Lecture 7 – March 6

- start with a leftover from Lecture 5 (π_1 of link complement)

Garside's solution to the word & conjugacy problems

↳ given 2 words w, w' in $\sigma_i^{\pm 1}$,
- WP: decide if w, w' = same elt of B_n
- CP: decide if w, w' conjugates of each other.

Many improvements since
- Garside 1969
- Thurston
- El Rifai–Morton early 90s – vastly improved sol^n
- Birman-Ko-Lee 1997 – "band generators", even better?)

Motivation:
- computing with braids
- first step to solving pb. of recognizing when 2 links are isotopic (Markov's thm!)

Garside uses: ① the semigroup of positive braids:

- observe: the presentation of B_n doesn't involve σ_i^{-1}
  → can use the same relations to define a semigroup (or monoid)

Def: $B_n^+ =$ generators $\sigma_1, \dots, \sigma_{n-1}$, relations same as in B_n. Write $V \equiv W$ for equality in B_n^+

So: two words in $\sigma_1 \cdots \sigma_{n-1}$ define the same elt of B_n^+ iff can pass from one to the other by successive substitutions

$$\cdots \sigma_i \sigma_j \cdots \longleftrightarrow \cdots \sigma_j \sigma_i \cdots$$
$$\cdots \sigma_i \sigma_{i+1} \sigma_i \cdots \longleftrightarrow \cdots \sigma_{i+1} \sigma_i \sigma_{i+1} \cdots$$

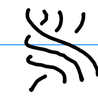
Then: Def: $D(W) := \{$ all words obtained from W by these operations $\}$
is finite because transformations preserve word length & only finitely many possibilities for each letter!

(→ easy theoretical sol^n to word problem in B_n^+: $V \equiv W$ in B_n^+ iff $D(V) \ni W$
can compute $D(V)$ by iteratively applying relations & checking if get new words…)

Thm: (Garside embedding): The natural map $i: B_n^+ \to B_n$ is injective.
ie: V, W positive braids $\Rightarrow$ $V = W$ iff $V \equiv W$
(so equality can be checked w/out involving inverses of generators.

② A particular element (the Garside element):

Def: $\Delta = (\sigma_1\sigma_2 \cdots \sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1 \in B_n^+$

[also: - the half-twist rotating everything by 180° 
- the longest permutation braid]

We'll find a normal form $\beta = \Delta^m P$, $m \in \mathbb{Z}$, $P \in B_n^+$ for braids $\beta \in B_n$

This normal form is more "robust" than Artin's (depends less on labelling of strings etc...)

Pf. Garside embedding thm:

- A thm of Ore says that embedding follows from the following properties:
  - (1) B_n^+ is left & right cancellable, i.e. $AX \equiv AY \Rightarrow X \equiv Y$, $XA \equiv YA \Rightarrow X \equiv Y$
  - (2) B_n^+ is right reversible, i.e. $X, Y \in B_n^+ \Rightarrow \exists U, V \in B_n^+$ s.t. $UX \equiv VY$.

I don't want to assume Ore's thm, so here's a simpler proof specific to B_n

- Assume $V, W \in B_n^+$ represent the same elt of B_n
  $\Rightarrow$ can pass from V to W via operations:
  - $\phi \longleftrightarrow \sigma_i \cdot \sigma_i^{-1}$, $\longleftrightarrow \sigma_i^{-1} \cdot \sigma_i$
  - $\sigma_i \cdot \sigma_{i+1} \cdot \sigma_i \longleftrightarrow \sigma_{i+1} \cdot \sigma_i \cdot \sigma_{i+1}$
  - $\sigma_i \cdot \sigma_j \longleftrightarrow \sigma_j \cdot \sigma_i$

  (that's a gal fact about presentation of group $G = \langle g_i \mid R \rangle$ as a semigroup $\langle g_i^{\pm 1} \mid g_i g_i^{-1} = 1, R \rangle$)

  Check easily: can indeed do all operations on words in $\sigma_i^{\pm 1}$ that you'd want

  e.g. $\sigma_i \cdot \sigma_j^{-1} \longleftrightarrow \sigma_j^{-1} \cdot \sigma_j \cdot \sigma_i \cdot \sigma_j^{-1} \longleftrightarrow \sigma_j^{-1} \cdot \sigma_i \cdot \sigma_j \cdot \sigma_j^{-1} \longleftrightarrow \sigma_j^{-1} \cdot \sigma_i$

  $\sigma_i^{-1} \cdot \sigma_j^{-1} \longleftrightarrow \sigma_i^{-1} \cdot \sigma_j^{-1} \cdot \underline{\sigma_i \cdot \sigma_i^{-1}} \longleftrightarrow \sigma_i^{-1} \cdot \sigma_j^{-1} \cdot \sigma_i \cdot \sigma_j \cdot \sigma_j^{-1} \cdot \sigma_i^{-1}$
  $\longleftrightarrow \sigma_i^{-1} \cdot \sigma_j^{-1} \cdot \sigma_j \cdot \sigma_i \cdot \sigma_j^{-1} \cdot \sigma_i^{-1}$
  $\longleftrightarrow \sigma_j^{-1} \cdot \sigma_i^{-1}$

- Observe: Δ^2, which we know to be central in B_n, is also central in B_n^+! Let $\Theta = (\sigma_1 \cdots \sigma_{n-1})^n \in B_n^+$
  (don't call it Δ^2 yet since I won't show $\Delta^2 \equiv \Theta$ yet, although it's true

(1) $\sigma_i \cdot \Theta \equiv \Theta \cdot \sigma_i \quad \forall i$

Use: $(*)$ if $1 \le i \le k-1$ then $(\sigma_1 \cdots \sigma_k)\sigma_i \equiv \sigma_{i+1}(\sigma_1 \cdots \sigma_k)$

Pf: ($\sigma_1 \cdots \sigma_k \sigma_i \equiv \sigma_1 \cdots \underline{\sigma_i \sigma_{i+1} \sigma_i} \sigma_{i+2} \cdots \sigma_k \equiv \sigma_1 \cdots \sigma_{i-1} \sigma_{i+1} \sigma_i \sigma_{i+1} \cdots \sigma_k$)

So: $\sigma_i \cdot (\sigma_1 \cdots \sigma_{n-1})^n \overset{(*)}{\equiv} (\sigma_1 \cdots \sigma_{n-1})^{i-1} \sigma_1 (\sigma_1 \cdots \sigma_{n-1}) \underset{(*)}{(\sigma_1 \cdots \sigma_{n-2})} \sigma_{n-1} (\sigma_1 \cdots \sigma_{n-1})^{n-i-1}$

$\equiv (\sigma_1 \cdots \sigma_{n-1})^{i-1} \sigma_1 (\sigma_2 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-1}) \sigma_{n-1} \underset{(*)}{(\sigma_1 \cdots \sigma_{n-1})^{n-i-1}}$

$\equiv (\sigma_1 \cdots \sigma_{n-1})^n \sigma_{n-1-(n-i-1)=i}$

(2) $\forall i \; \exists \, V_i \in B_n^+$ s.t. $\Theta \equiv \sigma_i \cdot V_i \equiv V_i \cdot \sigma_i$

In fact, $\Theta \equiv \sigma_i \cdots \sigma_{n-1} (\sigma_1 \cdots \sigma_{n-1})^{n-1} \sigma_1 \cdots \sigma_{i-1}$

Pf: $\Theta = (\sigma_1 \cdots \sigma_{n-1})^{i-1} \underset{(*)}{(\sigma_1 \cdots \sigma_{n-i})} \underset{(*)}{(\sigma_{n-i+1} \cdots \sigma_{n-1})} (\sigma_1 \cdots \sigma_{n-1})^{n-i}$

$\equiv$ what we want.

- Consider a seq. of transfs. from V to W through words in $\sigma_i^{\pm 1}$.

→ hence: let m = max. # of σ_i^{-1} appearing in the given sequence

modify each word by
- replacing each σ_i^{-1} by V_i
- adding $(\Theta)^{m-\nu}$ in front, ν = # of V_i inserted

then get a sequence $\Theta^m V \rightsquigarrow \Theta^m W$

where each move is $\equiv$: obvious if move was not involving inverses;

$A \cdot \sigma_i \cdot \sigma_i^{-1} \cdot B \longleftrightarrow A \cdot B$

$\wr$ becomes $\qquad \wr$ becomes

$\Theta^k \cdot \tilde{A} \cdot \sigma_i \cdot V_i \cdot \tilde{B} \equiv \Theta^k \cdot \tilde{A} \cdot \Theta \cdot \tilde{B} \equiv \Theta^{k+1} \cdot \tilde{A} \cdot \tilde{B}$

- So $V = W$ in $B_n \Rightarrow \Theta^m V \equiv \Theta^m W$ in B_n^+ for some m.

Just need <u>left-cancellation</u> $AX \equiv AY \Rightarrow X \equiv Y$.

Pf. of left-cancellation: enough to prove it when A = a single letter! (induction)

<u>Lemma</u>: $\sigma_i X \equiv \sigma_k Y \Rightarrow$
- if $i = k$ then $X \equiv Y$ (left cancellation)
- $|i-k| \geq 2$: $\exists Z$ s.t. $X \equiv \sigma_k Z$, $Y \equiv \sigma_i Z$
- $|i-k| = 1$: $\exists Z$ s.t. $X \equiv \sigma_k \sigma_i Z$, $Y \equiv \sigma_i \sigma_k Z$.

PF:

simult. induction on $\begin{cases}\text{word length}\\ \#\text{ operations}\end{cases}$ needed to pass from $\sigma_i X$ to $\sigma_k Y$.

- true if X, Y have word length 0 or 1.
- if pass $\sigma_i X \to \sigma_k Y$ in a single operation, this is obvious
- assume true whenever $\#\text{ops.} \le n-1$ & for all shorter words:

look at 1st operation

$$\underset{1\text{ op.}}{\sigma_i X \equiv \sigma_j W} \underset{(n-1)\text{ ops.}}{\equiv \sigma_k Y}$$

$-\ i=j:\ X \equiv W,$ by induction on chain len. $\left(\begin{array}{l} W \equiv \cdots Z \\ Y \equiv \cdots Z \end{array}\right.$ ✓

$-\ j=k:\ W \equiv Y,$ $\begin{array}{l} X \equiv \cdots Z \\ W \equiv \cdots Z \end{array}$ ✓

$\to$ can assume $j \notin \{i,k\}$.

now see why need all 3 cases of Lemma to prove 1st one

- if $i=k$: $-\ |j-i| \geq 2$: by ind. on chain length, $\exists Z, Z'$ $\begin{array}{l} X \equiv \sigma_j Z,\ W \equiv \sigma_i Z \\ W \equiv \sigma_i Z',\ Y \equiv \sigma_j Z' \end{array}$

$$\sigma_i Z \equiv \sigma_i Z' \underset{\text{induction on word length}}{\Rightarrow} Z \equiv Z', \text{ \& so } X \equiv Y.$$

$-$ similarly $|j-i|=1$ $X \equiv \sigma_j \sigma_i Z,\ W \equiv \sigma_i \sigma_j Z \equiv \sigma_i \sigma_j Z',\ Y \equiv \sigma_j \sigma_i Z'$, but $Z \equiv Z'$.

Worst case scenario $\Bigg[$ • if $|i-k| \geq 2$ and $|i-j| = |j-k| = 1$: $\exists Z, Z'$ $\left|\begin{array}{l} X \equiv \sigma_j \sigma_i Z,\ W \equiv \sigma_i \sigma_j Z \\ W \equiv \sigma_k \sigma_j Z',\ Y \equiv \sigma_j \sigma_k Z' \end{array}\right.$

(chain len. induction)

word len induction: $\sigma_i \sigma_j Z \equiv \sigma_k \sigma_j Z' \Rightarrow \exists V / \left.\begin{array}{l} \sigma_j Z \equiv \sigma_k V \\ \sigma_j Z' \equiv \sigma_i V \end{array}\right\}$

induction again $\Rightarrow$ $\exists U, U'$ s.t. $\begin{array}{l} Z \equiv \sigma_k \sigma_j U,\ V \equiv \sigma_j \sigma_k U \\ Z' \equiv \sigma_i \sigma_j U',\ V \equiv \sigma_j \sigma_i U' \end{array}$

again on $V \Rightarrow \sigma_k U \equiv \sigma_i U'$
$\Rightarrow U \equiv \sigma_i T,\ U' \equiv \sigma_k T$

then $X \equiv \sigma_j \sigma_i Z \equiv \sigma_j \sigma_i \sigma_k \sigma_j U \equiv \sigma_j \sigma_i \sigma_k \sigma_j \sigma_i T$
$\equiv \sigma_j \sigma_k \sigma_j \sigma_i \sigma_j T$
$\equiv \sigma_k \underbrace{\sigma_j \sigma_k \sigma_i \sigma_j T}$.

$Y \equiv \sigma_j \sigma_k Z' \equiv \sigma_j \sigma_k \sigma_i \sigma_j U' \equiv \sigma_j \sigma_k \sigma_i \sigma_j \sigma_k T$
$\equiv \sigma_j \sigma_i \sigma_j \sigma_k \sigma_j T$
$\equiv \sigma_i \underbrace{\sigma_j \sigma_k \sigma_i \sigma_j T}$ ✓

All cases work like this — use word len induction to eventually find the right prefix in X & Y. ▲

NB: this lemma actually says very specific things about cancellation process!