

RECAP

Absolutely free algebra over  $X$

$\underline{F}(X) = (\text{terms over } X; \text{ natural operations})$

Free algebra for  $\mathcal{K}$  over  $X$

$$\underline{F}_{\mathcal{K}}(X) = \underline{F}(X) / \Delta_{\mathcal{K}}$$

$$\Delta_{\mathcal{K}} = \bigwedge \{ \alpha \in \text{Con } \underline{F}(X); \underline{F}(X) / \alpha \in S(\mathcal{K}) \}$$

$\rightarrow \underline{F}_{\mathcal{K}}(X) \in SP(\mathcal{K})$

ⓐ (i)  $s \Delta_{\mathcal{K}} t$

(ii)  $\mathcal{K} \models s \approx t$

(iii)  $HSP(\mathcal{K}) \models s \approx t$

(iv)  $\underline{F}_{\mathcal{K}}(X) \models s \approx t$

useful ⓑ

$\forall m: X \rightarrow A \exists! \underline{F}(X) \rightarrow \underline{A}$  extending  $m$ ,  
namely  $\hat{m}$

EXAMPLE

write  $xx, xy \cdot z \approx zy \cdot x$

$$\mathcal{K} = \{ (A, \cdot); (A, \cdot) \models \{x \cdot x, (x \cdot y) \cdot z \approx (z \cdot y) \cdot x\} \}$$

What is  $\underline{F} := \underline{F}_x(x, y)$ ?

$y \cdot xy \approx x$

playing with identities  $\rightsquigarrow$  each term is equivalent (modulo  $\lambda_x$ ) to one of  $\{x, y, xy, yx\}$  (use (ii))

candidate  $\underline{B} := \{ \cancel{x}, \cancel{y}, \cancel{xy}, \cancel{yx}; * \}$

*	x	y	xy	yx
x	x	xy	yx	y
y	yx	y	x	xy
xy	y	yx	xy	x
yx	xy	x	y	yx

4 distinct

Is  $\underline{B} \cong \underline{F}$ ? Not clear, e.g. why  $xy \not\sim x$  ( $\mathcal{K} \not\models xy \sim x$ )

Enough to show  $\underline{B}$  satisfies  $uu \approx u, uv \cdot w \approx wv \cdot u$  (for all  $u, v, w \in B$ !)

*	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

*	00	11	01	10
00	00	01	10	11
11	10	11	00	01
01	11	10	01	00
10	01	00	11	10

$$(u_1, u_2) * (v_1, v_2) = (u_2 + v_1 + v_2, u_1 + u_2 + v_1)$$

$\underline{B} \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, *)$   $\vec{u} * \vec{v} = A\vec{u} + A^2\vec{v}$   
verification now easy

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad A^2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

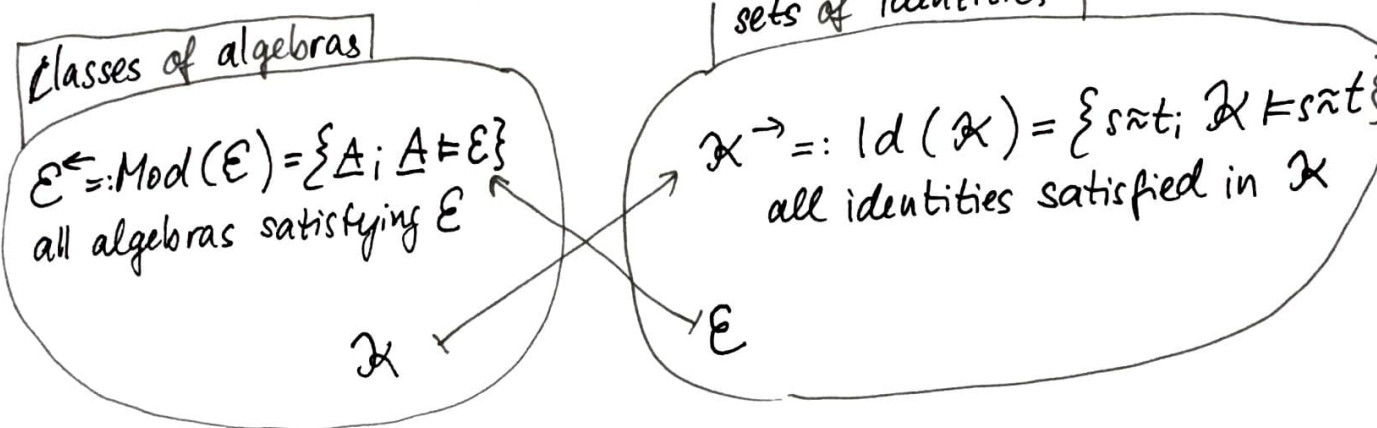
**Mod-Ideals: #1 Galois correspondence in UA**

$\Sigma$  - still fixed

Alg := all algebras in signature  $\Sigma$

Ident := all identities in  $\Sigma$  over  $X = \{x_1, x_2, \dots\}$

relation  $\Phi \subseteq \text{Alg} \times \text{Ident}$      $\underline{A} \Phi s \approx t$  iff  $\underline{A} \models s \approx t$



↓  
antiisomorphisms

(closed classes of algebras,  $\subseteq$ )  $\leftrightarrow$  (closed classes of identities,  $\subseteq$ )  
 $= \{\text{Mod}(E); E \subseteq \text{Ident}\}$      $= \{\text{Id}(A); A \subseteq \text{Alg}\}$

!!! closed classes of algebras = varieties  
 !!! closed classes of identities = equational theories

"variety = class of algebras defined by identities"  
 $\Leftarrow$  we know  
 $\Rightarrow$  we now prove

**THEOREM (Birkhoff '35)** For every class of algebras  $\mathcal{K}$   
 $HSP(\mathcal{K}) = Mod(I\delta(\mathcal{K}))$

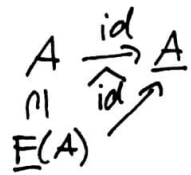
Proof:  $\subseteq \checkmark$

$\supseteq$  • take  $\underline{A} \in Mod(I\delta(\mathcal{K}))$

$\underline{A}$  satisfies all the identities satisfied in  $\mathcal{K}$

• define  $\beta = \ker \hat{id} \in Con(\underline{F(A)})$

(ie  $s \beta t$  iff  $\hat{id}(s) = \hat{id}(t)$ )



• note  $\underline{F(A)}/\beta \cong \underline{A}$  (1st iso. t.)

!  $\lambda_{\mathcal{K}} \leq \beta$ :  $s \lambda_{\mathcal{K}} t \xRightarrow{thm.} \mathcal{K} \models s \approx t$

$\implies \underline{A} \models s \approx t \xRightarrow{def. of \beta} s \beta t$

PROP.  $\implies \underline{F_{\mathcal{K}}(A)} \in SP(\mathcal{K})$

$\underline{A} \cong \underline{F(A)}/\beta \xrightarrow{2nd iso} \underline{F(A)}/\lambda_{\mathcal{K}}$

$\underline{F(A)}/\lambda_{\mathcal{K}}$

$\in HSP(\mathcal{K})$

• so we have anti isomorphism (varieties,  $\subseteq$ )  $\leftrightarrow$  (closed cl. of id,  $\subseteq$ )

• sometimes easy to show  $\mathcal{K}$  is a variety, hard to find  $\mathcal{E}$  such that  $\mathcal{K} = Mod(\mathcal{E})$

Ex.  $\mathcal{V}, \mathcal{W}$  varieties of groups

$\mathcal{V} \circ \mathcal{W} := \{ \underline{G}; \exists \underline{N} \trianglelefteq \underline{G} \ \underline{N} \in \mathcal{V}, \underline{G}/\underline{N} \in \mathcal{W} \}$  is a variety

$\mathcal{V} = \mathcal{W} =$  abelian groups  $\mathcal{V} \circ \mathcal{W} =$  2-step solvable

FINITE BASE

variety  $\mathcal{A}$  is finitely based if  $\mathcal{A} = \text{Mod}(\mathcal{E})$   
for some finite  $\mathcal{E}$

say  $\mathcal{A} = \text{HSP}(\underline{A})$ ,  $\underline{A}$  finite with finite  $\Sigma$

- not necessarily finitely based
- no algorithm to check whether ~~there is~~ it is  
(McKenzie '96)

Examples

- finitely based : finite groups (Oates, Powell '64)

$$\text{HSP}(\underline{D}_8) = \text{HSP}(\underline{Q}_8) = \text{Mod}(x^4 \approx 1, x^2 y \approx x y^2, \text{group axioms})$$

↑
↑

dihedral
quaternion

- non-finitely based
  - a 7-element algebra with a binary op. (Lyndon '54)
  - a 3-element ——— " ——— (Murski '65)

	0	1	2
0	0	0	0
1	0	0	1
2	0	2	2

THE OTHER SIDE

$E$  ... set of identities

closure of  $E = \text{Id}(\text{Mod } E)$  ... all identities that ~~syntactically follow~~ semantically follow from  $E$

Def.  $E \models s \approx t$  if  $\forall A \underline{A} \models E \Rightarrow \underline{A} \models s \approx t$

$s \approx t$  semantically follows from  $E$

... would be nice if ...

closure of  $E =$  all identities that syntactically follow from  $E$

? Def.  $E \vdash s \approx t$  if  $s \approx t$  can be obtained from  $E$  by "such and such" syntactic manipulations

we wish  $E \models s \approx t$  iff  $E \vdash s \approx t$

? Thm  $E \models s \approx t$  iff  $E \vdash s \approx t$

Todos

- what is "such and such" ?
- prove  $\Rightarrow$  in Thm

Example

E = { group axioms, x^2 ≈ 1 } ⊢ xy ≈ yx

says every group satisfying x^2 ≈ 1 is commutative  
it can be shown by syntactic manipulations:

xy ≈ xyxx ≈ xyxyx ≈ yx

closer look

xy ≈ xy · 1 ≈ xy · xx ≈ ...  
z ≈ z · 1                      1 ≈ xx  
applied to z=xy                      xy ≈ xy  
substitution                                      ↓  
xy · 1 ≈ xy · xx  
applying operations  
to identities

we have used

- ≈ is an equivalence on F(x)
  - invariant under applying operations
  - invariant under substitutions
- ⊆ ⇒ ≈ is a congruence of F(x)
- ① substitution = endomorphism of F(x)
  - ② invariant under substitutions  
= fully invariant: s ≈ t ⇒ e(s) ≈ e(t) ∀ e ∈ End(F(x))

UA

9.8

we have observed:  $\approx$  is a fully invariant congruence of  $\underline{F}(X)$  ( $\approx = \text{Id}(X)$ )

Is it enough? YES!

Def. equational theory = fully invariant congruence of  $\underline{F}(X)$

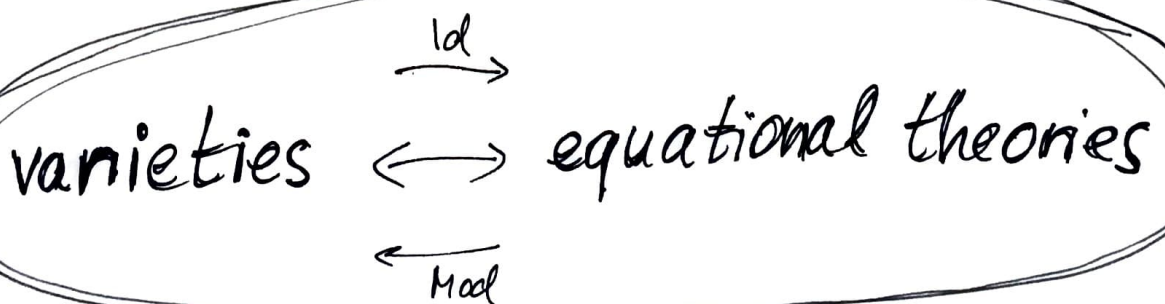
$\mathcal{E} \vdash s \approx t$  if  $(s, t)$  is in the equational theory generated by  $\mathcal{E}$

(can be described in a more concrete way...)

Theorem  $\mathcal{E} \models s \approx t$  iff  $\mathcal{E} \vdash s \approx t$

( $\Rightarrow \text{Id}(\text{Mod}(\mathcal{E})) = \text{equational theory generated by } \mathcal{E}$ )

so we have anti isomorphisms (mutually inverse)



Proof: nice exercise (not required for exam)