, S_n, S_X, $GL_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid g^{-1} \text{ exists}\}$

(V vsp $GL(V) = \{T: V \to V \mid \begin{matrix} T \text{ linear} \\ T^{-1} \text{ exists} \end{matrix}\}$

(2) $\mathbb{R}^+ = (\mathbb{R}, +)$, additive group of a vector space

(3) $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ (non-zero elements of a field)

(4) $C_n = (\mathbb{Z}/n\mathbb{Z}, +)$ the cyclic group of order n

$(\mathbb{Z}/n\mathbb{Z})^\times$

Non examples: (1) $(\mathbb{Z}_{\geq 0}, +)$ (1 has no inverse)

(2) $(\mathbb{Z}, \cdot)$ (2 has no inverse

(3) $(GL_n(\mathbb{R}), +)$ ~~not~~ $g + (-g) = 0$

(4) $(\mathbb{Z}_{\geq 1}, \gcd)$

Examples: Symmetry groups

Have set X + "additional structure" on X.

symmetry: maps $f, f^{-1}: X \to X$ which are inverse, preserve the structure

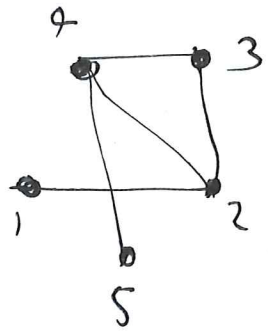
(1) $V = \mathbb{R}^n$ Vsp. extra structure = linear structure

symmetry group = $GL_n(\mathbb{R})$.

(2) $X = \mathbb{R}^n$, + distance function $d(x,y) = \|x - y\|$

("Euclidean space") $\mathrm{Isom}(\mathbb{E}^n) = \{f: \mathbb{R}^n \to \mathbb{R}^n \mid d(f(x), f(y)) = d(x,y)\}$

(3) Graph: pair (V, E), V = set of "vertices"
E = set of pairs of vertices "edges".

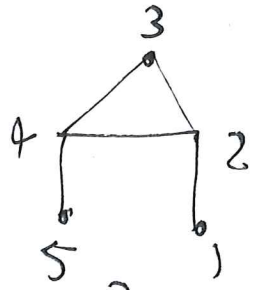
$G =$ 

$\{1,2\} \in E$

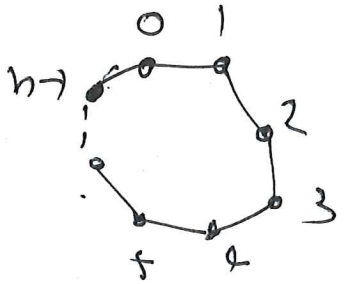
$\{1,4\} \notin E$

Automorphism group: $\mathrm{Aut}(G) = \{\sigma \in S_V \mid \{x,y\} \in E \text{ iff } \{\sigma(x), \sigma(y)\} \in E\}$

eg. for graph above:



$\mathrm{Aut}(G) = \{id, (24)(15)\}$

Eg. write C_n for graph 

("n-cycle")

What is $\mathrm{Aut}(C_n)$?

- include a copy of $(\mathbb{Z}/n\mathbb{Z}, +)$: rotations
- also n reflections

Resulting group is called Dihedral group of order $2n$.

Let r be the map $r(i) = i+1 \pmod n$

Then $\{R = r^0, Rr^1, r^2, r^3, \ldots r^{n-1}\}$ are distinct:

image of 0 by r^j is j.

And $r^n = id$ (ex: map $[a]_n \to r^a$ is a bijection, respects operation)

let p be the map $p(i) = -i \mod n$

This is a reflection, fixing 0.

Let $g \in \mathrm{Aut}(C_n)$. Then $g(0) = i$ for some i.

Then $(r^{-i}g)(0) = r^{-i}(g(0)) = r^{-i}(i) = 0$.

Let $h = r^{-i}g$. Then either $h(1) = 1$ (then $h(-1) = -1$)

or $h(1) = -1$ (" $h(-1) = 1$)

so either $h = id$ or $h = p$. so either $g = r^i$ or $g = r^i p$

Conclusion: every element is one of

$$\{r^i\}_{i=0}^{n-1} \cup \{r^i p\}_{i=0}^{n-1}.$$

all different:

$i \neq j$ $\begin{cases} r^i \neq r^j & \text{(checked)} \\ r^i p \neq r^j p & \text{(right cancellation)} \end{cases}$

$r^i \neq r^j p$ because $r^{i-j} \neq p$ (only rotation to fix 0 is $id \neq p$)

Also, $r^i r^j = r^{i+j}$, $r^i (r^j p) = r^{i+j} p$

what is pr^i? compute $pr^i p^{-1} = pr^i p$ ($p^2 = id$ so $p = p^{-1}$)

$(pr^i p)(j) = pr^i(-j) = p(i-j) = j - i = r^{-i}(j)$

so $pr^i = r^{-i} p$

Homomorphisms

Problems: Are $(\mathbb{Z}/2\mathbb{Z}, +)$, $(\{\pm 1\}, \times)$ the same group?

Are $(\mathbb{R}, +)$, $(\mathbb{R}_{>0}, \times)$ the same group?

Def: Let $(G, \cdot)$, $(H, *)$ be groups. A (group) homomorphism from G to H is a map $f: G \to H$ s.t. $\forall x, y \in G$:

$$f(x \cdot y) = f(x) * f(y)$$

Write $\mathrm{Hom}(G, H)$ for the set of such maps

Examples: (0) Always have trivial hom $f(x) = e_H$.

(1) $\mathrm{sgn}: S_n \to \{\pm 1\}$

(2) $\det: GL_n(F) \to F^\times$

(3) Quotient map $(\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$

Lemma: Let $f \in \mathrm{Hom}(G, H)$. Then:

(1) $f(e_G) = e_H$

(2) $f(g^{-1}) = (f(g))^{-1}$

Pf: (1) e_G, e_H are the unique solutions to $xx = x$ in G, H resp.

and $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$

(2) $f(g) f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$ so $f(g), f(g^{-1})$ are inverse in H.

Def: Call $f \in \mathrm{Hom}(G, H)$ an isomorphism if it is bijective

1.4. The dihedral group

Let P_n be the regular polygon with n sides. Let $D_{2n} = \mathrm{Aut}(P_n)$ be the set of maps of the plan that map P_n to itself.

- Label vertices $0, 1, \cdots, n-1$ (in fact, label them using $\mathbb{Z}/n\mathbb{Z}$).
- Then have a map $c \in D_{2n}$ ("cycle"), with $c([i]) = [i+1]$. Note that $c^j([i]) = [i+j]$.
- And a map $r \in D_{2n}$ ("reflection" by the vertical axis) with $r([i] = -[i])$. Note that $r^2 = \mathrm{id}$ and that $rcr = c^{-1}$.

LEMMA 59. *Suppose $g \in D_{2n}$ fixes $[0]$. Then g is either* id *or r. Any $g \in D_{2n}$ can be written uniquely in the form $c^j r^\varepsilon$ for $j \in \mathbb{Z}/n\mathbb{Z}$ and $\varepsilon \in \mathbb{Z}/2\mathbb{Z}$.*

PROOF. For the first claim if we fix $[0]$ then we either fix $[1]$, at which point we fix everything by induction or we map $[1]$ to $[-1]$ at which point we reverse signs by induction.

For the second, suppose $g(0) = j$. Then $c^{-j}g$ fixes zero, so either $c^{-j}g = \mathrm{id}$ or $c^{-j}g = r$. For uniqueness, suppose $c^j r^\varepsilon = c^k r^\delta$. Then $c^{j-k} = r^{\delta-\varepsilon}$ so c^{j-k} fixes 0 so $j \equiv k(n)$. This means that also $r^\varepsilon = r^\delta$ so $\varepsilon = \delta$. □

COROLLARY 60. $\#D_{2n} = 2n$.

LEMMA 61. $c^j r^\varepsilon c^k r^\delta = c^{j+\sigma k} r^{\varepsilon+\delta}$ *where $\sigma = +$ if $\varepsilon = 0$ and $\sigma = -$ if $\varepsilon = 1$.*

PROOF. if $\varepsilon = 0$ clear. If $\varepsilon = 1$ we have

$$c^j r c^k r r r^\delta = c^j (rcr)^k r^{1+\delta} = c^{j-k} r^{1+\delta}.$$

□

REMARK 62. We saw that D_{2n} is *generated* by r, c.