Admin

HW2 due today 11:59PM

working on HW1 grading

potentially move Friday OH.

Group Actions

Groups are defined abstractly, but they arose (by Galois) as concrete symmetries.

e.g. roots of x^4-1 are $\{1, i, -1, -i\}$,

This has a symmetry via complex conjugation, which preserves the polynomial but shuffles the roots.

"Group" back then was, in modern language, a subgroup of S_n, or really $\Sigma(S)$.

(c.f. Cayley's thm. unifying these perspectives)

Why make this change?

Abstract group theory becomes the grammar by which we discuss symmetry in math.

Consider

- $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ reflection about a hyperplane H
- $M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$ via $A \longmapsto A^t$
- $\mathbb{C} \longrightarrow \mathbb{C}$ via $z \longmapsto \bar{z}$
- $\{\text{functions } \mathbb{R} \to \mathbb{R}\} \longrightarrow \{\text{functions } \mathbb{R} \to \mathbb{R}\}$ via $f(x) \longmapsto f(-x)$

$$\{\text{functions } \mathbb{R} \to \mathbb{R}\} = \mathrm{Fun}(\mathbb{R}, \mathbb{R})$$

These all have the same feature - do it twice and you end up doing nothing.

Recall C_2 the cyclic group of order 2, say $C_2 = \{e, g\}$. Then $g^2 = e$.

These represent symmetries of

- $\mathbb{R}^n$
- $M_n(\mathbb{R})$
- $\mathbb{C}$
- $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$

and the structure of these symmetries is the same for all of them. We say C_2 acts on

- $\mathbb{R}^n$ via reflection about a hyperplane H
- $M_n(\mathbb{R})$ via transposition
- $\mathbb{C}$ via conjugation
- $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$ via $f(x) \longmapsto f(-x)$.

Thus C_2 encodes this "style" of symmetry.

So we can analyze them in a uniform way.

For instance, we will call all the above maps "g"

$g: \mathbb{R}^n \longrightarrow \mathbb{R}^n$

$g: M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$

$g: \mathbb{C} \longrightarrow \mathbb{C}$

$g: \mathrm{Fun}(\mathbb{R},\mathbb{R}) \longrightarrow \mathrm{Fun}(\mathbb{R},\mathbb{R})$

> RmK. If we look $g: GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ via $A \mapsto A^{-1}$, this "averaging" would fail, since we can't add in $GL_n(\mathbb{R})$.

$id = g \circ g \ (= g^2)$

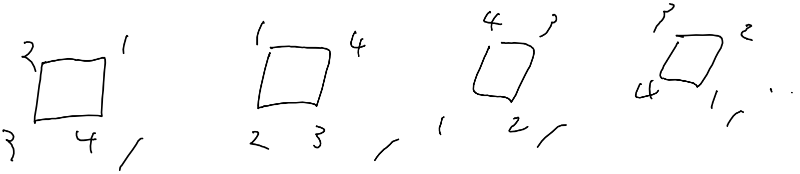
Consider, in each case $\dfrac{x + \overbrace{gx}}{2}$ "averaging over C_2"

- $v \longmapsto \dfrac{v + gv}{2}$ = projection of v onto H
- $A \longmapsto \dfrac{A + A^t}{2}$, a symmetric matrix = projection to $\mathrm{Sym}_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$
- $z \longmapsto \dfrac{z + \overline{z}}{2} = \mathrm{Re}(z)$
- $f \longmapsto \dfrac{f(x) + f(-x)}{2}$ an even function, = projection onto $\mathrm{Even}(\mathbb{R},\mathbb{R}) \subseteq \mathrm{Fun}(\mathbb{R},\mathbb{R})$

This uniform procedure on these C_2 symmetries afforded us a way to find the "fixed axis" of these symmetries.

Consider

- powers of i: $i, -1, -i, 1, \ldots$
- derivatives of $\sin(x)$: $\sin(x), \cos(x), -\sin(x), -\cos(x), \ldots$
- rotations of a square



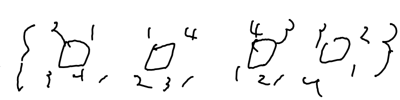
These are all 4-periodic.

Let $C_4 = \langle g \rangle$ be the cyclic group of order 4.

Then C_4 <u>acts</u> on the above

- $g: \{i, -1, -i, 1\} \longrightarrow \{i, -1, -i, 1\}$
  $\alpha \longmapsto i\alpha$

- $g: \{\sin(x), \cos(x), -\sin(x), -\cos(x)\} \longrightarrow \{\ldots\}$
  $f \longmapsto f'$

- $g:$  $\longrightarrow \{\ldots\}$
  rotate by $90°$ ccwise

So this style of symmetry is encoded in C_4.

So by an "action" of a group G on a set S, we mean a way to interpret elements of G as symmetries of S.
Formally, this is a map $G \longrightarrow \Sigma(S)$.

Consider $S_n = \{\text{bijections } \{1, \dots, n\} \to \{1, \dots, n\}\}$.

Certainly, S_n <u>acts</u> on $\{1, \dots, n\}$

Let $\sigma \in S_n$. Then σ yields

$$\{1, \dots, n\} \longrightarrow \{1, \dots, n\}$$

Consider

$$\sigma : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$
$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \longmapsto \begin{pmatrix} a_{\sigma(1)} \\ \vdots \\ a_{\sigma(n)} \end{pmatrix}$$

or

$$\sigma : \mathbb{R}[x_1, \dots, x_n] \longrightarrow \mathbb{R}[x_1, \dots, x_n]$$
$$f(x_1, \dots, x_n) \longmapsto f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

Rmk. $\sum_{i=1}^n x_i$, $\sum_{i<j} x_i x_j$, $\sum_{i<j<k} x_i x_j x_k$, $\dots$, $\prod_{i=1}^n x_i$

are all <u>fixed</u> by the S_n action on $\mathbb{R}[x_1, \dots, x_n]$

Can we classify <u>all</u> fixed polynomials?

Cf. "Fundamental theorem of symmetric polynomials"

$GL_n(\mathbb{R})$ certainly acts on $\mathbb{R}^n$

Let $A \in GL_n(\mathbb{R})$

$$\rightsquigarrow \quad A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$
$$v \longmapsto A \cdot v$$

Also on $\mathbb{R}[x_1, \dots, x_n]$ via

$$A : \mathbb{R}[x_1, \dots, x_n] \longrightarrow \mathbb{R}[x_1, \dots, x_n]$$
$$f\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto f\left(A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right)$$

Rmk. $S_n \hookrightarrow GL_n(\mathbb{R})$ via permutation matrices; a permutation $\sigma \in S_n$ induces a matrix A_σ whose i^{th} column is $e_{\sigma(i)}$.

This allows the previous S_n actions to align with these $GL_n(\mathbb{R})$ actions.

Application: Fermat's little theorem

Theorem. Let p be prime and $a \in \mathbb{Z}$. Then
$$a^p \equiv a \mod p.$$

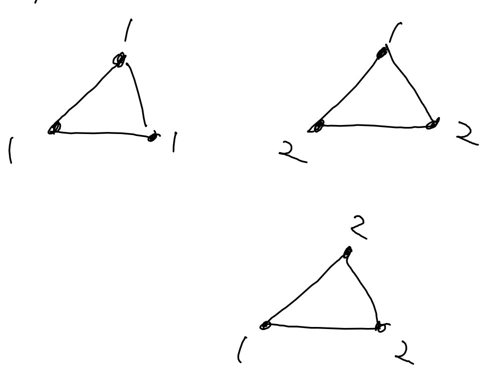
Rmk. You can't use this one on HW 2!

Pf. WLOG take $a \geq 0$.

$\left(\begin{array}{l} \text{If } p \text{ odd, } (-a^p) = -a^p \\ \text{If } p = 2, \ -1 \equiv 1 \mod 2 \end{array} \right)$

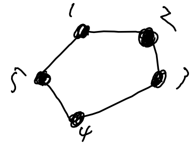
Consider the set of necklaces with p many beads, each labeled by a symbol $\{1, 2, \dots, a\}$.

e.g. $p = 3$ $a = 2$

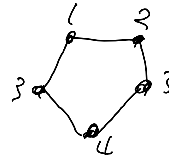


these are the same necklace!

we allow rotations but not reflection



vs.



Fact. there are an integer number of necklaces

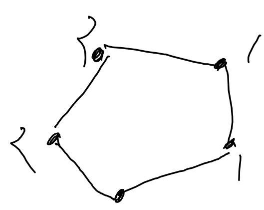
Pf. yup

We will count the number of necklaces.

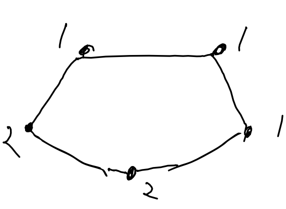
How?

Notice that a necklace can be described a a string of length p with alphabet $\{1, 2, \ldots, a\}$.

e.g. 1 2 2 1 1 $\rightsquigarrow$



but 1 1 2 2 1 $\rightsquigarrow$



which is the same necklace!

Note. There are a^p total such strings

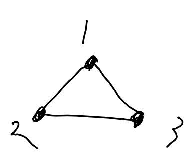
There are a strings with all letters repeated

11111   22222   33333

So there are $\boxed{a^p - a}$ many strings with at least two distinct labels

Claim. There are $\frac{a^p - a}{p}$ many necklaces with at least two distinct labels.

Indeed, given a necklace, what are the possible strings encoding it? These are precisely the cyclic permutations of one specific choice of string.

e.g. given  , the valid strings

are 123, 213, 312

In other words, C_p acts on the set of all such strings. Strings like 11111, 22222, 33333 are fixed points of this action.

Consider a fixed string S. Let H be the subgroup $\{\sigma \in C_p \mid \sigma S = S\}$.

By Lagrange's theorem, $|H| \mid p$, so $|H| = 1$ or $|H| = p$.

$|H| = p$ means everything fixes S, which only occurs for 11111, 22222, etc.

Hence, $|H| = 1$, i.e. only the identity fixes S.

That is, $\{S, \sigma S, \sigma^2 S, \ldots, \sigma^{p-1} S\}$ has p elements, and is precisely the set of labels for the corresponding necklace.

That is, consider

$$\{\text{Strings}\} \xrightarrow{f} \{\text{necklaces}\},$$ a surjection

Given a necklace N represented by string S, the preimage (fiber) $f^{-1}[N]$ is $\{S, \sigma S, \ldots, \sigma^{p-1} S\}$, "the orbit of S under C_p".

Thus, $\{\text{Strings w/ at least 2 distinct labels}\}$

$$\downarrow$$

$\{\text{necklaces with at least 2 distinct labels}\}$

is a surjection where all fibers have p elements. $\square$