Universal Algebra and its Links with Logic,
Algebra, Combinatorics, and Computer Science
Proc. "25. Arbeitstagung über Allgemeine Algebra", Darmstadt 1983
P. Burmeister et al. (eds.)

14 – 28

GEOMETRICAL REASONING AND ANALOGY IN UNIVERSAL ALGEBRA

H. P. Gumm

Most students of classical algebra will sooner or later appreciate the close connection between algebraic and geometric concepts. Geometric concepts are parts of experience in everyday life. They are easy to visualize, figures can be drawn, rules and theorems can actually be seen. Algebraic theorems and formulas are usually much harder to grasp for the unexperienced. Many textbooks therefore dwell in geometrical visualizations and proofs for some simple algebraic theorems like the binomial or the Pythagorean theorem. It takes years of apprenticeship until a familiarity with the permitted manipulations of abstract strings and formulas is achieved. Geometric visualization is not restricted to the segment of geometry that is actually being experienced. It is easy to invent analogies. As an example consider the classification of the possible sets of solutions to a system of linear equations. Even though a many - dimensional space is not a part of experience it is easy to imagine the different hyperplanes that intersect to give infinitely many, exactly one, or no solution. And in devising a proof it is very helpful to keep the geometric pictures in mind to stake out the rough lines for a proof. Later the gaps will have to be filled with calculations.

What is then the geometry, what are the geometric pictures that can aid in studying universal algebras? The experience with classical algebra first gives us the choice between a projective approach and an affine approach. What should the projective geometry associated with a universal algebra be? In the classical case of modules there is a one-to-one correspondence between subspaces and the congruence relations they induce. So in the universal algebra case, the subspaces of the projective (pseudo-) geometry should correspond to the congruence relations of the algebra A ; thus studying the lattice Con(A) of congruences on A would be studying the projective geometry of A. Geometrically important concepts as e.g. the Desarguesian or the Pappian laws can be translated into lattice theoretical concepts for Con(A). A first theorem in this environment is due to B.Jonsson /17/:

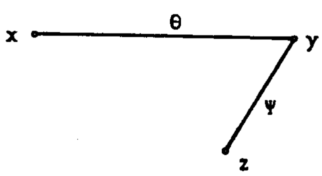
Let A have permutable congruences, then Con(A) is arguesian.
Here the arguesian law is nothing but the lattice theoretical phrasing of the Desarguesian law, thus the conclusion of the theorem is :

The projective geometry of A is Desarguesian.
The hypothesis requires that for any two congruences Θ and Ψ , the relational product $\Theta\circ\Psi$ is a congruence again, which is the same as saying $\Theta\circ\Psi = \Psi\circ\Theta$. This condition is well known to imply that Con(A) is a modular lattice, and indeed R.Freese and B.Jonsson were able to show in / 6/:

Let A and all subdirect subalgebras of $A\times A$ have modular congruence lattices. Then Con(A) is arguesian.
Here it is not enough if A has a modular congruence lattice. Freese and Jonsson use a simple trick which is both easy and well known but very helpful in what follows:

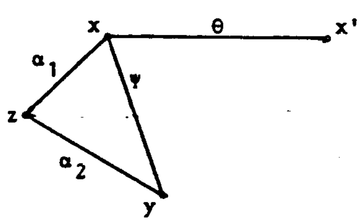
Trick: Every congruence relation Θ on an algebra A is a subalgebra of $A\times A$. Θ is actually embedded subdirectly in $A\times A$.
It is exactly those subdirect powers of A which Freese and Jonsson require to have modular congruence lattices.
Other "projective" investigations concern finite algebras whose projective geometry is one-dimensional. It had for a long time been open whether the number of nontrivial subspaces would always have to be one more than a prime power. A counterexample was given by W.Feit / 5 /, resting on work of P.Palfy and P.Pudlak / 19/.
In the affine approach which was introduced and systematically studied by R.Wille /21/, we let the points correspond to elements of the algebra A, and we take as lines the classes of congruence relations on A. A class of a congruence relation Θ will be called a Θ-line. The collection of classes of a fixed congruence

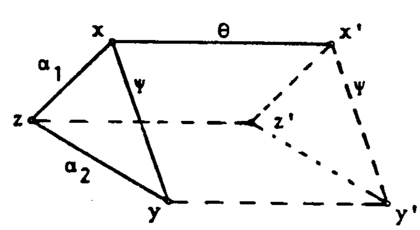
relation then will be a class of pairwise parallel lines.
This enables us to draw pictures where points represent elements of A and lines represent congruence classes of some congruence Θ, in which case we sometimes lable the line with the letter Θ and call them "Θ-lines". We shall draw two lines parallel if they represent classes of the same congruence relation.
As a first example of the connections between algebraic and geometric properties we look at permuting congruence relations Θ and Ψ. The fact that Θ and Ψ permute can geometrically be expressed as follows:
Let l be a Θ-line and g a Ψ-line and suppose l and g intersect with y a point of intersection. For any points x on l and z on g there exists a point u making (x,y,z,u) a parallelogram. Pictorially:



yields

The case that all congruences in all algebras of some variety permute is captured in Mal'cevs famous theorem, stating that this is equivalent to the existence of a ternary term m(x,y,z) satisfying the equations m(x,y,y) = x and m(x,x,y) = y. Since m is compatible with all congruences, it is easy to see that this is in turn equivalent to saying that m(x,y,z) is always a fourth parallelogram point in the situation of the above figure.
The equations are abtained by letting Θ or Ψ shrink to the identity congruence. This simple <u>parallelogram principle</u> was extremely fruitful for further investigations. So it was easy to conclude that the congruence class geometries of algebras in such a "permutable" variety obey the <u>Little law of Desargues</u> which is given pictorially as





<u>implies</u>

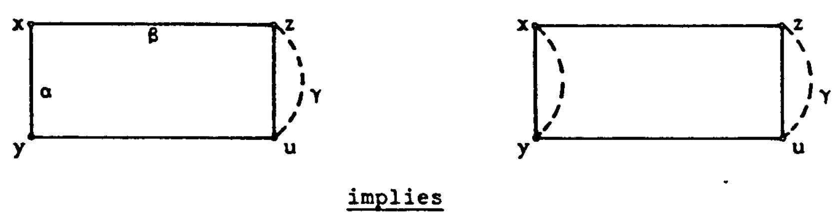
This is to be read as: Given x,y,z,x', connected by Ψ, α_1, α_2 and Θ-lines there exist y' and z' with the relations indicated, where lines drawn parallel in the figure mean lines of the same congruence relation. Here y' and z' can be constructed as m(x',x,y) resp. m(x',x,z).

If we let x and y coincide, i.e. we take $\Psi = 0$, the identity congruence, then we see that the parallelogram principle follows. In other words, the varieties in which the Little Desarguesian law holds are precisely the permutable varieties. Unfortunately this result seems not to fit in with the projective version of Freese and Jonsson that, projectively, the Desarguesian theorem characterizes the modular varieties. The resolution of this problem though will be achieved when we come to slightly reformulating the little Desarguesian law.

Affine geometry in modular algebras

To do affine geometry in congruence modular algebras we need some geometrical substitute for the parallelogram principle. This was found in the following principle /8 /:

<u>Shifting Lemma:</u> Let α, β and γ be congruences in a congruence modular algebra A and x,y,z,u be points of A. Suppose moreover that $\alpha \wedge \beta \leq \gamma$ then

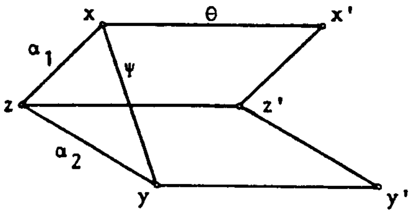


The proof of this lemma is extremely simple, nevertheless the lemma itself is probably the most important tool for the geometrical study of modular varieties. The second tool we need is the simple trick we have already met, to think of a congruence Θ on A as a subalgebra of A×A.

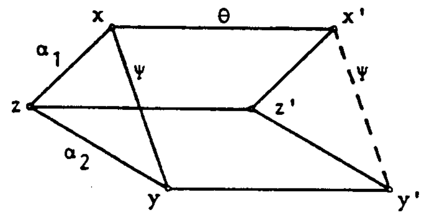
We shall show now how these two ingredients, or simple modifications thereof suffice to develop the affine geometry of congruence modular algebras.

Let us start with the theorems of Desargues and Pappus. Clearly we must modify the formulation of Desargues' law slightly to /9/:

The Little Desarguesian law: Let $\Theta,\alpha_1,\alpha_2,\Psi$ be congruences with $\Theta\wedge\alpha_1 \leq \Psi$ and $\Theta\wedge\alpha_2 \leq \Psi$ and let x,y,z,x',y',z' be elements of A then



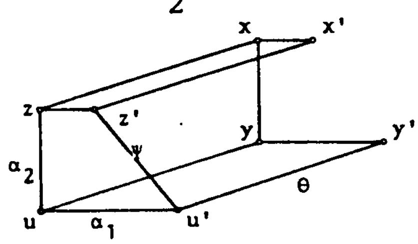
implies



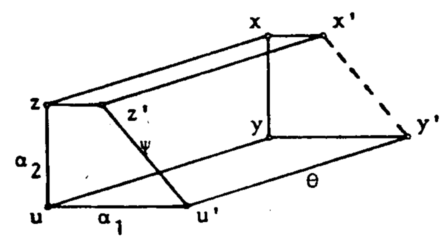
We note that as in the shifting lemma we require all necessary points already to exist and we need "dimensionality conditions" for the congruences (resp. subspaces) involved. We obtain, in complete analogy to the Freese - Jonsson result:

Let A and all subdirect subalgebras of A×A have modular congruences. Then the affine geometry of A satisfies the Little Desarguesian law.

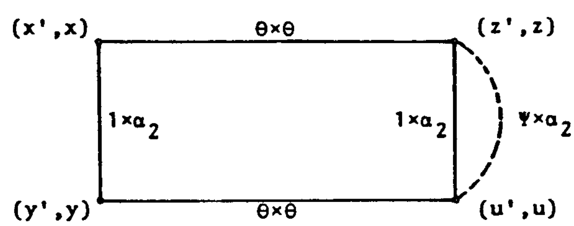
The proof becomes more transparent if we restate the theorem in a slightly more general version, namely:
Given points x,y,z,u,x',y'z',u' and congruences $\Theta,\alpha_1,\alpha_2,\Psi$ with $\Theta\wedge\alpha_1 \leq\Psi$ and $\Theta\wedge\alpha_2\leq \Psi$ then



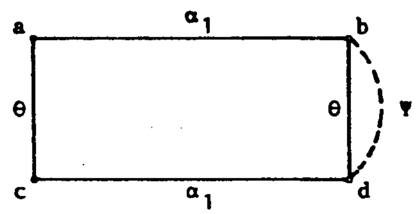
implies



The idea for a proof develops when we imagine this figure as a three-dimensional configuration and look at it "from the side", namely along the α_1 -lines. The figure we see is



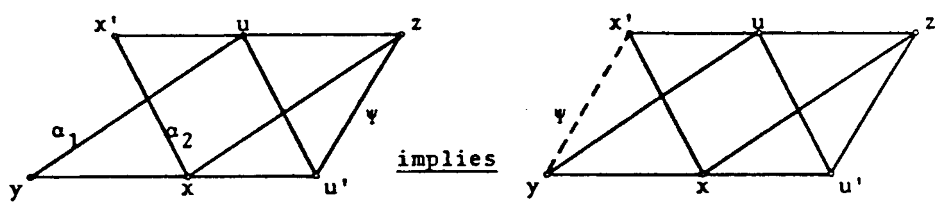
where now the points are elements of the algebra α_1. If we can apply the shifting lemma to this situation, showing that $(x',x)\ \Psi\times\Theta\ (y',y)$ we are done. Well, by hypothesis the algebra α_1 again is congruence modular, thus we are left to check that in this algebra $1\times\Theta \wedge \Theta\times\alpha_2 \leq \Psi\times\Theta$. This is true for elements (a,b), (c,d) from the algebra α_1 by a second application of the shifting lemma. For ((a,b),(c,d)) from the left hand side we obtain, using the fact that $\Theta\wedge\alpha_2 \leq \Psi$, the configuration



from which by the shifting lemma we may conclude $(a,c) \in \Psi$, so $((a,b),(c,d)) \in \Psi\times\Theta$.

Analogously we may formulate a version of the <u>Little Pappian theorem</u>:

Let $\Theta, \Psi, \alpha_1, \alpha_2$ be congruences with $\Theta\wedge\alpha_1 \leq \Psi$ and $\Theta\wedge\alpha_2 \leq \Psi$ and x,y,z,u,x',u' points then we obtain with a similar proof:

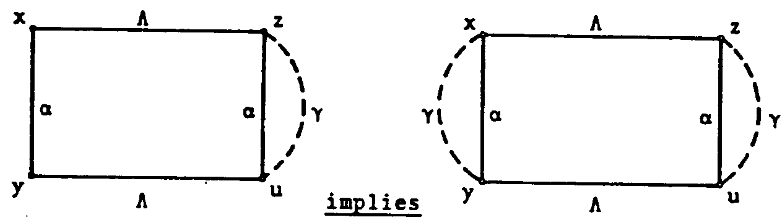


<u>Let A and all congruences of A have modular congruence lattices. Then the affine geometry of A is Pappian.</u>

At this point some interesting questions may be raised: Since the analogy of projective and affine versions seems perfect in the case of the Desarguesian law there should be a similar analogy with the Pappian law. Thus a projective version of the Pappian law should be discovered for modular varieties. More generally an interesting question arises: <u>Is there a general translation between affine and projective properties of congruence modular algebras?</u>

Reviewing some known theorems

Once certain principles and ways of reasoning have been applied successfully one may review known theorems trying to look at them in a new light. We elaborate two examples. Before we go on though we shall say a few more words about the relationship of congruence modularity and the shifting lemma. On the level of varieties the shifting lemma is equivalent to modularity. On the level of single algebras though, modularity lies between the shifting lemma and a slight generalization thereof, the shifting principle /10/:

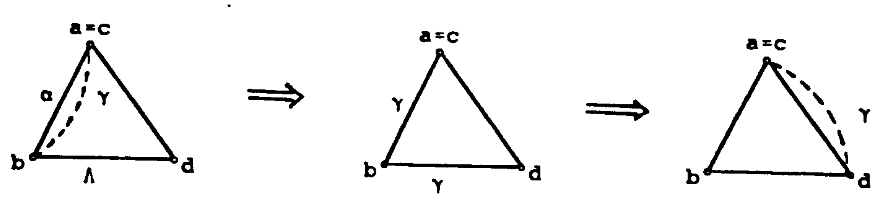


where α and γ are congruences, but Λ may be any reflexive, symmetrical subalgebra of $A^{\times}A$. As in the shifting lemma we assume $\alpha \wedge \Lambda \leq \gamma$. W.l.o.g. $\gamma \leq \alpha$, otherwise replace γ by $\gamma \wedge \alpha$. Thus to show modularity, it is enough to show the shifting principle. We now come to our first example, which is an improvement of a theorem of J.Hagemann /14/, due to S.Bulman-Fleming, A.Day and W.Taylor/ 2 /:

Let all subalgebras of A×A have regular congruences, then A has modular congruences.

Here A is said to have regular congruences, if congruences are uniquely determined by any of their classes.

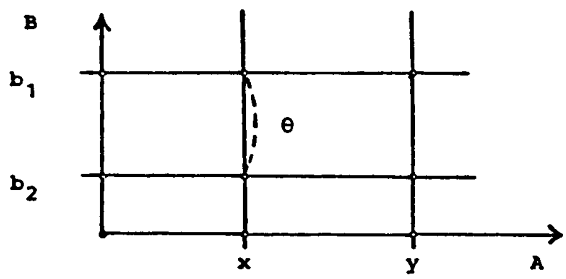
To prove the shifting principle, we look at Λ, the subalgebra of AxA, and need to show that in this algebra we have $\gamma\times\alpha = \gamma\times\gamma$. Since the above version of the shifting principle becomes trivial for the case a = c:



it follows that the (a,a)-class of $\gamma\times\alpha$ coincides with the (a,a)-class of $\gamma\times\gamma$, thus $\gamma\times\alpha = \gamma\times\gamma$ by regularity.

As a second example we consider refinement theorems for direct products. If $A\times B \cong C\times D$ one wants to have canonical refinements (see / 1/) such that $A \cong E_1\times E_2$, $B \cong F_1\times F_2$, $C \cong E_1\times F_1$ and $D \cong E_2\times F_2$. Let $A\times B$ be given with the canonical projection kernels π_1 and π_2 and consider the congruences Θ and Ψ on $A\times B$ yielding the decomposition corresponding to $C\times D$. Then the shifting lemma yields that a congruence relation Θ_B may be defined on B as

$$b_1\ \Theta_B\ b_2 \Leftrightarrow \exists x \quad (x,b_1)\ \Theta\ (x,b_2)$$
$$\Leftrightarrow \forall y \quad (y,b_1)\ \Theta\ (y,b_2)$$



One has canonical refinements if and only if in such a way the congruences Θ and Ψ split in congruence relations Θ_A, Θ_B, Ψ_A and Ψ_B, which provide the factors for the refinement.
Here the shifting lemma is being applied in a very special situation and the argument is not restricted to congruence modular algebras. Even the fact that Θ and Ψ split in the desired way may be formulated as an easy geometrical principle. In this spirit H.Bauer and R.Wille / 1 / have given an elegant proof for Hashimoto's refinement theorem for products of posets (/16/).
In modular varieties Θ and Ψ do generally not split as requested. So called "skew" congruences have to be introduced, but they too can be geometrically analysed so that for modular varieties and in the presence of chain conditions one obtains a cancellation and refinement theorem "up to isotopy". In the proof of this result /13/ , unfortunately affine and projective reasoning is being mixed so a "purer" proof of this result using the above methods would be desirable.

Using geometry to guide syntactical inferences

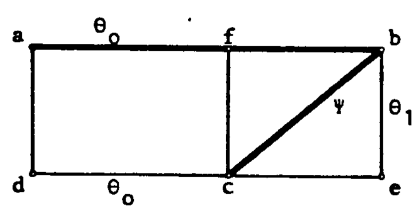
The difference between the configuration theorems encountered so far in permutable and in modular varieties can shortly be subsumed by:

In permutable varieties points with the desired relations may be generated, whereas in modular varieties the points already are supposed to exist satisfying some of the desired relations and the rest of the relations can be concluded.

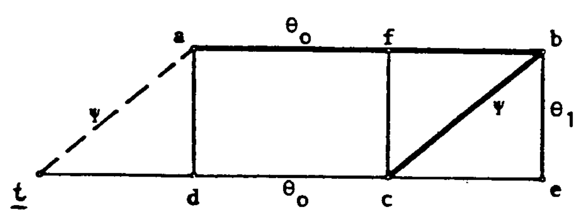
The prime example for this distinction is the comparison of the parallelogram principle versus the shifting lemma.

We shall see in this chapter though, that we do have a version of the parallelogram principle in modular varieties. The parallelogram principle holds, provided some auxiliary points are given. Moreover, the fourth-parallelogram point is provided by a ternary term t(x,y,z) which does share many properties with a Mal'cev term / 8 /:

In every modular variety there exists a ternary term t(x,y,z) such that t(x,y,y) = x, and, given a configuration



with $\Theta_0 \wedge \Theta_1 \leq \Psi$, t(a,b,c) completes a,b,c to a Θ_0-Ψ-parallelogram.



The proof of this theorem is a prime example of how geometrical analogy may be used to stake out a proof and fill the gaps later with calculations. We shall give this geometric idea. It is noteworthy that the proof implicitly involves multiple substitutions of terms into other terms.

We start with the terms and equations given by A.Day /4 /, describing congruence modularity: A variety $\underline{V}$ is congruence modular iff there is a number n and quaternary terms $m_0, m_1, \ldots, m_n$ such that the following equations are true in $\underline{V}$:

(M0) $m_0(x,y,z,u) = x$

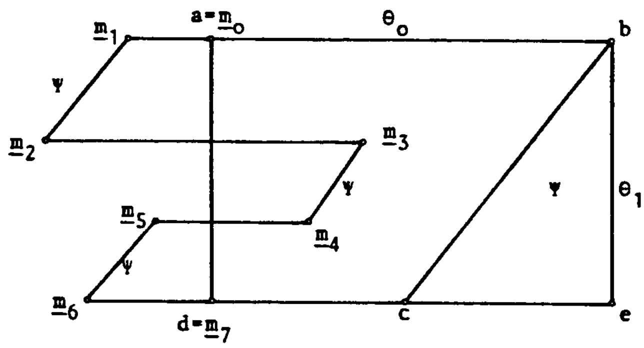
(M1) $m_i(x,x,y,y) = x$ for all $0 \leqslant i \leqslant n$,

(M2) $m_i(x,y,x,y) = m_{i+1}(x,y,x,y)$ for $0 \leqslant i < n$, i even

(M3) $m_i(x,y,z,z) = m_{i+1}(x,y,z,z)$ for $0 \leqslant i < n$, i odd

(M4) $m_n(x,y,z,u) = y$.

Let us draw the result of applying these terms to the points in the given configuration. We define $\underline{m}_i := m_i(a,d,b,c)$. Then the equations give us relations between these points $\underline{m}_i$. Using (M0), (M2), (M3), (M4), we obtain a figure which we draw for the case n = 7:

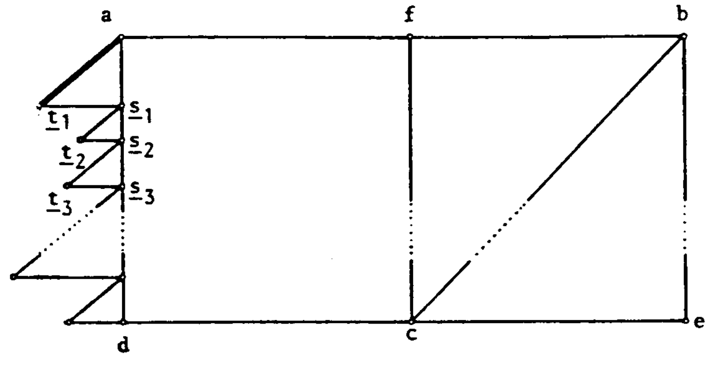


Now the rough idea how to construct a Ψ-line from a to the bottom line becomes immediately apparent: The little Ψ-pieces between $\underline{m}_i$ and $\underline{m}_{i+1}$ for odd i should be shifted to the appropriate positions, starting at a, to connect to the desired line. Substituting a and d in the first places of the Day-terms and substituting some of b,c,e in the last two places, more precisely, setting

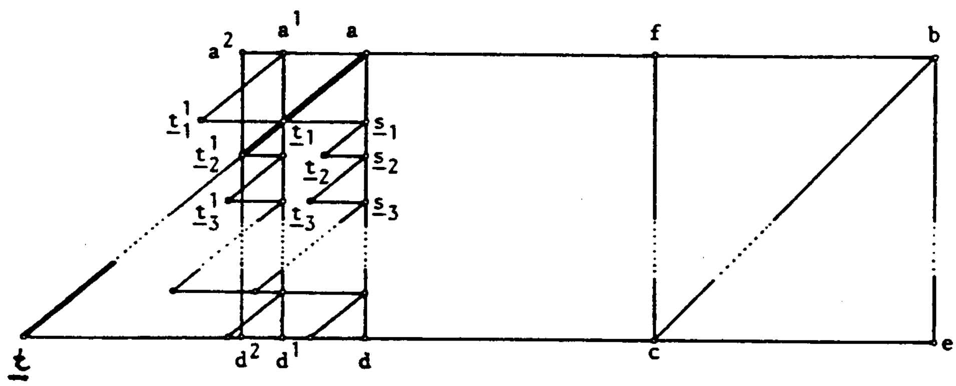
$\underline{t}_i := m_i(a,d,c,e)$ for i odd, $\underline{t}_i := m_i(a,d,b,c)$ for i even,

$\underline{s}_i := m_i(a,d,c,c)$ for i odd, $\underline{s}_i := m_i(a,d,b,e)$ for i even

we obtain a configuration as in



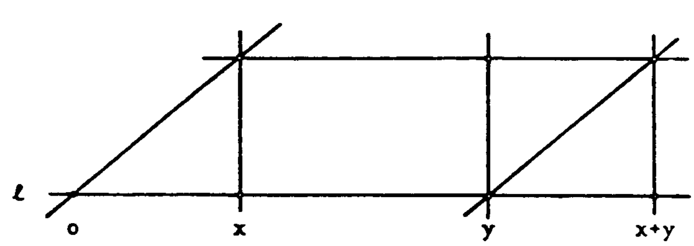
Now we do have some control about the horizontal position of the little Ψ-pieces. Consider t_1, the first of the resulting peaks, then it is easy to find a point a^1 on the top line and d^1 on the bottom line above , resp. below t_1. Applying the terms as before, but replacing a with a^1 and d with d^1 we find a new set of peaks, but in the same horizontal position. Now the second Ψ-line of the new set of peaks joins up with the first Ψ-line of the old peaks and it is clear how to walk down diagonally until the bottom line is reached.



Since all points are constructed by applying Day's terms to the original points it is clear that syntactically the above method results in a continued substitution of terms into other terms, yielding a final term t(x,y,z) with the required property.

Coordinatization

We shall start with the simple idea of coordinatizing an affine line l using an abelian group. After embedding l into a plane and using two more mutually non-parallel lines l' and l", the addition x+y may easily be performed as shown in the picture below. Note that beforehand we must have selected an arbitrary element 0 on l to serve as the zero for addition.



We now assume that an algebra A in a modular variety is given. In our analogy then the A will be the line 1 which we embed into the "plane" $A \times A$. Note that in $A \times A$ we may represent A as $\{(0,x) | x \in A\}$ or as $\{(x,0) | x \in A\}$, both being lines corresponding to the projection congruences π_1, resp. π_2. 0 is chosen arbitrarily in A. For the third line 1", the choice is not quite as obvious. Since the geometrical operations we want to perform are parallel shifts and finding points of intersection, we need a congruence relation Δ such that every Δ-line intersects every π_1-line and every π_2-line. An obvious candidate for 1" seems to be the diagonal $d = \{(x,x) | x \in A\}$ and therefore Δ should be at least the congruence relation generated by d in $A \times A$,

$$\Delta := \langle \{((x,x),(y,y)) \mid (x,y) \in A \times A\} \rangle_{A \times A} .$$

Now, however, d need not be a line by itself, but the class of Δ containing d might be some $\bar{d}$ properly containing d. Such a $\bar{d}$ will certainly intersect each π_1- and each π_2-line, and if A is contained in a modular variety, it follows from the modified parallelogram principle that so will each other line of Δ. Finally, to construct x+y as above, points of intersections ought to be unique. This is the only hypothesis which is not guaranteed by modularity, but we shall see soon how to handle this case. Let us now for a moment assume that points of intersection are unique. It is easy to see with the shifting lemma that this is equivalent to requiring that d itself is a line, i.e. $\bar{d} = d$. Now the familiar definition of x+y may be given and its properties developed. Proving associativity, commutativity and cancellativity leads to versions of exactly the geometrical configuration theorems which we met earlier. Since addition is defined via congruence relations and each such congruence relation is preserved by all polynomials of A it is not surprising that every polynomial of A is a homomorphism with respect to the ternary operation x-y+z. (Considering x-y+z instead of the group operations x+y and -x is preferable in any case, since it removes the discussion about choosing some arbitrary element for a zero.) <u>Thus A is polynomially equivalent to a module over some ring R.</u> Moreover all the algebras A in a fixed modular variety where d is a congruence class do form a subvariety of modules, the variety of "abelian algebras".

In the case that d by itself is not a line, intuitively $\bar{d}$ becomes too "thick" so that $\bar{d}$ intersects horizontal and vertical lines in more than one point, and as a consequence x+y cannot be defined uniquely. The obvious idea is to factor A by this "thickness" of $\bar{d}$. The idea indeed works thanks to the shifting lemma. The definition

$$b\,[1,1]\,c \iff \exists x \quad (x,b)\ \Delta\ (x,c)$$

yields a congruence relation $[1,1]$ on A so that the coordinatization of $A/[1,1]$ works as described above, and $A/[1,1]$ is an abelian algebra.

More generally, given two congruences Θ and Ψ, we may reuse our trick of replacing A×A by its subalgebra Θ and we may replace d by those pieces of the diagonal which are congruent modulo Ψ to obtain:

$$\Delta_\Theta^\Psi := \langle\{((x,x),(y,y)) \mid (x,y) \in \Psi\}\rangle_\Theta$$

This is a congruence relation on the algebra Θ. Then, just as before we set

$$b\,[\Theta,\Psi]\,c \iff \exists x \quad (x,b)\ \Delta_\Theta^\Psi\ (x,c)$$

and get that $[\Theta,\Psi]$ becomes a congruence relation on A, which is called the <u>commutator of Θ and Ψ</u>. This congruence multiplication was invented by J.D.H.Smith /20/, J.Hagemann and C.Herrmann /15/ and further completed and reinterpreted in /12/ and /7/. It reduces precisely to the familiar notion of commutators in groups and to the notion of ideal multiplication in rings. In distributive varieties the commutator of Θ and Ψ equals their intersection. All the notions and analogies from those theories, like primeness, nilpotency and solvability become available in general for modular varieties. They have provided a wealth of new insight into their structure theory. As an example we mention the following theorem which generalizes the famous Jonsson-lemma /18/. The essential idea for such a generalization is due to Hrushovskii, the present form is from /10/. We define $\sqrt{A}$ as the intersection of all prime congruences of A, and assume that A is in the (modular) variety generated by some class $\underline{K}$. Then

<u>$A/\sqrt{A}$ is in $P_S HSP_U(\underline{K})$</u>.

In a distributive variety, primeness reduces to finitely subdirect irreducibility, so here $\sqrt{A} = 0$. Clearly, if A is abelian then no congruence relation will be prime, since $[\Theta,\Psi] = 0$ for all congruences Θ and Ψ. Thus $\sqrt{A} = 1$. In this way we have identified two "ends" of any modular variety and indeed, if certain restrictions are placed on the variety, it frequently will split into those two ends. Numerous results have been obtained in this direction, we only mention /11/ and the work of R.Freese and R.McKenzie /7/ and S.Burris and R.McKenzie /3/, but a general decomposition theory still has to be found.

References

1 H.Bauer, R.Wille: A proof of Hashimoto's refinement theorem. THD preprint 734, Darmstadt 1983.

2 S.Bulman-Fleming, A.Day, W.Taylor: Regularity and modularity of congruences. Algebra Universalis 4 (1974), 58-69.

3 S.Burris, R.McKenzie: Decidable varieties with modular congruences lattices. Memoirs of the A.M.S., 32 (1981), Number 246.

4 A.Day: A characterization of modularity for congruence lattice of algebras. Canad. Math. Bull. 12 (1969), 167-173.

5 W.Feit: An interval in the subgroup lattice of a finite group which is isomorphic to M_7. Algebra Universalis, to appear.

6 R.Freese, B.Jonsson: Congruence modularity implies the Arguesian identity. Algebra Universalis 7 (1977), 191-194.

7 R.Freese, R.McKenzie: Residually small varieties with modular congruence lattices. Transactions of the A.M.S., 246 (1981), 419-430.

8 H.P.Gumm: Über die Lösungsmengen von Gleichungssystemen über allgemeinen Algebren. Math.Z. 162 (1978), 51-62.

9 H.P.Gumm: The Little Desarguesian Theorem for modular varieties. Proc. of the A.M.S. 80 (1980), 393-397.

10 H.P.Gumm: Geometrical methods in congruence modular algebras. Memoirs of the A.M.S. , 45 (1983), Number 286.

11 H.P.Gumm: Congruence modularity is permutability composed with distributivity. Arch.d.Math. 36 (1981), 569-576.

12 H.P.Gumm: An easy way to the commutator in modular varieties. Arch.d. Math. 34 (1980), 220-228.

13 H.P.Gumm, C.Herrmann: Algebras in modular varities: Baer refinements, cancellation and isotopy. Houston J. of Math. 5 (1979), 503-523.

14 J.Hagemann: On regular and weakly regular congruences. THD preprint, Darmstadt 1973.

15 J.Hagemann, C.Herrmann: A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity. Arch.d.Math. 32 (1979), 234-245.

16 J.Hashimoto: On direct product decomposition of partially ordered sets. Ann. of Math. 54 (1951), 315-318.

17 B.Jonsson: On the representation of lattices. Math. Scand. 1 (1953), 193-206.

18 B.Jonsson: Algebras whose congruence lattices are distributeve. Math. Scand. 21 (1967), 110-121.

19 P.P.Palfy, P.Pudlak: Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups. Algebra Universalis 11 (1980), 22-27.

20 J.D.H.Smith: Mal'cev varieties. Lecture Notes in Math., Springer Verlag, Berlin - New York, 1976.

21 R.Wille, Kongruenzklassengeometrien. Lecture Notes in Math., Vol.113, Springer Verlag, Berlin - New York, 1970.

Gesellschaft für Strahlen- und
Umweltforschung mbH München (GSF)
Instit. für Medizinische Informatik
und Systemforschung (MEDIS)
Ingolstädter Landstr. 1
D-8042 Neuherberg, West-Germany