- can loosen our def'n of "definable in"
  Now say: $\mathcal{A}$ is definable in $\mathcal{B}$ iff $\mathcal{A} \cong \mathcal{A}'$ for some $\mathcal{A}'$ definable in $\mathcal{B}$ in previous strict sense.
  (isomorphic to)

- still have: if $\mathcal{A}$ definable in $\mathcal{B}$ then $\mathcal{A}$ strong undec $\Rightarrow$ $\mathcal{B}$ too

<u>Theorem</u> There exists a strongly undecidable group $(G, \cdot, e)$. Therefore theory of groups is undecidable.

<u>Pf.</u> - let G be group $S_{\mathbb{Z}}$ of all permutations of set $\mathbb{Z} = \{\ldots -1, 0, 1, 2, \ldots\}$ w/ composition $\circ$ as group operation
- will show $\mathcal{Z} = \langle \mathbb{Z}, +, *, 0, 1 \rangle$ definable in G w/ params
- Consider $\sigma : \mathbb{Z} \to \mathbb{Z}$ defined by
$$\sigma(k) = k+1$$
then $\sigma \in S_{\mathbb{Z}}$

- let $Z = \{\sigma^i : i \in \mathbb{Z}\}$ Observe: $\sigma^i(k) = k+i$
  will be domain of our def'n of $\mathbb{Z}$ in G.

- Claim: $Z = \{\tau \in G \mid \tau\sigma = \sigma\tau\}$
  (so Z definable by fmla w/ parameter σ
  "$x\sigma = \sigma x$")

<u>Why</u>. ($\subseteq$) every el't of Z commutes w/ σ of course: $\sigma^i \sigma = \sigma\sigma^i = \sigma^{i+1}$

($\supseteq$) Sps $\tau\sigma = \sigma\tau$

$\Rightarrow \tau\sigma^i = \sigma^i\tau$ for any $i \in \mathbb{Z}$

- evaluating both sides of eq'n @ $k=0$ gives $\tau(i) = \tau(0)+i$
- since holds $\forall i$, follows $\tau = \sigma^j$ where $j = \tau(0)$ ✓

Remains to show $+, *, 0, 1$ definable in G.

~~[illegible]~~

- 0 ($=\sigma^0 = e$ in Z) and 1 ($=\sigma^1 = \sigma$ in Z) definable w/ params e and σ resp. by fmlas $x = e$ and $x = \sigma$
- $+$ is definable by ~~[illegible]~~ $\cdot$ since this is corr. operation on Z

- so need only show $*$ is definable
- we prove divisibility $|$ is definable first:

<u>Claim</u> $i | j$ iff $\sigma^i \neq e$ and for every $\tau \in G$ we have:

$$\sigma^i\tau = \tau\sigma^i \Rightarrow \sigma^j\tau = \tau\sigma^j$$

... or $j = 0$

$\leftarrow$ view as relation on $Z = \{\sigma^i\}$

(thus "$i | j$" definable in G by:
"$x, y \in \mathbb{Z}$" $\wedge$ $(\forall z (xz = zx \Rightarrow$
$yz = zy)$
$\vee\ y = 0))$

Pf: $(\Rightarrow)$ Sps $i | j$ for some $i, j \in \mathbb{Z}$, $j \neq 0$. Then $i \neq 0$ so $\sigma^i \neq e$.
For any $\tau \in G$ we have: if τ commutes w/ σ^i then commutes w/ $\sigma^j = \sigma^i \sigma^i \cdots \sigma^i$ etc.

$(\Leftarrow)$ Sps $\sigma^i \neq e$ (i.e. $i \neq 0$) and every τ that commutes w/ σ^i commutes w/ σ^j etc.

– Consider $\tau \in G$ defined by
$\tau(k) = k + i$ if $i | k$
$= k$ o.w. (is a permutation!)

– then τ commutes w/ σ^i by construction (why?)

– Hence τ commutes w/ σ^j by hypothesis

i.e. we have
$\tau(k) + j = \tau(k+j)$ for all $k \in \mathbb{Z}$

If $i \neq j$ then plugging in i above we get $\tau(i) + j = \tau(i+j)$ i.e. $2i + j = i + j \Rightarrow i = 0$, contradiction ✓

Show next time: divisibility allows us to define multiplication $*$.

Given $|$ definable, how to define $*$? Sufficient to show function $y(k) = k^2$ definable.

Why: Since $(i+j)^2 = i^2 + 2ij + j^2$ can define $w = b$ by
"compute $i+j$, i^2, j^2, $(i+j)^2$
find a $(= (i+j)^2 - i^2 - j^2)$ $(= 2ij)$
s.t. $a + i^2 + j^2 = (i+j)^2$
find b s.t. $b + b = a$"

So how to define $y = k^2$?

- For integers a, b let $\mathrm{lcm}(a,b) = c$ if c is either positive or negative lcm of a, b

- $\mathrm{lcm}(a,b) = c$ definable using division:
  "c is divisible by a and also b and if c' is too, then c' divisible by c"

- Now observe: since $k, k+1$ coprime
  $\mathrm{lcm}(k, k+1) = k(k+1)$ or $-k(k+1)$
  $= k^2+k$ or $-k^2-k$

  likewise
  $\mathrm{lcm}(k, k-1) = k^2-k$ or $-k^2+k$

  thus $y = k^2$ iff ~~$y = \ldots$~~
  $y = 0 \wedge k = 0$
  or $y = 1 \wedge (k = 1$ or $-1)$
  or $y \neq 0, 1 \wedge y$ is unique integer that is both an $\mathrm{lcm}(k, k+1) - k$ and an $\mathrm{lcm}(k, k-1) + k$

in our lang $\longrightarrow$
0 is $e = \sigma^0$
1 is σ
-1 is inverse of σ

putting all together: $*$ is definable in G, so $\langle \mathbb{Z}, 0, 1, +, * \rangle$ definable so G strongly undecidable. ✓

Corollary the theory of groups:

$\forall x, y, z$

$$(xy)z = x(yz)$$
$$xe = ex = x$$
$$\exists x' (xx' = x'x = e)$$

... is undecidable!

On the other hand, it turns out:

Fact: theory of abelian groups is decidable

i.e. there is an algorithm which, given a fmla written in lang of groups, determines if it holds or not in all abelian groups.

→ partic we used commutativity of certain elements to define the ring $\langle \mathbb{Z}, 0, 1, +, * \rangle$ in our strongly undecidable group.

Next: WTS there is a strongly undecidable graph $G = \langle V, E \rangle$

<u>Def'n</u> a <u>graph</u> is a structure $\mathcal{G} = (G, E)$ where E is a symmetric, irreflexive binary relation on G.

<u>Claim 1</u> There is a strongly undecidable structure $\mathcal{A} = \langle A, S \rangle$ where $S \subseteq A^4$ is a <u>quaternary</u> relation on A.

<u>Pf</u>. Let $A = \mathbb{Z}$ and let

$$S = \{(0, k, l, k+l) : k, l \in \mathbb{Z}\}$$
$$\cup \{(1, k, l, kl) : k, l \in \mathbb{Z}\}$$

Easy to define $\langle \mathbb{Z}, 0, 1, +, * \rangle$ in this structure. ✓
(Exercise)

<u>Claim 2</u>. There is a strongly undecidable structure $\mathcal{B} = (B, T)$ where T is a <u>binary</u> relation on B

<u>Pf</u>: Let $B = A \cup A^2 \cup \{\infty\}$ ← formal symbol
$= \mathbb{Z} \cup \mathbb{Z}^2 \cup \{\infty\}$

Define T to be:

$\{((a,b),(c,d)) : (a,b,c,d) \in S\}$
$\cup \{(a,(a,b)) : a,b \in A\}$
$\cup \{((a,b),b) : a,b \in A\}$
$\cup \{(\infty,a) : a \in A\}$
$\cup \{((a,b),\infty) : a,b \in A\}$

We show A definable in $\mathcal{B}$
Clearly A definable by $T(\infty,x)$

S definable by:

$S(x,y,z,w)$ iff
"$x,y,z,w \in A$"
$\wedge \exists p,q\, [T(p,\infty) \wedge T(q,\infty) \wedge T(x,p) \wedge T(p,y) \wedge T(z,q) \wedge T(q,w) \wedge T(p,q)]$

<u>Theorem</u> There is a strongly undecidable graph $\mathcal{G} = (G,E)$

<u>Pf</u>: Let $\mathcal{B} = (B,T)$ be our strongly undecidable structure above.

For every $b \in B$ introduce three distinct vertices b_1, b_2, b_3

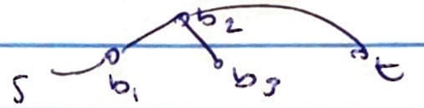
Let $G = \{b_1, b_2, b_3 \mid b \in B\} \cup \{s, t\}$

Let E be all pairs

$(b_1, b_2), (b_2, b_1)$, $(b_2, b_3), (b_3, b_2)$

and also $(s, b_1), (b_1, s)$

and also $(t, b_2), (b_2, t)$



and also $(b_1, b_3'), (b_3', b_1)$ wherever $(b, b') \in T$

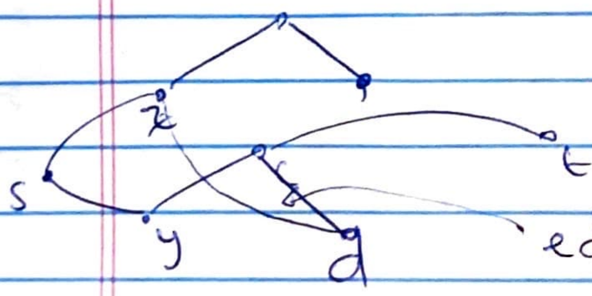
Easy to define B (take as our universe the set of b_1's):

$$E(s, x)$$

How to define T? Use parameters s, t

$T(x,y)$ iff "$x, y \in B$"

$$E(x,s) \wedge E(y,s) \wedge \exists c,d\,[E(c,t) \wedge \neg E(d,t) \wedge E(c,d) \wedge E(y,c) \wedge E(x,d) \wedge d \neq y \wedge d \neq t]$$



117C: topics

More undecidability!
- word problem for groups
- undecidable tilings of $\mathbb{R}^2$
- etc.

Decidable theories
- Elimination of quantifiers (technique to show decidability)
- Dense linear orderings
- Tarski: theory of real closed fields is decidable
- when valid formulas are decidable/undecidable

P vs. NP
- NP and P problems
- complexity theory

Some Descriptive Set theory??