A Rough Introduction to Universal Algebra and Model Theory

by

Aahana Jain

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Contents

CHAPTER 1

Introduction

This is an informal summary of what I studied with the FB1 algebra group at TU Wien from May to July 2024. In an attempt to not be too wordy, the Universal Algebra section only highlights key information and some interesting facts. At least at a beginner's level, I find it fascinating how it has generalised theorems of classical algebra (such as Galois Correspondences or Abelian Algebras), and my main incentive to study this topic was to understand how generalisation works.

I started by studying Universal Algebra from [Bar] and Chapter 8 of [Bodb]. I then moved on to Chapter 11 and 12 of the same as I was interested in Maltsev operations.

After this, I switched to [Boda] to look at something more group theoretic. [Cam] was integral for understanding Oligomorphic Permutation Groups, especially to gain a more group theoretic understanding of the topic than a model theoretic one. I was unfortunately unable to complete studying Automorphism, but I did reach a question that I found to be quite interesting:

What classes of finite groups are Fraïssé classes?

The property with which difficulty usually arises is the amalgamation property, which is why I was interested in the amalgams of p-groups and what classes of groups satisfy the amalgamation property.

CHAPTER 2

Universal Algebra

2.1 Preliminaries

Semigroup: A semigroup is a set S together with a binary operation $\cdot$ (that is, a function $\cdot : S \times S \to S$) that satisfies the associative property: *For all $a, b, c \in S$, the equation $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds.*

Semilattice: A semilattice is an algebra $S = (S, *)$ satisfying, for all $x, y, z \in S$,

1. $x * x = x$,
2. $x * y = y * x$,
3. $x * (y * z) = (x * y) * z$.

Lattice: A partially ordered set (poset) $(L, \leq)$ is called a **lattice** if it is both a join- and a meet-semilattice, i.e.

1. Each two-element subset $\{a, b\} \subseteq L$ has a *join* (i.e. least upper bound, denoted by $a \vee b$) and dually
2. A *meet* (i.e. greatest lower bound, denoted by $a \wedge b$). This definition makes $\wedge$ and $\vee$ binary operations.

Both operations are monotone with respect to the given order: $a_1 \leq a_2$ and $b_1 \leq b_2$ implies that $a_1 \vee b_1 \leq a_2 \vee b_2$ and $a_1 \wedge b_1 \leq a_2 \wedge b_2$.

B is a **sublattice** of A if $B \subseteq A$ and B is closed under the operations $\vee, \wedge$.

Theorem: In a semilattice S, define $x \leq y$ if and only if $x * y = x$. Then $(S, \leq)$ is an ordered set in which every pair of elements has a greatest lower bound. Conversely, given an ordered set P with that property, define $x * y = \inf(x, y)$. Then $(P, *)$ is a semilattice.

Proof. Let $(S, *)$ be a semilattice, and define $\leq$ as above. First, we check that $\leq$ is a partial order.

1. $x * x = x$ implies $x \leq x$.
2. If $x \leq y$ and $y \leq x$, then $x = x * y = y * x = y$.
3. If $x \leq y \leq z$, then $x * z = (x * y) * z = x * (y * z) = x * y = x$, so $x \leq z$.

Since $(x * y) * x = x * (x * y) = (x * x) * y = x * y$ we have $x * y \leq x$; similarly $x * y \leq y$. Thus $x * y$ is a lower bound for $\{x, y\}$. To see that it is the greatest lower bound, suppose $z \leq x$ and $z \leq y$. Then $z * (x * y) = (z * x) * y = z * y = z$, so $z \leq x * y$, as desired.

Conversely, let $x * y = \inf(x, y)$. Then,

1. $x * x = \inf(x, x) = \text{x}$
2. $x * y = \inf(x, y) = \inf(\text{y, x}) = y * x$
3. $x * (y * z) = \inf(x,\ \inf(y, x)) = \inf(x, y, z) = \inf((\inf(x, y)), z) = (x * y) * z$

Boolean Algebra: A boolean algebra is an algebra $\langle A, \wedge, \vee, -, \rangle$ such that $\langle A, \wedge, \vee, \rangle$ is a lattice and $\forall a, b \in A$, the following equalities hold:

1. Distributive
2. $(a \vee b)^- = a^- \wedge b^-$
3. $(a \wedge b)^- = a^- \vee b^-$
4. $a^{--} = a$
5. $(a^- \wedge a) \vee b = b$
6. $(a^- \vee a) \wedge b = b$

Thus, a boolean algebra is a distributive lattice with a unary operation of complementation adjoined.

Examples of Lattices:

1. Chains, i.e. Linear orders.

2. Power set of X := $(P(X), \subseteq)$

3. Groups: (Con(G), $\subseteq$) $\cong$ (NormalSub$(G), \subseteq$))

Dual Lattice to $(L, \vee, \wedge)$ is $(L, \wedge, \vee)$. $x \leq y$ in L iff $x \geq y$ in L^{dual}.

Definition: A poset $(X, \subseteq)$ is a *complete lattice* if all its subsets have both a join and a meet, i.e. if $\forall\ A \subseteq X$, $supA = \vee A$ and $inf A = \wedge A$ exist.

Defintion: Let S be a set. A *closure operator* on S is a function $\mathrm{C} : \mathcal{P}(S) \to \mathcal{P}(S)$ such that for all $A, B \subseteq S$,

- $A \subseteq \mathrm{C}(A)$,
- $A \subseteq B \Rightarrow \mathrm{C}(A) \subseteq \mathrm{C}(B)$,
- $\mathrm{C}(\mathrm{C}(A)) = \mathrm{C}(A)$.

Definition: A is closed if $\mathrm{C}(A) = A$.

Examples:

1. Topological space - standard

2. Groups: Closure of a subgroup generated by subset A (= Sg(A)) = normal subgroup generated by A.

3. X = Z x Z; C(A) =

Proposition: $C : \mathcal{P}(X) \to \mathcal{P}(X)$ is a closure operator. Then:

1. $C(A)$ is closed ($\forall A \subseteq X$), i.e. it is the smallest (w.r.t $\subseteq$) closed set of X containing A.

2. Intersection of closed sets is closed.

3. Closure operator $\to$ complete lattice, i.e. L_C := (closed sets, $\subseteq$) is a complete lattice with $\wedge a = \bigcap a$ and $\vee a = C(\bigcup a)$.

Theorem: $\forall$ complete lattices M, $\exists X$ and closure operator C on X s.t. $M = L_C$.

Definitions:

1. $a \in L$ is *compact* ("finite-like") if $\forall A \subseteq L$, $a \leq \vee A \Rightarrow \exists$ finite subset $B \subseteq A$ s.t. $a \leq \vee B$.
2. A complete lattice L is algebraic if $\forall x \in L$ is a join of compact elements $\iff$ join of all compact elements below x.
3. A closure operator C on a set X is said to be algebraic if for every $A \subseteq X$, $C(A) = \bigcup\{C(B) : B$ is a finite subset of $A\}$.

Definition: An algebra $\mathbf{A}$ is *locally finite* if every finitely generated subalgebra is finite. A class $\mathcal{K}$ of algebras is locally finite if every member of $\mathcal{K}$ is locally finite.

Definition: A lattice L is *modular* if for every $x, y, z \in L$ with $x \leq z$,

$$x \vee (y \wedge z) = (x \vee y) \wedge z.$$

Theorem: Let C be a closure operator on X. Then

1. L_C is algebraic
2. Compact elements of X = sets $C(F)$ with F finite.

Homomorphism:

1. $f : A \rightarrow B$ is a *homomorphism* between algebras of signature Σ if it preserves all the basic operations.
2. Suppose A and B are two algebras of the same type $\mathcal{F}$. A mapping $\alpha : \mathbf{A} \rightarrow \mathbf{B}$ is called a *homomorphism* from A to B if

   $$\alpha f^{\mathbf{A}}(a_1, \ldots, a_n) = f^{\mathbf{B}}(\alpha a_1, \ldots, \alpha a_n)$$

   for each n-ary f in $\mathcal{F}$ and each sequence $a_1, ..., a_n$ from A.

Definiton:

1. A field F is said to be a *field extension*, denoted F/K, of a field K if K is a subfield of F.
2. Let K be a field and let $f(x)$ be a polynomial in $K[x]$. We say that $f(x)$ *splits* in K if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of K such that

   $$f(x) = \lambda(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

3. We say that a field extension L/K is a *splitting field* if $f(x)$ splits in L and there is no proper intermediary subfield M in which $f(x)$ splits.

Zorn's Lemma: If F is a nonempty family of sets such that for each chain C of members of F there is a member of F containing $\bigcup C$ (i.e., C has an upper bound in F), then F has a maximal member M (i.e., $M \in F$ and $M \subseteq A \in F$ implies $M = A$).

Def: Given an algebra A, define, for every $X \subseteq A$,

$$\mathrm{Sg}(X) = \bigcap\{B : X \subseteq B \text{ and } B \text{ is a subuniverse of } A\}.$$

We read $\mathrm{Sg}(X)$ as "the *subuniverse* generated by X".

2.2 Congruence

Definition: A *congruence* $\sim$ of an algebra **A** is an equivalence relation that is preserved by all operations in **A**, i.e. $\sim \leq A^2$.

Example:A *congruence* on a **group** G is an equivalence relation $\equiv$ on G such that:

1. $a \equiv b \implies a^{-1} \equiv b^{-1}$
2. $a \equiv b, c \equiv d \implies ac \equiv bd$

Theorem: *(Congruence Condition)* The following are equivalent:

1) A is abelian.

2) Δ is a congruence class of $Cg_A(\Delta')$

3) Δ is a congruence class of a congruence of A^2

Proposition: Let A = algebra with $R \subseteq A^3$ s.t. for every $a \in A$, $\exists i \in \{1, 2, 3\}$ the binary relation defined by:

$$\forall (x_1, x_2, x_3) \in R \ ((x_1, x_2, x_3) \wedge x_i = a)$$

is the graph of an automorphism of A. Then A is abelian.

Two important congruences are:

1. The largest congruence - Δ_A = diagonal relation $\{(a, a) \mid a \in A^3\}$
2. The smallest congruence (i.e. the trivial congruence) - ∇_A = universal relation A^2

Definition: An algebra A without proper congruences is **simple** (i.e. an algebra that only has the above two congruences).

Examples:

- Let G be a permutation group on a set A. Let $\mathbf{A}$ be an algebra with domain A and signature G. Define $g^{\mathbf{A}} := g \ \forall g \in G$. Then A is simple iff G is primitive (as a permutation group???)
- Let $\mathbf{A}$ be an algebra and $\mathbf{B}$ be an expansion of $\mathbf{A}$ by all constant operations. A polynomial over $\mathbf{A}$ is a term in the signature of B. A *polynomial operation* of A is a *term operation* of B.
- Two algebras A_1 and A_2 with the same domain A are called **polynomial equivalent** if they have the same polynomial operations.

Note: Polynomial equivalent algebras have the same congruences.

Lemma: Let $\mathbf{B}$ be an algebra and $X \subseteq B^2$. Then the smallest congruence of B that contains X, denoted $\mathrm{Cg}_B(X)$, is the symmetric transitive closure of:

$$T := \{(p(a), p(b)) \mid (a,b) \in X,\ p = \text{unary polynomial op. of } B\}.$$

Congruence Lattice

Let $\mathrm{Con}(\mathcal{A})$ be the set of congruences on the algebra $\mathcal{A}$. Because congruences are closed under intersection, we can define a *meet* operation:

$$\wedge : \mathrm{Con}(\mathcal{A}) \times \mathrm{Con}(\mathcal{A}) \to \mathrm{Con}(\mathcal{A})$$

by simply taking the *intersection of the congruences* $E_1 \wedge E_2 = E_1 \cap E_2$.

On the other hand, congruences are not closed under union. However, we can define the *closure of any binary relation* E, with respect to a fixed algebra $\mathcal{A}$, such that it is a congruence, in the following way:

$$\langle E \rangle_{\mathcal{A}} = \bigcap \{F \in \mathrm{Con}(\mathcal{A}) \mid E \subseteq F\}.$$

Note that the closure of a binary relation is a congruence and thus depends on the operations in $\mathcal{A}$, not just on the carrier set. Now define:

$$\vee : \mathrm{Con}(\mathcal{A}) \times \mathrm{Con}(\mathcal{A}) \to \mathrm{Con}(\mathcal{A})$$

as $E_1 \vee E_2 = \langle E_1 \cup E_2 \rangle_{\mathcal{A}}$.

For every algebra $\mathcal{A}$, $(\mathrm{Con}(\mathcal{A}), \wedge, \vee)$ with the two operations defined above forms a lattice, called the congruence lattice of $\mathcal{A}$.

If A is an algebra and $\theta_1, \theta_2 \in \text{Con}(A)$, then $\theta_1 \circ \theta_2$ is the binary relation on A defined by $(x, y) \in \theta_1 \circ \theta_2$ if and only if there exists $z \in A$ such that $(x, z) \in \theta_1$ and $(z, y) \in \theta_2$. If $\theta_1, \theta_2 \in \text{Con}(A)$ such that $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$, we say that θ_1 and θ_2 are permutable. An algebra A is called congruence permutable if $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ for all $\theta_1, \theta_2 \in \text{Con}(A)$.

For any algebra A, two permutable congruences θ_1, θ_2 of A are *complementary factor congruences* if $\theta_1 \vee \theta_2 = 1$ and $\theta_1 \wedge \theta_2 = 0$ (1 and 0 are top and bottom elements in the lattice $\text{Con}(A)$).

2.2.1 Tame Congruence Theory

Having introduced the congruence lattice, I would now like to mention *Tame Congruence Theory* (TCT), which was developed by Ralph Mckenzie and David Hobby. [MMT87] has a great amount of information on this and more, the most of the content here has been taken from [McK90]. TCT shows that every finite algebra can be usefully regarded as a sort of amalgam of algebras belonging to five basic classes:

1. G-sets
2. Finite vector space over finite field
3. 2-element boolean algebra
4. 2-element lattice
5. 2-element semi-lattice

Let **A** be a finite algebra and $\langle \alpha, \beta \rangle$ be a pair of congruences of **A**. Assume $\alpha \prec \beta$, i.e. α is a proper subset of β and β lies properly between them. Then, $\langle \alpha, \beta \rangle$ is analagous to a **prime quotient** in the lattice Con(**A**).

Example: Let **A** be a simple algebra $\Rightarrow$ α and β are its only congruences.

- Associate with $\langle \alpha, \beta \rangle$ a set of subsets of $A = M_{A(\alpha,\beta)}$, the memebers of which are minimal sets $\langle \alpha, \beta \rangle$, i.e. minimal members in the collection of subsets $M \subseteq A$ such that for some polynomial function f of **A**, f(A) = M and $\exists$ at least one pair of β-congruence elements x and y such that $(f(x), f(y)) \notin \alpha$.
- At least one pair of β-congruent elements $\langle x, y \rangle$.

In TCT it is shown that each set $M \in M_{A(\alpha,\beta)}$ is of the form $K(A)$ for some idempotent polynomial function e and for every $k \in M_A(\alpha, \beta)$, there exist polynomial functions that induces a bijection from M onto K and its inverse map from K onto M.

- Call a unary polynomial e of A idempotent if it satisfies $e(e(a)) = e(a)$ for every element a of A. Define the induced algebra $A|_M$ to be the set M with all operations on M that are restrictions of operations of A (for an arbitrary number of variables) under which M is closed.

- All induced $\langle\alpha, \beta\rangle$ - minimal algebras $A|_M$ are isomorphic to one another (cryptomorphic) via polymorphic bijections.

- $\langle\alpha, \beta\rangle$ traces are sets N which, for some $M \in M_{A(\alpha,\beta)}$, they are identical with some $\beta|_M$-equivalence classes that contain at least two $\alpha|_M$-equivalence classes.

Decidable Varieties

A variety $\mathcal{V}$ in language $\mathcal{L}$ is **decidable** if there exists an algorithm to determine precisely which sentences of $\mathcal{L}$ are true in every algebra in the variety.

- Any decidable locally finite variety decomposes as the varietal product of three very special varieties:

  1. S - uniform type 1 $\equiv$ class of categories having a fixed number of finite objects.
  2. A - uniform type 2 $\equiv$ variety of all modules over a certain finite ring.
  3. D - uniform type 3: Discriminator variety - "very like" the variety of Boolean algebras in many respects.

This result gives an algorithm for reducing:

- "Is the variety generated by the finite algebra **A** decidable?"

- "Is the variety of modules over the finite ring R decidable?"

Finite Groups & Finite Lattices

Pálfy & Pudlák proved that every finite lattice is isomorphic to the congruence lattice of some finite algebra if and only if every finite lattice is an interval in the lattice of subgroups of some finite group. The method involved showing that every finite lattice is embedded as an interval in a finite lattice with some special properties.

If **A** is a finite algebra whose congruence lattice **L** has these special properties, then the induced algebra on some "minimal set" in **A** still has **L** as its congruence lattice (isomorphically), and the polynomial maps of the minimal algebra, minus the constant maps, form a transitive group of permutations.

2.3 Galois Correspondences

Definition: Given two sets X and Y, define a relation $R \subseteq X \times Y$. Let $\mathcal{P}(X) \to \mathcal{P}(Y)$,

$$A \mapsto A^{\to} := \{b \in Y; \forall a \in A, (a,b) \ \in R\}$$

and $\mathcal{P}(Y) \to \mathcal{P}(X)$,

$$B \mapsto B^{\leftarrow} := \{a \in X; \forall b \in B, (a,b) \ \in R\}$$

If the above pair of functions satisfy the following, it is a *Galois Correspondence*:

1. If $A \subseteq X$, we have $A \subseteq A^{\to\leftarrow}$
2. If $B \subseteq Y$, we have $B \subseteq B^{\leftarrow\to}$
3. If $A \subseteq A_2 \subseteq X$, we have $A_2^{\to} \subseteq A_1^{\to}$
4. If $A \subseteq X$, we have $A^{\to} = A^{\to\leftarrow\to}$

Definiton: Let C, D be closure operators.

1. $C \subseteq X$ is C-closed iff $A = B^{\leftarrow}$ for some $B \subseteq Y$.
2. $B \subseteq Y$ is D-closed iff $B = A^{\to}$ for some $A \subseteq X$.
3. $A \mapsto A^{\to\leftarrow}$ is a lattice isomorphism, taking $L_C \to L_D^{\text{dual}}$
4. $B^{\leftarrow\to} \mapsto B$ is its inverse

Examples of Galois Correspondence

1. Galois Theory

$X :=$ splitting field of $f \in \mathbb{Q}[x]$

$Y := \mathrm{Aut}_{\mathbb{Q}} X$

$(a, f) \in R$ iff $f(a) = a$

The elements closed under this correspondence are the Galois subfields of X and the subgroups of Y, which is the Fundamental theorem of Galois Theory.

2. Hilbert's Nullstellensatz

$X := \mathbb{C}^n$

$Y := \mathbb{Q}[x_1, \ldots, x_n]$

$(\vec{a}, f) \in R$ iff $f(\vec{a}) = 0$

The elements closed under this correspondence are algebraic varieties and Radicals of $\mathbb{Q}[x_1, \ldots, x_n]$ (Nullstellensatz).

3. Mod-Id (Galois Correspondence in Universal Algebra)

- Define classes of algebra as $\mathcal{E}^{\leftarrow} = \mathrm{Mod}(\mathcal{E}) = \{A; A \models \mathcal{E}\}$ = all algebras satisfying $\mathcal{E}$
- Define identities of algebras as $\mathcal{K}^{\rightarrow} = \mathrm{Id}(\mathcal{K}) = \{A; A \models \mathcal{K}\}$ = all identities satisfied in $\mathcal{K}$

$X :=$ algebras in signature Σ

$Y :=$ identities in signature Σ

$(A, \mu \approx \nu)$ iff A satisfies $\mu \approx \nu$

The elements closed under this correspondence are classes closed under H, S, P, and Equational theories (this is Birkhoff's theorem).

Birkhoff's theorem gives, for every class $\mathcal{K}$ of τ-algebras, a characterisation of the class of all τ-algebras that satisfy all identities satisfied by $\mathcal{K}$. Conversely, for every set of τ-identities Σ, there exists a syntactic characterisation of the set of all universal conjunctive consequences of Σ. This is expanded in section 8.5.2 of [Bodb].

4. Pol-Inv (Galois Correspondence in Universal Algebra)

$X :=$ operations on A (finite A)

$Y :=$ relations on A

The objects closed under this correspondence are clones and coclones.

5. Vector Spaces

$X = Y :=$ vector space of finite dimension with inner product

$(\vec{v}, \vec{w}) \in R$ iff $\vec{v} \perp \vec{w}$

The elements closed under this are vector subspaces.

2.4 Varieties

[MMT87] contains an incredible amount of information on this topic (along with algebras a lattices; Commutator Theory here is particularly interesting).

We start by defining a variety.

Let $\mathcal{K}$ be a class of algebras of fixed signature Σ. Let,

- $H(\mathcal{K}) :=$ all algebras that are isomorphic to quotients $(A/\sim)$ of algebras from $\mathcal{K}$.
- $S(\mathcal{K}) :=$ all algebras that are isomorphic to subalgebras of algebras from $\mathcal{K}$.
- $P(\mathcal{K}) :=$ all algebras that are isomorphic to products of algebras from $\mathcal{K}$.

Then, the **variety** generated by $\mathcal{K}$ (the smallest variety containing $\mathcal{K}$) is $V(\mathcal{K}) := H(\mathcal{K}) \bigcup P(\mathcal{K}) \bigcup S(\mathcal{K}) \bigcup HS(\mathcal{K}) \bigcup ... \bigcup PHSP(\mathcal{K}) \bigcup ...$

Definiton: $\mathcal{K}$ is a *variety* if it is closed under H, S, and P.

1. H, S, P are closure operators, i.e. $SS(\mathcal{K}) = S(\mathcal{K}), ...$
2. $SH(\mathcal{K}) \subseteq HS(\mathcal{K}), PS(\mathcal{K}) \subseteq SP(\mathcal{K}), PH(\mathcal{K}) \subseteq HP(\mathcal{K})$
3. $V(\mathcal{K}) = HSP(\mathcal{K})$
4. $\mathcal{K}$ is a variety iff $HSP(\mathcal{K}) \subseteq \mathcal{K}$

Lemma 9.2 The following inequalities hold: $SH \leq HS$, $PS \leq SP$, and $PH \leq HP$. Also, the operators H, S, and IP are idempotent.

Proof. Suppose $A = SH(K)$. Then for some $B \in K$ and onto homomorphism $\alpha : B \to C$, we have $A \leq C$. Thus $\alpha^{-1}(A) \leq B$, and as $\alpha(\alpha^{-1}(A)) = A$, we have $A \in HS(K)$.

If $A \in PS(K)$ then $A = \sum_{i \in I} A_i$ for suitable $A_i \leq B_i \in K$, $i \in I$. As $\sum_{i \in I} A_i \leq \sum_{i \in I} B_i$, we have $A \in SP(K)$.

Next, if $A \in PH(K)$, then there are algebras $B_i \in K$ and epimorphisms $\alpha_i : B_i \to A_i$ such that $A = \sum_{i \in I} A_i$. It is easy to check that the mapping $\alpha : \sum_{i \in I} B_i \to \sum_{i \in I} A_i$ defined by $\alpha(b)(i) = \alpha_i(b(i))$ is an epimorphism; hence $A \in HP(K)$.

It is a routine exercise to verify that $H^2 = H$, etc.

1. A nonempty class $\mathcal{K}$ of algebras of type $\mathcal{F}$ is called a variety if it is closed under subalgebras, homomorphic images, and direct products.
2. As the intersection of a class of varieties of type $\mathcal{F}$ is again a variety, and as all algebras of type $\mathcal{F}$ form a variety, we can conclude that for every class $\mathcal{K}$ of algebras of the same type there is a smallest variety containing $\mathcal{K}$.

3. If $\mathcal{K}$ is a class of algebras of the same type let $V(K)$ denote the smallest variety containing K. We say that $V(K)$ is the variety generated by K. If K has a single member A we write simply $V(A)$. A variety V is finitely generated if V = V (K) for some finite set K of finite algebras.

2.5 Decomposition

- An algebra $\mathbf{A}$ is *(directly) indecomposable* if $\mathbf{A}$ is not isomorphic to a direct product of two nontrivial algebras.
- Let $(A_i)_{i\in I}$ be an indexed family of algebras of type F. The (direct) product $\mathbf{A} = \prod_{i\in I} A_i$ is an algebra with universe $\prod_{i\in I} A_i$ and such that for $f \in F^n$ and $a_1, \ldots, a_n \in \prod_{i\in I} A_i$,

  $$f^{\mathbf{A}}(a_1, \ldots, a_n)(i) = f^{\mathbf{A}_i}(a_1(i), \ldots, a_n(i))$$

  for $i \in I$, i.e., $f^{\mathbf{A}}$ is defined coordinate-wise.
- Each finite algebra is isomorphic to a direct product of directly indecomposable algebras.
- R is *subdirectly irreducible (SI)* if it is not isomorphic to a nontrivial subdirect product.
- As a consequence, an algebra A is directly indecomposable iff the only factor congruences on A are 0 and 1.
- A subdirectly irreducible algebra is directly indecomposable.

Defintion:

1. An algebra $\mathbf{A}$ is a *subdirect product* of an indexed family $(A_i)_{i\in I}$ of algebras if

   a) $\mathbf{A} \leq \prod_{i\in I} A_i$, and

   b) $\pi_i(\mathbf{A}) = A_i$ for each $i \in I$,

   Notation: $R \leq_{sd} \prod_{i\in I} A_i$

2. An algebra $\mathbf{A}$ is *subdirectly irreducible* (SI) if for every subdirect embedding $\alpha : \mathbf{A} \to \prod_{i\in I} A_i$, there is an $i \in I$ such that $\pi_i \circ \alpha : \mathbf{A} \to A_i$ is an isomorphism, i.e. if it is not isomorphic to a non-trivial subdirect product.

Theorem: If $\mathcal{K}$ is a variety, then every member of $\mathcal{K}$ is isomorphic to a subdirect product of subdirectly irreducible members of K.

Mckenzie characterisation: Finitely generaled variety (i.e. HSP($\mathbf{A}$), $\mathbf{A}$ finite) is *directly representable* it it has finitely many finite direct indecomposables.

Let η_1 and η_2 be the kernel of the projections of the corresponding index. We have:

- $\eta_1, \eta_2 \in$ Con(R).
- $R/\eta_1 \cong A_1$, $R/\eta_2 \cong A_2$
- $\eta_1 \wedge \eta_2 = O_R = \Delta$

Trivial iff $\eta_1 = 0$ or $\eta_2 = 0$.

Theorem: If $\mathbf{A}$ = algebra, $\alpha_i \in \mathrm{Con}(\mathbf{A})$, $i \in I$, $\cap_{i \in I} \alpha_i = O_A$. Then $h : \mathbf{A} \to \prod A_i/\alpha_i, a \mapsto (a/\alpha_i)$ is an injective homomorphism and

$$\mathbf{A} \cong h(\mathbf{A}) \leq_{sd} \prod_{i \in I} A_i/\alpha_i$$

This decomposition is trivial iff $\exists i$ s.t. $\alpha_i = 0$.

Definition: Let L = complete lattice. $1 \neq a \in L$ is *completely $\wedge$-irreducible* if $\wedge_{i \in I} b_i = a \Rightarrow \exists i, b_i = a$.

$\mathbf{A}$ is subdirectly irreducible iff O_A is completely $\wedge$-irreducible in Con($\mathbf{A}$). More generally, for $\alpha \in \mathrm{Con}(\mathbf{A})$, $\mathbf{A}/\alpha$ is SI iff α is completely $\wedge$-irreducible in Con($\mathbf{A}$).

Examples:

1. Simple algebras $\equiv \mathrm{Con}(\mathbf{A}) = 0, 1 \Rightarrow$ SI $\Rightarrow$ directly indecomposable.
2. A finite abelian group is SI iff it is $\cong \mathbb{Z}_{p^k}$
3. S_n, A_n are SI.
4. Non-trivial distributive lattice is SI iff it is two elements.

Theorem (Birkhoff): Every algebra is isomorphic to a subdirect product of SI algebras.

Def: A *representation* of an algebra A is a collection $h_i : i \in I$ of homomorphisms with domain A which collectively separate the points of A. That is, if $a, b \in A$ with $a \neq b$, then there must exist $i \in I$ such that $h_i(a) \neq h_i(b)$

2.6 Free Algebras

- Let X be a set of (distinct) objects called variables. Let $\mathcal{F}$ be a type of algebras. The set $T(X)$ of terms of type $\mathcal{F}$ over X is the smallest set such that
  1. $X \cup F_0 \subseteq T(X)$.
  2. If $p_1, \ldots, p_n \in T(X)$ and $f \in F_n$, then the "string" $f(p_1, \ldots, p_n) \in T(X)$.
- Given Σ = signature, X = set of variables, **define** the Σ-*term* over X as a formal meaningful expression formed by
  - Variables in X
  - Symbols in Σ
  - Composition of the above

Definition: Σ-identity: ordered pair (s, t) of terms in Σ, written $s \approx t$:

- For algebra $\mathbf{A}$ (in sig. Σ), $\mathbf{A}$ satisfies $s \approx t$ if $\forall m : X \to A$, $\hat{m}(s) = \hat{m}(t)$
- For class of algebras $\mathcal{K}$,

$F(X)$ = absolutely free algebra over X in sig. Σ = all Σ terms over X.

Fact: $\forall$ algebras $\mathbf{A}$, $\forall$ $m : X \to A$, $\exists!$ homomorphism $F(X) \to \mathbf{A}$ extending $m = \hat{(}m)$.

Free algebra for a class: Given $\mathcal{K}$ = set of algebras (in sig. Σ), X = set of variables, define $\lambda_{\mathcal{K}} \in$ Con(F(X)) by

$$\lambda_{\mathcal{K}} := \bigwedge\{\alpha \in \text{Con}(\mathbf{F}(\text{X}); \mathbf{F}(X)/\alpha \in S(\mathcal{K})\}$$

Then, the *free algebra for a class* is $F_{\mathcal{K}} = \mathbf{F}(\text{X})/\lambda_{\mathcal{K}}$

2.7 Clones

Def: A set $\mathcal{C}$ of operations on A of arity ≥ 1 is a (function) clone if:

1. $\mathcal{C}$ is closed under forming term operations (in sig. $\Sigma = \mathcal{C}$).
   Eg: If $f \in \mathcal{C}$ ternary and $g \in \mathcal{C}$ binary, then $h \in \mathcal{C}$, where

$$h(a_1, a_2, a_3, a_4) := f(g(a_1, a_2), a_3, a_4)$$

2. $\mathcal{C}$ contains all the projections.
3. $\mathcal{C}$ is closed under "composition".

Notation: $\mathcal{C}_n$ = n-ary members of $\mathcal{C}$.

# (all clones on A; $\subseteq$) is a complete algebraic lattice:

- $\bigwedge$ = intersection
- $\bigvee$ = smallest clone containing the union

The number of clones are:

- For $|A| = 2$, finite and countable (Post's lattice)
- For $|A| > 2$, finite continuum many clones (

Def: $\mathbf{A}$ = algebra,

- Clo($\mathbf{A}$) = all term operations of $\mathbf{A}$
- Clo$_n$($\mathbf{A}$) = all n-ary operations of $\mathbf{A}$
  = the subuniverse of $\mathbf{A}^{A^n}$ generated by the n-ary projections
  = (?) is isomorphic to the free algebra for $\{\mathbf{A}\}$ (or HSP($\mathbf{A}$)) over n-element set of variables.

Remarks:

- If Clo($\mathbf{A}$) is a clone, all clones are of this form?
- If Clo($\mathbf{A}$) = Clo($\mathbf{B}$), $\mathbf{A}$ and $\mathbf{B}$ are term equivalent.

Theorem: Clo$_n$($\mathbf{A}$) $\simeq F_{\{\mathbf{A}\}}(\{x_1, ..., x_n\} = F_{HSP(\mathbf{A})}(\{x_1, ..., x_n\}$

2.8 Commutator Theory

The **commutator** of a group is $[x, y] = x^{-1}y^{-1}xy$. This operation can formulate many important concepts of abelian groups, the centre of a group, normal groups, solvable groups, and nilpotent groups. (This operation will be of interest in addressing the question of interest presented at the end of this report).

In Universal Algebra, Commutator theory tries to generalise such group theoretic definitions and results to arbitrary algebras.

Definition: Let $\mathbf{A}$ be any algebra. The *centre* of $\mathbf{A}$ is the binary relation

$$\langle a, b\rangle \in Z(\mathbf{A})$$

iff for $n \geq 1$ and for every term op. $t \in \mathrm{Clo}_{n+1}\mathbf{A}$ and $\forall c_1, ..., c_n, d_1, ..., d_n \in A$

$$t(a, c_1, ..., c_n) = t(a, d_1, ..., d_n) \leftrightarrow t(b, c_1, ..., c_n) = t(b, d_1, ..., d_n) \tag{2.1}$$

$\mathbf{A}$ is abelian iff $Z(\mathbf{A}) = A \times A$.

Definition 4.148. Let α, β, η be congruences of an algebra A. We say that α *centralises* β modulo η, written

$$C(\alpha; \beta; \eta),$$

if for all $n \geq 1$, and for every $t \in \mathrm{Clo}_{n+1}A$, $\langle a, b\rangle \in \alpha$, and $\langle c_1, d_1\rangle, \ldots, \langle c_n, d_n\rangle \in \beta$ we have

$$t(a, c_1, \ldots, c_n) \equiv_\eta t(a, d_1, \ldots, d_n) \iff t(b, c_1, \ldots, c_n) \equiv_\eta t(b, d_1, \ldots, d_n).$$

Lemma: The centre of A is a congruence on A.

Theorem: These statements are equivalent for any algebra A.

1. A is Abelian.
2. $\{\langle a, a\rangle : a \in A\}$ is a coset of a congruence on A^2.
3. $\langle\langle x, x\rangle, \langle y, z\rangle\rangle \in \Delta(A)$ iff $y = z$ for all $x, y, z \in A$.
4. A^4 has a subuniverse S such that:
    a) $\langle x, y, x, y\rangle \in S$ for all $x, y \in A$.
    b) $\langle x, y, u, v\rangle \in S \iff \langle y, x, v, u\rangle \in S \iff \langle u, v, x, y\rangle \in S$ for $x, y, u, v \in A$.
    c) $\langle x, x, y, z\rangle \in S \iff y = z$ for $x, y, z \in A$.
5. $\langle x, x, y, z\rangle \in S(A)$ iff $y = z$ for all $x, y, z \in A$.

See [MMT87] for the proofs of the above.

2.9 PP-Constructability

Let $\mathbb{A}, \mathbb{B}$ be relational structures and $\phi(x_1, ..., x_n) = \tau$-formula. Then the relation defined by ϕ is the relation:

$$\{(a_1, \ldots, a_n) \mid A \models \varphi(a_1, \ldots, a_n)\}$$

If the involved formula φ is primitive positive, then this relation is said to be *pp-definable* in A.

Let ϕ be a first-order formula over the relational signature τ. Then ϕ is called **primitive positive** or **pp** if and only if it is of the form $\exists x(\psi_1 \wedge \cdots \wedge \psi_l)$, where $\psi_1, \ldots, \psi_l$ are atomic τ-formulas.

Let A, B be relational structures. We say that B is a **pp-power** of A if it is isomorphic to a structure with domain A^n $(n \geq 1)$ whose relations are pp-definable from A.

We say that A **pp-constructs** B if B is homomorphically equivalent to a pp-power of A.

We consider the following quasi-order:

$$\mathbb{A} \leq \mathbb{B} \text{ iff } \mathbb{A} \text{ pp-constructs } \mathbb{B}.$$

Every element in our poset is a $\equiv$-class where the equivalence relation is:

$$\mathbb{A} \equiv \mathbb{B} \text{ iff } \mathbb{A} \leq \mathbb{B} \text{ and } \mathbb{B} \leq \mathbb{A}.$$

Proposition: Let $\mathcal{B}$ be a finite structure with at least two elements and $\mathbf{A}$ is an affine idempotent algebra such that $\mathrm{Clo}(\mathbf{A}) = \mathrm{Pol}(\mathcal{B})$. Then there exists a prime p such that $\mathcal{B}$ pp-constructs $(\mathbb{Z}_p; +, 1)$.

2.10 Maltsev Conditions

Definition: A Maltsev (also Mal'cev) operation $m(x, y, z)$ is a ternary operation satisfying the identities $m(y, x, x) \approx m(x, x, y) \approx y$.

Note that every group has a Maltsev term: $m(x, y, z) = xy^{-1}z$. Similarly, every ring and module has a Maltsev term $m(x, y, z) = x - y + z$.

Strong Matlsev conditions = condition for a variety $\mathcal{V}$ or algebra $\mathbf{A}$ or clone $\mathcal{C}$ of the the form

$$\exists \text{ terms } t_1, ..., t_n \text{ s.t. } \mathcal{V} \models \text{ some identities with these terms.}$$

Examples:

1. $\exists$ Mal'tsev term $p(x, y, z)$, $\mathcal{V} \models p(x, x, y) \approx y \approx p(y, x, x)$
    - Groups: $p(x, y, z) = x \cdot y^{-1} \cdot z$
    - Quasigroups:
2. $\exists$ majority term $x(x, y, z)$, $\mathcal{V} \models p(x, x, y) \approx m(x, y, x) \approx p(y, x, x) \approx x$
    - Lattices: $m(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$

Definitions:

- $\mathbf{A}$ is *congruence permutable* (CP) if $\forall \alpha, \beta \in \mathrm{Con}(\mathbf{A})$, $\alpha \circ \beta = \beta \circ \alpha$
- Variety $\mathcal{V}$ is CP if $\forall\ \mathbf{A} \in \mathcal{V}$, $\mathbf{A}$ is CP.
- A relation $R \subseteq A \times B$ is **rectangular**
  if $\forall a, a' \in A,\ \forall b, b' \in B,\ (a, b'), (a', b), (a', b') \in R \ \Rightarrow\ (a, b) \in R$
  $\Leftrightarrow \eta_A \circ \eta_B = \eta_B \circ \eta_A$, where η = projection kernel.

Theorem (Maltsev '54): Let $\mathcal{V}$ be a variety.

- $\mathcal{V}$ is CP.
- $\forall$ **A, B** $\in \mathcal{V}, \forall R \leq$ **A** $\times$ **B**, R is rectangular.
- $\mathcal{V}$ has a Maltsev term.

2.11 Abelian Algebras

Definition: We call an algebra A *affine* if it is polynomially equivalent to an R-module (for some ring R with identity).

Note that according to this definition, every commutative group is affine (by picking $R = \mathbb{Z}$ as the ring; and defining the scalar multiplication $n \cdot x := x + x + \cdots + x$ (n times)).

Definition: Let A be an algebra. A polynomial $p : A^3 \to A$ of A is called *central* if it satisfies

$$p(f(x_1, \ldots, x_n), f(y_1, \ldots, y_n), f(z_1, \ldots, z_n)) = f(p(x_1, y_1, z_1), \ldots, p(x_n, y_n, z_n)),$$

for all basic operations f of A.

Lemma: Let A be affine. Then $(x, y, z) \mapsto x - y + z$ is the unique Maltsev polynomial operation of A. Moreover, m(x, y, z) is central.

Definition: An algebra A is *Abelian* if it satisfies the term condition, i.e., for every term t of arity $k + 1$, all $a, b \in A$ and tuples $c, d \in A^k$,

$$t(a, c) = t(a, d) \implies t(b, c) = t(b, d).$$

Some examples of abelian algebras

1. Every affine algebra is abelian.
2. A semilattice $(L, \wedge)$ is abelian if $|L| = 1$.
3. A group $(G, \cdot, e, -1)$ is abelian if and only if $x \cdot y \approx y \cdot x$.
4. A ring $(R, +, 0, -, \cdot)$ is abelian if and only if $x \cdot y \approx 0$.

Theorem 12.12 (Fundamental theorem of abelian algebras; see [?]). Let A be an algebra with a Maltsev term m. Then the following are equivalent:

1. A is abelian.
2. A is affine.
3. There exists an abelian group $(A; +, -, 0)$ such that the operation $(x, y, z) \mapsto x - y + z$ is central in A and in $\mathrm{Clo}(A)$.
4. m is central.

For the proofs of the theorems and lemmas mentioned in this section, see [Bodb].

2.12 Some interactions between group theory and universal algebra

All of the following information is taken from [McK90], which is a very very interesting paper and I would highly recommend anyone read it if they are interested in anything even remotely related to this topic. A key notion here is that the congruence lattice is a very important invariant of an algebra.

- An algebra is abelian iff it is polynomially equivalent to a module over a ring.
- $[\theta, \psi]$ = commutator of two congruences θ and ψ.
- For any set $\{\theta, \psi, \delta\} \cup \{\psi_i : i \in I\}$ of congruences on an algebra that belongs to a **congruence modular variety**, the commutator is
  - Symmetric and sub-multiplicative, i.e.
    $$[\theta, \psi] = [\psi, \theta] \subseteq \theta \cap \psi$$
  - Joint-distributive, i.e.
    $$[\theta, \vee\{\psi_i \mid i \in I\}] = \vee[\theta, \psi_i \mid i \in I]$$
- Commutator of congruence of a quotient algebra A/δ is determined from commutators in A by the rule
  $$[\theta/\delta, \psi/\delta] = [\theta, \psi] \vee \delta/\delta \quad \text{if} \quad \delta \subseteq \theta \cap \psi.$$
- Restricted to the algebra in a fixed congruence-modular variety; this commutator is the **largest binary commutator** that possesses all of these properties.

The lattice of normal subgroups of a group, with the commutator operation, is a lattice-ordered monoid.

- Suppose G = group, and the variety generated by G is **residually small**, i.e., $\exists$ a cardinal number λ such that every group $K \in G$ can be embedded into a product of groups of cardinality $\leq \lambda$.
- If G is finite, the variety it generates will be residually small just in case all the nilpotent groups in this variety are abelian, and this holds iff the Sylow subgroups of G are abelian.
- If $\mathcal{V}$ = residually small congruence-modular variety of algebras, then
  $$\mathcal{V} \models x \wedge [y, y] = [x \wedge y, y];$$
  where (x, y) are pairs of variables ranging over pairs of congruences of any algebra in $\mathcal{V}$.

Universal algebra reduces very general problems to groups and rings:

Example: Characterisation of finite algebras that generate a variety containing only a finite number of directly indecomposable algebras → characterising the finite rings of finite representation type.

Congruence Equations of Finite Groups

A congruence of group ≡ normal subgroup → we deal with the labelled structure lattice $\mathbf{L(G)}$, i.e. the lattice of normal subgroups of finite group G (where prime quotients have labels supplied by the theory).

As groups have permuting congruences, the possibilities are restricted.

CHAPTER 3

Automorphism Groups

3.1 Some Model Theory

- A **Structure or Model** $\mathcal{M}$ is a set (domain) with certain specified functions M and relations (subsets of M^n) for various n, and some distinguished elements called constants.
- A language $\mathcal{L}$ is relational if it has no function or constant symbols.
- A **Formula** is a well-formed sequence of symbols in the language.

Definition: A structure $\mathcal{M}$ is ω-categorical if:

1. $\mathcal{M}$ is countably infinite.
2. Whenever $|\mathcal{M}| = |\mathcal{N}|$ and both $\mathcal{M} \cong \mathcal{N}$ satisfy the same first-order sentences, $\mathcal{M} \equiv \mathcal{N}$.

Lemma: Let $\mathcal{M}$ be a countably infinite structure. The Following are equivalent:

1. $\mathcal{M}$ is ω-categorical.
2. $\text{Aut}(\mathcal{M})$ is oligomorphic.

Definition: A structure $\mathcal{M}$ is homogeneous if:

1. $\mathcal{M}$ is countable.
2. Whenever U and V are finite substructures of $\mathcal{M}$, there exists an isomorphism $f : U \to V$ that extends to an automorphism of $\mathcal{M}$.

Building Homogeneous Structures

Suppose $\mathcal{C}$ is a non-empty class of finite $\mathcal{L}$-structures with the following properties:

1. $\mathcal{C}$ is closed under isomorphisms.
2. $\mathcal{C}$ is closed under substructures (Hereditary property).
3. Whenever $A, B \in \mathcal{C}$, there exists $D \in \mathcal{C}$ such that $A \subseteq D$ and $B \subseteq D$ (Joint Embedding Property - JEP).
4. Whenever $A, B_1, B_2 \in \mathcal{C}$ and $f_i : A \to B_i$ (for $i = 1, 2$) are embeddings, there exists $D \in \mathcal{C}$ and embeddings $g_i : B_i \to D$ (for $i = 1, 2$) such that $g_1 \circ f_1(a) = g_2 \circ f_2(a)$ for all $a \in A$ (Amalgamation Property - AP).

If D and the embeddings g_i can be chosen such that:

$$g_1(B_1) \cap g_2(B_2) = g_1 \circ f_1(A) = g_2 \circ f_2(A)$$

then $\mathcal{C}$ has *strong amalgamation.*

Note: The empty set is not considered as a structure in model theory.

The following is a list of all homogenous graphs:

1. Rado graph $\mathbb{R}$.
2. Universal and homogeneous K_n-free graphs, where K_n is a complete graph on n vertices.
3. Disjoint union of (same size) complete graphs.
4. Complement of (3).
5. Special finite cases: 5-cycle and the "window" graph.

3.2 Algebraicity

Model-Theoretic Algebraic Closure

Let A be a structure. $B \subseteq A$. The algebraic closure of B over A, denoted as $\mathrm{acl}_A(B)$, is the set of elements of A that lie in finite sets that are first-order definable over A with parameters from B.

Group-Theoretic Algebraic Closure

Let $G \leq \mathrm{Sym}(A)$ be a permutation group acting on A, and let $B \subseteq A$ be finite. Then $\mathrm{acl}_A(B)$ is the set of elements of A that lie in the orbit of B under the action of G.

Lemma: If G is a closed group of automorphisms of an algebraic structure A, then:

$$\mathrm{acl}_A(B) = \mathrm{acl}_{\mathrm{Aut}(G)}(B)$$

B is algebraically closed in A if $\mathrm{acl}_A(B) = B$. A has no algebraicity if all finite subsets of A are algebraically closed in A.

Theorem: Let A be a homogeneous structure. Then the age of A has strong amalgamation if and only if $G \cong \mathrm{Aut}(A)$ has no algebraicity.

Lemma: Let G be a permutation group on a domain D with finite orbits, and let $A, B \subseteq D$ be finite. Then $\exists g \in G$ such that $g(A) \cap B = \emptyset$.

Definition: Let $C_1 \leq C_2$ be classes of finite structures with disjoint union property. Then the generic superposition of $C_1 \cup C_2 = C_1 \times C_2$ is the class of $(T_1 \cup T_2)$-structures A such that the T-reduct of A is in C_i for $i = 1, 2$.

If A_1 and A_2 are countable homogeneous structures with stable ages without algebraicity, then $A_1 \times A_2$ denotes the Fraïssé limit of the age of A_1 and the age of A_2.

3.3 Oligomorphic Permutation Groups

We study Oligomorphic Permutation Groups as there is a link between oligomorphicity of permutation groups and first-order logic. [Cam] already provides a great overview of the topic, and I will be including some of the information presented there and in Chapter 3 of [Boda] describes its connection with logic.

Recall that a permutation group is a subgroup of the symmetric group S_n. A permutation group G on a set A is:

- *k-transitive* if for $s, t \subseteq A$ with pairwise distinct entries, there exists $g \in G$ s.t. $g(s) = t$. Transitive if it is 1-transitive.
- k-set transitive if $\forall s, t \subseteq A$ of cardinality k, $\exists g \in G$ s.t. $g(s) = \{g(a) \mid a \in s\} = t$.
- *Highly set transitive* if it is k-set transitive $\forall k \geq 1$.
- *Highly transitive* if it is k-transitive $\forall k \geq 1$.

A permutation group G (a subgroup of the symmetric group S_n on a set Ω) is said to be *oligomorphic* if G has only finitely many orbits on Ω^n for every natural number n.

Having definited an oligomorphic permutation group (henceforth referred to as OPG), following are some interesting properties and consequences:

- A permutation group is oligomorphic if G has only finitely many orbits of k-tuples for each $k \geq 1$. This gives us a sequence of natural numbers corresponding to the *number of orbits* on n-tuples.
- If G_i is a transitive permutation group on Ω_i, the cartesian product $\Pi_i G_i$ is the set of functions $f : I \to \cup_i \Omega_i$ satisfying $f(i) \in G_i$ for all $i \in I$. This gives us two natural action:
  1. *Intransitive* action on the disjoint union of the sets Ω_i:

     $$\text{if } \alpha \in \Omega_i, \text{ then } \alpha f = \alpha f(i)$$

     If each group G_i is transitive, then the sets Ω_i are the orbits of the cartesian product.
  2. The *product action* is the standard componentwise action on the cartesian products of the sets Ω_i.

Congruence (G is transitive on Ω) = equivalence relation on Ω which is G-invariant. We say that G is **primitive** if its only congruences are the trivial and universal congruences.

Examples of imprimitive groups are *wreath products*, which will be outlined below.

Wreath product

Let C be a group and let D be a group acting on a set Δ. Define

$$K := \mathcal{C}^{\Delta} = \{f \mid f : \Delta \to \mathcal{C}\} \quad \text{is a group under pointwise multiplication.}$$

Given $f_1, f_2 \in K$ and $\delta \in \Delta$:

$$(f_1 f_2)(\delta) := f_1(\delta) f_2(\delta).$$

- The identity element 1_K of K maps every element of Δ to the identity element of $\mathcal{C}$.
- Define an action D^K (conjugation) taking $f \in K$ to $f^d \in K$ for $d \in C$ by specifying $f^d(s) = f(sd^{-1})$.
- The map $f \mapsto f^d$ is an automorphism of K.

Definition: The **wreath product** (denoted as an operation as Wr) W of $\mathcal{C}$ by Δ is denoted by

$$W := K \rtimes \Delta = \mathcal{C}^{\Delta} \rtimes \Delta$$

Lemma: Let $G \leq Sym(\mathbb{N})$ be oligomorphic and $\Delta \in \mathbb{N}^n$ for $n \in \mathbb{N}$. Then G_Δ is oligomorphic as well. Hence, every closed OPG must have continuous cardinality.

The connection between oligomorphicity and first order logic

- Let **A** be a τ-structure, $\phi(x_1, \ldots, x_c)$ be a first-order formula with free variables from $x_1, \ldots, x_c$.
- If $a_1, \ldots, a_k \in A$, then $A \models \phi(a_1, \ldots, a_k)$ if formula ϕ evaluates in A to true when instantiating x_i with a_i.
- SInv $-$ Aut: SInv(Ω) = sets of all relations r on A s.t. all permutations in G are automorphisms of r.

Theorem: Let A = structure s.t. Aut(A) is oligomorphic. Then A is SInv(Aut(A)) iff A is first-order definable over A.

Conclusion

If T is a theory, T is satisfiable $\iff$ a model exists.

3.3.1 Small index property

Following are the normal subgroups of some classical examples of permutation groups:

- A group A of order-preserving permutations of $\mathbb{Q}$ has two non-trivial normal subgroups:

  1. L = permutations fixing all sufficiently large positive rationals.
  2. R = permutations fixing all sufficiently large negative rationals.

  $$A/L \cap R \cong L/L \cap R \times R/L \cap R$$

  $L \cap R$ = order-preserving permutations of bounded support (a function $f : \mathbb{R}^n \to \mathbb{R}$ has **bounded support** if there exists a closed interval $I \subseteq \mathbb{R}^n$ such that $f(x) = 0$ if $x \notin I$.

- The only two non-trivial normal subgroups of symmetric group of countable degree Sym(Ω) are:

  1. FSym(Ω), the finitary symmetric group, consisting of all permutations moving only finitely many points.
  2. Alt(Ω), the alternating group, consisting of finitary permutations which are even permutations of their supports. Alt(Ω) is a normal subgroup of FSym$(\Omega$ of index 2.

- The automorphism group of the random graph is *simple*. Given any two elements g, b with $g \neq 1$, it is possible to write h as the product of three copies of g or g^{-1}.

Small Index Property

Let G be a permutation group of countable degree. A subgroup H has **small index** if $|G : H| < 2^{\aleph_0}$.

- The continuum hypothesis says that there is no set whose cardinality is strictly between that of $\mathbb{R} and \mathbb{Z}$. If this holds, it says that H has finite or countable index.
- The stabiliser of any finite set has small index.
- G has
    - **SIP** if any subgroup of G of small index contains the pointwise stabiliser of a finite set.
    - **strong SIP** if every subgroup of small index lies between the pointwise and setwise stabilisers of a finite set.
- If G is a closed oligomorphic group with SIP, then the topology of G is determined by the following group structure: a subgroup is open if and only if it has small index, so subgroups of small index form a neighborhood basis of identity.

Some groups that have strong SIP are the symmetric group S, $A =$ Group of order-preserving permutatio and Aut(Rado).

A permutation group that does not have strong SIP is S Wr S in its imprimitive action. In general, a permutation group not having strong SIP can be constructed by producing automorphism group of Fraissé limits, which have infinite elementary abelian 2-groups as quotients as they have "too many" subgroups of small index.

An interesting theorem along these lines is the following:

Theorem: Let $\mathcal{C}$ be a non-trivial Fraïssé class with the free amalgamation property and G be the automorphism group of its Fraïssé limit. Then G is simple.

3.4 The Fraïssé limit and Amalgamation properties

Definition 1. Let L be a language. An L-structure is a pair $\mathcal{A} = (A, (Z^{\mathcal{A}})_{Z \in L})$, where

- A is a non-empty set, the universe of $\mathcal{A}$,
- $Z^{\mathcal{A}} \in A$ if Z is a constant,
- $Z^{\mathcal{A}} : A^n \to A$ if Z is an n-ary function symbol, and
- $Z^{\mathcal{A}} \subseteq A^n$ if Z is an n-ary relation symbol.

Definitions 2.

1. A relational structure $\underline{A}$ is called *homogeneous* if every isomorphism between finite substructures of $\underline{A}$ can be extended to an automorphism of $\underline{A}$.

2. The *age* of a τ-structure $\underline{A}$ is the class of all finite τ-structures that embed into $\underline{A}$.

3. A class $\mathcal{C}$ has the *joint embedding property* (JEP) if for any two structures $\underline{B}_1, \underline{B}_2 \in \mathcal{C}$ there exists a structure $\underline{C} \in \mathcal{C}$ that embeds both $\underline{B}_1$ and $\underline{B}_2$, and $B_1 \cup B_2$ is also called the free amalgam of B_1, B_2.

4. A τ-structure C is an amalgam of B_1 and B_2 if for $i \in \{1, 2\}$ there are embeddings f_i of B_i to C such that $f_1(a) = f_2(a)$ for all $a \in B_1 \cap B_2$.

Proposition 3. Let $\mathcal{A}$ be homogeneous with a finite signature. Then $\mathrm{Aut}(\mathcal{A})$ is oligomorphic (and hence $\mathcal{A}$ is ω-categorical).
Proof. By the homogeneity of $\mathcal{A}$, the orbit of an n-element subset B of $\mathrm{Aut}(\mathcal{A})$ is given by the substructure induced by $\mathcal{A}$ on B. But there are finitely many non-isomorphic substructures of $\mathcal{A}$ of size n. As we have seen earlier (2), this also bounds the number of orbits of n-tuples of $\mathrm{Aut}(\mathcal{A})$.

Definitions 4. An isomorphism-closed class $\mathcal{C}$ of finite τ-structures

- has the *free amalgamation property* if for all $\underline{B}_1, \underline{B}_2 \in \mathcal{C}$ the free amalgam of $\underline{B}_1$ and $\underline{B}_2$ is contained in $\mathcal{C}$;

- has the *amalgamation property* if every amalgamation diagram $(\underline{B}_1, \underline{B}_2)$ of structures $\underline{B}_1, \underline{B}_2 \in \mathcal{C}$ has an amalgam $\underline{C} \in \mathcal{C}$;

- is an *amalgamation class* if it contains at most countably many non-isomorphic structures, has the amalgamation property, and is closed under isomorphisms and taking induced substructures.

Some examples of Amalgamation Classes:

1. The class of all finite forests (simple, acyclic graphs)

2. The class of all finite graphs G such that there is no embedding from the 5-cycle into G.

3. Let D be the tournament obtained from the directed cycle C_3 of length three by adding a new vertex u, and adding the edges (u, v) for every vertex v of C_3. Let D' be the tournament obtained from D by flipping the orientation of each edge. The class of all finite tournaments that embeds neither D nor D' is an amalgamation class.

Theorem 5 (Fraïssé). Let τ be a countable relational signature and let $\mathcal{C}$ be an amalgamation class of τ-structures. Then there is a homogeneous and at most countable τ-structure C whose age equals $\mathcal{C}$. The structure C is unique up to isomorphism, and called the *Fraïssé-limit* of $\mathcal{C}$ (often denoted by $\mathrm{Flim}(\mathcal{C})$).

Some examples of Fraïssé limits:

1. Let $\mathcal{C}$ be the class of all **finite graphs**. The Fraïssé-limit of $\mathcal{C}$ is the countable random graph (V, E).

2. The Fraïssé limit of the class of all finite linear orderings is equivalent to the structure $\langle \mathbb{Q}, < \rangle$ up to isomorphism.

Proposition 6. The age of every homogeneous relational structure has the amalgamation property.

Proof. Let $\underline{A}$ be a homogeneous structure and let $(\underline{B}_1, \underline{B}_2)$ be an amalgamation diagram with $\underline{B}_1, \underline{B}_2 \in \mathrm{Age}(\underline{A})$. Then there are embeddings $e_i : \underline{B}_i \hookrightarrow \underline{A}$, for $i \in \{1, 2\}$, and by the homogeneity of $\underline{A}$ there exists an automorphism $\alpha \in \mathrm{Aut}(\underline{A})$ such that $\alpha(e_1(x)) = e_2(x)$ for every $x \in \underline{B}_1 \cap \underline{B}_2$. Let $\underline{C}$ be the substructure of $\underline{A}$ with domain $\alpha(e_1(\underline{B}_1)) \cup e_2(\underline{B}_2)$. Then the embedding $f_1 : \underline{B}_1 \to \underline{C}$ given by $\alpha \circ e_1$ and the embedding e_2 show that $\underline{C}$ is an amalgam of $(\underline{B}_1, \underline{B}_2)$.

Definition: A *strong amalgam* of $\underline{B}_1, \underline{B}_2$ is an amalgam $\underline{C}$ of $\underline{B}_1, \underline{B}_2$ with embeddings $f_i : \underline{B}_i \to \underline{C}$ such that $f_1(\underline{B}_1) \cap f_2(\underline{B}_2) = f_1(\underline{B}_1 \cap \underline{B}_2) = f_2(\underline{B}_1 \cap \underline{B}_2)$. We say that a class $\mathcal{C}$ has the *strong amalgamation property* if all $\underline{B}_1, \underline{B}_2 \in \mathcal{C}$ have a strong amalgam in $\mathcal{C}$.

3.5 The Random Graph and Some of its Relations

Let R denote the countable random graph (Rado Graph)

- R is a countably infinite graph that can be constructed (with probability 1) by choosing independently at random for each pair of its vertices whether to connect the vertices by an edge (i.e. connect each pair of vertices by an edge independently with probability 1/2).

- **(Number theoretic definition:)** Take the base set $S = \{p \mid \text{ prime } p, p \equiv 1 \bmod 4\}$. Join $p, q \in S$ by an edge when $\left(\dfrac{p}{q}\right) = 1 \Longleftrightarrow \left(\dfrac{q}{p}\right) = 1$.

The Extension Property

- An infinite graph Γ has the extension property (EP) if for any two disjoint finite subsets $A, B \subset N$, there is a vertex $v \in N - A - B$ such that v is connected to all vertices in A and no vertices in B.
- Lemma: If Γ_1 and Γ_2 are two infinite graphs, both having EP, then $\Gamma_1 \cong \Gamma_2$.

★ *Any two Rado graphs are isomorphic. Hence, there is only one Rado graph (unique upto isomorphism).*

Properties of the Rado Graph

- R is the **Fraïssé limit** of the class of finite graphs.
- R is homogeneous and contains all finite (and indeed all countable) graphs as induced subgraphs.
- If $G = \mathrm{Aut}(R)$, $\mathrm{F}_n(G)$ is the number of labeled graphs on n vertices $= 2^(n(n-1))/2$.

$\mathrm{f}_n(G)$ = number of unlabeled graphs on n vertices = (asymptotically) $\frac{F_n(G)}{n!}$

Definition: A graph is **homogeneous** if any isomorphism between finite induced subgraphs extends to an automorphism of the graph.

The operation σ_x **of switching** a graph with respect to a set X of vertices consists in replacing edges between X and its complement by non-edges and vice versa, while keeping things inside/outside X the same as before.

A permutation g is a switching automorphism of Γ if $\Gamma^g = \sigma_X(\Gamma)$ for some set X.

1. $\mathrm{S}(R)$ = group of switching automorphisms of R.
2. $\mathrm{B}(R)$ = group of switching automorphisms and anti-automorphisms of R.

There are only 5 closed supergroups of R:

1. $\mathrm{Aut}(R)$
2. $D(R)$ = dualities (automorphisms and anti-automorphisms of $\mathbb{R}$) - is 2-transitive and contains $\mathrm{Aut}(R)$ as a normal subgroup of index 2.
3. $\mathrm{S}(R)$ is 2-transitive.
4. $\mathrm{B}(R)$ is 3-transitive and contains $\mathrm{S}(R)$ as a normal subgroup of index 2.
5. The Symmetric Group

3.6 Miscellaneous Group Theory

Before thinking about the amalgamations of certain kinds of groups, here are some interesting notions in Group Theory, some of which is relevant to the discussion that follows.

A group G is **residually finite** if: (the following definitions are equivalent)

- For every element $g \neq 1_G$, there exists a homomorphism $f : G \rightarrow$ finite group such that $f(g) \neq 1$.
- $\cap$ of all its subgroups of finite index is trivial.
- It can be embedded inside the product of a family of finite groups.
- If for each non-identity element in the group, $\exists$ a subgroup of finite index not containing that element.

G is **residually nilpotent** if it satisfies the following conditions:

- Given any non-identity element, $\exists J \triangleleft G$ not containing the element, such that the quotient group is nilpotent.
- The lower central series reaches the identity element at or before the nth stage.
- The nilpotent residual of the group is the trivial subgroup.
- $\cap$ of all nilpotent-quotient subgroups.
- $\cap$ of all members of the (finite) lower central series of the group $\Rightarrow$ nth member of the transfinite lower central series.

A free product of two finite p-groups amalgamating a cyclic subgroup is residually p-finite.

3.7 The Class of Finite Groups

Let $\mathcal{K}$ be the class of all finite groups. $\mathcal{K}$ is clearly closed under isomorphism and taking induced substructures. It follows the JEP as two finite groups can be embedded in their direct product. We now only have to prove that $\mathcal{K}$ follows the amalgamtion property to see that it has a Fraïssé limit.

Definition 8 Let G be a finite group, $H \subseteq G$ a subgroup. We define the left transversal S of H as the fixed set of left coset representatives (representatives of the aforementioned equivalence classes). Given an element $a \in G$ and its unique product decomposition $a = sh$ in terms of $s \in S$, $h \in H$, we denote $s = a^{\sigma}$, $h = a^{-\sigma+1}$.

Theorem 9 The class $\mathcal{K}$ of all finite groups satisfies the Amalgamation Property.

Proof. See the proof of Theorem 4.13 in [Arr].

The Fraïssé limit of the class of finite groups is known to be *Hall's Universal Group.* The satisfaction of the requirements of Fraïssé's theorem can easily be seen from the definition of the group, and the existence is proved in [Hal59] **Definition 9** Let U be a countable, locally finite group. We say U is Hall's universal group if the following hold:

- Every finite group $G \in \mathcal{K}$ admits an embedding $G \subseteq U$.
- Given $G_0, G_1 \in \mathcal{K}$, any embeddings $f_0 : G_0 \subseteq U, f_1 : G_1 \subseteq U$ are conjugate by some inner automorphism of U.

Demonstration of the Permutational Product:
Consider the Dihedral group $D_8 = \langle x, y \mid x^4 = 1, y^2 = 1\rangle$ and the cyclic group $\mathbb{Z}_8 = \langle r \mid r^8 = 1\rangle$. $D_8 \cap \mathbb{Z}_8 = \mathbb{Z}_4 = \langle r^2 \mid r^8 = 1\rangle = \langle x \mid x^4 = 1\rangle$.

We will build the permutational product of D_8 and $\mathbb{Z}_8$ using the condition in equation 2.1. For that, we have to determine $\rho(\mathbb{Z}_8)$ and $\rho'(D_8)$.

Let the left transversal of $\mathbb{Z}_4$ in $\mathbb{Z}_8$ be $S = \{1, r\}$ and the left transversal of $\mathbb{Z}_4$ in D_8 be $T = \{1, y\}$.

$\rho(\mathbb{Z}_8)$**:** Consider an element $a = r^n \in \mathbb{Z}_8, n \in \{2, 4, 6, 8\}$.

- For $(1, t, r^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho_a(1, t, r^m) = ((r^{n+m})^\sigma, t, (r^{n+m})^{-\sigma+1}) = \begin{cases} (1, t, (r^{n+m})) & \text{m is even} \\ (r, t, (r^{n+m-1})) & \text{m is odd} \end{cases} \tag{3.1}$$

- For $(r, t, r^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho_a(r, t, r^m) = ((r^{n+m+1})^\sigma, t, (r^{n+m+1})^{-\sigma+1}) = \begin{cases} (r, t, (r^{n+m})) & \text{m is even} \\ (1, t, (r^{n+m+1})) & \text{m is odd} \end{cases} \tag{3.2}$$

Now, consider an element $a = r^n \in \mathbb{Z}_8, n \in \{1, 3, 5, 7\}$.

- For $(1, t, r^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho_a(1, t, r^m) = ((r^{n+m})^\sigma, t, (r^{n+m})^{-\sigma+1}) = \begin{cases} (r, t, (r^{n+m-1})) & \text{m is even} \\ (1, t, (r^{n+m})) & \text{m is odd} \end{cases} \tag{3.3}$$

- For $(r, t, r^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho_a(r, t, r^m) = ((r^{n+m+1})^{\sigma}, t, (r^{n+m+1})^{-\sigma+1}) = \begin{cases} (1, t, (r^{n+m+1})) & \text{m is even} \\ (r, t, (r^{n+m})) & \text{m is odd} \end{cases} \tag{3.4}$$

$\rho'(D_8)$: Consider an element $b = y^l x^n \in D_8,\ l \in 0, 1$.

- For $(s, 1, x^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho'_b(s, 1, x^m) = (s, (y^l x^{n+m})^{\tau}, (y^l x^{n+m})^{-\tau+1}) = \begin{cases} (s, 1, x^{n+m}) & l = 0 \\ (s, l, x^{n+m}) & l = 1 \end{cases} \tag{3.5}$$

- For $(y, t, x^m) \in \mathbb{Z}_8 \times D_8 \times \mathbb{Z}_4$

$$\rho_a(s, y, x^m) = (s, (yx^m y^l x^n)^{\tau}, (yx^m y^l x^n)^{-\tau+1}) = \begin{cases} (s, y, (x^{n+m})) & l = 0 \\ (s, 1, (x^{n-m})) & l = 0 \end{cases} \tag{3.6}$$

Clearly, for $h_0 \in \mathbb{Z}_4$, ρ_h and ρ'_h coincide:

$$\rho_{h_0}(s, t, h) = (s, t, hh_0) = \rho'_{h_0}(s, t, h)$$

as required.

3.8 The Class of p-groups

The question I was particularly interested in towards the end of the project was this: *Fixing p, is the class of p-groups a Fraisse class?*

The answer is *no*, and I wrote an article [Jai] to show why that is the case.

Bibliography

[Arr] Roger Asensi Arranz. Fraïssé Limits.

[Bar] Libor Barto. Universal Algebra.

[Boda] Manuel Bodirsky. Automorphism Groups.

[Bodb] Manuel Bodirsky. Graph Homomorphisms and Universal Algebra Course Notes.

[Cam] Peter J. Cameron. Oligomorphic Permutation Groups.

[Hal59] Phillip Hall. Some constructions for locally finite groups. *J. London Math. Soc.*, 34:305–319, 1959.

[Jai] Aahana Jain. Fraïssé Limits and the Class of p-groups.

[McK90] R. McKenzie. Some interactions between group theory and the general theory of algebras. In L.G. Kovács, editor, *Groups—Canberra 1989*, volume 1456 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1990.

[MMT87] Ralph Mckenzie, George McNulty, and Walter Taylor. *Algebras, Lattices and Varieties (Vol 1*. Wadsworth Brooks/Cole, 1987.