# The Structure of Finite Algebras: Tame Congruence Theory

# The Prehistory of Tame Congruence Theory

1. Humans reached anatomical modernity 100,000-300,000 years ago.

   (braincase anatomy, jaw anatomy, skeletal structure)

2. Humans reached cultural modernity 50,000-65,000 years ago.

   (art, symbolic thought, and advanced tool making)

3. Ishango bone dated to 18,000-20,000 years ago.

   (were primes known then?)

4. Gauss introduced the word "congruence" in his thesis in 1801. In a review published in *The Monthly Review; or Literary Journal, Enlarged* we read:

   *M. Gauss begins with new names and new signs. If a number* $\mathbf{a}$ *divides the difference of* $\mathbf{b}$ *and* $\mathbf{c}$*, then* $\mathbf{b}$ *and* $\mathbf{c}$ *are said to be congruous (congrus) according to* $\mathbf{a}$*, which is called the modulus. The sign appropriate to this congruity is* $\equiv$*, so that, in this new symbolical language,* $\mathbf{b} \equiv \mathbf{c}$ (modulus $\mathbf{a}$).

# Congruences on $\langle \mathbb{Z}; \cdot, +, - \rangle$

A congruence on $\mathbb{Z}$ is an equivalence relation $\theta$ that is compatible with the arithmetic operations:

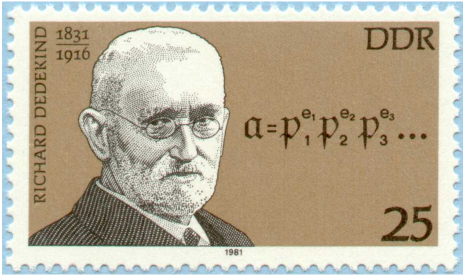
$$\begin{array}{rll} a_1 & \equiv a_2 & \pmod{\theta} \\ b_1 & \equiv b_2 & \pmod{\theta} \\ \hline \\ a_1 \diamond b_1 & \equiv a_2 \diamond b_2 & \pmod{\theta} \end{array}$$

where $\diamond \in \{\cdot, +, -\}$. Say that $\theta$ *is compatible with* $\diamond$, or $\diamond$ *is compatible with* $\theta$, or $\diamond$ is a *polymorphism* of $\theta$.

One can classify the compatible equivalence relations on $\mathbb{Z}$; they are congruence modulo $n$ ($\theta_n$) for some $n \in \{0, 1, 2, \ldots\}$.

These equivalence relations form an algebraic distributive lattice under the operations $\theta_m \vee \theta_n = \theta_m + \theta_n = \theta_{\text{gcd}(m,n)}$ and $\theta_m \wedge \theta_n = \theta_m \theta_n = \theta_{\text{lcm}(m,n)}$.

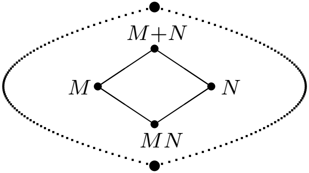
# Congruences on $\langle A; \cdot, +, - \rangle$



Dedekind needed to understand congruences on more general subrings $A \subseteq \mathbb{C}$. He called a subset $M \subseteq \mathbb{C}$ a 'module' if it could serve as the modulus of a congruence of some such ring.

"$a \equiv b \pmod{M}$" means $a - b \in M$. Congruence mod $M$ is an equivalence relation iff $M \subseteq \mathbb{C}$ is an additive subgroup.

The collection of 'modules' is a 'lattice' under inclusion, and Dedekind investigated the arithmetic of this lattice.



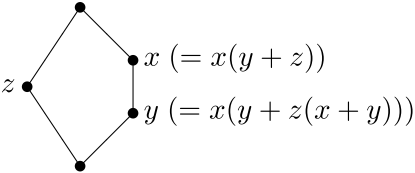
# Some of Dedekind's results

**Thm.**

- The 'lattice' of 'modules', $\mathbf{Con}(\mathbb{C})$, satisfies the *modular law*:

$$x(y+z) \approx x(y+z(x+y)).$$

- The modular law holds in a lattice iff the lattice contains no pentagon as a sublattice.



- The sublattice of 'modules' generated by $X = \langle 10, 1+15\sqrt{2}\rangle$, $Y = \langle 15, 1+10\sqrt{2}\rangle$, and $Z = \langle 15, 1+6\sqrt{2}\rangle$ is free and has 28 elements.
- A 3-variable identity holds in the lattice of modules iff it is a consequence of the modular law.

# The Grätzer-Schmidt Theorem

It is not hard to prove that the lattice of congruences of any algebra is an 'algebraic' lattice. (That is, it is a complete lattice that is generated under complete join by its compact elements.)

Grätzer and Schmidt proved the converse.

**G-S Thm.** (1963) Every algebraic lattice is representable as the congruence lattice of an algebra.

Their construction produces an infinite algebra even in the case where one wants to represent a finite lattice.

**Open Question.** Is every finite lattice the congruence lattice of a finite algebra?

# The $P^5$ paper

Péter Pál Pálfy and Pavel Pudlák attacked the preceding open problem and proved that

**$\mathbf{P^5}$ Thm.** (1980) The following are equivalent:

1. every finite lattice is the congruence lattice of a finite algebra.
2. every finite lattice is the congruence lattice of a finite $G$-set.
3. every finite lattice is an interval in the subgroup lattice of some finite group.

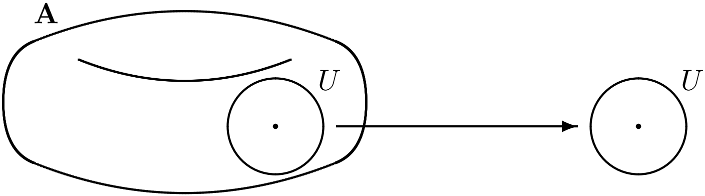
Discuss $M_n$. Smallest undecided cases are $M_{16}, M_{23}, M_{35}$.

# The History of Tame Congruence Theory

McKenzie used the techniques of the $P^5$ paper to extend the $P^5$ results in *Finite Forbidden Lattices* (1982). In 1983, Hobby and McKenzie began to develop these techniques more and they published their results in *The Structure of Finite Algebras* (1988). This book uses model-theoretic inspiration to develop a localization theory for finite algebras.

# Tame Congruence Theory is a Localization Theory

This means that the theory is based on a method for selecting small subsets of an algebra, restricting structure to that subset, calculating locally, and piecing together local data to solve globally stated problems.



There are three main ingredients to a localization theory.

1. Localization: Identify subsets which support good local approximations. Describe how to restrict structure to these "neighborhoods".
2. Classification: Describe how to calculate locally.
3. Globalization: Describe how to combine local results.

# The ‘simplest’ setting

Assume that $\mathbb{A}$ is a finite simple algebra. (“Simple” means: the only nontrivial proper congruences are the trivial and the total congruences.) TCT defines a subset $U \subseteq A$ to be a *neighborhood* of $\mathbb{A}$ if $U = e(A)$ is the image of an idempotent unary polynomial operation $e$ of $\mathbb{A}$. ($e(x) \in \mathrm{Pol}_1(\mathbb{A})$, $e(e(x)) = e(x)$.) TCT asserts that:

1. minimal neighborhoods of $\mathbb{A}$ exist and any two are polynomially isomorphic.
2. the points of $A$ are separated by the unary polynomials whose ranges are minimal neighborhoods.
3. $A$ is the connected union of its minimal neighborhoods.
4. the minimal localizations $\mathbb{A}|_U = \langle U; \{ef \mid f \in \mathrm{Pol}(\mathbb{A})\}\rangle$ are pairwise polynomially isomorphic.
5. each minimal localization is one of the following types:
    1. (type $\mathbf{1}$) a simple $G$-set.
    2. (type $\mathbf{2}$) a 1-dimensional vector space over a finite field.
    3. (type $\mathbf{3}$) a 2-element Boolean algebra.
    4. (type $\mathbf{4}$) a 2-element lattice.
    5. (type $\mathbf{5}$) a 2-element semilattice.

# An example

Let $\mathbb{F}$ be a finite field. Let $M = \mathbb{F}^2$ be a module over the ring $R = M_2(\mathbb{F})$. $M$ is a finite simple $R$-module. The idempotent unary polynomials of $M$ have the form $E(x) = ex + v$ where $e \in R$ satisfies $e^2 = e$ and $ev = 0$.

The identity polynomial $E(x) = x$ on $M$ is one of these, so $M$ itself is a neighborhood of itself. Any constant polynomial $E(x) = v$ is idempotent, so singleton subsets of $M$ are neighborhoods.

Else $E(x) = ex + v$ for an idempotent element $e \in R$ of rank one. The image $E(M) = U$ is a coset of a 1-dimensional subspace of $\mathbb{F}^2$. (Conversely, every coset of a 1-dimensional subspace is a neighborhood. The 'geometry of neighborhoods' is the ordinary plane geometry consisting of points, lines, whole plane.) The structure $M|_U$ is that of an $eRe$-module on the set $U$. $eRe$ is a field isomorphic to $\mathbb{F}$, so $M|_U$ is a 1-dimensional vector space. (The type of $M|_U$ is $\mathbf{2}$: 'vector space type' or 'affine type'.)

# Nonsimple examples

Let $\mathbf{L} = \langle L; \vee, \wedge\rangle$ be a lattice. Restriction to an interval, $[a, b]$, $a < b$, is an instance of localization. The function $e(x) = a \vee (b \wedge x)$ is an idempotent unary polynomial whose image is $[a, b]$, so intervals are neighborhoods. This implies that intervals of $L$ are good local approximations of $L$. Here, $U = e(L)$ will have lattice polynomial operations $\vee|_U$ and $\wedge|_U$, and possibly more induced polynomial operations.

Similarly, restriction to a principal ideal $[0, b]$ in a Boolean, $\mathbf{B}$, algebra is an instance of localization. $e(x) = b \wedge x$. $U = e(B)$ has underlying Boolean algebra polynomials $\vee|_U, \wedge|_U, e(\neg x), 0, b$.

A Sylow $p$-subgroup $P$ of a finite group $G$ is an example of a neighborhood of $G$. It need not be a minimal neighborhood, but it will be minimal if $G$ is nilpotent. The localization $G|_P$ includes the group operations on $P$, but will typically contain additional structure (unless $P$ is a direct factor of $G$).

# Applications

**Applications from the book.** (All assume some finiteness conditions.)

1. Classication of varieties by Maltsev conditions.
2. Understanding the structure of residually small varieties.
3. Understanding the structure of decidable varieties.
4. Understanding the free spectrum function.
5. Understanding the structure of simple algebras.

**Some later applications.**

1. Classification of minimal (abelian) varieties.
2. Understanding congruence identities.
3. CSP applications.
4. Growth rates of finite algebras.
5. Understanding the structure of varieties with many projective and free algebras.