On Clone Congruences and Simple Clones With Mal’cev Operation

MASTERARBEIT
zur Erlangung des akademischen Grades
Diplom-Ingenieur
im Masterstudium
Computermathematik

Eingereicht von:
Neumüller Mario, Bakk. techn.

Angefertigt am:
Institut für Algebra

Beurteilung:
Assoz. Univ.-Prof. Dipl.-Ing. Dr. Erhard Aichinger

Linz, August 2015
Abstract

In this thesis we interpret clones as algebras, and we study their congruences and simple clones. In the first part we follow the approach form A.I. Mal’cev and interpret a clone \( H \) on a set \( A \) as an algebra \( H = (H; \ast, \xi, \tau, \triangle, \pi_1^2) \). Furthermore we study an additional approach to interpret \( H \) as an algebra which includes functions of infinite arity and again study the congruences of the resulting algebra. Moreover we will investigate connections between the congruences of the clone of term functions of an algebra \( A := (A; H) \), its equational theory, and subvarieties of \( V(A) \).

In the second part we are preparing for the main goal of this thesis, which is characterizing the simple clones with Mal’cev operation. Therefore we need to study quasi primal algebras, commutator theory, affine algebras and minimal varieties.

At the end we are able to give a characterization when a clone \( H \) is simple provided it has a Mal’cev operation.
Zusammenfassung


Im zweiten Teil erarbeiten wir uns die nötige Theorie, die wir benötigen um die Charakterisierung der einfachen Klone mit Mal’cev Operation durchzuführen. Unter anderem befassen wir uns mit quasi-primalen Algebren, Kommutatortheorie, affinen Algebren und minimalen Varietäten.

Im letzten Teil geben wir eine Charakterisierung der einfachen Klone mit Mal’cev Operation an.
Acknowledgments

First and foremost I would like to thank my supervisor Assoz.Univ-Prof. Erhard Aichinger for answering my questions and guiding me during the process of writing this thesis. But mostly I want to thank him for inspiring me in various lectures and furthermore I am thankful that he taught me basically everything I know in algebra, starting from linear algebra up to universal algebra.

Further I wish to express my sincere thanks to my parents who supported me every single day. Without them I would not have been able to dedicate all of my focus on my studies.

Last but not least I am very grateful to my colleagues who made my life easier in various situations by helping me out and I am thankful that in this 5 years of studying some of them have become close friends.

Neumüller Mario
Linz, July 2015
Contents

1 Introduction
   1.1 Preliminaries ............................................. 1

2 Congruences on Clones .................................... 3
   2.1 Clones interpreted as subalgebras of $M_A$ ................. 3
   2.2 Congruences of Boolean clones .............................. 8
   2.3 Subdirectly irreducible clones .............................. 14
   2.4 Fully invariant congruences, subvarieties and clone congruences . 16
   2.5 Clones of functions with infinite arity .................... 20
   2.6 Left and right congruences ................................ 24

3 Preparing Topics .............................................. 29
   3.1 Quasi-primal algebras ...................................... 29
   3.2 Commutator theory ......................................... 32
   3.3 Affine algebras ............................................ 43

4 Simple Clones ............................................... 47
   4.1 Minimal varieties ......................................... 47
   4.2 Simple clones and maximal congruences .................... 50
Kapitel 1

Introduction

Clone Theory has its beginning in different fields such as logic, universal algebra, or computer science (circuit theory). There are plenty of equivalent definitions but one of the most elementary definitions is the following

Definition 1.1. Let $A$ be a nonempty set. A subset $C \subseteq \{ f : A^n \rightarrow A \mid n \in \mathbb{N} \}$ is called clone on $A$ if $C$ satisfies the two properties beneath.

1. $\{ \pi^n_i \mid n \in \mathbb{N}, i \leq n \} \subseteq C$, where $\pi^n_i : A^n \rightarrow A$ is the $i$-th projection map.

2. If $f, g_1, \ldots, g_m \in C$, $f$ is a $m$-ary function, and $g_1, \ldots, g_m$ are $k$-ary functions then $f(g_1, \ldots, g_m) \in C$ where
   
   $(f(g_1, \ldots, g_m))(x_1, \ldots, x_k) = f(g_1(x_1, \ldots, x_k), \ldots, g_m(x_1, \ldots, x_k))$
   
   for $x_1, \ldots, x_k \in A$.

At first glance this definition does not allow us to use the machinery of universal algebra since $C$ is just a set of functions and has no underlying algebraic structure.

One way to overcome this situation was given by A. I. Mal’cev by interpreting $C$ as a subuniverse of the algebra $(O(A); *, \xi, \tau, \triangle, \pi^n_i)$ of type $(2, 1, 1, 1, 0)$. The universe $O(A)$ of this algebra are all finitary functions on $A$ and the fundamental operations model the properties of a clone. We will also present an additional possibility to transform $C$ into a subuniverse of an algebra $(A^{\mathbb{N}}; \circ, (\pi_i), i \in \mathbb{N})$ where the universe is the set of all functions of infinite arity (see section 2.5).

Now with these approaches a clone $C$ is just a certain algebra and we are able to use the concepts of universal algebra in order to study the properties of $C$. We will dedicate a certain focus on the congruences of a clone and on those clones (with a Mal’cev operation) that only have trivial congruences, called simple clones.

1.1 Preliminaries

We assume that the reader is familiar with the basic concepts of universal algebra (for example as described in [2]). The following listing contains the definitions and notations of the most frequently used terms and objects in this thesis.
• If not stated otherwise, \( A \) will denote a finite set.

• \( O^{[n]}(A) := \{ f : A^n \rightarrow A \} \) will denote the set of all \( n \)-ary functions on \( A \). \( O(A) := \bigcup_{n \geq 1} O^{[n]}(A) \). For \( F \subseteq O(A) \), \( F^{[n]} := F \cap O^{[n]}(A) \).

• For \( F \subseteq O(A) \), \( \langle F \rangle := \bigcap \{ H \mid H \) is a clone on \( A \), \( F \subseteq H \} \) denotes the smallest clone containing \( F \).

Let \( \pi_i^n : A^n \rightarrow A \), \( \pi_i^n(x_1, \ldots, x_n) := x_i \) be the \( i \)-th projection map on \( A \). The clone of all projections on \( A \) is denoted by \( J_A := \{ \pi_i^n : A^n \rightarrow A \mid n \in \mathbb{N}, i \leq n \} \).

Let \( c_a^n : A^n \rightarrow A \), \( c_a^n(x_1, \ldots, x_n) := a \) be the \( n \)-ary constant function with value \( a \). The set of all constant functions is denoted by \( C_A := \{ c_a^n \mid a \in A, \ n \in \mathbb{N} \} \).

• We will write sometimes \( f(\vec{x}) \) instead of \( f(x_1, \ldots, x_n) \) if \( n \) is clear from the context. For \( f \in O^{[1]}(A) \) and \( k \in \mathbb{N} \), \( f^k(x) := f(\ldots f(f(x))\ldots) (k \text{ times}) \).

• Algebras will be denoted by \( A, B, \ldots \) (sometimes also by capital bold letters \( A, B, \ldots \)) and their types by \( \mathcal{F}_A, \mathcal{F}_B, \ldots \).

• For an algebra \( A \) the congruence lattice of \( A \) will be denoted by \( \text{Con}(A) \) and \( \nabla := \{(a, b) \mid a, b \in A \} \), \( \Delta := \{(a, a) \mid a \in A \} \). If \( B \subseteq A^2 \) then we will write \( \text{Cg}(B) \) for the congruence generated by \( B \).

• Let \( A := (A; F) \) be an algebra, then \( T(A) \) denotes the terms using the operation symbols of \( A \) in the variables \( \{x, y, z\} \cup \{x_i \mid i \in \mathbb{N}\} \).

\( \text{Clo}(A) := \langle F \rangle \) will be the set of term functions of \( A \) and \( \text{Pol}(A) := \langle F \cup C_A \rangle \) the set of polynomial functions on \( A \).

• \( \mathcal{V} \) will denote a variety. For a variety generated by an algebra \( A \) we write \( V(A) \). The set of all subvarieties of \( \mathcal{V} \) is abbreviated by \( \text{Su}(\mathcal{V}) \). The free algebra for the variety \( \mathcal{V} \) freely generated by the set \( X \) is denoted by \( F_{\mathcal{V}}(X) \).

For a variety \( \mathcal{V} \) of type \( \mathcal{F} \) and a set of variables \( X \), an identity of \( \mathcal{V} \) is abbreviated by \( p \approx q \), where \( p, q \) are terms of \( \mathcal{V} \) over \( X \). \( \text{Id}(X) \) is the set of all identities of type \( \mathcal{F} \) over \( X \). \( \text{Id}_\mathcal{V}(X) \) will denote all identities fulfilled by \( \mathcal{V} \) over \( X \).

Let \( \Sigma \subseteq \text{Id}(X) \). Then \( \text{Mod}(\Sigma) \) is the variety generated by \( \Sigma \). We will write \( T \) for \( \text{Mod}(\{x \approx y\}) \) (trivial variety).
Kapitel 2

Congruences on Clones

In this chapter we will interpret a clone on a set $A$ as an object in universal algebra. This means we are trying to equip a clone with an algebraic structure such that we can use the concepts of universal algebra (e.g. congruences) to study clones. To do so we follow the approach of A.I. Mal'cev in [9].

2.1 Clones interpreted as subalgebras of $\mathbb{M}_A$

Definition 2.1. Let $A$ be a nonempty set. Let $\mathbb{M}_A := (O(A), *, \xi, \tau, \triangle, e)$ be an algebra of type $(2,1,1,1,0)$, where for all $m, n \in \mathbb{N}$, for all $f \in O(A)^m$ and $g \in O(A)^n$ we have that

1. $(f * g)(x_1, \ldots, x_{m+n-1}) := f(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_{m+n-1})$.
2. $(\xi f)(x_1, \ldots, x_n) := f(x_2, x_3, \ldots, x_n, x_1)$ if $n > 1$ and $(\xi f)(x_1) := f(x_1)$ if $n = 1$.
3. $(\tau f)(x_1, \ldots, x_n) := f(x_2, x_1, x_3, \ldots, x_n)$ if $n > 1$ and $(\tau f)(x_1) := f(x_1)$ if $n = 1$.
4. $(\triangle f)(x_1, \ldots, x_{n-1}) := f(x_1, x_1, x_2, \ldots, x_{n-1})$ if $n > 1$ and $(\triangle f)(x_1) := f(x_1)$ if $n = 1$.
5. $e(x_1, x_2) := x_1$

We call a subalgebra of $\mathbb{M}_A$ a clone on $A$. Additionally let $C(A)$ denote the set of all subuniverses of $\mathbb{M}_A$. We will call a clone in the sense of Definition 1.1 a clone of functions.

Notation. If $H \in C(A)$ we will denote the associated clone on $A$ i.e. $(H; *, \xi, \tau, \triangle, e)$, by $\mathbb{H}$.
Since a clone of functions $C$ on a set $A$ is closed under composition (definition 1.1) and is also closed under identifying and permuting variables, it follows that $C$ is closed under $\ast, \xi, \tau$ and $\triangle$. In other words each clone of functions $C$ on a set $A$ can be interpreted as a subuniverse of $\mathbb{M}_A$. The next Lemma shows that the other direction is also true.

**Lemma 2.2.** Let $A$ be a nonempty set, then every subuniverse of $\mathbb{M}_A$ is a clone of functions on $A$.

**Proof.** Let $\mathbb{H} \subseteq \mathbb{M}_A$. First of all we have to show that $J_A \subseteq H$. This follows by an inductive argument and the fact that for all $n, k \in \mathbb{N}$ we have:

$$\pi_1^n \ast \pi_1^2 = \pi_1^{n+1} \text{ and } \xi(\pi_k^n) = \begin{cases} \pi_1^n & k = n \\ \pi_k^{n+1} & k < n \end{cases}. \quad (2.1)$$

Let now $n, m \in \mathbb{N}$, $f \in H^{[n]}$ and $g_1, \ldots, g_n \in H^{[k]}$. We have to prove that $f(g_1(x_1, \ldots, x_k), \ldots, g_n(x_1, \ldots, x_k)) \in H$. The proof will be done in 2 steps. First of all we prove that

$$f(g_1(x_1, \ldots, x_k), g_2(x_{k+1}, \ldots, x_{2k}), \ldots, g_n(x_{k(n-1)+1}, \ldots, x_{nk})) \in H$$

and then we show

if $f(x_1, \ldots, x_{nk}) \in H$ then $h(x_1, \ldots, x_k) := f(x_1, \ldots, x_k) \overbrace{\cdots \overbrace{x_1, \ldots, x_k}}^{\text{n times}} \in H$.

Let us begin with proving the first step and define the functions $h_i$ recursively for $1 \leq i \leq n$

$$h_1(x_1, \ldots, x_{n+k-1}) := \xi^{n-1}(f \ast g_1)$$
$$h_i(x_1, \ldots, x_{n+ik-1}) := \xi^{ar(h_{i-1})} \ast g_i$$

Clearly for all $1 \leq i \leq n$, $h_i \in H$ and we see that

$$h_n(x_1, \ldots, x_{nk}) = f(g_1(x_1, \ldots, x_k), g_2(x_{k+1}, \ldots, x_{2k}), \ldots, g_n(x_{k(n-1)+1}, \ldots, x_{nk})) \in H.$$ 

For the second step let $p(x_1, \ldots, x_{nk}) \in H$. For $n = 1$ we see that the statement is obvious. Let $n > 1$ and assume the property is true for $1 \leq m < n$. We know

$$\triangle((\xi^2 \triangle)^{k-1})(p) \in H.$$ 

But

$$\triangle((\xi^2 \triangle)^{k-1}(p))(x_1, \ldots, x_{(n-1)k}) = p(x_k, x_{k+1}, \ldots, x_{(n-1)k}, x_1, x_2, \ldots, x_{k-1}, x_{k-1}).$$
Notice that we can generate any permutation of \( \{x_1, \ldots, x_{nk}\} \) with the operations \( \tau \) and \( \xi \). Let \( \sigma \in H \) such that \( \sigma(p)(x_k, x_{k+1}, \ldots, x_{(n-1)k}, x_1, x_2, \ldots, x_{k-1}, x_{k-1}) = p(x_1, \ldots, x_{(n-1)k}, x_1, \ldots, x_k) \). Now we have that
\[
g(x_1, \ldots, x_{(n-1)k}) := \Delta((\xi^2 \Delta)^{k-1}(\sigma(p)))(x_1, \ldots, x_{(n-1)k}) \in H
\]
and
\[
g(x_1, \ldots, x_{(n-1)k}) = p(x_1, \ldots, x_{(n-1)k}, x_1, \ldots, x_k).
\]
But this function only depends on \((n-1)k\) variables and the statement follows by the induction hypothesis.

**Definition 2.3.** Let \( A \) be a nonempty set, \( H \subseteq C(A) \). \( \theta \subseteq H^2 \) is called a congruence of \( H \) if it is a congruence of \( \mathbb{H} = (H; \ast, \xi, \tau, \Delta, e) \).

**Definition 2.4.** Let \( A \) be a nonempty set. We define a unary function \( ar : O(A) \to \mathbb{N} \), and we let \( ar(f) \) be the \( n \in \mathbb{N} \) with \( f \in O^{[n]}(A) \).

**Example 2.5.**
Let \( H \subseteq C(A) \). It is not hard to check that
\[
\kappa := \{(f, g) \in H^2 \mid ar(f) = ar(g)\}
\]
is really a congruence of \( H \). \( \kappa \) is called the **arity congruence**.

**Example 2.6.**
Let \( H \) be the clone generated by \( + \) and \( \neg \) where \( + : \{0, 1\}^2 \to \{0, 1\} \) is the addition modulo 2 and \( \neg : \{0, 1\} \to \{0, 1\} \) is the negation operation.
Then \( \kappa_c := \{(f, g) \mid ar(f) = ar(g) \land \exists c \in \{0, 1\} : f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) + c\} \) is a congruence.

**Example 2.7.** The following examples of clone congruences can be found in [8]. Let \( A := \{1, \ldots, k\} \):

1. Let \( \rho \) be a unary relation on \( A \) with \( 2 \leq |\rho| \leq k-1 \) and let \( \kappa_{0,\rho} \) be defined by
\[
(f, g) \in \kappa_{0,\rho} \iff ar(f) = ar(g) \land \{f, g\} \subseteq Pol_k(\rho) \land (\forall \bar{x} \in \rho^{ar(f)} : f(\bar{x}) = g(\bar{x})).
\]
Then \( \kappa_{0,\rho} \) is a congruence on \( Pol(\rho) \).

2. Let \( \rho \in Eq(A) \) and let \( \kappa_E \) be defined by
\[
(f, g) \in \kappa_E :\iff ar(f) = ar(g) \land \{f, g\} \subseteq Pol(\rho) \land (\forall \bar{a} \in A^{ar(f)}(f(\bar{a}), g(\bar{a})) \in \rho).
\]
Then \( \kappa_E \) is a congruence on \( Pol(\rho) \).
3. If we consider closed classes, this means subalgebras of \((O(A); *, \xi, \tau, \triangle)\), we can even find classes with continuum many congruences. (Note that closed classes correspond to sets of functions that are closed under composition but do not necessarily contain all projection maps.)

First of all we give an example of a closed class \(C\) of \(O(A)\) with an infinite basis (this example was first published by J. I. Janov and A. A. Mucnik in 1959):

\[
g^n_{I, J}(x_1, \ldots, x_n) := \begin{cases} 
1 & \exists i \in I : (x_i \in \{1, 2\} \land (\forall x_j \in J \cup (I \setminus \{i\}) : x_j = 2)) \\
0 & \text{else}
\end{cases}
\]

for disjoint subsets \(I, J\) of \(\{1, \ldots, n\}\).

\[
C := \bigcup_{n \geq 1} \{g^n_{I, J} \mid I, J \subseteq \{1, \ldots, n\} \land I \cap J = \emptyset\}
\]

\[
B := \{g^n_{\{1, \ldots, n\}, \emptyset} \mid n \in \mathbb{N}\}
\]

Then for \(B, C\), we have:

(a) \(C\) is a subclass of \(A\).

(b) \(\forall n \in \mathbb{N} : g^n_{\{1, \ldots, n\}, \emptyset}\) can not be generated by \(B \setminus \{g^n_{\{1, \ldots, n\}, \emptyset}\}\).

(c) \(B\) is an infinite basis for \(C\).

A proof of these properties can be found in [8]. Now we can define a congruence on \(C\) for each subset \(N \subseteq \mathbb{N}\)

\((s, t) \in \kappa^N :\iff\)

\(\{s, t\} \subseteq C \land ar(t) = ar(s) \land (s = t \lor \{s, t\} \subseteq \{g^n_{I, J} \mid n \in \mathbb{N} \land |I| = N \lor I \neq \emptyset \lor I = J = \emptyset\}\).

Note that for \(N \neq N'\) we have that \(\kappa^N \neq \kappa^{N'}\). (This follows for example from the fact that if \(I, I' \neq \emptyset\) then \((g^n_{I, \emptyset}, g^n_{I', \emptyset}) \in \kappa^N\) if \(|I|, |I'| \in \mathbb{N}\).) Therefore there must be continuum-many congruences on the closed class \(C\).

**Lemma 2.8.** Let \(H\) be in \(C(A)\). Then \(\kappa\) is the only maximal congruence of \(H\).

**Proof.** Assume \(\theta \in \text{Con}(\mathbb{H})\) with \(\kappa \subset \theta \subset \nabla\). Then there exist \((f, g) \in \theta\) such that \(ar(f) = n > m = ar(g)\). Since \(\theta\) is a congruence we get that \((\Delta^{n-1}f, \Delta^{n-1}g) \in \theta\) and
therefore \((\pi_n^* (\triangle n^{-1} f), \pi_n^* (\triangle n^{-1} g)) \in \theta\). Now we have
\[
(\pi_n^* (\triangle n^{-1} f))(x_1, \ldots, x_{n+1}) = \pi_n^*(\triangle n^{-1} f(x_1, x_2, x_3, \ldots, x_{n+1})
\]
\[= \pi_n^*(f(x_1, \ldots, x_1, x_2, x_3, \ldots, x_{n+1})
\]
\[= x_{n+1}
\]
\[
(\pi_n^* (\triangle n^{-1} g))(x_1, \ldots, x_{n+1}) = \pi_n^*(\triangle n^{-1} g(x_1), x_2, \ldots, x_n)
\]
\[= \pi_n^*(g(x_1, \ldots, x_1), x_2, \ldots, x_n)
\]
\[= x_n.
\]
This means \((\pi_{n+1}^*, \pi_n^*) \in \theta\). Observe that by applying \(\xi\), \(\triangle\) and by substituting \(\pi_1^2\) via * we get that \(\forall r \in \mathbb{N}: (\pi_{r+1}^*, \pi_r^*) \in \theta\). Let \(h \in H\) and \(ar(h) = k\). Since \((\pi_2^2, \pi_1^1) \in \theta\) we obtain \((\pi_2^* \circ h, \pi_1^* \circ h) = (\pi_2^*(h(x_1, \ldots, x_k), x_{k+1}), \pi_1^*(h(x_1, \ldots, x_{k+1}))) = (\pi_{k+1}^*, h) \in \theta\).

Let \(h \in H\) with \(ar(h) = k\). Of course we have \((\pi_{k+1}^*, \tilde{h}) \in \theta\) and by transitivity also \((\pi_{k+1}^*, \pi_{k+1}^*) \in \theta\) and finally \((h, \tilde{h}) \in \theta\) which implies \(\theta = \nabla\).

\(\square\)

**Remark 2.9.** 1. In [3, Definition 4.1] we find an equivalent definition of clone congruences which refers to our Definition 1.1 of a clone. This definition is the following

**Definition 2.10.** Let \(C\) be a clone on set \(A\). A binary relation \(\alpha \subseteq C \times C\) is called a **clone congruence** if

(a) \((f, g) \in \alpha\) then \(ar(f) = ar(g)\).

(b) \(\alpha\) is an equivalence relation.

(c) \((f, \tilde{f}) \in \alpha^{[m]}\) and \((g_i, \tilde{g}_i) \in \alpha^{[n]}\) for \(i \in \{1, \ldots, m\}\) then
\[
(f(g_1, \ldots, g_m), \tilde{f}(\tilde{g}_1, \ldots, \tilde{g}_m)) \in \alpha^{[n]}.
\]

2. Since \(\kappa\) is the only maximal congruence of \(\text{Con}(\mathbb{H})\) for a clone of functions \(H\) it is natural to consider \(\mathbb{H}/\kappa\).

One can easily prove the following \(\mathbb{H}/\kappa \cong \mathbb{S} := (\mathbb{N}, \ast^\mathbb{S}, \triangle^\mathbb{S}, \tau^\mathbb{S})\), where the operations are defined in the following way. For \(n, m \in \mathbb{N}\)

\[
n \ast^\mathbb{S} m := n + m - 1, \tau^\mathbb{S}(n) = \xi^\mathbb{S}(n) := n\ 	ext{and} \ \Delta^\mathbb{S}(n) = \begin{cases} n - 1 & n > 1 \\ 1 & n = 1 \end{cases}
\]

We can see this by the mapping \(\phi : H/\kappa \to \mathbb{N}, f \mapsto ar(f)\), which is well defined by the definition of \(\kappa\), and an isomorphism.
3. Schweigert already mentioned in [14, Remark 1.3-1.5] that one could consider to construct direct products, subalgebras and homomorphic images of clones. We have already seen that every subalgebra of a clone $C$ is a clone of functions on $A$. If one considers a countable direct product of clones on a set $A$ this could be the motivation to think about clones of functions with functions of infinite arity. Let $C$ be a clone on $A$. Consider the direct product

$$
\Pi_{n \in \mathbb{N}} C = \{(f_1, f_2, \ldots) \mid \forall i \in \mathbb{N} : f_i \in C\}.
$$

For example the sequence of functions $(\pi^i_{n})_{i \in \mathbb{N}} \in \Pi_{n \in \mathbb{N}} C$. One can interpret this sequence as a function of infinite arity. We will see more details about this interpretation in a later section.

4. Let $f \in O^{[n]}(A)$ and define $g : A^{n+1} \rightarrow A, (x_1, \ldots, x_{n+1}) \mapsto f(x_1, \ldots, x_n)$. This means $f$ and $g$ differ only in dummy variables but since $ar(f) < ar(g)$ we get from Lemma 2.8 that $Cg((f, g)) = \nabla$. This situation will be the motivation for an interpretation of clones with functions of infinite arity (see section 2.5).

### 2.2 Congruences of Boolean clones

We call a clone on a set $A$ a **Boolean clone** if $A = \{0, 1\}$. In this section we are focusing on the congruences of the subalgebras of $M_{A,0,1}$.

The following lemma will be useful for several times especially in the proof of the next theorem.

**Lemma 2.11.** Let $\mathbb{H} \leq M_{A}$ and $\theta \in \text{Con}(\mathbb{H})$. If

1. $(\pi^n_i, \pi^n_j) \in \theta$ for $i \neq j$ or
2. $(\pi^n_i, c^a_n) \in \theta$ for some $a \in A$

then $\theta = \kappa$.

**Proof.** First of all assume $i > j$. Since $(\pi^n_i, \pi^n_j) \in \theta$ we also know that $(\xi^{n-i+1}(\pi^n_i), \xi^{n-i+1}(\pi^n_j)) = (\pi^n_1, \pi^n_j) \in \theta$ for $j' = n - i + 1 + j$. For $f \in H[k], k \in \mathbb{N}$ we have

$$
\Delta^{n-1}(\xi^{n-1}(\pi^n_1 * f))(x_1, \ldots, x_k) = \xi^{n-1}(\pi^n_1 * f)(x_1, \ldots, x_1, x_1, \ldots, x_k)
\quad = (\pi^n_1 * f)(x_1, \ldots, x_k, x_1, \ldots, x_1)
\quad = \pi^n_1(f(x_1, \ldots, x_k), x_1, \ldots, x_1)
$$

Analogous we get that $\Delta^{n-1}(\xi^{n-1}(\pi^n_j * f))(x_1, \ldots, x_k) = \pi^n_j(f(x_1, \ldots, x_k), x_1, \ldots, x_1)$. Therefore $(\Delta^{n-1}(\xi^{n-1}(\pi^n_1 * f))(x_1, \ldots, x_k), \Delta^{n-1}(\xi^{n-1}(\pi^n_j * f))(x_1, \ldots, x_k)) = (f, \pi^n_1) \in$
\(\theta\). With the help of the transitivity of \(\theta\) we get for all \(k \in \mathbb{N}\) and \(f, g \in H^k\) that 
\((f, g) \in \theta\).
Assume now that \((\pi^n_i, c^n_a) \in \theta\) and let \((f, g) \in \kappa\). Thus \((\pi^n_i, c^n_a) \in \kappa\) then either \(i = 1\) or \(i \neq 1\) and therefore \((\pi^n_i, c^n_a) = (\xi^{-1}(\pi^n_i), \xi^{-1}(c^n_a)) \in \kappa\). Hence, \((\pi^n_i \ast f, c^n_a), (\pi^n_i \ast g, c^n_a) \in \kappa\) and by transitivity \((\pi^n_i \ast f, \pi^n_i \ast g) \in \kappa\). Finally by identifying the correct variables we get that \((f, g) \in \kappa\).

If we restrict ourselves to Boolean clones of functions (i.e. clones of functions on \(A = \{0, 1\}\)) the congruences have been fully characterized by Gorlov in [5].

**Theorem 2.12.** Each congruence lattice of a Boolean clone has one of the following forms

\[
\begin{array}{c|c}
\kappa & \kappa \\
\hline
\text{L}_4 & \text{All other Boolean clones} \\
\end{array}
\]

where \(\kappa_c := \{(f, g) \mid \text{ar}(f) = \text{ar}(g) \land \exists a \in \{0, 1\} : f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) + a\}\), 
\(\text{L}_4 := \langle +^{(3)} \rangle, \text{L}_5 := \langle +^{(3)}, \neg \rangle\) and \(+^{(3)}\) and \(+\) are the binary and ternary addition modulo 2.

**Remark 2.13.**
1. A direct consequence of the theorem above is that every Boolean clone is subdirectly irreducible.
2. In [5] Gorlov, even proved a more general version of Theorem 2.12. He characterized all congruences of closed post classes (a set of boolean functions closed under composition but not necessarily containing all projections).

**Proof of Theorem 2.12:**

Let \(\text{maj} : \{0, 1\}^3 \to \{0, 1\}\) be the majority function, let \(+^{(3)} : \{0, 1\}^3 \to \{0, 1\}\) denote the ternary plus modulo 2 and let \(+ : \{0, 1\} \to \{0, 1\}\) denote the plus modulo 2.

We consider the following clones of Boolean functions (we stick to the notation of E. Post of [13]):

\(D_3 = \langle \text{maj}, \neg \rangle\) (clone of self-dual boolean functions),

\(L_1 = \langle +, \neg \rangle = \{f \in O(\{0, 1\}) \mid \exists a_0, \ldots, a_1 \in \{0, 1\} : f(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} a_i x_i\}\)

( Note that \(c_0, c_1 \in L_1\) and \(\neg(x) = x + c_1\) for \(x \in \{0, 1\}\)),

\(P_2 = \langle \land \rangle\) and

\(S_2 = \langle \lor \rangle\).
Since E. Post characterized all boolean clones in [13] we know (see Figure 2.1 and Table 2.2) that for each boolean clone $C$ exactly one of the following statements must be true

1. $H \subseteq D_3$, $H \cap L_1 = J_{\{0,1\}}$ and $maj \in C$.
2. $H \subseteq L_1$, $H \not\subseteq \{R_1, R_4, R_6, R_8, R_{11}, R_{13}\}$ and $+(3) \in H$.
3. $H \cap L_1 = H \cap S = J_{\{0,1\}}$ and therefore $P_2 \subseteq H$ or $S_2 \subseteq H$.
4. $H \subseteq L_1$ and $H \in \{R_1, R_4, R_6, R_8, R_{11}, R_{13}\}$.

<table>
<thead>
<tr>
<th>Generators</th>
<th>Headers</th>
<th>Generators</th>
<th>Headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_1$</td>
<td>$\langle maj, +(3) \rangle$</td>
<td>$P_2$</td>
<td>$\langle \land \rangle$</td>
</tr>
<tr>
<td>$D_2$</td>
<td>$\langle maj \rangle$</td>
<td>$S_2$</td>
<td>$\langle \lor \rangle$</td>
</tr>
<tr>
<td>$D_3$</td>
<td>$\langle maj, \neg \rangle$</td>
<td>$R_1$</td>
<td>$\langle e \rangle$</td>
</tr>
<tr>
<td>$L_1$</td>
<td>$\langle +, \neg \rangle$</td>
<td>$R_4$</td>
<td>$\langle \neg \rangle$</td>
</tr>
<tr>
<td>$L_2$</td>
<td>$\langle \leftrightarrow \rangle$</td>
<td>$R_6$</td>
<td>$\langle c_1 \rangle$</td>
</tr>
<tr>
<td>$L_3$</td>
<td>$\langle + \rangle$</td>
<td>$R_8$</td>
<td>$\langle c_0 \rangle$</td>
</tr>
<tr>
<td>$L_4$</td>
<td>$\langle +(3) \rangle$</td>
<td>$R_{11}$</td>
<td>$\langle c_0, c_1 \rangle$</td>
</tr>
<tr>
<td>$L_5$</td>
<td>$\langle +(3), \neg \rangle$</td>
<td>$R_{13}$</td>
<td>$\langle c_0, c_1, \neg \rangle$</td>
</tr>
</tbody>
</table>

Table 2.1: Description of the clones $D, L, R$ clones.
Figure 2.1: The lattice of clones on 2 elements
We will prove that in each of the 4 cases $\text{Con}(\mathbb{H}) = \{\Delta, \kappa, \nabla\}$ or $\text{Con}(\mathbb{H}) = \{\Delta, \kappa_c, \kappa, \nabla\}$.

It is straightforward to check that $H$ has only the 3 trivial congruences if $H \subseteq \{R_1, R_4, R_6, R_8, R_{11}, R_{13}\}$. In order to make the proof more structured we will treat each of the remaining cases in a separate lemma.

**Lemma 2.14.** Let $H \in C(\{0, 1\})$ with $H \subseteq D_3 = \langle \text{maj}, \neg \rangle$ and $\text{maj} \in H$. Then $\text{Con}(\mathbb{H}) = \{\Delta, \kappa, \nabla\}$.

**Proof.** Let $\theta \in \text{Con}(\mathbb{H})$ with $\Delta \subseteq \theta \subseteq \nabla$. By Lemma 2.8 we get that $\theta \subseteq \kappa$ and since $\theta$ is not trivial there must exist $(f, g) \in \theta$ with $n := ar(f) = ar(g)$ and $f(a_1, \ldots, a_n) \neq g(a_1, \ldots, a_n)$ for some $\bar{a} \in \{0, 1\}^n$.

1. Case: $\bar{a} \in \{(0, \ldots, 0), (1, \ldots, 1)\}$

Then we have that $(\Delta^n \circ f, \Delta^n \circ g) = (id, \neg) \in \theta$. Hence,

$$(\pi_1^2(x_1, x_2), \pi_2^2(x_1, x_2)) = (\text{maj}(x_1, x_2, \neg, x_2), \text{maj}(x_1, x_2, x_2)) \in \theta.$$ 

Therefore by Lemma 2.11 $\theta = \kappa$.

2. Case: $\bar{a} \in \{0, 0, 0\}$, $(1, 1, 1)$

In this case we construct two binary functions $\hat{f}(y_1, y_2)$ and $\hat{g}(y_1, y_2)$ by identifying variables of $f$ and $g$ in the following way:

$$x_i \mapsto \begin{cases} 
   y_1 & a_i = 0 \\
   y_2 & a_i = 1
\end{cases}$$

Note that $(\hat{f}, \hat{g}) \in \theta$ and $\hat{f}(0, 1) = f(\bar{a}) \neq g(\bar{a}) = \hat{g}(0, 1)$. Furthermore we know that $S[2] = \{\pi_1^2, \pi_2^2, \neg(\pi_1^2), \neg(\pi_2^2)\}$ since if $h \in S[2]$ we have that $h(0, 0) = \neg h(1, 1)$ and $h(1, 0) = \neg h(0, 1)$ and so $h$ is determined by $h(0, 0)$ and $h(1, 0)$. The four possible combinations correspond exactly to $\{\pi_1^2, \pi_2^2, \neg(\pi_1^2), \neg(\pi_2^2)\}$.

By some case distinctions and elementary calculations it follows form $(f, g) \in S[2]$ and $\hat{f} \neq g$ that $(\pi_1^2, \pi_2^2) \in \kappa$ and by Lemma 2.11 $\theta = \kappa$. \hfill \Box

**Lemma 2.15.** Let $H \in C(\{0, 1\})$ with $H \subseteq L_1 = \{f \in O(\{0, 1\}) | \exists a_0, \ldots, a_4 \in \{0, 1\}: f(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^n a_i x_i\}$, $H \notin \{R_1, R_4, R_6, R_8, R_{11}, R_{13}\}$ and $+(3) \in H$. Then $\text{Con}(\mathbb{H}) = \{\Delta, \kappa_c, \kappa, \nabla\}$.

**Proof.** Let $\theta \in \text{Con}(H) \setminus \{\Delta\}$. The only clones which fulfill the assumptions are $L_1 = \langle +, \neg \rangle$, $L_2 = \langle \leftrightarrow \rangle$, $L_3 = \langle \langle \rangle \rangle$, $L_4 = \langle +^{(3)} \rangle$, $L_5 = \langle +^{(3)}, \neg \rangle$ (see figure 2.2 and table 2.2). We distinguish two cases

1. Case: $\Delta \subseteq \theta \subseteq \kappa_c$

Now there must be $(f, g) \in \theta$ with $n := ar(f) = ar(g)$ and $f(\bar{x}) = g(\bar{x}) + 1$, otherwise $\theta = \Delta$. But then

$$(+^{(3)}((\pi_1^n, f(\bar{x}), f(\bar{x}))), +^{(3)}((\pi_1^n, f(\bar{x}), g(\bar{x})))) = (\pi_1^n + f(\bar{x}) + f(\bar{x}), \pi_1^n + f(\bar{x}) + g(\bar{x})) = (\pi_1^n, \pi_1^n + 1) \in \theta$$

$$(\pi_1^n, \pi_1^n) \in \theta$$
Hence, \((id, -) \in \theta\) by identifying variables. But this means that \(\neg \in H\) thus \(H \in \{L_1, L_5\}\). This means we are considering functions of the clones \(L_1\) or \(L_5\). Observe that we can represent a \(f\) in \(H\) in the following way
\[
f(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} a_i x_i \text{ for some } a_i \in \{0, 1\}.
\]
With this representation we can conclude that \((f, g) \in \kappa_c \setminus \Delta \iff f(\bar{x}) = a_0 + h(\bar{x})\) and \(g(\bar{x}) = b_0 + h(\bar{x})\) for all \(\bar{x} \in \{0, 1\}^n\) and with \(a_0 \neq b_0\) (assume \(a_0 = 1\)). But then
\[
(h + id + \neg, h + id + id) = (h + c_1, h + c_0) = (f, g) \in Cg((id, -)) \subseteq \theta
\]
and therefore \(\theta = \kappa_c\).

2. Case: \(\theta \not\subseteq \kappa_c\)

In this case there must be two \(\theta\)-congruent functions \(f, g\) of the form \(f(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} a_i x_i\) and \(g(x_1, \ldots, x_n) = b_0 + \sum_{j=0}^{n} b_j x_j\) and \((f, g) \not\in \kappa_c\). Hence there \(\exists i \in \{1, \ldots, n\}: a_i \neq b_i\) because otherwise \((f, g) \in \kappa_c\). Without loss of generality assume that \(i = 1\) and \(a_1 = 1, b_1 = 0\). Then we have
\[
(+^{\Delta}(id(x_1), g(x_1, x_2, \ldots, x_2), g(x_2, \ldots, x_2)), +^{\Delta}(id(x_1), f(x_1, x_2, \ldots, x_2), f(x_2, \ldots, x_2)))
\]
\[
= (id(x_1) + g(x_1, x_2, \ldots, x_2) + g(x_2, \ldots, x_2), f(x_1, x_2, \ldots, x_2) + f(x_2, \ldots, x_2))
\]
\[
= (x_1 + b_1 x_1 + b_1 x_2, x_1 + a_1 x_1 + a_1 x_2)
\]
\[
= (x_1, x_2) \in \theta
\]
and this implies \(\theta = \kappa\).

\[\square\]

**Lemma 2.16.** Let \(H \in C(\{0, 1\})\) with \(\langle \land \rangle \subseteq H\) or \(\langle \lor \rangle \subseteq H\). Then \(\text{Con}(H) = \{\Delta, \kappa, \triangledown\}\).

**Proof.** As in the proof of Lemma 2.15 we get that a non-trivial congruence \(\theta\) of \(H\) must contain a pair of functions \((f, g)\) with \(n := ar(f) = ar(g)\) and \(\exists a \in \{0, 1\}^n: f(a_1, \ldots, a_n) \neq g(a_1, \ldots, a_n)\).

1. Case: \(\Delta^{n-1}(f), \Delta^{n-1}(g)\) \(\cap \{\neg, c_1, c_1^1\} \neq \emptyset\)

Let \(h \in \{\neg, c_1^0, c_1^1\} \cap H\). For each possible case of \(h\) we construct two unary functions \(\hat{f}(y_1), \hat{g}(y_1)\) by substituting \(h\) and identifying the variables of \(f\) and \(g\), i.e. \((\hat{f}, \hat{g}) \in \theta\).

We set
\[
\hat{f}(y_1) = \Delta^{n-1}(f(q_1(y_1), \ldots, q_n(y_n)))\hat{g}(y_1) = \Delta^{n-1}(g(q_1(y_1), \ldots, q_n(y_n)))
\]
where the \(q_i\)'s are defined differently in each of the three cases

1. If \(h = c_1^1\) then \(q_i = \begin{cases} c_1^0 & a_i = 0 \\ id & \text{ else} \end{cases}\)
With this definition we get that for each possible value of $h$ there exists $b \in \{0, 1\}$ $\tilde{f}(b) = f(\tilde{a}) \neq g(\tilde{a}) = \tilde{g}(b)$. Hence, $(\tilde{f}, \tilde{g}) \in \{(id, c_0^1), (id, c_1^1), (c_1^0, c_1^0), (\neg, c_1^0), (\neg, c_1^0), (id, \neg)\}$. If $(\tilde{f}, \tilde{g}) \in \{(id, c_0^1), (id, c_1^1), (\neg, c_1^0), (\neg, c_1^0)\}$ we conclude by Lemma 2.11 $\theta = \kappa$ (Note that $(\neg \ast \neg, c_0^1 \ast c_0^1) = (id, c_1^0)$ for $a \in \{0, 1\}$). Next case would be $(\tilde{f}, \tilde{g}) = (c_0^1, c_1^1)$ then let $\sigma \in \{\land, \lor\} \cap H$ and thus $(id, c_1^0) = (\sigma(id, c_0^0), \sigma(id, c_1^0)) \in \kappa$ for some $a \in \{0, 1\}$ and therefore $\theta = \kappa$.

The last case we have to consider is $(\tilde{f}, \tilde{g}) = (id, \neg)$. Again if $\sigma \in \{\land, \lor\} \cap H$ then $(id, c_1^0) = (\sigma(id, id), \sigma(id, \neg)) \in \kappa$ for some $a \in \{0, 1\}$ and once again $\theta = \kappa$.

2. Case: $\Delta^{n-1}(f), \Delta^{n-1}(g) = id$

Then there must exist an element $\tilde{a} \in A^n \setminus \{(0, \ldots, 0), (1, \ldots, 1)\}$ such that $f(\tilde{a}) \neq g(\tilde{a})$. As in Lemma 2.14 we can construct two binary functions $\tilde{f}, \tilde{g}$ from $f$ and $g$ with $(\tilde{f}, \tilde{g}) \in \theta$ and w.l.o.g $\tilde{f}(0,1) = 0$ and $\tilde{g}(0,1) = 1$. By the construction of $\tilde{f}$ and $\tilde{g}$ we still have that $\tilde{f}(x, x) = \tilde{g}(x, x) = x$. We conclude that $(\tilde{f}, \tilde{g}) \in \{(\land, \pi_2^0), (\land, \lor), (\pi_1^2, \pi_2^2), (\pi_1^2, \lor)\}$. In each of the remaining cases we can show that $(\pi_1^2, \pi_2^2) \in \theta$.

1. $(\land, \pi_2^0) \in \theta$: $(\tau(\land), \tau(\pi_2^0)) = (\land, \pi_1^0) \in \theta$ but then $(\pi_1^0, \pi_2^0) \in \theta$. (Works analogously for the case $(\pi_2^0, \lor) \in \theta$).

2. $(\land, \lor) \in \theta$: $(x_1 \lor (x_1 \land x_2), (x_1 \land (x_1 \land x_2)) = (\pi_1^2(x_1, x_2), x_1 \land x_2) \in \theta$. The rest is analogous to the case before.

This concludes the proof of Theorem 2.12.

### 2.3 Subdirectly irreducible clones

In the last section we have already seen that every clone on a two element set is subdirectly irreducible. Now we are going to analyze if there is any connection when an algebra $A$ is subdirectly irreducible and its clone of polynomial functions. The following theorem was first proved by Schweigert in [15, Theorem 5.3].

**Theorem 2.17.** Let $A$ be an algebra. Then we have
KAPITEL 2. CONGRUENCES ON CLONES

Pol(\(\mathbb{A}\)) is subdirectly irreducible \(\Rightarrow\) \(\mathbb{A}\) is subdirectly irreducible

Before we can prove this theorem we need one lemma

Lemma 2.18. Let \(\mathbb{A}\) be an algebra and \(\theta \in \text{Con}(\mathbb{A})\) and let

\[
\alpha_\theta := \{(f, g) \in \text{Pol}(\mathbb{A})^2 \mid ar(f) = ar(g) \land \forall a_1, \ldots, a_n : (f(a_1, \ldots, a_n), g(a_1, \ldots, a_n)) \in \theta\}
\]

Then

1. \(\alpha_\theta \in \text{Con}(\text{Pol}(\mathbb{A}))\)

2. The mapping \(\phi : \text{Con}(\mathbb{A}) \to \text{Con}(\text{Pol}(\mathbb{A})), \theta \mapsto \alpha_\theta\) is a meet homomorphism.

Proof. 1) Let \(\theta \in \text{Con}(\mathbb{A})\). It is straightforward to prove that \(\alpha_\theta\) is an equivalence relation. Let \((f, g) \in \alpha_\theta\). It is clear from the definition that if we manipulate the variables of \(f\) and \(g\) the result will be again an element of \(\alpha_\theta\). We still have to show that \(\alpha_\theta\) is closed under \(*\). Let therefore be \((h_1, h_2) \in \alpha_\theta\), \(ar(h_1) = ar(h_2) = n\), \(ar(f) = ar(g) = m\) and \(a_1, \ldots, a_{n+m-1} \in A\). First of all we have that \(ar(f * h_1) = ar(f) + ar(h_1) - 1 = ar(g) + ar(h_2) = ar(g * h_2)\). Observe that

\[
(f(h_1(a_1, \ldots, a_n), a_{n+1}, \ldots, a_{n+m-1}), g(h_1(a_1, \ldots, a_n), a_{n+1}, \ldots, a_{n+m-1})) \in \theta
\]

since \((f, g) \in \alpha_\theta\).

Moreover,

\[
(g(h_1(a_1, \ldots, a_n), a_{n+1}, \ldots, a_{n+m-1}), g(h_2(a_1, \ldots, a_n), a_{n+1}, \ldots, a_{n+m-1})) \in \theta
\]

since \((h_1, h_2) \in \alpha_\theta\) and \(g \in \text{Pol}(\mathbb{A})\) and therefore preserves the congruences of \(\mathbb{A}\).

We have shown that \((f * h_1, g * h_1)\) and \((g * h_1, g * h_2) \in \alpha_\theta\) therefore we also get \((f * h_1, g * h_2) \in \alpha_\theta\) by transitivity.

2) Let \(\theta_1, \theta_2 \in \text{Con}(\mathbb{A})\). We have to show that \(\alpha_{\theta_1 \cap \theta_2} = \alpha_{\theta_1} \cap \alpha_{\theta_2}\).

\[
(f, g) \in \alpha_{\theta_1 \cap \theta_2} \iff \forall a_1, \ldots, a_n \in A : (f(\bar{a}), g(\bar{a})) \in \theta_1 \cap \theta_2
\]

\[
\iff \forall a_1, \ldots, a_n \in A : (f(\bar{a}), g(\bar{a})) \in \theta_1 \land (f(\bar{a}), g(\bar{a})) \in \theta_2
\]

\[
\iff (f, g) \in \alpha_{\theta_1} \land (f, g) \in \alpha_{\theta_2}
\]

\[
\iff (f, g) \in \alpha_{\theta_1} \cap \alpha_{\theta_2}
\]

\(\square\)

Now we can proof Theorem 2.17:
Proof. Let $A$ be an algebra such that $\text{Pol}(A)$ is subdirectly irreducible. Assume $A$ is reducible. Then there exist $\theta_1, \theta_2 \in \text{Con}(A) \setminus \{\Delta_A\}$ such that $\theta_1 \cap \theta_2 = \Delta_A$. Let $\phi$ be defined as in Lemma 2.18. We know that $\phi$ is a meet homomorphism and we claim the following

Claim. $\phi(\theta) = \Delta_{\text{Pol}(A)} \iff \theta = \Delta_{\text{Pol}(A)}$.

It is clear that $\phi(\Delta_A) = \Delta_{\text{Pol}(A)}$. The other direction is true as well. Assume $\theta \neq \Delta_A$ then there exists $(a, b) \in \theta$ with $a \neq b$. Thus $\forall n \in \mathbb{N} : (c^n_a, c^n_b) \in \alpha_\theta$ which is a contradiction to $\alpha_\theta = \Delta_{\text{Pol}(A)}$.

We get that $\Delta_{\text{Pol}(A)} = \phi(\Delta_A) = \phi(\theta_1 \cap \theta_2) = \phi(\theta_1) \cap \phi(\theta_2)$. Since $\phi(\theta_1), \phi(\theta_2) \neq \Delta_{\text{Pol}(A)}$ we have a contradiction to the irreducibility of $\text{Pol}(A)$.

\[\square\]

2.4 Fully invariant congruences, subvarieties and clone congruences

Our goal in this section is to establish an important connection between the subvarieties of an algebra $A$ and the congruences of the clone of term functions $\text{Clo}(A)$. The link between this two lattices will be certain fully invariant congruences of the term algebra of $A$.

This connection is well understood and the reader can find more details about it in [2, Chapter 2, Section 14].

Definition 2.19. Let $H \in C(A), \theta \in \text{Con}(H)$.

1. We call $\theta$ fully invariant if $\forall \phi \in \text{End}(H) : (f, g) \in \theta \Rightarrow (\phi(f), \phi(g)) \in \theta$

2. $\text{Con}_{fi}(H) := \{\alpha \in \text{Con}(H) \mid \alpha \text{ is fully invariant}\}$

The following lemma is well known and can be found for example in [2, Lemma 14.4].

Lemma 2.20. For an algebra $A$ the set of fully invariant congruences $\text{Con}_{fi}(A)$ forms an algebraic lattice.

Notation. For the rest of this section $X$ will denote a set of pairwise distinct variables and $\mathcal{F}$ will be a fixed type (signature). $T(X)$ will denote the terms over $X$ of type $\mathcal{F}$ and $T(X)$ will be the term algebra of type $\mathcal{F}$ over $X$.

Definition 2.21. Let $\sigma : \text{Id}(X) \to T(X) \times T(X)$ denote the bijection

$\sigma(p \approx q) := (p, q)$.

Lemma 2.22. If $\theta \in \text{Con}_{fi}(T(X))$ and $p \approx q \in \text{Id}(X)$ then

$T(X)/\theta \models p \approx q \iff (p, q) \in \theta$
Proof. Assume $T(X)/\theta \models p \approx q$ for $p, q \in T(X)$. Now we know

$$T(X)/\theta \models p \approx q$$

$\Rightarrow p(x_1/\theta, \ldots, x_n/\theta) = q(x_1/\theta, \ldots, x_n/\theta)$

$\Rightarrow p(x_1, \ldots, x_n)/\theta = q(x_1, \ldots, x_n)/\theta$

$\Rightarrow (p, q) \in \theta$

For the second implication assume that $(p, q) \in \theta$. We have to show that

$$T(X)/\theta \models p \approx q$$

i.e. for arbitrary terms $t_1, \ldots, t_n \in T(X)$ we must verify

$$p(t_1/\theta, \ldots, t_n/\theta) = q(t_1/\theta, \ldots, t_n/\theta).$$

For $t_1, \ldots, t_n \in T(X)$ we define a function $\beta : T(X) \rightarrow T(X)$ with

$$\beta(t_i) := t_i \text{ for } 1 \leq i \leq n$$

$$\beta(f(s_1, \ldots, s_m)) := f(\beta(s_1), \ldots, \beta(s_m))$$

where $f \in \mathcal{F}(m)$, $m \in \mathbb{N}$ and $s_i \in T(X)$ for $1 \leq i \leq m$.

Of course it follows immediately from the definition that $\beta$ is an endomorphism of $T(X)$, and since $\theta$ is fully invariant and $(p, q) \in \theta$ by assumption, we obtain

$$(\beta(p(x_1, \ldots, x_n)), \beta(q(x_1, \ldots, x_n))) \in \theta$$

$\Rightarrow (p(t_1, \ldots, t_n), q(t_1, \ldots, t_n)) \in \theta$

$\Rightarrow p(t_1, \ldots, t_n)/\theta = q(t_1, \ldots, t_n)/\theta$

$\Rightarrow p(t_1/\theta, \ldots, t_n/\theta) = q(t_1/\theta, \ldots, t_n/\theta)$

and we can conclude $T(X)/\theta \models p \approx q$. \hfill \Box$

Theorem 2.23. Let $\Sigma \subseteq \text{ld}(X)$. Then the following are equivalent

1. There exists a class $K$ of algebras such that $\text{ld}_K(X) = \Sigma$;

2. $\sigma(\Sigma) \in \text{Conf}_f(T(X))$.

Proof. Let $K$ be a class of algebras such that $\text{ld}_K(X) = \Sigma$. It is not hard to verify that $\sigma(\text{ld}_K(X))$ is an equivalence relation of $T(X)$. Let $f \in \mathcal{F}(n)$ and for $i \in \{1, \ldots, n\}$ let $p_i \approx q_i \in \text{ld}_K(X)$. Then $f(p_1, \ldots, p_n) \approx f(q_1, \ldots, q_n)$ and therefore $(f(p_1, \ldots, p_n), f(q_1, \ldots, q_n) \in \sigma(\text{ld}_K(X))$.

Let now $\alpha$ be an endomorphism of $T(X)$ and let $(p, q) \in \sigma(\text{ld}_K(X))$. Then it is straightforward to check that also $p(\alpha(x_1), \ldots, \alpha(x_n)) \approx q(\alpha(x_1), \ldots, \alpha(x_n))$ and of
course \((p(\alpha(x_1),\ldots,\alpha(x_n)),q(\alpha(x_1),\ldots,\alpha(x_n))) \in \sigma(\text{Id}_K(X))\).

For the other direction assume that \(\sigma(\Sigma)\) is a fully invariant congruence of \(T(X)\). We define \(K := \{T(X)/\sigma(\Sigma)\}\). We have

\[
p \approx q \in \text{Id}_K(X) \iff T(X)/\sigma(\Sigma) \models p \approx q \iff (p,q) \in \sigma(\Sigma) \iff p \approx q \in \Sigma
\]

\[\square\]

**Definition 2.24.** We call \(\Sigma \subseteq \text{Id}(X)\) an *equational theory* (of type \(F\) over \(X\)) if there exists a class of algebras \(K\) with \(\text{Id}_K(X) = \Sigma\).

**Corollary 2.25.** Let \(F\) be a type and \(X\) be set of variables. The set of equational theories of type \(F\) over \(X\) forms an algebraic lattice. Moreover, this lattice is isomorphic to the lattice of fully invariant congruences on the term algebra of type \(F\) over \(X\).

**Proof.** Follows with Lemma 2.20 and Theorem 2.23. \(\square\)

**Lemma 2.26.** Let \(A\) be an algebra of type \(F\). The mapping

\[
\psi : \text{Su}(V(A)) \to [\sigma(\text{Id}_A(X)), \nabla_{T(X)}]_{\text{Con}_f(T(X))}
\]

\[
W \mapsto \sigma(\text{Id}_W(X))
\]

is an order-reversing isomorphism.

**Proof.** First of all notice that \(\psi(W) \in [\sigma(\text{Id}_A(X)), \nabla_{T(X)}]_{\text{Con}_f(T(X))}\) by 2.23. Next we will show that for \(W,V \in \text{Su}(V(A))\) we have that \(W \subseteq V \iff \psi(W) \supseteq \psi(V)\).

If \(W \subseteq V\) the statement is clear. Let now \(\psi(V) \subseteq \psi(W)\) and let \(B \in W\) and \(p \approx q \in \text{Id}_V(X)\). Now we know that \((p,q) \in \psi(V) \subseteq \psi(W)\) and therefore \(B \models p \approx q\) and we get \(B \in V\).

For surjectivity suppose that \(\theta \in [\sigma(\text{Id}_A(X)), \nabla_{T(X)}]_{\text{Con}_f(T(X))}\) and define \(W_\theta := \text{Mod}(\sigma^{-1}(\theta))\). By the definition of \(W_\theta\) we obtain \(\theta \subseteq \psi(W_\theta)\). Assume now that \((t,s) \in \psi(W_\theta)\). Therefore \(t \approx s \in \text{Id}_{W_\theta}(X)\). Since \(\theta \in \text{Con}_f(T(X))\) we know by 2.22

\[
T(X)/\theta \models p \approx q \iff (p,q) \in \theta.
\]

So

\[
T(X)/\theta \in W_\theta
\]

and by our conclusion from before we get that \(T(X)/\theta \models t \approx s\). But this is equivalent to \((t,s) \in \theta\) (or \(t \approx s \in \sigma^{-1}(\theta)\)). Hence \(\theta = \psi(W_\theta)\) and therefore \(\psi\) is surjective. \(\square\)
We recall that our goal was to find a connection between the subvarieties of \( A \) and the clone congruences of \( \text{Clo}(A) \).

Now that we have successfully established a link between the subvarieties of \( A \) and the fully invariant congruences of the term algebra of \( A \) we have achieved the first half of our goal. For the second half we will find a relationship between \( \text{Con}_{f_1}(T(X)) \) and \( \text{Con}(\text{Clo}(A)) \).

**Theorem 2.27.** Let \( A \) be an algebra. Then the interval above the equational theory of \( A \) is isomorphic to \( \text{Con}(\text{Clo}(A)) \{\nabla\} \). The isomorphism is given by

\[
\phi : \left[\sigma(\text{Id}_h(X)), \nabla_{T(X)}\right]_{\text{Con}_{f_1}(T(X))} \to \text{Con}(\text{Clo}(A)) \{\nabla\}
\]

\[
\theta \mapsto \{ (t^A, s^A) \mid (t, s) \in T(X)^2 : (t, s) \in \theta \}
\]

**Proof.** Let \( \theta_1, \theta_2 \) be in \( \left[\sigma(\text{Id}_h(X)), \nabla_{T(X)}\right]_{\text{Con}_{f_1}(T(X))} \). Similar to the proof of Corollary 2.26 first of all we prove that \( \theta_1 \subseteq \theta_2 \Leftrightarrow \phi(\theta_1) \subseteq \phi(\theta_2) \).

The implication from left to right is trivial. So suppose that \( \phi(\theta_1) \subseteq \phi(\theta_2) \) and let \( (t, s) \in \theta_1 \). Then by assumption \( (t^A, s^A) \in \phi(\theta_1) \subseteq \phi(\theta_2) \) and there exists \( (p, q) \in \theta_2 \) with \( t^A = p^A \) and \( s^A = q^A \) or we can just write \( A \models p \approx t, q \approx s \). But since \( \sigma(\text{Id}_h) \subseteq \theta_2 \) also \( (p, t), (q, s) \in \theta_2 \) and therefore \( (t, s) \in \theta_2 \). Hence \( \phi \) is a monomorphism.

Let \( \alpha \in \text{Con}(\text{Clo}(A)) \{\nabla\} \) and define \( \alpha' := \{ (t, s) \in T(X)^2 : (t^A, s^A) \in \alpha \} \). Clearly \( \phi(\alpha') = \alpha \) and \( \phi \) is also surjective. \( \square \)

As a direct consequence from 2.26 and 2.27 we get the corollary beneath.

**Corollary 2.28.** For an algebra \( A := (A; F) \) with \( F \subseteq O(A) \) we have that \( \text{Con}(\text{Clo}(A)) \{\nabla\} \) and \( \text{Su}(V(A)) \) are dually isomorphic.

Finally we want to present a picture that summarizes the connections between \( \text{Su}(V(A)) \), \( \text{Con}_{f_1}(T(X)) \) and \( \text{Con}(\text{Clo}(A)) \).
2.5 Clones of functions with infinite arity

We are presenting in this chapter a different interpretation of clones of functions. Roughly speaking, we are interpreting each function in a clone as a function of infinite arity. This will have the effect that functions which only differ in dummy variables are interpreted as equal. The motivation for this can be found in Remark 2.9. As before we will analyze if this interpretation will influence the congruences of the clones.

Definition 2.29. 1. \( I_A := (A^{\mathbb{N}}, \circ, (\pi_i)_{i \in \mathbb{N}}) \) where \( A \) is a nonempty set and

- \( \forall f \in A^{\mathbb{N}} \forall (g_i)_{i \in \mathbb{N}} \in A^{\mathbb{N}} : (f \circ (g_i)_{i \in \mathbb{N}}(x_1, x_2)) := f(g_1(x_1, x_2), g_2(x_1, x_2), \ldots) \)
- \( \forall (a_i)_{i \in \mathbb{N}} \in A^{\mathbb{N}} : \pi_j(a_1, a_2, a_3, \ldots) = a_j. \)

2. If \( C \) is a subuniverse of \( I_A \) and in addition we have that \( \forall f \in C \forall n \in \mathbb{N} \forall a_1, \ldots, a_n \in A \forall (b_i)_{i \in \mathbb{N}}, (c_i)_{i \in \mathbb{N}} \in A^N : f(a_1, \ldots, a_n, b_1, b_2, \ldots) = f(a_1, \ldots, a_n, c_1, c_2, \ldots) \), then we call \( C \) an essential clone.

3. \( F(A) := \{ C \subseteq A^{\mathbb{N}} | C \text{ fulfills 2}) \}. \)

Definition 2.30. 1. \( - : O(A) \rightarrow A^{\mathbb{N}}, f \mapsto \tilde{f} \), where \( \tilde{f}(x_1, x_2, \ldots) := f(x_1, \ldots, x_{\text{ar}(f)}). \)
2. For $H \in C(A)$ is $\bar{H} := \{ \bar{f} \mid f \in H \}$.

3. For $\theta \in \text{Con}({\mathbb{H}})$ is $\bar{\theta} := \{(\bar{f}, \bar{g}) \mid (f, g) \in \theta\}$.

4. For $H \in C(A)$ we define $\mathbb{H} := (\bar{H}; \circ, (\pi_i)_{i \in \mathbb{N}})$

**Remark 2.31.** 1. A similar way to describe $\bar{H}$ is via the following relation $\sim$ which is defined as $f \sim g :\iff f(x_1, \ldots, x_n) = g(x_1, \ldots, x_m)$. The relation $\sim$ is an equivalence relation and is identifying functions if they are equal up to dummy variables (variables which have no effect on the function). This means $\bar{H}$ could alternatively be defined as the factor set of $H$ by $\sim$ or $\bar{H} = H/\sim$.

2. Let us go back to Remark 2.9 where we considered $Cg((f, g))$ with $f \in O^{|n|}(A)$, $g : A^n \rightarrow A$, $g(x_1, \ldots, x_m) := f(x_1, \ldots, x_n)$ and $n < m$. In the old interpretation $Cg((f, g)) = \nabla$ but since $g(x_1, \ldots, x_m) = f(x_1, \ldots, x_n)$ we get that $\bar{f} = \bar{g}$ and therefore $Cg((\bar{f}, \bar{g})) = \Delta$.

Now the question arises if there do really exist proper nontrivial congruences of $\mathbb{H}$. Fortunately the answer is ‘yes’. Consider the following example

**Example 2.32.** For an algebra $A$ and $\alpha \in \text{Con}(A)$ consider

$$\theta(\alpha) := \{(\bar{f}, \bar{s}) \in \overline{\text{Clo}(A)}^2 \mid \forall (a_i)_{i \in \mathbb{N}} : (\bar{f}(a_1), \ldots, \bar{s}(a_1, \ldots)) \in \alpha\}$$

It is straightforward to verify that $\theta(\alpha)$ is an equivalence relation on $\overline{\text{Clo}(A)}$. Now we recall the fact that the elements in $\overline{\text{Clo}(A)}$ are only depending on finitely many variables and so we can use the arguments in the first part of the proof of Lemma 2.18 to prove that $\theta(\alpha)$ is really a congruence relation.

**Lemma 2.33.** Let $A \neq \emptyset$. $\mathbb{F}(A)$ forms a lattice with respect to $\subseteq$.

**Proof.** It is clear that $\mathbb{F}(A)$ is lattice with the operations

$$H_1 \land H_2 := H_1 \cap H_2$$
$$H_1 \lor H_2 := \bigcap \{H \in \mathbb{F}(A) \mid H_1 \cup H_2 \subseteq H\}$$

☐

**Theorem 2.34.** Let $A \neq \emptyset$. $\phi : C(A) \rightarrow \mathbb{F}(A), H \mapsto \bar{H}$. Then $\phi$ is a lattice isomorphism.

**Proof.** Let $H \in C(A)$ first of all we have to show that $\bar{H} \in \mathbb{F}(A)$. We know for all $n \in \mathbb{N}$ and $i \leq n$ we have $\overline{\pi_i^n} = \pi_i$ and so $\forall i \in \mathbb{N} : \pi_i \in \bar{H}$.

Let $f \in H$ with $f \in H$ and $(\bar{g}_i)_{i \in \mathbb{N}} \in \bar{H}^\mathbb{N}$ with $g_i \in H$ for all $i$. We have to show $f \circ (\bar{g}_i)_{i \in \mathbb{N}} \in \bar{H}$.

$\forall (a_i)_{i \in \mathbb{N}} :$
\[(\bar{f} \circ (\bar{g}_i)_{i \in \mathbb{N}})(a_1, \ldots) = \bar{f}(\bar{g}_1(a_1, \ldots), \bar{g}_2(a_1, \ldots), \ldots) = \bar{f}(g_1(a_1, \ldots, a_{n_1}), g_2(a_1, \ldots, a_{n_2}), \ldots) = f(g_1(a_1, \ldots, a_{n_1}), g_2(a_1, \ldots, a_{n_2}), \ldots, g_k(a_1, \ldots, a_{n_k})) = f(h_1, \ldots, h_k)(a_1, \ldots, a_N) \quad (*)\]

Where \(N := \text{max}\{n_i \mid i \in [k]\}\) and \(\forall i \in [k] : h_i(x_1, \ldots, x_N) := g_i(x_1, \ldots, x_n)\). Since \(g_i \in H\) we also have \(h_i \in H\) and because \(f \in H\) we get that \(f(h_1, \ldots, h_k) \in H\). Now we have \(f(h_1, \ldots, h_k) \in H\) and with (\(*)\) it follows that \(f(h_1, \ldots, h_k) = \bar{f} \circ (\bar{g}_i)_{i \in \mathbb{N}}\).

The injectivity and homomorphism properties will follow if we can show the following claim

**Claim.** \(\forall H, K \in C(A) : \bar{H} \subseteq \bar{K} \iff H \subseteq K\).

If \(H \subseteq K\) then it follows from the definition that \(\bar{H} \subseteq \bar{K}\). So let now \(\bar{H} \subseteq \bar{K}\) and \(f \in H\). We know that \(\bar{f} \in \bar{H}\) and therefore \(\bar{f} \in \bar{K}\). There must exist a \(g \in K\) such that \(\bar{g} = \bar{f}\) i.e. \(\forall (a_i)_{i \in \mathbb{N}} : \bar{f}(a_1, \ldots, a_n) = \bar{g}(a_1, \ldots)\). If \(ar(f) := n, ar(g) := m\) and \(\mathcal{N} := \text{max}\{n, m\}\) then we have that \(\forall a_1, \ldots, a_{\mathcal{N}} : f(a_1, \ldots, a_{\mathcal{N}}) = g(a_1, \ldots, a_{\mathcal{N}})\).

\(f\) and \(g\) are only differing through dummy variables, but since \(g \in K\) and \(K \in C(A)\) we get that \(f \in K\) (just add or remove the fictitious variables from \(g\) to obtain \(f\)).

What is still left to prove is the surjectivity of \(\psi\). Let \(G \in \mathbb{F}(A)\). We define

\[H_G := \{ h \in O(A) \mid \exists g \in G \forall a : h(a_1, \ldots, a_n) = g(a_1, \ldots) \}\]

First of all we will show that \(\overline{H_G} = G\).

Let \(f \in \overline{H_G}\). Then there is a \(h \in H_G\) : \(\bar{h} = \bar{f}\). Moreover, \(\exists g \in G \forall a : h(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)\). We get that \(\bar{f} = \bar{h} = g \in G\).

Let \(g \in G\). Since \(G \in \mathbb{F}(A)\) there exists a \(n \in \mathbb{N}\) such that for all \(a_1, \ldots, a_n\) and \(b, c\) we have \(g(a_1, \ldots, a_n, b_1, b_2, \ldots) = g(a_1, \ldots, a_n, c_1, c_2, \ldots)\). We define \(k : A^n \rightarrow A, k(x_1, \ldots, x_n) := g(x_1, \ldots, x_n, x_n, \ldots)\). It follows that \(k \in H_G\) and for all \((a_i)_{i \in \mathbb{N}}\) we get

\[g(a_1, \ldots, a_n, a_n, \ldots) = k(a_1, \ldots, a_n) = \bar{k}(a_1, \ldots)\]

But this means \(g = \bar{k}\) and therefore \(g \in \overline{H_G}\).

Finally we show \(H_G \in C(A)\). It holds that \(\forall n \forall i \leq n \forall a : \pi_i^n(a_1, \ldots, a_n) = \pi_i(a_1, \ldots)\) and therefore \(J_A \subseteq H_G\). Let \(f \in H_G^{[k]}\) and \(g_1, \ldots, g_k \in H_G^{[n]}\), then \(\bar{f}, \bar{g}_1, \ldots, \bar{g}_k \in \overline{H_G} = G\). One has \(f \circ (\bar{g}_i)_{i \in \mathbb{N}} \in \overline{H_G} \) for \((\bar{g}_i) = (g_i, \ldots, g_k, \pi_{k+1}, \ldots)\) and with the same arguments as in the beginning of the prove we get that \(f(g_1, \ldots, g_k) = f(\bar{g}_i)_{i \in \mathbb{N}}\). We conclude that there exists \(q \in H_G\) such that \(\bar{q} = f(\bar{g}_1, \ldots, \bar{g}_k)\). Again this means that \(q\) and \(f(g_1, \ldots, g_k)\) are equal up to dummy variables. But from the definition of \(H_G\) it follows if \(q \in H_G\) then also \(f(g_1, \ldots, g_k) \in H_G\).

All in all we have proved that \(\overline{H_G} = G\) and \(H_G \in C(A)\) therefore \(\phi(H_G) = G\). 

\(\square\)
Theorem 2.34 shows that each clone of functions corresponds to exactly one essential clone. The reason why we introduced our approach with functions of infinite arity was that we wanted to study congruences with elements $\langle \bar{f}, \bar{g} \rangle$ such that $ar(f) \neq ar(g)$. The next theorem shows that it makes almost no difference if we look at the congruences of $\mathbb{H}$ or $\mathbb{H}$.

**Theorem 2.35.** Let $A \neq \emptyset$, $H \in C(A)$ and let $\psi : \text{Con}(\mathbb{H}) \setminus \{\nabla\} \to \text{Con}(\mathbb{H})$, $\theta \mapsto \bar{\theta}$. Then $\psi$ is a lattice isomorphism.

**Proof.** The proof will be very similar to the proof of 2.34. We will start to show that $\psi$ is well-defined i.e. $\bar{\theta} \in \text{Con}(\mathbb{H})$. Let $\langle \bar{f}, \bar{g} \rangle \in \bar{\theta}$ with $(f, g) \in \theta$ and $(\bar{c}_i)_{i \in \mathbb{N}}, (\bar{d}_i)_{i \in \mathbb{N}} \in \bar{H}^N$ with $(\bar{c}_i, \bar{d}_i) \in \bar{\theta}$ and $(c_i, d_i) \in \theta$. Then for all $\bar{a}$ we have

\[
(f \circ (\bar{c}_i)_{i \in \mathbb{N}})(a_1, \ldots) = f(c_1(a_1, \ldots, a_{n_1}), \ldots)
\]

Where $N := \max\{n_i \mid i \in [k]\}$ and $\forall i \in [k] : h_i(x_1, \ldots, x_N) := c_i(x_1, \ldots, x_{n_i})$. We can do this analogously for $g$ and get $(g \circ (\bar{d}_i)(a_1, \ldots)) = g(r_1, \ldots, r_l)(a_1, \ldots, a_M)$. Since $\theta \subseteq \kappa$ it follows $k = ar(f) = ar(g)$ and $\forall (c_i) = ar(d_i)$ and so $M = N$. From $(c_i, d_i) \in \theta$ we conclude $(h_i, r_i) \in \theta \forall i$ and from $(f, g) \in \theta$ we get $(f(h_1, \ldots, h_k), g(r_1, \ldots, r_k) \in \theta$. Finally from (1) it follows $(f(h_1, \ldots, h_k), (g(r_1, \ldots, r_k)) = (f \circ (\bar{c}_i)_{i \in \mathbb{N}}), g \circ (\bar{d}_i)) \in \bar{\theta}$.

In order to prove that $\psi$ is a monomorphism we show that the following claim holds.

**Claim.** $\forall \theta_1, \theta_2 \in \text{Con}(\mathbb{H}) : \bar{\theta}_1 \subseteq \bar{\theta}_2 \iff \theta_1 \subseteq \theta_2$.

Again the direction from right to left is clear. For the other direction assume $\bar{\theta}_1 \subseteq \bar{\theta}_2$ and let $(f, g) \in \theta_1$. We know that $\langle f, g \rangle \in \bar{\theta}_1 \subseteq \bar{\theta}_2$. So there must exist a pair of functions $(h_1, h_2) \in \theta_2$ such that $\langle f, g \rangle = (h_1, h_2)$. Since $\theta_1, \theta_2 \subseteq \kappa$ we know $ar(f) = ar(g)$ and $ar(h_1) = ar(h_2)$. Together with $(\bar{f}, \bar{g}) = (h_1, h_2)$ we can conclude that $(f, g)$ can be constructed from $(h_1, h_2)$ by manipulating dummy variables i.e. $(f, g) \in \theta_2$.

We still have to prove the surjectivity of $\psi$.

Let $\alpha \in \text{Con}(\mathbb{H})$. We define $\theta_\alpha := \{(f, g) \in H^2 \mid ar(f) = ar(g) \land \exists (h_1, h_2) \in \alpha \forall \bar{a} \in A^N \colon \bar{h}_1(a_1, \ldots) = f(a_1, \ldots, a_n), \bar{h}_2(a_1, \ldots) = g(a_1, \ldots, a_m)\}$.

Like before we show that $\theta_\alpha = \alpha$. Let $(f, g) \in \theta_\alpha, (\bar{f}, \bar{g}) \in \bar{\theta}_\alpha$. $\exists (\bar{h}_1, \bar{h}_2) \in \alpha \forall \bar{a} : \bar{h}_1(a_1, \ldots) = f(a_1, \ldots, a_m), \bar{h}_2(a_1, \ldots) = g(a_1, \ldots, a_m)$. Now we have $\bar{f} = \bar{h}_1$ and $\bar{g} = \bar{h}_2$, so $(\bar{f}, \bar{g}) \in \alpha$.

For the other inclusion let $(f, g) \in \alpha$. We know $f, g \in \bar{H}$ therefore $\exists f_1, g_1 \in H \forall \bar{a} : f(a_1, \ldots) = f_1(a_1, \ldots, a_m), g(a_1, \ldots) = g_1(a_1, \ldots, a_m)$. We can assume that $n = m$ (if $n \neq m$ we extend the arity of $f_1$ or $g_1$ by adding dummy variables). We get that $(f_1, g_1) \in \theta_\alpha$ and so $(\bar{f}_1, \bar{g}_1) \in \bar{\theta}_\alpha$ and $(\bar{f}, \bar{g}) = (f, g)$.
Let \( h \in H \), we know \( \overline{h}(a_1, \ldots) = h(a_1, \ldots, a_n) \) and of course \( (h, h) \in \theta_a \). In addition \( \theta_a \) is symmetric and transitive, therefore \( \theta_a \in Eq(H) \).

Let \( (f, g) \in \theta_a \) we will show \( (\xi(f), \xi(g)) \in \theta_a \). Since \( (f, g) \in \theta_a \) it follows \( (\bar{f}, \bar{g}) \in \theta_a = \alpha \in Con(H) \).

It holds that \((\xi(f), \xi(g)) = (\bar{f} \circ (p_i)_{i \in \mathbb{N}}, \bar{g} \circ (p_i)_{i \in \mathbb{N}})\) with \( (p_i)_{i \in \mathbb{N}} = (\pi_2, \ldots, \pi_n, \pi_1, \pi_{n+1}, \ldots) \). We know \( \alpha \in Con(H) \) and so \((\xi(f), \xi(g)) \in \alpha = \overline{\theta_a}\) therefore there exists \( (f_1, g_1) \in \theta_a \) such that \( f_1 = \xi(f), g_1 = \xi(g) \). \( f_1, \xi(f) \) and \( g_1, \xi(g) \) are equal up to dummy variables and \( ar(\xi(f)) = ar(\xi(g)) \). From \( (f_1, g_1) \in \theta_a \) and the definition of \( \theta_a \) we finally get \((\xi(f), \xi(g)) \in \theta_a \). It is completely analogous to show that \( \theta_a \) is closed under \( \tau, \Delta \) and \(*\).

On the one hand we know now that for a clone of functions \( H \) on a set \( A \) the lattice Con\( (\overline{H}) \)\( \setminus \{ \nabla \} \) is isomorphic to Con\( (\overline{H}) \) and on the other hand Corollary 2.28 states that Con\( (\overline{H}) \)\( \setminus \{ \nabla \} \) is dual isomorphic to the subvariety lattice of \( V(A) \) with \( A = (A; H) \).

It follows that the subvarieties of \( A = (A; H) \) correspond to the congruences of \( \overline{H} \), especially the minimal varieties of \( A \) correspond to the maximal congruences of \( \overline{H} \).

2.6 Left and right congruences

In the previous section we have seen that it makes no difference to consider clones of functions as subalgebras of \( M_A \) or as clones of functions with infinite arity if one is studying congruences of clones.

Nevertheless we will focus on the essential clones in this section or to be more precise on the operation \( \circ \) of \( \overline{H} \). Similar as in ring theory we are going to split up \( \circ \) in two operations by fixing either the first argument or the second one.

**Definition 2.36.** Let \( \overline{H} \) be a essential clone, \( f \in \overline{H} \) and \( (g_i)_{i \in \mathbb{N}} \in H^\mathbb{N} \). We define

1. \[
\lambda^H_f : H^\mathbb{N} \mapsto H, \quad \lambda^H_f((g_i)_{i \in \mathbb{N}})(x_1, x_2, \ldots) := f(g_1, g_2, \ldots)(x_1, x_2, \ldots)
\]
\[
\lambda^H_{(g_i)_{i \in \mathbb{N}}} : H \mapsto H, \quad \lambda^H_{(g_i)_{i \in \mathbb{N}}}(f)(x_1, x_2, \ldots) := f(g_1, g_2, \ldots)(x_1, x_2, \ldots)
\]

2. We call \( \alpha \subseteq \overline{H}^2 \) a left congruence of \( H \) if \( \alpha \) is compatible with \( \lambda^H_f \) for all \( f \in H \) and \( \alpha \in Eq(\overline{H}) \). Let Con\( _L(\overline{H}) := \{ \alpha \subseteq \overline{H}^2 \mid \alpha \) is a left congruence \} .

3. We call \( \alpha \subseteq \overline{H}^2 \) a right congruence of \( H \) if \( \alpha \) is compatible with \( \lambda^H_{(g_i)_{i \in \mathbb{N}}} \) for all \( (g_i)_{i \in \mathbb{N}} \in H^\mathbb{N} \) and \( \alpha \in Eq(\overline{H}) \). Con\( _R(\overline{H}) := \{ \alpha \subseteq \overline{H}^2 \mid \alpha \) is a right congruence \} .

From now on we will fix a clone \( H \) and the corresponding essential clone \( \overline{H} \) for this section and omit the \( H \) and write \( \lambda_f \) and \( \lambda_{(g_i)_{i \in \mathbb{N}}} \).

Like in Ring Theory we get that a \( \theta \in Con(\overline{H}) \) if and only if it is a left and a right congruence.
Lemma 2.37. We have that $\text{Con}(\mathbb{H}) = \text{Con}_{L}(\mathbb{H}) \cap \text{Con}_{R}(\mathbb{H})$.

Proof. First of all it is clear that every congruence of $\mathbb{H}$ is also a left and a right congruence of $\mathbb{H}$.

Now let $\theta \in \text{Con}_{L}(\mathbb{H}) \cap \text{Con}_{R}(\mathbb{H})$, $(h_{1}, h_{2}) \in \theta$ and let $(f_{i})_{i \in \mathbb{N}}, (g_{i})_{i \in \mathbb{N}} \in \hat{H}$ with $(f_{i}, g_{i}) \in \theta$. We have to show that $(h_{1} \circ (f_{i})_{i \in \mathbb{N}}, h_{2} \circ (g_{i})_{i \in \mathbb{N}}) \in \theta$.

Since for all $(f_{i}, g_{i}) \in \theta$ we get that

$$(\lambda_{h_{2}}((f_{i})_{i \in \mathbb{N}}, \lambda_{h_{2}}((g_{i})_{i \in \mathbb{N}})) = (h_{1}(f_{1}, f_{2}, \ldots), h_{2}(g_{1}, g_{2}, \ldots)) \in \theta.$$ We also know that $(h_{1}, h_{2}) \in \theta$ and thus

$$(\lambda_{(f_{i})_{i \in \mathbb{N}}}(h_{1}), \lambda_{(f_{i})_{i \in \mathbb{N}}}(h_{2})) = (h_{1}(f_{1}, f_{2}, \ldots), h_{2}(f_{1}, f_{2}, \ldots)) \in \theta.$$ Hence $(h_{1}(f_{1}, \ldots), h_{2}(g_{1}, \ldots)) = (h_{1} \circ (f_{i})_{i \in \mathbb{N}}, h_{2} \circ (g_{i})_{i \in \mathbb{N}}) \in \theta.$

□

Another question we can ask for left and right congruences is if there are any maximal left and right congruences. We will see that we can definitely answer this question for the left congruences but things get more complicated for right congruences.

First of all we need a small lemma.

Lemma 2.38. Let $\theta \in \text{Con}_{L}(\mathbb{H})$. Then $\theta = \nabla \iff \exists i, j \in \mathbb{N} : i \neq j, (\pi_{i}, \pi_{j}) \in \theta$.

Proof. Clearly $(\pi_{i}, \pi_{j}) \in \theta$ for all $i, j \in \mathbb{N}$ if $\theta = \nabla$. Suppose $(\pi_{i}, \pi_{j}) \in \theta$ for $i \neq j$ and let $f, g \in \hat{H}$.

We know that $(f, g) = (\pi_{i}(f, f, \ldots, f, \, g^{\text{1st pos.}}, f, \ldots), \pi_{j}(f, f, \ldots, f, \, g^{\text{1st pos.}}, f, \ldots))$.

But $(\pi_{i}(f, f, \ldots, f, g, f, \ldots), \pi_{j}(f, f, \ldots, f, g, f, \ldots)) \in \theta.$ □

Theorem 2.39. Let $\theta \in \text{Con}_{R}(\mathbb{H})$. Then there exists a maximal element $\theta_{\text{max}}$ in $\text{Con}_{L}(\mathbb{H})$ with $\theta \subseteq \theta_{\text{max}}$.

Proof. We will proof this statement with the help of Zorn’s Lemma. Define

$$A_{\theta} := \{\alpha \in \text{Con}_{L}(\mathbb{H}) \mid \theta \subseteq \alpha \subseteq \nabla\}$$

and let $T$ be a linear ordered subset of $A_{\theta}$. Moreover, define $\beta := \bigcup_{\alpha \in T} \alpha$ and note that

1. $\forall \alpha \in T : \alpha \subseteq \beta$ and we also have $\theta \subseteq \beta$
2. It is straightforward to show that $\beta \in \text{Con}_{L}(\mathbb{H})$ since $T$ is linear ordered.
3. By our previous lemma we get that

$$\beta \neq \nabla \iff \forall i \neq j : (\pi_{i}, \pi_{j}) \notin \beta \iff \forall \alpha \in T \forall i \neq j : (\pi_{i}, \pi_{j}) \notin \alpha.$$ Hence $\beta \neq \nabla$ since $T \subseteq A_{\theta}$.
We conclude that $\beta$ is an upper bound for $T$ and $\beta \in A_\theta$. By the Lemma of Zorn we get the existence of a maximal element $\theta_{\text{max}} \in A_\theta$. 

\textbf{Remark 2.40.}  1. Observe that if we set $\theta = \Delta$ in 2.39 we get that $\text{Con}_L(\overline{H})$ has a maximal element.

2. The problem with the right-congruences is that we do not know an analogon for lemma 2.38 and therefore we are not able to guarantee that $\beta := \bigcup_{\alpha \in T} \subset \nabla$.

$\text{Con}_L(\overline{H})$ and $\text{Con}_R(\overline{H})$ can also be interpreted in equational logic in the following way: Remember that $\text{Con}(\overline{H})$ is isomorphic to $\text{Su}(V(\mathbb{A}))$ where $\mathbb{A} := (A; H)$. Let $W$ be a subvariety of $V(\mathbb{A})$ and let $\text{ld}_W(X)$ be the set of all equations that are fulfilled by $W$, then the isomorphism was given by $\text{ld}_W(X) \mapsto \{(t^A, s^A) \mid t \approx s \in \text{ld}_W(X)\}$.

Additionally we need a short introduction about Birkhoff's equational calculus (see for example [2, Chapter 2, Section 14]):

\textbf{Definition 2.41.} Let $\mathcal{F}$ be a type and $X$ be an infinite set of variables. Let $t$ be a term of type $\mathcal{F}$ over $X$. The \textit{subterms} of $t$ are defined in the following way

1. $t$ is a subterm of $t$.

2. If $f(t_1, \ldots, t_n)$ is a subterm of $t$ and $f \in \mathcal{F}_n$ then $t_i$ is a subterm of $t$ for all $i$.

\textbf{Definition 2.42.} Let $\Sigma \subseteq \text{ld}(X)$ (for some type $\mathcal{F}$), $t, p, q \in T(X)$ and let $p$ be subterm of $t$. Moreover, let $s$ be the result by replacing the occurrence of $p$ by $q$. $\Sigma$ is \textit{closed under replacement} if $p \approx q \in \Sigma$ implies $t \approx s \in \Sigma$.

\textbf{Definition 2.43.} Let $\Sigma \subseteq \text{ld}(X)$ (for some type $\mathcal{F}$), $t, s, p_1, \ldots, p_n \in T(X)$. $\Sigma$ is \textit{closed under substitution} if $t \approx s \in \Sigma$ implies that $u \approx v \in \Sigma$ where $u, v$ are the resulting terms if we replace simultaneously each variable $x_i$ in $t$ and $s$ by $p_i$.

\textbf{Definition 2.44.} Let $\Sigma \subseteq \text{ld}(X)$ (for some type $\mathcal{F}$). The \textit{deductive closure} $D(\Sigma)$ is the smallest set that is closed under the following rules

1. If $t \in T(X)$ then $t \approx t \in \Sigma$.

2. If $t \approx s \in \Sigma$ then $s \approx t \in \Sigma$.

3. If $t \approx s$, $s \approx u \in \Sigma$ then $t \approx u \in \Sigma$.

4. $\Sigma$ is closed under substitution.

5. $\Sigma$ is closed under replacement.
We know that $D(\text{Id}_W(X)) = \text{Id}_W(X)$. Roughly spoken the congruences correspond to sets of equations that are closed under reflexivity, symmetry, transitivity, substitution and replacements of terms. We will see that also the left- and right congruences correspond to sets of equations with the same properties except that we have to omit substitution for left congruence and replacement of terms for right congruences.

Lemma 2.45. Let $\mathcal{A} := (A; H)$ and $X$ be a infinite set of pairwise distinct variables. We define a function $\phi$ by

$$
\phi : \mathcal{P}(\bar{H^2}) \to \text{Id}_V(\mathcal{A})(X), \quad \phi(M) := \{(t, s) \in T(X) \mid (\bar{t^A}, \bar{s^A}) \in M\}
$$

Then for $\alpha, \beta \subseteq \bar{H^2}$

1. $\phi(\alpha)$ is closed under substitution iff $\alpha \in \text{Con}_R(\bar{H^2})$.

2. $\phi(\beta)$ is closed under replacement iff $\beta \in \text{Con}_L(\bar{H^2})$.

Proof. Let $\alpha \subseteq \bar{H^2}$ with $\phi(\alpha)$ closed under substitution and let $(\bar{f}, \bar{g}) \in \alpha$ with $f, g \in H$ and $(\bar{h}_i)_{i \in \mathbb{N}} \in H^H$ with $h_i \in H$. We have to show that $\lambda((h_i)_{i \in \mathbb{N}})(f), \lambda((h_i)_{i \in \mathbb{N}})(g) \in \alpha$. Since $\mathcal{A} = (A; H)$ there must be $n$-variable terms $t, s, u, t \in T(X)$ such that $\bar{t}^A = \bar{f}$, $\bar{s}^A = \bar{g}$ and for all $i \in \mathbb{N}$ $\bar{u}^A_i = \bar{h}_i$. Then by assumption we know that $(t(u_1, \ldots, u_n), (s(u_1, \ldots, u_n)) \in \phi(\alpha)$ and therefore $(\bar{t}^A(u_1^A, \ldots, u_n^A), (s(u_1^A, \ldots, u_n^A)) \in \alpha$. But

$$(\bar{t}^A(u_1^A, \ldots, u_n^A), (s(u_1^A, \ldots, u_n^A)) = (\bar{t}^A \circ (u_1^A), \ldots, (u_n^A), (s^A) \circ (u_1^A)) = (f \circ h_i, \ldots, g \circ (h_i)) = \lambda((h_i)_{i \in \mathbb{N}})(f), \lambda((h_i)_{i \in \mathbb{N}})(g)).$$

Suppose now that $\alpha \in \text{Con}_R(\bar{H^2})$, let $(t, s) \in \phi(\alpha)$ and $u_1, \ldots, u_n \in T(X)$. Then $(\bar{t}^A, \bar{s}^A) \in \alpha$. Hence, $(\lambda((u_i^A)_{i \in \mathbb{N}})(\bar{t}^A), \lambda((u_i^A)_{i \in \mathbb{N}})(s^A)) \in \alpha$. Thus $(\bar{t}^A \circ (u_1^A), \ldots, (u_n^A), (s^A) \circ (u_1^A)) \in \alpha$ and because of $(\bar{t}^A \circ (u_1^A), \ldots, (u_n^A), (s^A) \circ (u_1^A)) \in \alpha$ it follows that $(\bar{t}^A(u_1, \ldots, u_n), (s(u_1, \ldots, u_n)) \in \phi(\alpha)$.

The proof of the second statement is similar to the first one. Assume that $\beta \subseteq \bar{H^2}$ with $\phi(\beta)$ closed under replacement. Let $h \in H$ and $(f_i, g_i) \in \beta$. Again there exist terms $u, t_i, s_i$ of $\mathcal{A}$ with $\bar{u}^A = h, \bar{t}^A_i = f_i, \bar{s}^A_i = g_i$. If we consider the term $(u(t_1, \ldots, t_n), u(s_1, \ldots, s_n)) \in \phi(\beta)$. With the same arguments as in the first proof we get that $(\bar{u}^A, \bar{t}^A, \bar{s}^A, (u_1^A, \ldots, u_n^A)) = (\lambda((f_i)_{i \in \mathbb{N}}), \lambda((g_i)_{i \in \mathbb{N}})) \in \beta$.

For the last implication let $\beta \in \text{Con}_L(\bar{H^2})$ and let $u$ be a term and $(t, s) \in \phi(\beta)$ such that $t$ is a subterm of $u$ we have to show that $(u, v) \in \phi(\beta)$ where $v$ is the resulting term when we replace the occurrence of $t$ in $u$ by $s$. Since $t$ is a subterm of $u$ there
must exist terms $h$ and $p_i$ such that $u = h(t, p_1, \ldots, p_k)$. We define two sequences of
terms by

$$a_i = \begin{cases} t & i = 1 \\ p_{i-1} & 2 \leq i \leq k + 1 \\ p_k & \text{else} \end{cases} \quad b_i = \begin{cases} s & i = 1 \\ p_{i-1} & 2 \leq i \leq k + 1 \\ p_k & \text{else} \end{cases}$$

for $i \in \mathbb{N}$.

Then we have

$$(\lambda_{\vec{h}}((a_{\vec{h}})_i)_{i \in \mathbb{N}}), \lambda_{\vec{h}}((b_{\vec{h}})_i)_{i \in \mathbb{N}}) = (h_{\vec{h}}(t_{\vec{h}}, p_{\vec{h}}_1, \ldots, p_{\vec{h}}_k), h_{\vec{h}}(s_{\vec{h}}, p_{\vec{h}}_1, \ldots, p_{\vec{h}}_k)) = (u_{\vec{h}}, v_{\vec{h}}) \in \beta$. Therefore we get that $(u, v) \in \phi(\beta)$. \hfill \Box
Chapter 3

Preparing Topics

In chapter one we developed an interesting connection between the subvarieties of an algebra \(A = (A; F)\), \(F \subseteq O(A)\) and the congruences of the clone of term functions \(\text{Clo}(A) = \langle F \rangle\). This link will be used later on to transfer properties of the variety \(V(A)\) and their subvarieties to the congruences of \(\text{Clo}(A)\).

Before we are able to do so we have to learn some interesting facts about some selected sections of universal algebra such as quasi-primal algebras, commutator theory and affine algebras.

3.1 Quasi-primal algebras

The term quasi-primal was first specified by Pixley in [11]. In this section we are following [2, Chapter 4, Section 10]

**Definition 3.1.** Let \(A\) be an algebra. \(A\) is called *quasi-primal* if every function on \(A\) that preserves all isomorphisms between subalgebras of \(A\) is a term function.

Pixley also found a Malcev condition for being quasi-primal.

**Theorem 3.2.** For an algebra \(A\) we have that \(A\) is quasi-primal iff the discriminator \(t(x, y, z) := \begin{cases} z & x = y \\ x & \text{else} \end{cases}\) is a term function of \(A\).

The proof of this theorem can be found in [12].

**Example 3.3.** Let \(\mathbb{B}_2 := \{0, 1\}; \land, \lor, \neg, 0, 1\) be the 2-element Boolean algebra. Then \(t(x, y, z) = ((x \land z) \lor \neg y) \land (x \lor z) \in \text{Clo}(\mathbb{B}_2)\).

**Definition 3.4.** An algebra \(A\) is called *hereditarily simple* if all subalgebras of \(A\) are simple.

The next two lemmas and their proofs can also be found in [2, Chapter 4, Lemma 10.1, 10.4].
Lemma 3.5. (Baker-Pizley) Let $\mathbb{A}$ be a finite algebra with a majority term $M(x, y, z)$ and let $n \geq 1, f \in O^{(n)}(A)$. If $f$ preserves the subalgebras of $\mathbb{A}^2$ (i.e. if $B \leq \mathbb{A}^2$ and $(a_1, b_1), \ldots, (a_n, b_n) \in B$ then $(f(a_1), f(b_1)) \in B$) then there exists an $n$-ary term $p$ of $\mathbb{A}$ such that $p^h = f$.

Proof. Recall that for $(a_1, b_1), \ldots, (b_n, a_n) \in (\mathbb{A}^n)^2$ the generated subuniverse can be described in the following way

$$\left((a_1, b_1), \ldots, (b_n, a_n)\right) = \left\{p\mathbb{A}^2(c_1, \ldots, c_m) \mid m \in \mathbb{N}, p \in T^{[m]}, c_i \in \{(a_1, b_1), \ldots, (b_n, a_n)\}\right\}.$$ 

Let $(a_1, b_1), \ldots, (b_n, a_n) \in (\mathbb{A}^n)^2$. Since $f$ preserves every subalgebra of $\mathbb{A}^2$ there exists a term $q$ such that $q^h((a_1, b_1), \ldots, (b_n, a_n)) = f((a_1, b_1), \ldots, (b_n, a_n))$ or in other words $q^h(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$ and $q^h(b_1, \ldots, b_n) = f(b_1, \ldots, b_n)$.

Let $p_S$ denote the term which equals $f$ on a subset $S$ of $A$.

We are proving by induction on $k := |S|$ that $p_S$ exists for every set $S \subseteq A^n$.

$k = 2$: We have already seen that $p_S$ exists for every $S$.

$k - 1 \rightarrow k$: Let $S \subseteq A^n$ with $|S| = k$ and choose 3 distinct elements from $S$, say $s_1, s_2, s_3$. Define $S_i := S \{s_i\}$ and by the induction hypothesis we get that there exist terms $p_i$ with $p_i|_{S_i} = f|_{S_i}$ for $i \in \{1, 2, 3\}$. Finally define

$$p_S(x_1, \ldots, x_n) := M(p_1(x_1, \ldots, x_n), p_2(x_1, \ldots, x_n), p_3(x_1, \ldots, x_n)).$$

Since at least always to $p_i$ coincide with $f$ on $S$ we obtain that $p_S$ is equal to $f$ on $S$. 

Lemma 3.6. (Fleischer) Let $\mathbb{A}, \mathbb{B}$ be algebras in a congruence permutable variety $\mathcal{V}$ of type $\mathcal{F}$, let $C \subseteq \mathbb{A} \times \mathbb{B}$. Let $\mathbb{A}'$ and $\mathbb{B}'$ be algebras of type $\mathcal{F}$ with universes $\pi_1(C)$ and $\pi_2(C)$ (where $\pi_i$ is the $i$-th projection map).

Then there exists an algebra $\mathbb{D}$ and surjective isomorphisms $\alpha : \mathbb{A}' \rightarrow \mathbb{D}$, $\beta : \mathbb{B}' \rightarrow \mathbb{D}$ such that

$$C = \{(c_1, c_2) \in A' \times B' \mid \alpha(c_1) = \beta(c_2)\}.$$ 

Proof. Let $C \subseteq \mathbb{A} \times \mathbb{B}$, let $\pi_1$ and $\pi_2$ denote the projection maps on the first respectively second variable. Define $\theta := ker(\pi_1) \lor ker(\pi_2)$ and let $\nu$ be the natural map from $C$ to $C/\theta$. Clearly $\pi_i|_C$ are epimorphisms and so with the help of the homomorphism theorem we define $\alpha : \mathbb{A}' \rightarrow C/\theta$ and $\beta : \mathbb{B}' \rightarrow C/\theta$ to be

$$\nu = \alpha \circ \pi_1|_C$$
$$\nu = \beta \circ \pi_2|_C$$

Now let $c \in C$. Then we can write $c = (\pi_1(c), \pi_2(c))$ and we get

$$\alpha(\pi_1(c)) = \nu(c) = \beta(\pi_2(c)).$$
So $c \in \{(c_1, c_2) \in A' \times B' \mid \alpha(c_1) = \beta(c_2)\}$.

Let now $(a, b) \in A' \times B'$ with $\alpha(a) = \beta(b)$ and let $c_1, c_2 \in C$ with $\pi_1(c_1) = a$ and $\pi_2(c_2) = b$. Then

$$\nu(c_1) = \alpha(\pi_1(c_1)) = \alpha(a) = \beta(b) = \beta(\pi_2(c_2)) = \nu(c_2).$$

To put it another way $(c_1, c_2) \in \theta$. Recall $\theta = \ker(\pi_1|_C) \vee \ker(\pi_2|_C)$ and since $V$ was congruence permutable we obtain $\theta = \ker(\pi_1|_C) \circ \ker(\pi_2|_C)$. So there exists a $c \in C$ with $\pi_1(c) = \pi_1(c_1) = a$ and $\pi_2(c) = \pi_2(c_2) = b$. But this means $(a, b) = c \in C$. □

Also the next theorem is due to Pixley and we are following the proof of [2, Chapter 4, Theorem 10.7].

Theorem 3.7. A finite algebra $A$ is quasi-primal iff $V(A)$ is arithmetical (congruence distributive and congruence permutable) and $A$ is hereditarily simple.

Proof. Assume that $A$ is quasi-primal. Then by the characterization of Pixley we know that the discriminator $t(x, y, z)$ is a term function of $A$ and so is $m(x, y, z) := t(x, t(x, y, z), z)$. But it is not hard to check that $m$ is a majority function and therefore $V(A)$ is congruence distributive. Obviously $A \models t(x, x, z) \approx z$, $t(x, y, y) \approx x$ and $t$ is also a Mal'cev term and therefore $V(A)$ is congruence permutable.

If the discriminator $t(x, y, z)$ is part of the term functions $A$ then each subalgebra of $A$ must be simple. Assume $S \leq A$ and $\theta \in \text{Con}(S)$ with $\Delta_S \subset \theta$. Then there exists $(a, b) \in \theta$ with $a \neq b$ and since $t$ is a term function we get that $(t(a, a, c), t(b, a, c)) = (c, b) \in \theta$ for arbitrary $c \in S$. With the transitivity of $\theta$ we get that $\theta = \nabla$.

For the other direction assume that $A$ is arithmetical and hereditarily simple. It is known that a variety $V$ is arithmetical iff it contains a majority term in its term functions (see [2] p. 80). Let $t$ be the discriminator on $A$. We also know by Theorem 3.5 that if $t$ preserves all subalgebras of $A^2$ then $t \in \text{Clo}(A)$.

So let $S \leq A^2$ and let for $i \in \{1, 2\}$ $S_i$ be the image of $S$ under the $i$-th projection map.

By Lemma 3.6 there exist an algebra $D$ and surjective homomorphisms $\alpha : S_1 \rightarrow D$, $\beta : S_2 \rightarrow D$ such that

$$S = \{(s_1, s_2) \in S_1 \times S_2 \mid \alpha(s_1) = \beta(s_2)\}.$$

First of all we know that $S_i \leq S$ and therefore the $S_i$ are simple. Moreover, $D \cong S_1/\ker(\alpha)$ or in other words $D$ is either trivial or $\alpha$ and $\beta$ are isomorphisms.

1. Case: $\alpha$, $\beta$ isomorphisms

We conclude that

$$S = \{(s_1, \beta^{-1}(\alpha(s_1)) \mid s_1 \in S_1\}$$

and observe that for $(u_1, u_2), (v_1, v_2) \in S$ we have that $(u_1, u_2) = (v_1, v_2)$ iff $u_1 = v_1$ iff $u_2 = v_2$.

For $(a_1, a_2), (b_1, b_2)$ and $(c_1, c_2) \in S$ we get
\[ (t(a_1, b_1, c_1), t(a_2, b_2, c_2)) = \begin{cases} (c_1, c_2) & a_1 = b_1 \\ (a_1, a_2) & a_1 \neq b_1 \end{cases} \]

So we get that in this case \( t \) preserves \( S \).

2. Case: \( \mathbb{D} \) trivial

It immediately follows that

\[ S = S_1 \times S_2 \]

Now we have that for \( (a_1, a_2), (b_1, b_2) \) and \( (c_1, c_2) \in C \)

\[ (t(a_1, b_1, c_1), t(a_2, b_2, c_2)) \in \{(a_1, a_2), (a_1, c_2), (c_1, a_2)\} \subseteq S. \]

\[ \square \]

### 3.2 Commutator theory

This section follows the book of R. Freese and R. McKenzie. We will only need some basic properties and theorems of this deep theory. For more details and information we refer to [4].

The basic idea of this theory is to generalize the notion of the commutator \([x, y] := x^{-1}y^{-1}xy\) in group theory to universal algebra.

If we define for \( M, N \leq G \), a group \([M, N] := \{[m, n] \mid m \in M, n \in N\}\) (generated subgroup of \( G \)) then the following property is well known for \( H := [M, N] \)

1. \( H \) is normal.

2. \( H \) is the least subgroup such that \( M/H \) commutes with \( N/H \) in \( G/H \).

In general there is more than one way to define a commutator in universal algebra. But for a congruence modular variety it can be shown that they are all equivalent (see [4, Chapter 4]). We will use a definition that is motivated by the properties we have seen above.

**Definition 3.8.** Let \( \mathcal{V} \) be variety (not necessarily modular), \( A \in \mathcal{V} \) and let \( \alpha, \beta, \delta \in \Con(A) \).

1. \( M(\alpha, \beta) \) is defined as the set of \( 2 \times 2 \) matrices of the form

\[
\begin{pmatrix}
(t(a_1, b_1, c_1), t(a_2, b_2, c_2)) & t(a_1, a_1^2, b_1(b_2^1, b_2^2)) \\
(t(a_1, a_1, b_1(b_2^1, b_2^2)) & t(a_2, a_2^2, b_2(b_1^1, b_1^2))
\end{pmatrix}
\]

where \( t \) is a term of \( A \) with arity \( n + m \) and \( a_i^1, b_i \in A \) with \( (a_i^1, a_i^2) \in \alpha \) and \( (b_i, b_i^2) \in \beta \) for \( 1 \leq i \leq n \) and \( 1 \leq k \leq m \).
2. We say \( \alpha \) centralizes \( \beta \) modulo \( \delta \) if for all matrices \( \left( \begin{array}{cc} u_1 & u_2 \\ u_3 & u_4 \end{array} \right) \in M(\alpha, \beta) \) we have that \((u_1, u_2) \in \delta \) implies \((u_3, u_4) \in \delta \).
We will abbreviate this property by \( C(\alpha, \beta; \delta) \).
3. \([\alpha, \beta]\) is the smallest \( \delta \) in \( \text{Con}(A) \) for which \( C(\alpha, \beta; \delta) \) is true.

By some basic calculations one can verify it is always true that \( \alpha \) centralizes \( \beta \) modulo \( \alpha \wedge \beta \) so the definition of 3) makes sense.
The properties listed beneath can be immediately derived from the definition of the commutator.

**Lemma 3.9.** For \( \alpha, \beta, \delta \in \text{Con}(A) \) and \( A \in \mathcal{V} \) for some variety \( \mathcal{V} \) we have

1. \( C(\alpha, \beta; \alpha \wedge \beta) \) holds
2. \( C(\alpha, \beta; \delta) \) is monotone in both arguments
3. \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M(\alpha, \beta) \iff \left( \begin{array}{cc} c & d \\ a & b \end{array} \right) \in M(\beta, \alpha) \)

**Definition 3.10.** We call an algebra \( A \) abelian if \( |\nabla, \nabla| = \Delta \).

**Notation.** If not stated otherwise then \( \mathcal{V} \) will denote from now on a congruence modular variety with Day terms \( m_0(x_1, x_2, x_3, x_4), \ldots, m_n(x_1, x_2, x_3, x_4) \) for some \( n \in \mathbb{N} \).
First of all we have to establish some important properties of the commutator.

**Definition 3.11.** \( \alpha, \beta \in \text{Con}(A) \) for some \( A \in \mathcal{V} \).
Then \( X(\alpha, \beta) := \{(m_i(a, b, d, c), m_i(a, a, c, c)) \mid 0 \leq i \leq n, \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M(\alpha, \beta)\} \).

**Lemma 3.12.** For \( \alpha, \beta, \delta \in \text{Con}(A) \) and \( A \in \mathcal{V} \) the following are equivalent

1. \( X(\alpha, \beta) \subseteq \delta \)
2. \( X(\beta, \alpha) \subseteq \delta \)
3. \( C(\alpha, \beta; \delta) \) holds
4. \( C(\beta, \alpha; \delta) \) holds

Moreover, we have that \( \text{Cg}(X(\alpha, \beta)) = [\alpha, \beta] \).

**Proof.** We start with the implication 3) \( \Rightarrow \) 1). Let \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M(\alpha, \beta) \) and let \((u_i, v_i) := (m_i(a, b, d, c), m_i(a, a, c, c)) \) for \( 0 \leq i \leq n \). We have to show that \((u_i, v_i) \in \delta \forall i \). We will do this by proving that every \((u_i, v_i) \) belongs to a matrix of the form \( \left( \begin{array}{cc} u & v \\ w & w \end{array} \right) \). Then we get \((u_i, v_i) \in \delta \) by the facts that \( C(\alpha, \beta; \delta) \) holds, \((w, w) \in \delta \) and Lemma 3.9.
Let \( t \) be the \( n + m \)-ary term that constructs the matrix \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \) with the \( n \)-tuples \( a^1, a^2 \) and \( m \)-tuples \( b^1, b^2 \). Consider the terms \( s_i : A^{4n+4m} \to A \).
CHAPTER 3. PREPARING TOPICS

\[ s_i(x^1, x^2, y^1, y^2, y^3, y^4, y^5, y^6) = m_i(t(y^1, y^2), t(x^1, y^3), t(y^4, y^5), t(x^2, y^6)) \]

where \( x^i \) and \( y^i \) are placeholders for a tuple of variables of length \( n \) or \( m \).

Together with the tuples \( \bar{a}^1 := (a^2, a^1), \bar{a}^2 := (a^1, a^2) \) and \( \bar{b}^1 := (a^1, b^1, b^2, a^2, b^2, b^1), \bar{b}^2 := (a^1, b^1, b^1, a^2, b^1, b^1) \). Observe that each \( s_i \) produces the matrix \( \begin{pmatrix} w_i & w_i \\ w_i & w_i \end{pmatrix} \).

\[
\begin{align*}
  s_i(\bar{a}^1, \bar{b}^1) &= m_i(t(a^1, b^1), t(a^2, b^2), t(a^2, b^2), t(a^1, b^1)) = t(a^1, b^1) =: w \\
  s_i(\bar{a}^1, \bar{b}^2) &= m_i(t(a^1, b^1), t(a^2, b^1), t(a^2, b^1), t(a^1, b^1)) = t(a^1, b^1) = w \\
  s_i(\bar{a}^2, \bar{b}^1) &= m_i(t(a^1, b^1), t(a^1, b^2), t(a^2, b^2), t(a^2, b^1)) = m_i(a, b, c, d) = u_i \\
  s_i(\bar{a}^2, \bar{b}^2) &= m_i(t(a^1, b^1), t(a^1, b^1), t(a^2, b^1), t(a^2, b^1)) = m_i(a, a, c, c) = v_i
\end{align*}
\]

1) \( \Rightarrow \) 4) We will use a certain property of the Day terms \( m_i, i \leq n \) of \( V \) that is:

For an algebra \( A \in V \), \( \gamma \in \con(A) \) and \( a, b, c, d \in A \) with \( (b, d) \in \gamma \). Then \( (a, c) \in \gamma \) if and only if for all \( 0 \leq i \leq n \) \( (m_i(a, a, c, c), m_i(a, b, c, d)) \in \gamma \).

Let now \( (b, d) \in M(\beta, \alpha) \) and let \( (b, d) \in \delta \). We want to show that \( C(\alpha, \beta; \delta) \) holds this means we have to show \( (a, c) \in \delta \).

First notice that \( (b, d) \in M(\alpha, \beta) \) and therefore \( (a, b) \in M(\alpha, \beta) \). (If \( t, a^1, a^2, b^1, b^2 \) construct the matrix \( (b, d) \) then \( t, a^1, a^2, b^2, b^1 \) construct \( (a, b) \).)

Now by assumption we know that \( X(\alpha, \beta) \subseteq \delta \) hence \( \forall i : (m_i(a, a, c, c), m_i(a, c, c, d)) \in \delta \). Finally by the above stated property we get that \( (a, c) \in \delta \).

The implications 4) \( \Rightarrow \) 2) and 2) \( \Rightarrow \) 3) follow immediately by swapping \( \alpha \) with \( \beta \) in the previous proofs. The fact that \( X(\alpha, \beta) \) is a set of generators for \([\alpha, \beta]\) follows directly form the previous equivalences. \( \square \)

**Lemma 3.13.** Let \( A \in V \) and let \( \alpha, \beta_i \in \con(A), i \in I \). Then we have

\[ [\alpha, \bigvee_{i \in I} \beta_i] = \bigvee_{i \in I} [\alpha, \beta_i] \]

**Proof.** First of all note that \( \bigvee_{i \in I} [\alpha, \beta_i] \leq [\alpha, \bigvee_{i \in I} \beta_i] \) by the monotonicity of the commutator.

By our previous lemma we know that for the second inclusion we have to show that \( C(\alpha, \beta; \bigvee_{i \in I} [\alpha, \beta_i]) \) holds where \( \beta := \bigvee_{i \in I} \beta_i \).

Let \( (u, v) \in M(\alpha, \beta) \) with \( (u, v) \in \bigvee_{i \in I} [\alpha, \beta_i] \) and let \( t \) be a term function and \( (a^1_1, a^2_1), \ldots, (a^1_n, a^2_n) \in \alpha, (b^1_1, b^2_1), \ldots, (b^1_m, b^2_m) \in \beta \) such that they construct \( (u, v) \).

Since \( \forall i : (b^1_l, b^2_l) \in \beta \) there exist \( c_{i,l} \in A \) and \( r_l \in I \) for \( 1 \leq l \leq N \) such that

\[ (b^1_l, c_{i,l}) \in \beta_{r_l}, (c_{i,2}, c_{i,3}) \in \beta_{r_2}, \ldots, (c_{i,N}, b^2_l) \in \beta_{r_N} \]

Consider the matrices \( B_i \) defined in the following way.
\[
B_1 := \begin{pmatrix} t(a^1, b_1^1, \ldots, b_m^1) \\ t(a^2, b_1^1, \ldots, b_m^1) \end{pmatrix}, \quad B_2 := \begin{pmatrix} t(a^1, c_{1,2}, \ldots, c_{m,2}) \\ t(a^2, c_{1,2}, \ldots, c_{m,2}) \end{pmatrix}, \quad \vdots \\
B_M := \begin{pmatrix} t(a^1, c_{1,N}, \ldots, c_{m,N}) \\ t(a^2, c_{1,N}, \ldots, c_{m,N}) \end{pmatrix}
\] \in M(\alpha, \beta_{r_1})
\]

Since \( \forall i : [\alpha, \beta_i] \leq \bigvee_{j \in I}[\alpha, \beta_j] \) we get by 3.12 that \( \forall i : C(\alpha; \beta_i; \bigvee_{j \in I}[\alpha, \beta_j]) \) holds. By assumption the first column of \( B_1 \) is in \( \bigvee [\alpha, \beta_i] \) and so we get inductively that \( (t(a^1, b^2), t(a^2, b^2) = (r, s) \in \bigvee [\alpha, \beta_i] \) and this concludes the proof.

**Lemma 3.14.** Let \( \Lambda, \mathbb{B} \in \mathcal{V} \) and \( \alpha, \beta \in \text{Con}(\Lambda) \) and \( \phi : \Lambda \rightarrow \mathbb{B} \) be an epimorphism and let \( \pi = \text{ker}(\phi) \). Then

\[ [\alpha, \beta] \vee \pi = \phi^{-1}([\phi(\alpha \vee \pi), \phi(\beta \vee \pi)]). \]

**Proof.** By Lemma 3.13 we conclude that \( [\alpha, \beta] \vee \pi = [\alpha \vee \pi, \beta \vee \pi] \). Hence we can assume that \( \alpha, \beta \geq \pi \). Now \( \phi \) maps the set of generators \( X(\alpha, \beta) \cup \pi \) (see Lemma 3.12 onto a set of generators in \( [\phi(\alpha), \phi(\beta)] \) and we obtain \( \phi([\alpha, \beta] \vee \pi) = [\phi(\alpha) \vee \phi(\beta)] \). But this is equivalent to \( [\alpha, \beta] \vee \pi = \phi^{-1}([\phi(\alpha \vee \pi), \phi(\beta \vee \pi)]). \)

**Definition 3.15.** An algebra \( \Lambda \) is said to be neutral if its congruence lattice fulfills the following identity

\[ \text{Con}(\Lambda) \models [x, y] \approx x \wedge y. \]

**Lemma 3.16.** Let \( \Lambda \) be an algebra in \( \mathcal{V} \). Then

1. If \( \Lambda \) is neutral then \( \text{Con}(\Lambda) \) is distributive.
2. Every subdirect product of finitely many neutral algebras is neutral.

**Proof.** Assume for the first statement that \( \Lambda \) is neutral i.e. \( \text{Con}(\Lambda) \models [x, y] \approx x \wedge y \). Let \( \alpha, \beta, \gamma \in \text{Con}(\Lambda) \). By the fact that \( \Lambda \) is neutral we get

\[ (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) = [\alpha, \beta] \vee [\alpha, \gamma] \]

\[ \overset{3.13}{=} [\alpha, \beta \vee \gamma] \]

\[ = \alpha \wedge (\beta \vee \gamma). \]
Hence $\text{Con}(\mathbb{A})$ is distributive.

For the second statement let $\mathbb{B}_1$ and $\mathbb{B}_2$ be neutral algebras in $\mathcal{V}$ and $\mathbb{A} \leq \mathbb{B}_1 \times \mathbb{B}_2$ with $\pi_1(A) = B_1$ and $\pi_2(A) = B_2$. Let $x, y \in \text{Con}(\mathbb{A})$, we have to show $[x, y] \approx x \wedge y$.

We will prove the second statement of the lemma with the help of 3 claims: For the following claims let $x, y \in \text{Con}(\mathbb{A})$ and $\eta_i := \ker(\pi_i)$ for $i \in \{1, 2\}$.

Claim 1. $(x \lor \eta_i) \land (y \lor \eta_i) = [x, y] \lor \eta_i$ for $i \in \{1, 2\}$.

Proof. Of course $\pi_1$ and $\pi_2$ are epimorphisms and by Lemma 3.14 we get for every $i \in \{1, 2\}$

$$[x, y] \lor \eta_i = \pi_i^{-1}([\pi_i(x \lor \eta_i), \pi_i(y \lor \eta_i)])$$

$$= \pi_i^{-1}(\pi_i(x \lor \eta_i) \land \pi_i(y \lor \eta_i))$$

$$= \pi_i^{-1}(\pi_i(x) \land \pi_i(y))$$

$$= (x \lor \eta_i) \land (y \lor \eta_i).$$

Notice that we use in the second equality the neutrality of $\mathbb{B}_1$ and $\mathbb{B}_2$ and so we have to proof the remaining two steps in order to complete the proof.

For simplicity let $i = 1$. First of all we will prove that $\pi_1(x) = \pi_1(x \lor \eta_1)$. It is clear that $\pi_1(x) \subseteq \pi_1(x \lor \eta_1)$. Let $(a, b) \in \pi_1(x \lor \eta_1)$ then there exists $(c, d) \in A$ such that $(a, c), (b, d) \in x \lor \eta_1$. Thus there exist $(e_1, f_1), \ldots, (e_n, f_n) \in A$ such that $((a, c), (e_1, f_1)) \in x, ((e_1, f_1), (e_2, f_2)) \in \eta_1, \ldots, ((e_n, f_n), (b, d)) \in \alpha$ for $\alpha = x$ if $n \equiv 0 \pmod{2}$ or $\alpha = \eta_1$ if $n \equiv 1 \pmod{2}$.

Observe that

1. $\pi_1(x) \in \text{Con}(\mathbb{B}_1)$
2. $e_i = e_{i+1}$ for $i \equiv 1 \pmod{2}$ and $(e_i, e_{i+1}) \in \pi_1(x)$ for $i \equiv 0 \pmod{2}$
3. $(a, e_1), (e_n, b) \in \pi_1(x)$

But then we get $(a, b) \in \pi_1(x)$. For $i=2$ the proof can be done analogously.

Last but not least we have to prove the equality $\pi_1^{-1}(\pi_1(x) \land \pi_1(y)) = (x \lor \eta_1) \land (y \lor \eta_1)$. Let $((a, b), (c, d)) \in (x \lor \eta_1) \land (y \lor \eta_1)$. If we repeat the same arguments from before we get that $(a, c) \in \pi_1(x)$ and $(a, c) \in \pi_1(y)$. But then obviously $(a, b), (c, d) \in \pi_1^{-1}(\pi_1(x) \land \pi_1(y))$. Suppose now that $((a, b), (c, d)) \in \pi_1^{-1}(\pi_1(x) \land \pi_1(y))$. Thus $(a, c) \in \pi(x) \land \pi(y)$ and so there exist $(e_1, f_1), (e_2, f_2) \in A$ such that $((a, e_1), (c, f_1)) \in x$ and $((a, e_2), (c, f_2)) \in y$. We know that $((a, e_1), (a, b)), ((c, f_1), (c, d))$ and $((a, e_2), (a, b)), ((c, f_2), (c, d)) \subseteq \eta_1$ and therefore $((a, b), (c, d)) \in (x \lor \eta_1) \land (y \lor \eta_1)$.

An immediate consequence of the claim is that $x \land y \leq [x, y] \lor \eta_i$ for $i \in \{1, 2\}$. But together with the modular law we get that

$$x \land y = (x \land y) \land ([x, y] \lor \eta_i) = [x, y] \lor (x \land y \land \eta_i)$$
for \( i \in \{1, 2\} \).

If we substitute \( x \land \eta_i \) and \( y \land \eta_i \) for \( x \) and \( y \) we get the following equation

\[
x \land y \land \eta_i = [x \land \eta_i, y \land \eta_i] \lor (x \land \eta_i \land y \land \eta_i \land \eta_j) = [x \land \eta_i, y \land \eta_i]\]

for \( i, j \in \{1, 2\} \) and \( i \neq j \).

In order to finish the proof we have to combine the two equations for \( i = 1 \) of the first pair and the second pair:

\[
x \land y = [x, y] \lor (x \land y \land \eta_1)
\]

\[
= [x, y] \lor [x \land \eta_1, y \land \eta_1]
\]

\[
= [x \lor (x \land \eta_1), y \lor (y \land \eta_1)]
\]

\[
= [x, y].
\]

This finishes the proof. \( \Box \)

With the help of the preceding lemmata we are able to prove the first important theorem that will be very useful in a later chapter.

**Theorem 3.17.** Let \( A \) be a finite simple algebra in \( V \) such that every proper subalgebra of \( A \) is trivial. Then \( A \) generates either a congruence distributive or an abelian subvariety of \( V \).

*Proof.* Suppose \( A \in V \) as stated above and \( V(A) \) is not abelian. Since \( \text{Con}(A) = \{\nabla, \Delta\} \) we get that \( [\Delta, \Delta] = \Delta \). But from this we conclude that \( \text{Con}(A) \models [x, y] \approx x \land y \). Hence \( A \) and its subalgebras are neutral.

Now we know by the fact that \( A \) is finite that \( F_{V(A)}(3) \) must be a finite subdirect power of \( A \). Moreover, by Lemma 3.16 \( F_{V(A)}(3) \) must be neutral and therefore \( \text{Con}(F_{V(A)}(3)) \) is distributive. The congruence distributivity of \( V(A) \) follows now by \( [7, \text{Theorem } 2.1] \). \( \Box \)

In the next chapters we are especially interested in so called strictly simple algebras (algebras which are simple and only have trivial subalgebras). We will need this notion in order to describe minimal varieties, which is exactly the reason why we proved Theorem 3.17.

For the same reason our next goal is to prove that a simple abelian algebra can only have trivial proper subalgebras (i.e. it is strictly simple).

**Theorem 3.18.** Let \( A \) be a simple abelian algebra and \( A \in V \). If \( S \) is a proper subalgebra of \( A \) then \( |S| = 1 \).

Before we can go on to the proof we need some preparation and have to establish some very interesting properties of the commutator concerning difference terms and term functions.
**Theorem 3.19.** If \( \mathcal{V} \) is a congruence modular variety then there exists a 3-ary term \( d \) satisfying the following properties.

1. \( \mathcal{V} \models d(y, y, x) \approx x \).
2. For \( (x, y) \in \alpha \in \text{Con}(\mathcal{A}) \) and \( \mathcal{A} \in \mathcal{V} \) we have \( (d(x, y, y), x) \in [\alpha, \alpha] \).
3. Let \( \alpha, \beta, \gamma \in \text{Con}(\mathcal{A}) \) and \( \mathcal{A} \in \mathcal{V} \), if \( \alpha \wedge \beta \leq \gamma \) then the implication of the following figure holds.

![Diagram](image)

**Proof.** Since we know that \( \mathcal{V} \) is congruence modular there must exist Day terms \( m_i(x, y, z, w) \) for \( 0 \leq i \leq n \) and some \( n \in \mathbb{N} \).
We define terms \( q_i(x, y, z) \) for \( 0 \leq i \leq n \) inductively

\[
q_0(x, y, z) := z
\]

\[
q_{i+1}(x, y, z) := \begin{cases} m_i(q_i(x, y, z), y, x, q_i(x, y, z)) & \text{if } i \text{ odd} \\ m_i(q_i(x, y, z), x, y, q_i(x, y, z)) & \text{if } i \text{ even} \end{cases}
\]

and set \( d(x, y, z) := q_n(x, y, z) \). Since all Day terms fulfill the equation \( m_i(x, y, y, x) \approx x \) we get that \( \mathcal{V} \models d(y, y, x) \approx x \).
For the second property we will proof the following claim.

**Claim.** If \( (x, y) \in \alpha \) then

1. \( (q_i(x, y, y), m_i(y, y, x)) \in [\alpha, \alpha] \) for \( i \) odd
2. \( (q_i(x, y, y), m_i(y, x, x)) \in [\alpha, \alpha] \) for \( i \) even.

In order to prove this claim we perform an induction on \( i \). For \( i = 0 \) we get

\( (q_0(x, y, y), m_0(y, y, x)) = (y, y) \in [\alpha, \alpha] \). Now assume \( i \geq 0 \) and \( i \) is odd. First of all we use the definition of \( q_{i+1} \) and the induction hypothesis and obtain

\[
q_{i+1}(x, y, y) = m_{i+1}(q_i(x, y, y), y, x, q_i(x, y, y))
\]

and

\[
(m_{i+1}(q_i(x, y, y), y, x, q_i(x, y, y)), m_{i+1}(m_i(y, y, x), y, x, m_i(y, y, x))) \in [\alpha, \alpha].
\]

(*)
With the help of the equations fulfilled by the Day terms we can write

\[ m_{i+1}(m_i(y, y, y, x), y, y, m_i(y, y, y, x)) = m_i(y, y, y, x) = m_{i+1}(y, y, y, x) = m_{i+1}(m_i(y, y, y, y), y, y, m_i(x, x, x, x)) \]

Recall the definition of the commutator \([\alpha, \alpha]\) and define the 10-variable term \(t\) as the term we encountered before

\[ t(x_1, \ldots, x_{10}) := m_{i+1}(m_i(x_2, x_3, x_4, x_5), x_6, x_1, m_i(x_7, x_8, x_9, x_{10})) \]

Moreover, let \(a^1 = (y), a^2 = (x), b^1 = (y, y, x, y, y, x, y, y, x, x), b^2 = (y, y, y, y, x, x, x, x, x, x)\). First of all note that \((a^1_i, a^2_i, b^1_i, b^2_i) \in \alpha\) for all \(i\) since \((x, y) \in \alpha\) and the additionally we can write the equation from before as \(t(a^1, b^1) = t(a^1, b^2)\).

Thus, \((t(a^1, b^1), t(a^1, b^2)) \in \alpha\) and by the definition of \([\alpha, \alpha]\) we get that \((t(a^1, b^1), t(a^2, b^2)) \in \alpha\). If we plugin for \(t\), \(a^2, b^1, b^2\) we get

\[ (m_{i+1}(m_i(y, y, y, x), y, x, m_i(y, y, y, x)), m_{i+1}(m_i(y, y, y, y), y, x, m_i(x, x, x, x))) \in [\alpha, \alpha]. \]

The first part of the claim follows now by transitivity with \((*)\) and by

\[ m_{i+1}(m_i(y, y, y, y), x, m_i(x, x, x, x)) = m(y, y, x, x). \]

The second part of the claim can be done analogously. For more details we refer to [4].

By the fact that \(\mathcal{V} \models m_n(x, y, z, w) \approx w\) since \(m_i\) are Day terms we get that \((d(x, y, y), x) \in [\alpha, \alpha]\) which proves the second statement.

For the last property assume \(\alpha, \beta, \gamma \in \text{Con}(A), \alpha \land \beta \leq \gamma\) and that the relations displayed by the figure beneath holds.

\[
\begin{array}{c}
\alpha \\
y \\
\beta \\
u \\
v \\
\gamma \\
x \\
z
\end{array}
\]

It is not hard to check that the following relations are true

a) \((d(u, v, y), d(y, y, y)) = (d(u, v, y), y) \in \beta\)

b) \((d(u, v, y), d(z, v, y)) \in \gamma\)

c) \((d(z, v, y), d(z, z, x)) = (d(z, v, y), x) \in \alpha\)

d) \((d(z, v, y), d(x, y, y)) \in \beta\)
If we take a look at the figure above we conclude that \((x,y) \in \alpha \land (\beta \lor \gamma)\) and by the second property of \(d\) we get \((d(x,y),x) \in [\alpha \land (\beta \lor \gamma), \alpha \land (\beta \lor \gamma)]\). Note that

\[
[\alpha \land (\beta \lor \gamma), \alpha \land (\beta \lor \gamma)] \leq [\alpha, \beta \lor \gamma] = [\alpha, \beta] \lor [\alpha, \gamma] \leq (\alpha \land \beta) \lor (\alpha \land \gamma) = \alpha \land \gamma.
\]

By d) we obtain that \((d(z,v,y),x) \in \beta \lor (\alpha \land \gamma)\) and with c) we have \((d(z,v,y),x) \in \alpha \land (\beta \lor (\alpha \land \gamma))\). Thus by the modular law we get \(\alpha \land (\beta \lor (\alpha \land \gamma)) = (\alpha \land \beta) \lor (\alpha \land \gamma) = \alpha \land \gamma\) and therefore by b) \((d(u,v),x) \in \gamma\).

The term \(d\) defined in the proof above is often called difference term. A very interesting property of this difference term is stated in the next theorem.

**Theorem 3.20.** Let \(A \in \mathcal{V}\) and abelian. Then every term function \(t \in \text{Clo}(A)\) commutes with the difference term of \(\mathcal{V}\) i.e.

\[
d(t(x_1,\ldots, x_n), t(y_1,\ldots, y_n), t(z_1,\ldots, z_n)) = t(d(x_1, y_1, z_1),\ldots, d(x_n, y_n, z_n))
\]

**Proof.** Let \(\eta_1, \eta_2\) be the kernels of the projections on the first and second component and define \(\theta := Cg(\{(x,y) \mid x,y \in A\})\) on \(A^2\). Then we have the following relations for \(x_i, y_i, z_i\) and \(1 \leq i \leq n\).

\[
\begin{array}{ccc}
(z_i, y_i) & \eta_1 & (y_i, y_i) \\
\eta_2 & \theta & \\
(z_i, x_i) & (x_i, x_i) & (y_i, x_i)
\end{array}
\]

On the one hand we can apply 3.20 (note that \(\eta_1 \land \eta_2 = \Delta_{A^2} \leq \theta\)) and obtain

\[
(d(x_i, y_i, z_i), d(x_i, x_i, x_i)) = d(x_i, y_i, z_i), x_i) \theta (z_i, y_i)
\]

and apply \(t\) on the congruences which results in

\[
(t(d(x_1, y_1, z_1),\ldots, d(x_n, y_n, z_n)), t(x)) \theta (t(z), t(y))
\]

But on the other hand we can do it the other way around. This means first applying \(t\) to the figures

\[
\begin{array}{ccc}
(t(z), t(y)) & \eta_1 & (t(y), t(y)) \\
\eta_2 & \theta & \\
(t(z), t(x)) & (t(x), t(x)) & (t(y), t(x))
\end{array}
\]
and using Theorem 3.20 afterwards

\[ (d(t(x), t(y), t(z)), t(x)) \theta (t(z), t(y)). \]

Observe that \( \theta = \{((x, x), (y, y)) \mid x, y \in A\} \cup \Delta_{A^2}\). But since we know that

\[ (d(t(x), t(y), t(z)), t(x)) \theta (t(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)), t(x)) \]

the proof is finished. \(\square\)

**Remark 3.21.** Theorem 3.20 is just a special case of a more general theorem in [4] (Proposition 5.7). In full glory the theorem states that the commuting condition for \(x_i, y_i, z_i\) is equivalent to \([\alpha, \beta] = \Delta\) provided \(x_i \beta y_i \alpha z_i\).

Finally we are able to prove that a proper subalgebra of a simple abelian algebra must be trivial.

**Proof of Theorem 3.18:** Let \(d\) be a difference term of \(A\), \(S\) be a subuniverse of \(A\) and let \(s \in S\). Then we define

\[ \theta := \{(x, y) \mid d(x, y, s) \in S\}. \]

We will see that \(\theta\) is a congruence of \(A\). reflexivity follows from \(d(x, x, y) \approx y\) (see Theorem 3.19). Suppose now that \((x, y) \in \theta\) i.e. \((x, y, s) \in S\). Since \(d\) is a term of \(A\) and \((x, y, s) \in S\) and \(d(y, y, s) = d(s, s, s) = s \in S\) also the following expression must be in \(S\)

\[ e := d(y, y, s), d(x, y, s), d(s, s, s)). \]

Now we use the fact that \(A\) is abelian and therefore \(d\) commutes with every term function of \(A\), especially with itself (Theorem 3.20). We get that

\[ e = d(d(y, x, s), d(y, y, s), d(s, s, s)) = d(d(y, x, s), s, s) = d(y, x, s). \]

Observe that we used in the last equality Theorem 3.19 2). To be more precise we have that \(\forall x \in A : (d(x, y, y), x) \in [\nabla, \nabla]\). But since \(A\) is abelian we get that \(d(x, y, y) = x\). Hence \(\theta\) is symmetric.

Assume \((x, y), (y, z) \in \theta\). We are following a similar strategy as before

\[ d(x, z, s) = d(d(x, z, s), d(y, y, s), d(s, s, s)) \]

Again since \(d\) is a term and all the arguments are in \(S\) we get that \(d(x, z, s) \in S\) and therefore \(\theta\) is an equivalence relation. The fact that \(\theta\) is a congruence follows from the circumstance that \(d\) is commuting with every term function of \(A\).

Since we know that \(\theta \in \text{Con}(A) = \{\Delta, \nabla\}\) we have to distinguish two cases:

1. Case: \(\theta = \nabla\)
   Let \(x \in A\). Then \((x, s) \in \theta = \nabla\) and it follows that \(x = d(x, s, s) \in S\). Hence \(S = A\)
which is a contradiction.

2. Case: $\theta = \Delta$
We have that
\[
\{s\} = s/\theta = \{a \in A \mid (a, s) \in \theta\} = \{a \in A \mid d(a, s, s) \in S\} = \{a \in A \mid a \in S\} = S
\]
\[
\square
\]

**Definition 3.22.** Let $A$ be an algebra and let $\alpha = C_g(\{(u, u), (v, v) \mid u, v \in A\})$ then we define $A_{\alpha} := (A \times A)/\alpha$.

We already know that a simple abelian algebra cannot have any proper subalgebras except trivial ones. It is even possible to give a detailed description of the variety generated by a finite simple abelian algebra as the next theorem shows. The proof of this deep result highly depends on commutator theory which is why we refer to [4] for the proof.

Before we can state the theorem we need the definition of a Boolean power. It should be mentioned that we only state the definition, for more details we refer to [2, Chapter 4].

**Definition 3.23.** Let $A$ be an algebra, $B$ be a Boolean algebra then we define the following objects:

1. Let $(X, \tau)$ be a topological space. A *subbasis* is a system $S$ of subsets of $X$ such that $S \subseteq \tau$ and for each open set $U$ and each $x \in U$, there are finitely many $S_1, \ldots, S_n \in S$ such that $x \in \bigcap_{i=1}^n S_i \subset U$.

2. $B^*$ denotes the topological space whose underlying set is the set of ultrafilters of $B$. Moreover, the topology of $B^*$ has a subbasis of the form $N_a = \{U \in B^* \mid a \in U\}$ for all $a \in B$.

3. $A[B^*]$ denotes the set of all continuous functions from $B^*$ to $A$, giving $A$ the discrete topology.


**Theorem 3.24.** Let $A$ be a finite simple abelian algebra with $n := |A|$ and $A \in \mathcal{V}$. Then $n$ is a prime power and

1. If $A$ has a trivial subalgebra, then
   
   (a) Every finite algebra of $V(A)$ is isomorphic to a direct power of $A$ and every infinite algebra of $V(A)$ is a Boolean power of $A$.
   
   Thus $V(A)$ is minimal.
   
   (b) All algebras in $V(A)$ of cardinality $\lambda$ are isomorphic, for each $\lambda$.  

CHAPTER 3. PREPARING TOPICS

2. If \( \mathbb{A} \) has no trivial subalgebra, then

(a) All finite algebras in \( V(\mathbb{A}) \) are direct powers of \( \mathbb{A} \) or \( \mathbb{A}_\varphi \) and all algebras in \( V(\mathbb{A}) \) are Boolean powers of \( \mathbb{A} \) or \( \mathbb{A}_\varphi \).

(b) \( V(\mathbb{A}_\varphi) \) is the unique subvariety of \( V(\mathbb{A}) \).

Observe that the fact that for a finite, simple, abelian algebra \( V(\mathbb{A}) \) is minimal iff \( \mathbb{A} \) has at least one trivial subalgebra is a direct consequence of 3.24. This fact will be very important later on when we examine minimal varieties of a locally finite congruence permutable variety.

3.3 **Affine algebras**

The aim of this section is to prove that every simple abelian algebra with at least one trivial subalgebra has a finitely based equational theory. This fact is well understood and for example in chapter 14 of [4] one can even find more general theorems concerning this topic which include our goal as a special case. But since this theorems would take us to far into commutator theory we have to find a different way to achieve our goal.

As a first step we will introduce affine algebras and some interesting properties that are fulfilled by them. The theory about affine algebras that we are going to state in this section follows chapter 2 of [16].

Let us consider abelian groups or to be more precise consider the following properties that are fulfilled by abelian groups.

**Lemma 3.25.** Let \( \mathbb{A} = (A; +, -, 0) \) be an abelian group and \( f \in O(\mathbb{A}) \). Then the following are equivalent

1. \( S := \{(a, b, c, d) \in A^4 \mid a - b + c = d \} \) is a subuniverse of \( (A; f)^4 \)
2. \( f \) commutes with the term function \( m(x, y, z) := x - y + z \)
3. \( f(u_1 + v_1, \ldots, u_n + v_n) + f(0, \ldots, 0) = f(u_1, \ldots, u_n) + f(v_1, \ldots, v_n) \) for all \( \bar{v}, \bar{u} \in A^n \)
4. \( f \) is a polynomial operation of the \( \text{End}(\mathbb{A}) \)-module \( \text{End}(\mathbb{A}) \cdot \mathbb{A} = (A; +, -, 0, \text{End}(\mathbb{A})) \)

**Proof.** The equivalence of 1) and 2) is obvious. For 2) \( \Rightarrow \) 3) one just has to consider \( f(u_1 + v_1, \ldots, u_n + v_n) = f(u_1 - 0 + v_1, \ldots, u_n - 0 + v_n) \) and the rest follows by assumption. For 3) \( \Rightarrow \) 4) we define \( \tilde{f}(x_1, \ldots, x_n) := f(x_1, \ldots, x_n) - f(0, \ldots, 0) \). Then we get \( \tilde{f}(u_1 + v_1, \ldots, u_n + v_n) = \tilde{f}(u_1, \ldots, u_n) + \tilde{f}(v_1, \ldots, v_n) \). Thus \( \tilde{f}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \tilde{f}(0, \ldots, 0, x_i, 0, \ldots, 0) \). If we interpret each summand as a function in \( x_i \) then this function is an endomorphism of \( \mathbb{A} \). For the last implication assume that \( f(x_1, \ldots, x_n) = \sum_{n=0}^{n} \phi_i(x_i) + c \) where the \( \phi_i \) are endomorphisms of \( \mathbb{A} \) and let \( (a_1, b_1, c_1, d_1) \in S \) for \( 1 \leq i \leq n \). We have to show that \( (f(a_1, \ldots, a_n), f(b_1, \ldots, b_n), f(c_1, \ldots, c_n), f(d_1, \ldots, d_n)) \in C \). But this follows immediately if we use the definition of \( f \) and exploit the fact that the \( \phi_i \) are endomorphisms of \( \mathbb{A} \). \( \square \)
Affine algebras were introduced to generalize this properties of abelian algebras to universal algebras. Hence it is clear where the motivation for the following definition comes from.

**Definition 3.26.** An algebra \( A = (A; F) \) is said to to be **affine** with respect to an abelian group \( A = (A; +, -, 0) \) if

1. \( m(x, y, z) := x - y + z \) is a term function of \( A \)
2. Every term function of \( A \) commutes with \( m \).

**Remark 3.27.** 1. Of course every point in Lemma 3.25 would yield an equivalent definition for the term affine.

2. Note that \( m(x, y, z) = x - y + z \) is a Mal’cev operation and therefore every affine algebra is congruence permutable.

3. If an \( A \) algebra is affine with respect to an abelian group we will denote the group by the concerning bold uppercase letter, in this case \( A \). Additionally since the term functions of an affine algebra are polynomial functions of \( \text{End}(A) \) a term function \( t \in \text{Clo}(A) \) can be represented as

\[
t(x_1, \ldots, x_m) = \sum_{i=1}^{n} r_i x_i + a \text{ for some } r_i \in \text{End}(A), a \in A.
\]

With the next lemma we will discover that the affine algebras we defined in this section are closely related to abelian algebras, which we have studied in the previous section.

**Lemma 3.28.** Let \( A = (A; F) \) be a an abelian algebra and \( V \in V \) and \( d \) be a difference term of \( A \). Then \( A := (A; +, -, 0) \) is an abelian group where the operations are defined for some fixed \( a \in A \) as follows

\[
g_1 + g_2 := d(g_1, a, g_2) \\
g_1 := d(a, g_1, a) \\
0 := a
\]

Moreover, \( d(x, y, z) = x - y + z \). Thus \( A \) is affine with respect to \( A \).

**Proof.** All the group axioms for \( A \) can be verified by using the fact that \( d \) commutes with itself (see 3.20) and using the equations \( d(x, y, y) \approx d(y, y, x) \approx x \) (\( A \) is abelian by assumption).

In order to show that \( x - y + z = d(x, y, z) \) we show that \( x - y = d(x, y, a) \).

\[
x - y = d(x, a, d(a, y, a)) \\
= d(d(x, a, a), d(a, a, a), d(a, y, a)) \\
= d(d(x, a, a), d(a, a, y), d(a, a, a)) \\
= d(x, y, a)
\]
Thus
\[ x - y + z = d(d(x, y, a), a, z) = d(d(x, y, a), d(a, a, a), d(a, a, z)) = d(d(x, a, a), d(y, a, a), d(a, a, z)) = d(x, y, z) \]

Note that this lemma was just a simplified version of a lemma in [4, Lemma 5.6]. More generally one can show that a Mal’cev algebra \( \mathbb{A} \) is affine if and only if it is abelian (see for example [4, Corollary 5.9]).

The following theorem gives us more information about the term functions of a finite affine algebra.

**Theorem 3.29.** Let \( \mathbb{A} \) be an affine algebra with respect to an abelian group \( A = (A; +, -, 0) \). Then there exists a unique subring \( R \) of \( \text{End}(A) \) and a unique submodule \( M \) of the \( R \)-module \( R \times_R A \) such that

\[
\text{Clo}(\mathbb{A}) = C(RA, M) = \left\{ \sum_{i=1}^{n} r_i x_i + a \mid n \geq 1, r_1, \ldots, r_n \in R, (1 - \sum_{i=1}^{n} r_i, a) \in M \right\}.
\]

**Proof.** We can define \( R \) and \( M \) in the following way

- \( R := \{ r \in \text{End}(A) \mid r x + (1 - r)y \in \text{Clo}(\mathbb{A}) \} \) and
- \( M := \{(r, a) \in \text{End}(A) \times A \mid (1 - r)x + a \in \text{Clo}(\mathbb{A}) \} \).

Let \( r, \hat{r} \in R, (r_1, a_1), (r_2, a_2) \in M \) and since \( \mathbb{A} \) is affine there exists by definition a Mal’cev term \( m(x, y, z) = x - y + z \) in the term functions of \( \mathbb{A} \). Then we have that

\[
1x + 0y \in \text{Clo}(\mathbb{A})
\]
\[
(r + \hat{r})x + (1 - r - \hat{r})y = (rx + (1 - r)y) - y + (\hat{r}x + (1 - \hat{r})y) \in \text{Clo}(\mathbb{A})
\]
\[
rx + (1 - r\hat{r})y = r(\hat{r}x + (1 - \hat{r})y) + (1 - r)y \in \text{Clo}(\mathbb{A})
\]

and

\[
r_1 x + (1 - r_1)y = ((1 - r_1)y + a_1) - ((1 - r_1)x + a_1) + x \in \text{Clo}(\mathbb{A})
\]
\[
(1 - r_1 - r_2)x + a_1 + a_2 = ((1 - r_1)x + a_2) - x + ((1 - r_2)x + a_2) \in \text{Clo}(\mathbb{A})
\]
\[
(1 - r_1 - r_2)x + a_1 + a_2 = r((1 - r_1)x + a_1) + (1 - r)x \in \text{Clo}(\mathbb{A})
\]

which proves that \( R \) is a subring of \( \text{End}(A) \), \( M \) is a submodule of \( R \times_R A \). Now let \( t(x_1, \ldots, x_n) \in \text{Clo}(\mathbb{A}) \). Remember that we already know from 3.25 that \( t \) is a
polynomial operation of $\text{End}(A)\ A$. Thus we can write $t(x_1, \ldots, x_n) = \sum_{i=1}^{n} r_i x_i + a$ for some $r_i \in \text{End}(A)$ and $a \in A$.

Since $t(x_1, \ldots, x_n) \in \text{Clo}(A)$ also $t(x, \ldots, x) = (\sum_{i=1}^{n} r_i)x + a \in \text{Clo}(A)$ and therefore $(1 - \sum_{i=1}^{n} r_i, a) \in M$. Note that for all $j \in \{1, \ldots, n\}$ we have

$$r_j x + (1 - r_j)y = \sum_{i=1}^{n} r_i x + a - (\sum_{i=1, i \neq j}^{n} r_i x + r_j y) + y \in \text{Clo}(A).$$

But this implies $r_j \in R$ for all $1 \leq j \leq n$ and therefore $t \in C(RA, M)$.

Suppose now that $\sum_{i=1}^{n} r_i x_i + a \in C(RA, M)$. Thus by definition we get

$$(\sum_{i=0}^{n} r_i)x + a \in \text{Clo}(A)\text{ and } r_j x + (1 - r_j)y \in \text{Clo}(A)\text{ for } 1 \leq j \leq n.$$}

One can show by induction that if $m(x, y, z) := x - y + z \in \text{Clo}(A)$ then also $p_k : A^{k+2} \rightarrow A$, $p_k(x_1, \ldots, x_{k+2}) := x_1 + \ldots + x_{k+1} - kx_{k+2}$ must be a term function of $A$.

Hence,

$$\sum_{i=1}^{n} r_i x_i + a = p_n(r_1 x_1 + (1 - r_1) x_1, \ldots, r_n x_n + (1 - r_n) x_1, (\sum_{i=1}^{n} r_i) x_1 + a, x_1) \in \text{Clo}(A).$$

We still have to prove the uniqueness of $R$ and $M$. Assume that $C(RA, M) = \text{Clo}(A) = C(RA, M')$. But then we get

$$R = \{ r \in \text{End}(A) \mid rx + (1 - r)y \in \text{Clo}(A) \} = R'$$

$$M = \{ (r, a) \in \text{End}(A) \times A \mid (1 - r)x + a \in \text{Clo}(A) \} = M'.$$

\[\square\]

**Theorem 3.30.** Every finite affine algebra is finitely based.

**Proof.** Let $A$ be a finite simple affine algebra. Then by Theorem 3.29 we get that

$$\text{Clo}(A) = \{ \sum_{i=1}^{n} r_i x_i + a \mid n \geq 1, r_1 \ldots r_n \in R, (1 - \sum_{i=1}^{n} r_i, a) \in M \}$$

for a $R \leq \text{End}(A)$ and a submodule $M$ of $R \times RA$.

Let $t$ be a term of $A$ and $r_i \in R, a \in A$ such that $t^K(x_1, \ldots, x_n) = \sum_{i=1}^{n} r_i x_i + a$. As in the proof of 3.29 we know

$$t(x_1, \ldots, x_n) \approx p_n(a_{r_1}(x_1, x_1), \ldots, a_{r_n}(x_n, x_1), s(x_1), x_1) \quad (*)$$

where $a_{r_i}(x, y) := r_i x + (1 - r_i)y$ for all $1 \leq i \leq n$ and $s(x) := (\sum_{i=1}^{n} r_i)x + a$.

Since there are only finitely many term functions of arity less or equal $2$ there exists a finite basis for the equations of $A$ in at most two variables. But with $(*)$ this is also a finite basis for the equations of $A$. \[\square\]
Chapter 4

Simple Clones

4.1 Minimal varieties

We have seen in the second chapter that for a clone $H$ on a finite set $A$ each maximal congruence of $\mathbb{H}$ corresponds exactly to a minimal variety of $(A; H)$. Our goal will be to characterize simple clones with a Mal’cev operation. In order to achieve this goal we use the already existing knowledge about minimal varieties in a congruence permutable variety. The most important theorems (and also their proofs) concerning minimal varieties in congruence permutable varieties are stated in this section.

**Definition 4.1.** Let $\mathcal{V}$ be a variety. $\mathcal{V}$ is called minimal if $\mathcal{V}$ has no nontrivial proper subvarieties.

The following examples are well known to be minimal varieties.

**Example 4.2.**
1. The variety of distributive lattices is minimal. Observe that this is the only minimal variety of lattices since the two element lattice belongs to every nontrivial variety of lattices.

2. The variety of Boolean algebras is minimal.

**Definition 4.3.** Let $A$ be an algebra. We call $A$ strictly simple if $A$ is simple and $A$ has no nontrivial proper subalgebras.

**Theorem 4.4.** Let $\mathcal{V}$ be a nontrivial variety. Then $\mathcal{V}$ has a minimal subvariety.

*Proof.* We already now that the lattice of subvarieties of $\mathcal{V}$ are dually isomorphic to a interval of the lattice of fully invariant congruences of $\mathbf{T}(X)$ (see Corollary 2.25). If we can find a maximal fully invariant congruence we are done.

Let $X$ be an infinite set of pairwise distinct variables and let $x, y \in X$ with $x \neq y$ and define

$$A := \{ \alpha \in \text{Con}_{f_1}(\mathbf{T}(X)) \mid \sigma(\text{Id}_\mathcal{V}(X)) \subseteq \alpha \subseteq \nabla_{\mathbf{T}(X)} \}.$$
Moreover, let $L$ be a linear ordered subset of $A$ and define $\bar{\alpha} := \bigcup_{\alpha \in L} \alpha$. Observe that

1. Clearly $\alpha \subseteq \bar{\alpha}$ and $\sigma(\operatorname{Id}_V(X)) \subseteq \bar{\alpha}$ holds by definition of $\bar{\alpha}$.

2. Since $L$ is linear ordered it is straightforward to show that $\bar{\alpha} \in \operatorname{Con}_{\mathfrak{f}}(T(X))$.

3. $\bar{\alpha} \subset \nabla_{T(X)}$ since for $\beta \in \operatorname{Con}_{\mathfrak{f}}(T(X))$ we have that $\beta = \nabla_{T(X)} \iff (x, y) \in \beta$.

This means $\bar{\alpha} \in A$ and it is an upper bound for the elements in $L$. By the Lemma of Zorn we get a maximal element of the interval $[\sigma(\operatorname{Id}_V(X)), \nabla_{T(X)}]$, say $\theta$ and then $\sigma^{-1}(\theta)$ must generate a minimal variety by Theorem 2.23 and Corollary 2.25.

Now we turn to the cardinality of minimal subvarieties in a locally finite variety. The following theorem can be found for example in [6, Theorem 7.2].

**Theorem 4.5.** If $V$ is a locally finite variety then $V$ has only finitely many minimal subvarieties.

**Proof.** Let $W$ be a minimal subvariety of $V$. Then $W$ must be generated by every nontrivial algebra of $W$, especially from the two generated free algebra of $W$. We know that the two generated free algebra of $W$ must be a homomorphic image of the two generated free algebra of $V$. Furthermore the two generated free algebra of $V$ only has finitely many nonisomorphic homomorphic images since the two generated free algebra is finite ($V$ is locally finite by assumption).

We can easily prove the following lemma:

**Lemma 4.6.** Let $\mathfrak{A}$ be an algebra and $V$ be a locally finite variety and not be trivial. If $V$ is minimal then there exists $\mathfrak{A} \in V$ such that $V(\mathfrak{A}) = V$ and $\mathfrak{A}$ is finite and strictly simple.

**Proof.** Since $V$ is minimal every $\mathfrak{B} \in V$ must generate $V$. Now choose an algebra $\mathfrak{B} \in V$ with minimal $|B|$. This algebra must be strictly simple otherwise there exists $\theta \in \operatorname{Con}(\mathfrak{B}) \setminus \{\Delta, \nabla\}$ or $C \subset \mathfrak{B}$ with $|C| \geq 2$ and we get $V(\mathfrak{B}/\theta)$ or $V(C)$ are contradicting the minimality of $V$.

Since $V$ is not the trivial variety there exists an algebra $\mathfrak{B} \in V$ with $|B| \geq 2$. Let $\mathfrak{A}$ be an algebra of the same type of $V$ with universe $\operatorname{Sg}(b_1, b_2)$ and $b_1, b_2 \in B$ with $b_1 \neq b_2$. Since $\mathfrak{A} \in V$ and $V$ is locally finite also $\mathfrak{A}$ is finite and therefore fulfills all desired properties.

Unfortunately the converse of this theorem is not true in general. A counterexample would be the following algebra:

$$\mathfrak{A} := (\{0, 1\}; \tau), \text{ where } \tau : \{0, 1\} \to \{0, 1\}, \tau(0) := 1, \tau(1) := 0$$
Clearly, $A$ is simple and has no subalgebras. If we consider $A^2$ and define a function $\alpha : \{0,1\}^2 \to \{a,b\}$, $\alpha(0,0) = \alpha(1,1) := a$ and $\alpha(1,0) = \alpha(0,1) := b$ for some distinct elements $a, b$, it follows immediately that $\alpha(x) = \alpha(\tau(x))$. To put it differently $B := \{(a,b); id\}$ is a homomorphic image of $A^2$ under $\alpha$. Note that $B \models \tau(x) \approx x$ which implies $V(B) \subseteq V(A)$.

For the congruence distributive case also the converse of Theorem 4.6 holds.

**Theorem 4.7.** Let $A$ be a finite strictly simple algebra. If $V(A)$ is congruence distributive then $V(A)$ is minimal.

**Proof.** Let $A$ be a finite strictly simple algebra. By Jónssons Theorem which can be found for example in [2, Chapter 4, Theorem 6.8] we know that the subdirectly irreducible members of $V(A)$ are in $HSP_u(A)$ where $P_u(A)$ denotes the ultraproducts of $A$. Furthermore we know that ultraproducts of a finite set $K$ of finite algebras are isomorphic to one element in $K$. In other words $P_u(A) = I(A)$ and since $A$ is strictly simple we have $HSI(A) = I(A)$. This means every subdirectly irreducible algebra of $V(A)$ is isomorphic to $A$.

Now assume $V(A)$ has a proper nontrivial subvariety $W$. But then for a subdirectly irreducible algebra $B \in W$ we have that $B \in I(A)$ and therefore $V(A) = V(B) \subseteq W$ which is a contradiction.

We do not have such a nice result for the congruence permutable case but we can classify the strictly simple algebras which generate a congruence permutable variety with a theorem from [4, Theorem 12.4].

**Theorem 4.8.** Let $A$ be a finite strictly simple algebra such that $V(A)$ is congruence permutable then $A$ is either quasi-primal or $A$ is abelian.

**Proof.** First of all congruence permutability implies congruence modularity and by Theorem 3.17 we know that $A$ generates either a congruence distributive or an abelian variety. In the case that $V(A)$ is abelian of course also $A$ is abelian and we are done.

It remains the case that $V(A)$ is congruence distributive. Now we can apply Jónssons Theorem and with the same arguments as in the proof of Theorem 4.7 we get that $V(A) = I(A)$. Thus every subalgebra of $A$ is simple or in other words $A$ is hereditarily simple. The statement follows now by Theorem 3.7.

We already know from the proof of 3.7 that a quasi-primal algebra generates a congruence distributive variety and therefore by Theorem 4.7 we know that a strictly simple quasi-primal algebra always generates a minimal variety. So the last step towards a characterization of minimal varieties in congruence permutable varieties is to describe when a strictly simple abelian algebra generates a minimal variety.

In section 3.2 we have already proved that a simple abelian algebra has no nontrivial subalgebras. This means a abelian algebra is strictly simple if and only if it is simple.
CHAPTER 4. SIMPLE CLONES

Additionally we know by Theorem 3.24 that a simple abelian algebra $A$ is minimal if and only if it has at least one trivial subalgebra. The theorems stated in this section and the arguments from before lead to the following description of minimal varieties in congruence permutable varieties:

**Corollary 4.9.** Let $A$ be a finite algebra and $V(A)$ congruence permutable. $V(A)$ is minimal if and only if one of the following conditions hold

1. $A$ is strictly simple and quasi-primal
2. $A$ is abelian and simple and has at least one trivial subalgebra

### 4.2 Simple clones and maximal congruences

We will state some facts about maximal clone congruences and we also give a characterization of simple clones with a Mal’cev term by carrying over the knowledge of minimal varieties we have worked out in the last section. To be more precise we will answer the following questions for a clone $H$ on a set finite $A$ with a Mal’cev term:

1. Is there a maximal congruence of $H$? ($H$ not necessarily containing a Mal’cev operation)
2. Are there only finitely many maximal congruences of $H$? ($H$ not necessarily containing a Mal’cev operation)
3. Which maximal congruences of $H$ are finitely generated?
4. Is there a characterization when $H = \text{Clo}(A)$ is simple in terms of $A = (A; H)$.
5. Is there a characterization when $H = \text{Pol}(A)$ is simple in terms of $A = (A; H)$

Just to prevent any misunderstandings we will give a definition of the objects we are talking about in this section

**Definition 4.10.** 1. A clone of functions $H$ is called *simple* if $H$ is simple.
2. A clone congruence $\theta$ of a clone $H$ (this means $\theta \in H$) is called *maximal* if the interval $[\theta, \mu] \subseteq \theta$ of $\text{Con}(H)$ has exactly two elements.

First of all it is not clear that the objects we have defined above do really exist. But this problem is solved by the next two lemmata.

**Lemma 4.11.** For every clone congruence $\theta$ of a clone $H$ there exists a maximal clone congruence $\theta_M$ with $\theta \subseteq \theta_M$.

*Proof. Consequence of Theorem 4.4 and Corollary 2.28.*
CHAPTER 4. SIMPLE CLONES

**Remark 4.12.** Alternatively one could also give a direct proof of Lemma 4.11 by using Zorn’s Lemma and the fact that for a clone congruence \( \theta \) we have

\[
\theta = \nabla \iff \exists i, j \in \mathbb{N} : i \neq j \land (\pi_i, \pi_j) \in \theta .
\]

**Lemma 4.13.** Let \( \mathbb{A} := (A; F) \) with \( F \subseteq O(A) \). Then \( \text{Cl}(\mathbb{A}) \) is simple iff \( V(\mathbb{A}) \) is minimal.

**Proof.** Follows immediately from the fact that \( \text{Con}(\text{Cl}(\mathbb{A})) \) and \( \text{Su}(V(\mathbb{A})) \) are dual isomorphic (see Corollary 2.28).

Since we have seen in the last section that a locally finite variety only has finitely many subvarieties, we get as a direct consequence the following statement.

**Theorem 4.14.** Let \( H \) be a clone on a finite set \( A \). Then we have

1. \( H \) has only finitely many maximal congruences.

2. If \( H \) contains a Mal’cev operation then every maximal congruence is finitely generated.

**Proof.** We define \( \mathbb{A} := (A; H) \) and since \( A \) is finite \( V(\mathbb{A}) \) is a locally finite variety. Now we can use Theorem 4.5 and get that \( V(\mathbb{A}) \) has finitely many minimal varieties. The first statement of the theorem follows by Corollary 2.28.

By the isomorphisms we have established in Chapter 2 it is clear that for \( \theta \in \text{Con}(\mathbb{A}) \) we have that

\[
\theta \text{ is finitely generated } \iff \text{Mod}(\{ t \sim s \mid (t^A, s^A) \in \theta \}) \text{ is finitely based }
\]

So if we find a finite basis for the varieties corresponding to the maximal congruences we have also found a finite set for the congruences. But by Corollary 4.9 we know that the concerning varieties are either quasi-primal or simple and abelian with at least one trivial subalgebra. We already know that quasi-primal implies congruence distributivity and hence we get a finite basis by Bakers Theorem ([II]).

In the other case \( \mathbb{A} \) is abelian and we have seen in the section 3.3 that this implies that \( A \) is affine. By theorem 3.30 we get hat \( A \) is finitely based. \( \square \)

If we look at the last theorems and their proofs it is not surprising that we can use the minimal varieties to characterize the simple clones with a Mal’cev operation. But we can also go one step further and characterize when \( \text{Pol}(\mathbb{A}) \) is simple.

**Theorem 4.15.** Let \( \mathbb{A} := (A; F) \) be finite with \( F \subseteq O(A) \) such that \( \text{Cl}(\mathbb{A}) \) contains a Mal’cev operation. Then

1. \( \text{Cl}(\mathbb{A}) \) is simple iff \( \mathbb{A} \) is quasi-primal and strictly simple or \( \mathbb{A} \) is a simple, abelian algebra with at least one trivial subalgebra.
2. Let $C_A$ denote the constant functions of $A$ and let $D \subseteq C_A$ with $|D| \geq 2$ and define $\mathbb{A}_D := (A; F \cup D)$.

Then $\text{Clo}(\mathbb{A}_D)$ is simple iff $\text{Clo}(\mathbb{A}_D) = O(A)$.

Proof. The first statement follows from the Lemma 4.13 and Corollary 4.9. Let us now consider the second statement. Let $D \subseteq C_A$ with $|D| \geq 2$ and $\mathbb{A}_D$ as in the assumptions above.

If $\text{Clo}(\mathbb{A}_D) = O(A)$ it follows immediately that $\mathbb{A}_D$ is quasi-primal (and therefore simple see proof of Theorem 3.7) and since $C_A \subseteq O(A)$ hence, $\mathbb{A}_D$ can not have any proper subalgebras. So $\mathbb{A}_D$ is quasi-primal and strictly simple which implies by the first part of the theorem that $\text{Clo}(\mathbb{A}_D)$ is simple.

Suppose now that $\text{Clo}(\mathbb{A})$ is simple. Again we can use the first part which tells us that we have two distinguish to cases for $\mathbb{A}_D$.

1. Case: $\mathbb{A}_D$ is simple, abelian and has at least one trivial subalgebra.

Since we know that $|D| \geq 2$ we also know that each subalgebra must have at least two elements. But this contradicts the fact that $\mathbb{A}_D$ has a trivial subalgebra.

2. Case: $\mathbb{A}_D$ is quasi-primal and strictly simple.

Since $\mathbb{A}_D$ is strictly simple and has at least two constant functions as fundamental operations the only subuniverse of $\mathbb{A}_D$ is $A$. If we look at the original definition of quasi-primal (Definition ??), the fact that $\mathbb{A}_D$ is quasi-primal simplifies to the following property:

Each function which preserves all automorphisms of $\mathbb{A}_D$ must be a term function.

(4.1)

Let $c_{a_1}, c_{a_2} \in D$ with $a_1 \neq a_2$ and let $\phi \in \text{Aut}(\mathbb{A}_D)$ then $a_1, a_2$ are fixed points of $\phi$. But it is a well known fact that the fixed points of automorphisms of an algebra $\mathbb{B}$ are a subuniverse of $\mathbb{B}$. Since $A$ is the only subuniverse of $\mathbb{A}_D$ it follows $\text{Aut}(\mathbb{A}_D) = \{id_A\}$.

With property 4.1 we conclude that $\text{Clo}(\mathbb{A}_D) = O(A)$.

It is clear that also $\text{Pol}(\mathbb{A})$ is covered by the second point in the theorem above ($D = C_A$). We want to emphasize this fact and state it as an extra corollary.

**Corollary 4.16.** Let $\mathbb{A}$ be a Mal’cev algebra. Then $\text{Pol}(\mathbb{A})$ is simple iff $\text{Pol}(\mathbb{A}) = O(A)$ ($\mathbb{A}$ is called polynomially complete).
Bibliography


53
BIBLIOGRAPHY


[16] Szendrei, Á., Clones in universal algebra, Montréal, Québec, Canada: Presses de l’Université de Montréal, 1986
Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe. Die vorliegende Diplomarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Linz, August 2015

Neumüller Mario