Werk

Label: Article

Jahr: 1985

PURL: https://resolver.sub.uni-goettingen.de/purl?316342866_0026|log21

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

COMMENTATIONES MATHEMATICAE UNVERSITATIS CAROLINAE

26,2 (1985)

A SIMPLE GEOMETRIC PROOF OF A THEOREM ON M_n

Jiří TŮMA

Abstract: The congruence lattice of a 2-dimensional vector space over a finite field has length two. A complete description of all sublattices of these congruence lattices which are again congruence lattices of finite algebras is given.

Key words: Congruence lattice, finite algebra, vector space over a finite field.

Classification: 06B10, 06B15

It is a well-known fact that the congruence lattice of the 2-dimensional vector space $\mathcal{A} = (A,F)$ over $GF(p^k)$ is isomorphic to M_n, the lattice of length two with $n = p^k + 1$ non-trivial elements. In a fixed coordinate system in $\mathcal{A}$ the non-trivial congruences are described as follows:

(1) any $x \in GF(p^k)$ defines a congruence $(a,b) \sim_x (c,d)$ iff $c = a + fx$ and $d = b + f$ for some $f \in GF(p^k)$,

giving thus p^k congruences; the last one is defined by

(2) $(a,b) \sim_\infty (c,d)$ iff $b = d$.

The next idea how to construct finite algebras with congruence lattices of length two was to add a new set G of operations to $\mathcal{A}$ in order to damage some of the congruences of $\mathcal{A}$. Algebras $\mathcal{B} = (A, F \cup G)$ have obviously congruence lattices of length not greater than two. This idea was disproved by Quackenbush in [1]. As a consequence of a more general theorem on congruence

permutable varieties he proved that the number of non-trivial congruences of $\mathcal{B}$ is again some prime-power plus one, provided it is at least three. Here we shall give an elementary geometric proof of this result. Moreover, our method allows to characterize completely the congruence lattices of algebras obtained by adding further operations to the 2-dimensional vector spaces over finite fields, as pointed out e.g. by P. Pudlák, P. Pálfy and H. Kurzweil.

Theorem. Let $\mathcal{A} = (A,F)$ be the 2-dimensional vector space over $GF(p^k)$ and G a set of operations on A. If the congruence lattice of the algebra $\mathcal{B} = (A,F \cup G)$ is isomorphic to M_m, $m \geq 3$, then there is a divisor l of k such that $m = p^l + 1$. Conversely, if l is a divisor of k, then there is a set H of operations on A such that the congruence lattice of the algebra $\mathcal{C} = (A,F \cup H)$ is isomorphic to M_{p^l+1}.

Proof. Suppose $\mathcal{B}$ has at least three non-trivial congruences P, Q, R, and choose a coordinate system in (A,F) such that $P = \sim_\infty$, $Q = \sim_0$, $R = \sim_1$ (cf. (1) and (2)). Set
$K = \{x \in GF(p^k)\colon \sim_x \text{ is a congruence of } \mathcal{B}\}$.

We prove that K is a subfield of $GF(p^k)$. We have $0,1 \in K$ by the choice of the coordinate system. Let x, y be elements of K and let us consider Figs. 1 and 2. The horizontal, vertical and cross full lines correspond to blocks of $\sim_\infty$, $\sim_0$ and $\sim_1$ resp., the dashed and dotted lines correspond to blocks of $\sim_x$ and $\sim_y$, resp.

We say that two points $M,N \in A$ are 1-joined iff there exist $U,V \in A$ such that $V \sim_\infty M \sim_x U \sim_0 V \sim_y N \sim_\infty U$.

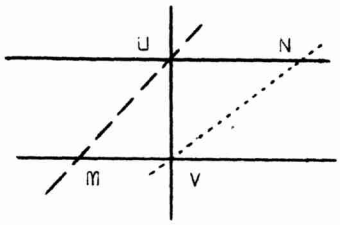

Fig. 1

Now consider the least equivalence relation S generated by all 1-joined couples. If M, N is such a couple and g is a unary operation from the clone generated by $F \cup G$, then g(M), g(N) are also 1-joined, hence S is a congruence of $\mathfrak{B}$. But if M, N are 1-joined and M = (a,b), then there is $f \in GF(p^k)$ such that U = = (a+fx,b+f), V = (a+fx,b) and N = $(a+fx+fy,b+f)$, therefore $M \sim_{x+y} N$. By reversing the whole process we get also $\sim_{x+y} \subseteq S$, hence $x + y \in K$.

To prove that K is closed under multiplication, suppose $x,y \neq 0$ and use Fig. 2 in the same way. This simple figure was suggested by Peter Pálfy.

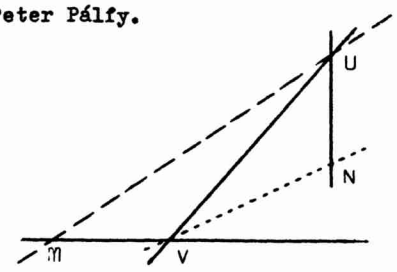

Fig. 2

We say that M, N are 2-joined iff there are $U,V \in A$ such that $V \sim_\infty M \sim_x U \sim_1 V \sim_y N \sim_o U$, and let T be the least equi-

valence relation generated by all 2-joined couples. By the same argument as above, T is a congruence of $\mathfrak{B}$. If M, N are 2-joined, then there is $f \in GF(p^k)$ such that U = (a+fx,b+f), V = = (aqfx - f,b) and N = $(a+fx^{-1}\ xy, b+fy^{-1})$, hence $T \subseteq \sim_{xy}$. Conversely, auppose $M \sim_{xy} N$ and M = (a,b), N = (c,d). Then we can take f = (d-b)y and U, V as above to get that M, N are 2-joined. It proves $T = \sim_{xy}$, hence $xy \in K$.

It follows that K is a subfield of $GF(p^k)$, therefore $|K| = p^l$ for some divisor l of k. Now $\sim_x$, $x \in K$, and $\sim_\infty$ are all non-trivial congruences of $\mathfrak{B}$, hence $m = p^l + 1$.

To prove the converse, the following lemma will be used. It is stated in a more general way than necessary, since the complete description of preserving mappings contained in it is of interest by itself.

Lemma. Suppose that K is a subfield of $GF(p^k)$. Let $g: X \to X$ be a mapping preserving all equivalence relations $\sim_x$, $x \in K \cup \{\infty\}$. Then g is of the form

(3) $g_{\alpha,u,v}(a,b) = (\alpha(a) + u, \alpha(b) + v)$,

where α is a linear map of the vector space $GF(p^k)$ over K, and $u,v \in GF(p^k)$ are arbitrary.

Proof. A straightforward verification shows that any mapping $g_{\alpha,u,v}$ preserves all equivalences $\sim_x$, $x \in K \cup \{\infty\}$.

To prove all preserving mappings are of this form, take a basis $a_1,\dots,a_q$ of the space $GF(p^k)$ over K, and set $A_0 = (0,0)$, $A_i = (a_i,0)$. We shall show that any mapping $g: X \to X$ preserving $\sim_x$, $x \in K \cup \{\infty\}$, is uniquely determined by its values in the points A_i, $i = 0,1,\dots,q$.

The following simple observation will be frequently used:

(4) if A, B, Z are elements of X, $x,y \in K \cup \{\infty\}$ are different, and $A \sim_x Z \sim_y B$, then the values of g in A, B determine the value in Z.

This is obvious, for g(Z) has to be the unique point in the intersection of the block of $\sim_x$ through g(A) and the block of $\sim_y$ through g(B).

Let Y_r denote the set of all $a \in GF(p^k)$ which can be expressed as linear combinations (over K) of a_i's with at most r nonzero coefficients, and set $X_r = Y_r \times Y_r \subseteq X$. Now we have $(0,0) \sim_0 (0,xa_i) \sim_{-x^{-1}} (a_i,0)$, $(0,0) \sim_\infty (xa_i,0) \sim_{-1} (0,xa_i)$, and $(xa_i,0) \sim_0 (xa_i,ya_j) \sim_\infty (0,ya_j)$. Using (4) in these three cases, we conclude that the values of g in X_1 are determined by $g(A_i)$, $i = 0,\ldots,q$.

Next we show that the values of g in X_r ($r \geq 1$) determine the ones in X_{r+1}. Let $\sum_I x_i a_i \in Y_r$ and $j \notin I$. Then $(0,0) \sim_0 (0, \sum_I x_i a_i + xa_j) \sim_{-x^{-1}} (a_j, \sum_I x_i a_i)$ and $(0,0) \sim_\infty (\sum_I x_i a_i + xa_j, 0) \sim_{-1} (0, \sum_I x_i a_i + xa_j)$. If $\sum_J y_i a_i$ is another point of Y_r and $k \notin J$, then $(\sum_I x_i a_i + xa_j, 0) \sim_0 (\sum_I x_i a_i + xa_j, \sum_J y_i a_i + ya_k) \sim_\infty (0, \sum_J y_i a_i + ya_k)$ Further applications of (4) prove that g is determined in X_{r+1} by its values in X_r.

The obvious induction on r gives that g is uniquely determined by the values $g(A_i)$, $i = 0,\ldots,q$.

Now set $g(A_0) = (u_0,v)$. Since g preserves $\sim_\infty$, we have $g(A_i) = (u_i,v)$ for some $u_i \in GF(p^k)$, $i = 1,\ldots,q$. Denote by α the linear map of $GF(p^k)$ over K defined by $\alpha(a_i) = u_i$. Then g and $g_{\alpha,u,v}$ have the same values in the points A_i, $i = 0,\ldots,q$, hence $g = g_{\alpha,u,v}$ by the previous part of the proof. □

End of the proof of Theorem. Let l be a divisor of k and K the subfield of $GF(p^k)$ of cardinality p^l. Consider the set H of all mappings of the form $g_{\alpha,0,0}$. The congruence lattice of the algebra $\mathcal{C} = (A, F \cup H)$ is a subset of $\{\sim_x : x \in GF(p^k) \cup \{\infty\}\}$. All equivalences $\sim_x$, $x \in K \cup \{\infty\}$ are congruences of $\mathcal{C}$ by the lemma. Now, if $x \notin K \cup \{\infty\}$, there is a linear mapping α of $GF(p^k)$ over K with $\alpha(x) = \alpha(1) = 1$. Then $g_{\alpha,0,0}((x,1)) = (1,1)$ and $g_{\alpha,0,0}((0,0)) = (0,0)$, hence the least congruence of $\mathcal{C}$ containing $\sim_x$ contains also $\sim_1$ and is therefore equal to $X \times X$.

It proves that all non-trivial congruences of $\mathcal{C}$ are of the form $\sim_x$, $x \in K \cup \{\infty\}$, hence the congruence lattice of $\mathcal{C}$ is isomorphic to M_{p^l+1}. □

Note. A reader familiar with the graphical compositions defined in [2] recognized that Figs. 1 and 2 defined two special graphical compositions and that we used the easier part of the concrete characterization of congruence lattices given therein, namely that any congruence lattice is closed under the results of all graphical compositions.

References

[1] R.W. QUACKENBUSH: A note on a problem of Goralčík, Coll. Math. Soc. János Bolyai, Vol. 17. Contributions to Universal Algebra, Szeged (Hungary)(1975), 363-364.

[2] H. WERNER: Which partition lattices are congruence lattices? Coll. Math. Soc. János Bolyai, Vol. 14. Lattice Theory, Szeged (Hungary)(1974), 433-453.

Mathematical Institute
Czechoslovak Academy of Sciences
Žitná 25, 115 67 Praha 1
Czechoslovakia

(Oblatum 17.10. 1984)