Mal'tsev conditions

1. Mal'tsev's Theorem

Two congruences α, β on an algebra A are said to *permute* if they commute: $\alpha\beta = \beta\alpha$.

Here $\alpha\beta$ is the composition, given by $x\ \alpha\beta\ z$ if and only if there exists y with $x\ \alpha\ y\ \beta\ z$. Notice that $\alpha\beta$ and $\beta\alpha$ are not necessarily equivalence relations.

A variety V is said to be *congruence permutable* if in any algebra in V any two congruence relations permute. The famous Russian algebraist Mal'tsev (also transliterated as Mal'cev) gave this characterization:

1.1 Theorem (Mal'tsev) For a variety V, the following are equivalent:

(a) V is congruence-permutable;

(b) there is a term $p(x, y, z)$ such that in V these laws hold:

$p(x, x, z) = z,$

$p(x, z, z) = x.$

For example, the variety of groups satisfies this condition with $p(x, y, z) = xy^{-1}z$. The same term, written additively as $x - y + z$, then works for rings, since rings have an additive group.

2. Mal'tsev conditions

Other theorems of the same general kind have been discovered, where a condition on a variety is characterized using the existence of terms obeying laws of some sort. Such a condition is now called a "Mal'tsev condition". Some typical examples, in additional to congruence permutability, are

- V is *congruence-distributive.* In other words, for any $\mathcal{A} \in V$, Con(A) is a distributive lattice.

  Example: The variety of all lattices; the variety of all Boolean algebras.

- V is *congruence-modular.* In other words, for any $\mathcal{A} \in V$, Con(A) is a modular lattice.

  Since the distributive law implies the modular law, any congruence-distributive variety is also congruence-modular. Also, we have:

  Proposition. Any congruence-permutable variety is congruence-modular.

- V is *arithmetic* (“arithmet′ic”). This means that V is both congruence-permutable and congruence-distributive.

  Example: The variety of rings generated by a finite field.

3. Some theorems showing Mal’tsev conditions

In addition to Mal’tsev’s theorem, the following facts hold, among others. Some of them refer to a *majority term*, which means a ternary term $m(x, y, z)$ obeying the three laws

$m(x, x, y) = x$, $m(x, y, x) = x$, $m(y, x, x) = x$

in the variety in question.

3.1 Theorem (Pixley) For a variety V, the following are equivalent:

(a) V is arithmetic;

(b) there are terms $p(x, y, z)$ and $m(x, y, z)$ such that in V, p obeys Mal’tsev’s laws of (b) in Theorem 1.1 and m is a majority term;

(c) there is a term $q(x, y, z)$ such that in V,

$q(x, x, z) = z$ (minority of entries),

$q(x, z, z) = x$ (minority of entries),

$q(x, y, x) = x$ (majority of entries).

3.2 Theorem (Jónsson) For a variety V, the following are equivalent:

(a) V is congruence-distributive;

(b) for some $n \geq 2$, there are terms $t_0, \ldots, t_n$ in x, y, z such that in V,

(i) $t_0(x, y, z) = x$, $t_n(x, y, z) = z$;

(ii) $t_i(x, y, x) = x$, for all i;

(iii) $t_i(x, x, z) = t_{i+1}(x, x, z)$ for i even, $t_i(x, z, z) = t_{i+1}(x, z, z)$ for i odd.

(Notice that the case $n = 2$ is equivalent to the existence of a majority term.)

3.3 Theorem (Day, Gumm) For a variety V, the following are equivalent:

(a) V is congruence-modular;

(b) for some $n \geq 0$, there are terms $t_0, \ldots, t_n$ and p in x, y, z such that in V,

(i) $t_0(x, y, z) = x$

(ii) $t_i(x, y, x) = x$, for all i;

(iii) $t_i(x, z, z) = t_{i+1}(x, z, z)$ for i even, $t_i(x, x, z) = t_{i+1}(x, x, z)$ for i odd.

(iv) $t_n(x, z, z) = p(x, z, z)$,

(v) $p(x, x, z) = z$.

4. Problems

Problem CC-1. Prove Mal'tsev's theorem.

Problem CC-2. Prove Pixley's theorem.

Problem CC-3. Another Mal'tsev condition:

Show that the following are equivalent for a variety V:

(i) V has a majority term;

(ii) intersections of congruences distribute over composition:

$$\alpha \cap (\beta\gamma) = (\alpha \cap \beta)(\alpha \cap \gamma).$$

Problem CC-4. Using Problem CC-3, show that a variety with a majority term is congruence-distributive (the case $n = 2$ of Jónsson's theorem).

(Method: Use (ii) of Problem CC-3, generalized to compositions of more than two congruences by an easy induction. Recall that $\alpha \vee \beta$ is the union of $\alpha\beta$, $\alpha\beta\alpha$, $\alpha\beta\alpha\beta$, etc.)

Problem CC-5. In the finite field $\mathbf{F}_q = \mathrm{GF}(q)$ with q elements, find a term or terms to show that $\mathrm{Var}(\mathbf{F}_q)$ is arithmetic.