Aside: Q from last time:
Can we expand our Thue process Π_M (corr. to semigroup w/ undec word problem)
by adding inverse substitutions to get a process Π_M'' corr. to group w/ undec. word prob?

A: no.
The problem: inverse subs give too much flexibility — won't be able to prove $\# Q_0 1^{(n)} \# \Rightarrow_{\Pi_M''} \# Q' \#$ implies our t.m. M halts on $1^{(n)}$

Why: Sps e.g. M halts on the empty string. Then we have $\# Q_0 \# \Rightarrow \# Q' \#$ for orig. process Π_M, hence also for Π_M' and Π_M''.

Now consider arbitrary input string $1^{(n)}$
We claim $\# Q_0 1^{(n)} \# \Rightarrow_{\Pi_M''} \# Q' \#$ for every n
Indeed: $\# Q_0 1^{(n)} \# \Rightarrow \# Q_0 \# \#^{-1} 1^{(n)} \# \Rightarrow$
$\# Q_N \# \#^{-1} 1^{(n)} \# \Rightarrow \# Q_N 1^{(n)} \# \Rightarrow \# Q' \#$ by above

Follows: $\exists$ tm M w/ undecidable halting prob that does not reduce to "word prob. for Π_M''"

20

E.g. if $\mathbb{Z} \cong \langle a \mid \emptyset \rangle$ $\quad \mathbb{Z} \cong \langle b \mid \emptyset \rangle$

$$\mathbb{Z} * \mathbb{Z} = \mathbb{F}_2 = \langle a, b \mid \emptyset \rangle$$

- Recall: a map $\varphi : \Gamma \to \Gamma'$ between groups is a homomorphism if $\varphi(gh) = \varphi(g)\varphi(h)$ $\forall g, h \in \Gamma$
- It is an isomorphism if it is also a bijection
- if $\Gamma = \Gamma'$ an isomorphism is an automorphism

- Given a fixed $h \in \Gamma$, the map $\varphi_h : \Gamma \to \Gamma$ defined by $\varphi_h(g) = h^{-1} g h$ ← "conjugate of g by h" is an automorphism of Γ, called an inner automorphism

(in general, not all automorphisms of group Γ are inner)

- A question of interest: if H, K are isomorphic subgroups of Γ and $\varphi : H \to K$ is an isomorphism, when is there a global automorphism $\hat{\varphi} : \Gamma \to \Gamma$ s.t. $\hat{\varphi} \restriction H \cong \varphi$?

- Answer: not always

- However: can construct a larger group Γ_φ containing Γ that does have an automorphism extending φ (in fact: an inner one).

Def'n Sps $\Gamma = \langle a_1, \dots, a_n \mid R_1, \dots, R_k \rangle$ is a (fin. presented) group and sps $\varphi: H \to K$ is an isomorphism between subgroups H, K of Γ.

Let t be a new letter.

The HNN extension of Γ wrt φ is the group:

$$\Gamma_\varphi = \langle a_1, \dots, a_n, t \mid R_1, \dots, R_k, (t^{-1} h t = \varphi(h)) \rangle$$

for every $h \in H$

- Actually: suffices to include $t^{-1} h t = \varphi(h)$ for h in some generating set for H (so if H finitely generated, Γ_φ is finitely presented)

- t called the "stable letter" of the extension

- We'll need two facts whose proofs we defer for now.

<u>Fact 1</u>: Let Γ' denote subgroup of Γ generated by $a_1, \dots, a_n$.

For $g \in \Gamma$, viewed as word on letters $a_1, \dots, a_n$, let g' denote corresponding word in Γ' (i.e. we compute g' in Γ_φ)

Then the map $i : \Gamma \to \Gamma'$ defined by $i(g) = g'$ is an isomorphism.

↳ In practice, we identify Γ' w/ Γ and write $\Gamma \subseteq \Gamma_\varphi$.

Next fact more technical — will use to realize HNN extensions by multiple φ at once.

<u>Def'n</u> A subgroup $L \subseteq \Gamma$ is <u>balanced</u> <u>wrt φ</u> if $\varphi(L \cap H) = L \cap K \; (= L \cap \varphi(H))$

<u>Fact 2</u> If $L \subseteq \Gamma$ is a subgroup that is balanced wrt φ, then the subgroup $L' \subseteq \Gamma_\varphi$ generated by L and t is the HNN extension $L_{\varphi|_{L \cap H}}$ of L wrt $\varphi|_{L \cap H}$, and $L' \cap \Gamma = L$.

↳ defer proofs for now.

Modular machines:

↳ new model of computation; more convenient than t.m.'s for proof of undecidability of word prob. for groups.

Def'n A modular machine $\mathcal{M}$ consists of ① a natural number $M > 1$

② for every pair of nat. numbers $a, b < M$, an instruction (a, b, c, D) where $c < M^2$ and $D \in \{L, R\}$

- A configuration of $\mathcal{M}$ is a pair $(\alpha, \beta) \in \mathbb{N}^2$.
- write $(\alpha, \beta) \to_{\mathcal{M}} (\alpha', \beta')$ if $\alpha = uM + a$, $\beta = vM + b$ and either

① (a, b, c, R) is an instruction in $\mathcal{M}$ and $\alpha' = uM^2 + c$ and $\beta' = v$; or

② $(a, b, c, L) \in \mathcal{M}$ and $\alpha' = u$ and $\beta' = vM^2 + c$

How to think about it:
- given config (α, β) write each in base M expansion:

$$\alpha = \alpha_0 + \alpha_1 M + \dots + \alpha_k M^k \qquad (\alpha_i, \beta_j < M)$$
$$\beta = \beta_0 + \beta_1 M + \dots + \beta_\ell M^\ell$$

- identify α w/ tuple $(\alpha_0, \alpha_1, \dots, \alpha_k)$
  β w/ $(\beta_0, \dots, \beta_\ell)$

- if ① and $c = c_0 + c_1 M$ then (α', β') corresponds to sequences

$$\alpha' \text{ "=" } (c_0, c_1, \alpha_1, \alpha_2, \ldots, \alpha_k)$$
$$\beta' \text{ "=" } (\beta_1, \beta_2, \ldots, \beta_e)$$

- if ②:

$$\alpha' \text{ "=" } (\alpha_1, \ldots, \alpha_k)$$
$$\beta' \text{ "=" } (c_0, c_1, \beta_1, \ldots, \beta_e)$$

We write $(\alpha, \beta) \to_{\mu}^{*} (\alpha', \beta')$ if there is a sequence of instructions s.t.

$$(\alpha, \beta) \to_{\mu} (\alpha^{1}, \beta^{1}) \to_{\mu} \cdots \to_{\mu} (\alpha^{n}, \beta^{n}) \to (\alpha', \beta')$$

<u>Theorem</u> There exists a modular machine μ s.t. the halting set

$$H(\mu) := \{(\alpha, \beta) \in \mathbb{N}^2 : (\alpha, \beta) \to_{\mu}^{*} (0, 0)\}$$

is not recursive.

<u>Pf</u>: - Let T be t.m w/ non-rec halting set; will assume whenever T halts, tape is empty (such T exist)

- We use $0, 1, \ldots, N-1$ to represent states $Q_0, \ldots, Q_{N-1}$ of T
  - ↳ we assume now Q_0 is halting state (so that 0 represents halting state)
- use $N, N+1, \ldots, M-1$ to rep symbols in T's alphabet (i.e. symbols on tape)

(25)

- given config of T:

$$a_k a_{k-1} \cdots a_1 Q a b_1 \cdots b_\ell \qquad (*)$$

(r/w head on a in state Q, tape empty beyond a_k and b_ℓ)

associate two configs of our mod. machine $\mathcal{M}$:

(i) $\alpha_1 = (Q, a_1, a_2, \ldots, a_k)$ $\beta_1 = (a, b_1, \ldots, b_\ell)$

(ii) $\alpha_2 = (a, a_1, \ldots, a_k)$ $\beta_2 = (Q, b_1, \ldots, b_\ell)$

- observe: T is halted (i.e. tape empty, state Q_0) iff $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 0$ (so $(0,0)$ is only m.m. config corresponding to halted state of T)

- to every instruction $(Q, a, b, \overset{L \text{ or } R}{D}, Q')$ of T we add two instructions $(Q, a, Q' + bM, D)$ and $(a, Q, Q' + bM, D)$ to $\mathcal{M}$.

- Observe if T in config $(*)$ above corresponding to $\mathcal{M}$-configs (i) and (ii) then if (Q, a, b, R, Q') is applicable T instruction, next config is:

$$a_k \cdots a_1 b Q' b_1, \ldots, b_\ell \qquad (*)'$$

- if we apply corr. rule $(Q, a, Q' + bM, R)$ to (i) we get

$$\alpha_1' = (Q', b, a_1, \ldots, a_k) \quad \beta_1' = (b_1, \ldots, b_\ell)$$

which corresponds to $(*)'$ in first way

- OTOH if we apply alt. rule $(a, q, q' + b\uparrow, R)$ to (ii) get
  $\alpha_2' = (q', b, a_1, \ldots, a_k)$ $\beta_2' = (b_1, \ldots, b_e)$
  $= \alpha_1'$ $= \beta_1'$
  same as before
  ($\hookrightarrow$ so both output $\mathcal{M}$-configs of first type when we move R)

- instead if (q, a, b, L, q') is app'cble instruct. of T, it goes to
  $a_k \ldots a_2 q' a_1 b b_1 \ldots b_e$ $(*)''$

- can check if we apply either corr'ing $\mathcal{M}$-instruction to (i), (ii) resp. we get config
  $(a_1, \ldots, a_k)$ $(q', b, b_1, \ldots, b_e)$
  which corresponds to $(*)''$ in second way

- Follows (w/ some more thought):
  can check if $\mathcal{M}$ halts on input word w by checking if (either one) of corresponding $\mathcal{M}$-configs (α_1, β_1) or (α_2, β_2) $\xrightarrow{*}_{\mathcal{M}} (0, 0)$
  $\Rightarrow$ halting set of $\mathcal{M}$ non-recursive ✓

- We'll use the m.m. M above to construct a group w/ unsolvable word prob.
- We begin w/ group
$$G = \langle t, x, y \mid xy = yx \rangle = \mathbb{Z} * \mathbb{Z}^2$$
and take finitely many HNN extensions s.t. word problem for M reduces to word prob. for resulting group.

- For every pair $\alpha, \beta \in \mathbb{Z}$ (not $\mathbb{N}$!) define group el't:
$$t(\alpha, \beta) := x^{-\alpha} y^{-\alpha} t x^{\alpha} y^{\alpha}$$

- Let $T = \langle t(\alpha, \beta) : \alpha, \beta \in \mathbb{Z} \rangle$ be subgroup of G generated by the $t(\alpha,\beta)$'s

<u>Claim</u> T is <u>freely</u> generated by the $t(\alpha,\beta)$'s for $\alpha, \beta \in \mathbb{Z}$ (i.e. T is a free group w/ these el'ts as generators)

<u>Pf</u>: - Let $A = \{t(\alpha,\beta) : \alpha, \beta \in \mathbb{Z}\}$
- Since x, y commute (but not w/ t) inverse of $t(\alpha,\beta)$ is $x^{\alpha} y^{\beta} t^{-1} x^{-\alpha} y^{-\beta}$
- Denote collection of all such by A^{-1} (so we get A^{-1} by replacing t's in $t(\alpha,\beta)$'s w/ t^{-1}'s)