8. CONGRUENCE MODULAR VARIETIES

The two broad families of congruence-modular varieties and congruence-distributive varieties are rather familiar to universal algebraists and fairly well understood. The tame congruence theory becomes somewhat simpler in these varieties, and it can be used to obtain results that seem inaccessible to conventional methods. We first recall the most recent characterization of congruence-modular varieties, and the classical characterization of congruence-distributive varieties.

THEOREM 8.1. (Gumm [16]) A variety $V$ is congruence-modular iff for some $n \geq 0$ there are terms $d_0(x, y, z), \ldots, d_n(x, y, z)$ in its language such that these equations hold in $V$.

1. $d_0(x, y, z) \approx x$, $d_i(x, y, x) \approx x$ for $1 \leq i \leq n$.
2. $d_i(x, y, y) \approx d_{i+1}(x, y, y)$ for even $i < n$.
3. $d_i(x, x, y) \approx d_{i+1}(x, x, y)$ for odd $i < n$.
4. $d_n(x, y, y) \approx p(x, y, y)$, $p(x, x, y) \approx y$.

THEOREM 8.2. (Jónsson [19]) A variety $V$ is congruence-distributive iff for some $n \geq 0$ there are terms $d_0(x, y, z), \ldots, d_n(x, y, z)$ in its language satisfying the equations 8.1 (1–3) and $d_n(x, y, z) \approx z$.

It is a reasonable exercise to prove the theorem of Jónsson. The theorem of Gumm is not so easily proved. These two theorems make it appear that for varieties, congruence-modularity is an amalgam of congruence-distributivity and congruence-permutability.

The next lemma introduces an idea that will be frequently used in Chapter 9. See Definition 6.12 for the notation $AI_S$.

LEMMA 8.3. Let $A$ be an algebra, $e \in E(A)$, $U = e(A)$, $\beta \in \text{Con } A$, and $S = a/\beta \cap U$ for some $a \in U$. If $V(A)$ is congruence-modular, congruence-distributive, or has permuting congruences, then $V(AI_S)$ has the same respective property.

PROOF. If $V(A)$ is congruence-permutable, then there is a Mal’cev operation $p \in \text{Clo}_3 A$, by Theorem 0.3(3). The operation $p'(x, y, z) = e(p(x, y, z))$, restricted to $S$, is Mal’cev and belongs to $\text{Clo}_3 (AI_S)$. To see this, let $x, y, z \in S$. Then $p'(x, y, z) \in U$, obviously, and

$$p'(x, y, z) \equiv p'(a, a, a) = e(a) = a (\text{mod } \beta),$$

125
so $p'(x, y, z) \in S$. Moreover,

$$p'(x, y, y) = e(p(x, y, y)) = e(x) = x,$$
and likewise $p'(x, x, y) = y$. Thus $V(AI_S)$ is congruence-permutable.

If $V(A)$ is congruence-distributive, then we have $d_0, \ldots, d_n \in \text{Clo}_3A$ satisfying Jónsson’s equations of Theorem 8.2. These equations imply $d_i'(x, x, x) \approx x$ for $i = 0, \ldots, n$. Thus we see that the operations $d_i'(x, y, z) = e(d_i(x, y, z))$, restricted to $S$, belong to $\text{Clo}_3(AI_S)$. Since the Jónsson equations are linear (having no superposition of one operation applied to the results of operations), we can easily check that these equations are satisfied by $d_0', \ldots, d_n'$. Thus $V(AI_S)$ is congruence-distributive.

The argument for modularity is very similar. All these arguments require the idempotence of the operations in the characteristic equations, and the linearity of these equations.

\[ \square \]

**COROLLARY 8.4.** Let $V$ be a locally finite variety and $k \in \{1, 2, 3, 4, 5\}$. If $k \in \text{typ}(V)$ and $V$ is congruence-modular, distributive, or permutable, then there is a minimal algebra $M$ of type $k$ such that $V(M)$ has the same respective congruence property.

**PROOF.** Suppose, for example, that $V$ is congruence-distributive and $k \in \text{typ}(V)$. There is a finite $A \in V$ and $\alpha \prec \beta$ in $\text{Con} A$ with $\text{typ}(\alpha, \beta) = k$. We choose $U \in M_A(\alpha, \beta)$ and a trace $N = U \cap a/\beta$ with $a \in U$. By Lemma 8.3, $V(AIN)$ is congruence-distributive. The algebra $M = (AI_N)/(\alpha|N)$ is a minimal algebra of type $k$ in this variety.

\[ \square \]

**THEOREM 8.5.** A locally finite variety $V$ is congruence-modular iff $\text{typ}(V) \cap \{1, 5\} = \emptyset$ and for all finite $A \in V$, $\alpha \prec \beta$ in $\text{Con} A$, and $U \in M_A(\alpha, \beta)$, the $(\alpha, \beta)$-tail of $U$ is empty.

**PROOF.** Let $V$ be a locally finite congruence-modular variety. Let $A$ be any finite algebra in $V$ with $0 \prec \beta$ in $\text{Con} A$. (By Lemma 2.18 and Corollary 5.3, it will suffice to consider only this case.) Choose any $U \in M_A(0, \beta)$, and let $N$ be a $(0, \beta)$-trace in $U$ and $B$ be the body of $U$. By the proof of Lemma 8.3, there are

$$d_0(x, y, z), \ldots, d_n(x, y, z), p(x, y, z) \in \text{Pol}_3A$$

such that $U$ and $N$ are closed under these operations and, restricted to $U$, they satisfy the equations 8.1 (1–4). The algebra $A|N$ cannot be unary or equivalent to a semilattice, since in either case it could not have polynomial operations satisfying those equations. Thus $\text{typ}(0, \beta) \notin \{1, 5\}$.

In proving that $B = U$, we can assume that $U = A$. We suppose now that $B \neq A$, say $t \in A - B$, and we proceed to a contradiction. Let $a$ and $c$ be any elements of $N$. 
For all \( i, 0 \leq i \leq n \), the function \( f_i(x) = d_i(a, x, c) \) satisfies
\[
f_i(t) \stackrel{\theta}{=} d_i(a, t, a) = a.
\]
Therefore \( f_i(t) \in B, f_i \notin \text{Sym } A \) (else \( f_i^{-1}(B) = B \)), and \( f_i \) must be constant on \( N \).
(Since \( A = U \) is \( (0, \beta) \)-uninodal.) Now we can prove inductively that \( d_i(a, b, c) = a \) for all \( i \leq n \) and \( a, b, c \in N \). This is true for \( i = 0 \), and if it holds for \( i = j < n \), then
\[
d_{j+1}(a, b, c) = d_{j+1}(a, c, c) = d_j(a, c, c) = a
\]
if \( j \) is even, and
\[
d_{j+1}(a, b, c) = d_{j+1}(a, a, c) = d_j(a, a, c) = a
\]
if \( j \) is odd. Now we have \( p(a, b, b) = d_n(a, b, b) = a \) for all \( a, b \in N \); and \( p(u, u, v) = v \) for all \( u, v \in A \).

Proceeding as in the proof of Lemma 4.20, we now construct another polynomial operation of \( A \). Let \( h(x, y) = p(x, y, y) \), and choose \( k > 1 \) such that \( h_k(x, y) = h(x, y) \), \( \ldots (h(x, y), y), \ldots, y \) satisfies \( h_k(x, y) = h_k((x, y)) = h_k(x, y) \). Since \( h_b(x) = h(x, b) \) is a permutation for \( b \in N \) (in fact \( h_b(a) = a \) for \( a, b \in N \)), it follows that \( h_k(x, b) = x \) for all \( x \in A \) and \( b \in N \). We set \( p'(x, y, z) = h_k^{-1}(p(x, y, z), z) \); and observe that \( p'(x, b, b) = h_k(x, b) = x \) when \( x \in A \) and \( b \in N \), and that \( p'(x, y, y) = y \) for all \( x, y \in A \).

Now we choose \( a \in N \), let \( t \in A - B \) as before, and define, for all \( x \in A \),
\[
g(x) = p'(x, p'(t, p'(t, x, a), a), a).
\]
For any \( b \in N \),
\[
p'(t, b, a) \stackrel{\theta}{=} p'(t, a, a) = t,
\]
implying that \( p'(t, b, a) = t \) since \( t \notin B \). Thus \( g(b) = b \), for \( b \in N \), and we have that \( g \in \text{Sym } A \). On the other hand, \( g(t) = a \) can be calculated, using the equations from the end of the last paragraph. This contradicts that \( g \) must leave \( A - B \) fixed, and the contradiction ends our proof that \( U = B \).

To finish the proof of the theorem, we now assume that \( V \) is locally finite and not congruence-modular. There is a finite algebra \( A \in V \) with \( \text{Con } A = L \) a non-modular lattice; for example, we can take \( A = F_4 \). By Lemma 6.1, there must exist a prime quotient \( (\alpha, \beta) \) in \( L \) and \( U \in M_A(\alpha, \beta) \) such that for \( U = A|_U \), we have \( \text{Con } U \) non-modular. This implies that either the \( (\alpha, \beta) \)-tail of \( U \) is non-empty, or else \( \text{typ}(\alpha, \beta) \in \{1, 5\} \). Otherwise, by Lemma 4.17 and Lemma 4.20, either \( |U| = 2 \) or \( U \) is a Mal'cev algebra; but in either case, \( \text{Con } U \) would be a modular lattice. \( \square \)

**Theorem 8.6.** A locally finite variety \( V \) is congruence-distributive iff \( \text{typ}(V) \cap \{1, 2, 5\} = \emptyset \) and for all finite \( A \in V, \alpha < \beta \) in \( \text{Con } A \), and \( U \in M_A(\alpha, \beta) \), we have \( |U| = 2 \).
PROOF. Let \( \mathcal{V} \) be a locally finite congruence-distributive variety. By Corollary 8.4, \( \text{typ}\{\mathcal{V}\} \cap \{1, 2, 5\} = \emptyset \). Since \( \mathcal{V} \) is congruence-modular, the previous theorem implies that in \( \mathcal{V} \) every \( \langle \alpha, \beta \rangle \)-minimal set \( U \) is equal to its body, and since \( \text{typ}(\alpha, \beta) \) must be 3 or 4, Lemma 4.17 implies that \( |U| = 2 \).

Conversely, if \( \mathcal{V} \) is locally finite and the \( \langle \alpha, \beta \rangle \)-minimal sets in \( \mathcal{V} \) are 2-element sets, then Lemma 6.1 provides a subdirect representation of \( \text{Con} \ A \) (for \( A \) finite in \( \mathcal{V} \)) in a product of two-element lattices, and from this it follows that \( \mathcal{V} \) is congruence-distributive.

The combination of Theorem 8.5 and Lemma 6.1 yields an interesting representation of the congruence lattices of finite algebras belonging to congruence-modular varieties, which is the content of the next theorem. Let \( A \) be a finite algebra in a congruence-modular variety. For any prime quotient \( \langle \alpha, \beta \rangle \) in \( A \) and \( \langle \alpha, \beta \rangle \)-minimal set \( U \), the algebra \( A \upharpoonright_U \) is either equivalent to a two-element bounded lattice or Boolean algebra, or it is a nilpotent Mal’cev algebra. (See Theorem 8.5, Lemmas 4.17, 4.20 and 4.36, and Theorem 4.31.) These algebras \( A \upharpoonright_U \) are E-minimal; and a complete description of all E-minimal Mal’cev algebras will be supplied in Theorem 13.9.

Quasigroups are defined right before Lemma 4.6. A loop is a quasigroup \( \langle A, \cdot, \cdot \rangle \) having an element \( 1 \) such that \( 1 \cdot x = x \cdot 1 = x \) for all elements \( x \). A loop with operators is an algebra, one of whose basic operations is the operation of a loop.

**THEOREM 8.7.** Let \( A \) be a finite algebra such that \( \mathcal{V}(A) \) is congruence-modular. There exist finite algebras \( B_1, B_2, \ldots, B_n \), each a loop with operators, such that \( B_1, \ldots, B_n \) are nilpotent and E-minimal, and

\[
\text{Con} \ A \cong \text{Con} \ B \equiv \prod_1^n \text{Con} \ B_i.
\]

**PROOF.** We take \( \langle \alpha_1, \beta_1 \rangle, \ldots, \langle \alpha_n, \beta_n \rangle \) to be a list of all the prime quotients in \( \text{Con} \ A \). Let \( B_i \in M_A(\alpha_i, \beta_i) \) for \( i = 1, \ldots, n \) and put \( B = \prod_1^n B_i \). For each \( i \), choose \( 1_i \in B_i \). If \( B_i \) is a two-element set, let \( x \cdot^i y \) be the operation of a group on \( B_i \) with identity element \( 1_i \). If \( |B_i| > 2 \) then since \( B_i \) equals its \( \langle \alpha_i, \beta_i \rangle \)-body and \( \text{typ}(\alpha_i, \beta_i) \notin \{1, 5\} \), we have \( \text{typ}(\alpha_i, \beta_i) = 2 \); in this case choose an operation \( d_i(x, y, z) \in \text{Pol}_3 A \upharpoonright_{B_i} \) satisfying the properties of Lemma 4.20, and put \( x \cdot^i y = d_i(x, 1_i, y) \) for \( x, y \in B_i \). By Lemma 4.20, \( \langle B_i, \cdot^i \rangle \) is a loop for \( i = 1, \ldots, n \); and \( \text{Con} \ \langle B_i, \cdot^i \rangle \cong \text{Con} \ A \upharpoonright_{B_i} \). Let \( x \cdot y \) be the binary operation on \( B \) such that \( \langle B, \cdot \rangle = \prod_1^n \langle B_i, \cdot^i \rangle \).

Now for \( i = 1, \ldots, n \), if \( |B_i| > 2 \) let \( B_i = \langle B_i, \cdot^i, \ldots \rangle \) have for its basic operations \( x 

and the members of \( \text{Pol}_1 A \upharpoonright_{B_i} \). If \( |B_i| = 2 \), let \( B_i = \langle B_i, \cdot^i \rangle \). By Theorem 4.31 and Lemma 4.36, when \( |B_i| > 2 \) the algebra \( A \upharpoonright_{B_i} \) is nilpotent. Since \( \text{Con} B_i = \text{Con} A \upharpoonright_{B_i} \), and \( \text{Pol} \ B_i \subseteq \text{Pol} A \upharpoonright_{B_i} \), it follows that \( B_i \) is nilpotent and E-minimal. When \( |B_i| = 2 \), it is obvious that the Abelian group \( B_i \) is nilpotent, and that \( \text{Con} B_i = \text{Con} A \upharpoonright_{B_i} \).
By Lemma 6.1, the mapping \( \theta \mapsto (\theta|_{B_i} : 1 \leq i \leq n) \) is a subdirect embedding of \( \text{Con } A \) into \( \prod^n_i \text{Con } B_i \).

To construct the basic operations of \( B \) (besides \( x \cdot y \)), we define for \( 1 \leq i, j \leq n \)

\[
M_{i,j} = \{ f : \text{for some } g \in \text{Pol}_1 A, f = g|_{B_i} \text{ and } f(B_i) \subseteq B_j \}.
\]

We define \( \Sigma \) to be the set of all sequences \( \sigma = \langle \sigma_1, \ldots, \sigma_n \rangle \) where for all \( j \in \{1, \ldots, n\} \) there is an \( i \) such that \( \sigma_j \in M_{i,j} \). For each \( \sigma \in \Sigma \), we define a function \( f_\sigma \in B^B \) by

\[
f_\sigma((b_1, \ldots, b_n)) = \langle \sigma_1(b_{i_1}), \ldots, \sigma_n(b_{i_n}) \rangle
\]

where \( \sigma_j \in M_{i_j,j} \) for all \( 1 \leq j \leq n \). Now we take\( B = \langle B, f_\sigma(\sigma \in \Sigma) \rangle \).

The proof of this theorem will be finished once it is shown that the mapping \( \pi \) defined by

\[
\pi(\theta) = \theta|_{B_1} \times \cdots \times \theta|_{B_n}
= \{(b, c) \in B : (b_i, c_i) \in \theta \text{ for all } 1 \leq i \leq n\}
\]

is a lattice isomorphism of \( \text{Con } A \) with \( \text{Con } B \). It should be obvious (from the description of the subdirect representation of \( \text{Con } A \) into \( \prod \text{Con } B_i \)) that \( \pi \) is one-to-one; and it is easy to see that \( \pi(\text{Con } A) \subseteq \text{Con } B \). We leave it as an Exercise (in fact, 8.8 (3)) to show that \( \pi(\text{Con } A) = \text{Con } B \) and \( \pi \) is a lattice isomorphism. \( \square \)

Theorem 8.7 could be useful for the investigation of the lattice varieties of the form \( \text{HSP}(\text{Con } V) \) derived from (locally finite) congruence-modular varieties \( V \). It has been conjectured that every such lattice variety either consists of distributive lattices or is identical with \( \text{HSP}(\text{Con } R,M) \) for some ring \( R \) with unit, where \( R,M \) is the variety of unitary \( R \)-modules.

Several results about the free spectra of congruence-modular varieties are proved in Chapter 12.

**Exercises 8.8**

1. Let \( V \) be a locally finite congruence-permutable variety. Prove (i): \( \text{typ}\{V\} \subseteq \{2, 3\} \); and (ii): for every finite \( A \in V \) and \( \alpha \prec \beta \) in \( \text{Con } A \) and \( (a, b) \in \beta - \alpha \), there exists \( u \equiv b \,(\text{mod } \alpha) \) with \( \{a, u\} \subseteq N \) for some \( (\alpha, \beta) \)-trace \( N \). Consult Lemmas 5.22 and 5.24. [There is an open question here. Do (i) and (ii) imply that \( V \) is congruence-permutable? In Theorem 9.14, we learn that \( \text{typ}\{V\} \subseteq \{2, 3\} \) if \( V \) is congruence-\( n \)-permutable for some \( n \).]

2. Let \( A \) be a finite algebra such that \( \text{typ}\{A\} = 2 \). Prove that for every \( \alpha \prec \beta \) in \( \text{Con } A \) and \( U \in M_A(\alpha, \beta) \), the \( (\alpha, \beta) \)-tail of \( U \) is empty. (See Lemma 4.27 and note that \( A \) is solvable.)
(3) Complete the proof of Theorem 8.7.

(4) Let $G$ be a finite group, $p_1, \ldots, p_n$ be the prime divisors of $|G|$, and $P_i$ be a Sylow $p_i$-subgroup of $G$ for $1 \leq i \leq n$. Show that the mapping

$$\theta \mapsto (\theta|_{P_i} : 1 \leq i \leq n)$$

is a lattice embedding of $\text{Con } G$ into $\prod_{i=1}^{n} \text{Con } P_i$, but not necessarily a subdirect embedding. (See Exercise 4.37(6) for a proof that the groups $P_i$ are $E$-minimal algebras.)