Math 128B, Mon May 10

Due dates for revisions: Wed May 26 (last day of finals)

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Last reading of the semester: Ch. 32.
- PS10 due tonight; PS11 outline due Fri.
- Final exam, **Tue May 25**.

  Comprehensive
  Will somewhat emphasize material not on Exams 1, 2, 3 (Review of groups and Ch 32)

Orbit-Stabilizer and conjugacy

(Orbits and Stabilizers under conjugation)

$gxg^{-1} = x \iff gx = xg$

G a group. Define

$$\operatorname{orb}_G(x) = \{gxg^{-1} \mid g \in G\} = \{y \in X \mid y = gxg^{-1} \text{ for some } g \in G\},$$

conjugacy class of x in G

$$\operatorname{stab}_G(x) = \{g \in G \mid gxg^{-1} = x\} \leq G.$$

= all elts g that conjugate x to itself

I.e., $\operatorname{orb}_G(x)$ is the conjuagacy class of x in G and $\operatorname{stab}_G(x)$ is precisely

$$C(x) = \{g \in G \mid gx = xg\} \leq G,$$

the *centralizer* of x in G. Gallian Ch. 3!

Theorem (Orbit-Stabilizer)

For $\cancel{i \in S}$ $x \in G$, ~~$|G| = |\operatorname{orb}_G(i)||\operatorname{stab}_G(i)|$~~

$|G| = |\operatorname{orb}_G(x)||\operatorname{stab}_G(x)|$

$= |\text{conj class}||C(x)|$

Example: Some orbits and stabilizers in S_5

$(a\ b\ c\ d\ e)$, $(a\ b\ c)$, and $(a\ c)(b\ d)$ (e.g., $(1\ 3)(2\ 4)$).

$(1\,2\,3\,4\,5) = (2\,3\,4\,5\,1) =$ etc.

$\boxed{\text{5-cycle } \alpha = (a\,b\,c\,d\,e)}$

$\#$ 5-cycles in $S_5 = \frac{5!}{5} = 24$

$120 = |S_5| = 24 \cdot \text{stab}_{S_5}(\alpha)$

$\kappa(\alpha) = |\text{stab}_{S_5}(\alpha)| = 5.$

Every elt of $\langle\alpha\rangle = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ commutes w/ α so $\text{stab}_{S_5}(\alpha) = \langle\alpha\rangle$.

$\boxed{\text{3-cycle } \underset{\beta}{(a\,b\,c)}}$ # 3-cycles $= \binom{5}{3}\left(\frac{3!}{3}\right) = \left(\frac{5\cdot 4}{2}\right)(2) = 20.$

$$|\mathrm{stab}_{S_5}(\beta)| = \frac{120}{20} = 6$$

Ex. $\beta = (123)$. $\langle \beta \rangle \leq C(\beta)$, $\langle (45) \rangle \leq C(\beta)$

$$C(\beta) = \{e, (123), (132), (45), (123)(45), (132)(45)\}$$

in A_5

not in A_5

$$\boxed{\gamma = (13)(24)}$$

$(12)(34)$

$(14)(23)$

$(15)(23)$

$$\boxed{\begin{array}{cc} 1 & 3 \\ 2 & 5 \end{array}}$$

$$\#\text{conj's of } \gamma = \binom{5}{1} \cdot 3 = 15$$

$$|C(\gamma)| = |\mathrm{Stab}_{S_5}(\gamma)| = \frac{120}{15} = 8$$

Recall: γ is in center of $\boxed{\begin{array}{cc} 1 & 4 \\ 2 & 3 \end{array}}$

$$D_4 = \{\overset{\text{even}}{e}, (1234), \underset{\text{even}}{(13)(24)}, (1432), (24), (13), \underset{\text{even}}{(12)(34)}, \underset{\text{even}}{(14)(23)}\}$$

So $C(\gamma) = D_4$.

The conjugacy classes of A_5

$|A_5| = \frac{120}{2} = 60$

Two permutations of the same cycle shape in S_n are conjugate in S_n, but two even permutations of the same cycle-shape in S_n may not be conjugate in A_n. (Why? Because maybe the element that conjugates alpha to beta is an odd permutation, which is no longer an element of A_n.)

Turns out: Conjugacy classes of even permutations in S_n are sometimes split into two conjugacy classes in A_n, and sometimes they remain conjugacy classes. But we can compute the sizes of conjugacy classes using stabilizers.

Ex. What is size of conj. class of $\beta = (1\,2\,3)$ in A_5?

comm w/ β

even

$$\mathrm{Stab}_{A_5}(\beta) = \mathrm{Stab}_{S_5}(\beta) \cap A_5$$

$$= \{e, (1\,2\,3), (1\,3\,2)\}$$

So # elts in c.c. of (123) in A_5 $= \frac{60}{3} = 20$

$\Rightarrow$ all 3-cycles in A_5 in same c.c.

---

c.c. of $\underbrace{(12345)}_{\alpha}$ in A_5

Orbit-Stab says that we can compute sizes of conj classes by computing sizes of stabilizers =

$\mathrm{Stab}_{A_5}(\alpha) = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4\}$

So # elts in $cl(\alpha) = \boxed{\frac{60}{5}} = 12$

So 5-cycles in A_5 are in two c.c. of size 12.

c.c. of $\gamma = (13)(24)$ in A_5

$$\mathrm{stab}_{A_5}(\gamma) = \mathrm{stab}_{S_5}(\gamma) \cap A_5$$

$$= \{e, (13)(24), (12)(34), (14)(23)\}$$

$$= V$$

elts in cc of $(13)(24)$ in A_5

$$= \frac{60}{4} = 15 = \text{all } (ab)(cd).$$

check: cc of $e = \{e\}$

$$\underset{e}{1} + \underset{(12)(34)}{15} + \underset{(123)}{20} + \underset{(12345)}{12} + \underset{(13524)}{12} = 60$$

Normal subgroups and simple groups

Conjugation stays in H

Definition

Let $H \leq G$. To say that H is **normal** means that for any $a \in H$ and $g \in G$, we have that $gag^{-1} \in H$. (Note that even if $gag^{-1} \in H$, it need not be the case that $gag^{-1} = a$.) In that case, we write $H \lhd G$.

Note that a subgroup $H \lhd G$ exactly when H is a union of conjugacy classes. $= \{e\} \cup cc \cup cc \cdots$

Definition

To say that a group G is **simple** means that the only normal subgroups of G are $\{e\}$ and G.

A_5 is simple

Brute force:

CC in A_5 have sizes
1, 15, 20, 12, 12.

Divisors of 60:
1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Except for 1 and 60, no divisor of 60 is the sum of 1 + one or more of 15, 20, 12, 12. So the only possible orders of a normal subgroup of A_5 are 1, 60.

1 yes $\quad 1+15=16$ no $\quad 1+12=13$ no

$1+20=21$ no

The Galois group of a field extension

Ch. 32!

F a field, E an extension of F.

An *automorphism* of E is a ring isomorphism $\varphi : E \to E$.

The *Galois group of E over F* is:

$$\mathrm{Gal}(E/F) = \{\varphi \in \mathrm{Aut}(E) \mid \varphi(x) = x \text{ for all } x \in F\}.$$

automorphisms of E that fix every element of F

If $H \leq \mathrm{Gal}(E/F)$, we define the *fixed field of H* to be

$$E_H = \{x \in E \mid \varphi(x) = x \text{ for all } \varphi \in H\}.$$

all elements of E that are fixed by
every element of H.

Examples (proofs later)

If E is splitting field of $f(x)$ over F, turns out that one really effective way to represent $\mathrm{Gal}(E/F)$ is as a group of permutations of the roots of f. roots $\{+i, -i\}$

Example: Splitting field of $x^2 + 1$ over $\mathbf{R}$. $= \mathbb{C} = \mathbb{R}(i)$

φ complex conjugation

$\varphi(a+bi) = a - bi$. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{id, \varphi\}$

X perm, φ is $(+i \ -i)$

Example: Splitting field of $x^2 - 5$ over $\mathbf{Q}$. $= \mathbb{Q}(\sqrt{5})$

$\alpha = \sqrt{5}$ roots $\pm\alpha$

$\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ $\varphi : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{5})$

$= \{id, \varphi\}$

$+\sqrt{5} \to -\sqrt{5}$

$-\sqrt{5} \to +\sqrt{5}$

More examples

roots $\{\alpha, \alpha\omega, \alpha\omega^2\}$

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.

$\alpha = \sqrt[3]{7}$, $\omega = e^{\frac{2\pi i}{3}}$

$\mathrm{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$

$\cong S_3$ on $\{\alpha, \alpha\omega, \alpha\omega^2\}$.

Example: Splitting field of $x^4 - 2$ over $\mathbf{Q}$.

Subgroups of Gal(E/F)

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.

Subfields of E containing F — upside down

Example: Splitting field of $x^3 - 7$ over $\mathbf{Q}$.

Fundamental Theorem of Galois Theory

Let F be a field of characteristic 0 or a finite field, and let E be the splitting field of some $f(x) \in F[x]$. Let $\mathcal{S}$ be the set of all subgroups of $\mathrm{Gal}(E/F)$, and let $\mathcal{F}$ be the set of all subfields of E containing F.
Define $\Phi : \mathcal{S} \to \mathcal{F}$ and $\Psi : \mathcal{F} \to \mathcal{S}$ by

$\Phi(H) = E_H =$ the fixed field of H,
$\Psi(K) = \mathrm{Gal}(E/K) =$ the group of all automorphism of E fixing K.

Then Φ and Ψ are inverses of each other, and therefore, bijections. Furthermore, if K, L subfields of E containing F, then

$$K \subseteq L \qquad \Leftrightarrow \qquad \mathrm{Gal}(E/K) \geq \mathrm{Gal}(E/L)$$

(I.e., Φ and Ψ are inclusion-reversing.)

Fundamental Theorem of Galois Theory, cont.

If K, L subfields of E containing F:

1. $[E : K] = |\mathrm{Gal}(E/K)|$, and therefore,

$$[K : F] = |\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)| = \frac{|\mathrm{Gal}(E/F)|}{|\mathrm{Gal}(E/K)|}.$$

2. K is a splitting field of some $g(x) \in F[x]$ if and only if $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$. In that case,

$$\mathrm{Gal}(K/F) \approx \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K).$$

3. The group $\mathrm{Gal}(E/F)$ acts on (permutes) the set $X = \{a_1, \dots, a_n\}$ of all zeros of $f(x)$ in E.
4. If $f(x)$ is irreducible, then $\mathrm{Gal}(E/F)$ acts transitively on $X = \{a_1, \dots, a_n\}$; i.e., for $i \neq j$, there exists some $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(a_i) = a_j$.

Picture of the Fundamental Theorem